Amazon Virtual Private Cloud

AWS PrivateLink

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

Technologie AWS PrivateLink et points de terminaison de VPC

La technologie AWS PrivateLink est hautement disponible et évolutive. Elle vous permet d'établir une connexion privée de votre VPC aux services AWS pris en charge, à des services hébergés par d'autres comptes AWS (services de points de terminaison de VPC), ainsi qu'à des services partenaires AWS Marketplace pris en charge. Pour communiquer avec le service, vous n'avez pas besoin de passerelle Internet, de périphérique NAT, d'adresse IP publique, de connexion AWS Direct Connect ou de connexion AWS Site-to-Site VPN. Par conséquent, vous contrôlez les points de terminaison d'API, les sites et les services spécifiques accessibles depuis votre VPC.

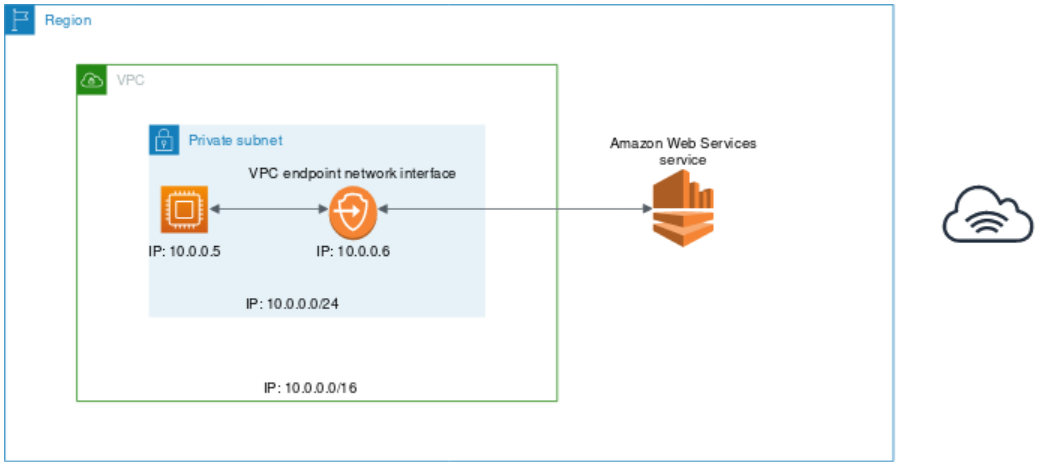
Vous pouvez créer votre propre service de point de terminaison de VPC, optimisé par la technologie AWS PrivateLink, et permettre à d'autres clients AWS d'accéder à votre service.

Concepts des points de terminaison d'un VPC

Les concepts clés liés aux points de terminaison d'un VPC sont les suivants :

- Point de terminaison d'un VPC : point d'entrée de votre VPC qui vous permet de vous connecter par réseau privé à un service. Voici les différents types de points de terminaison d'un VPC. Créez le type de point de terminaison d'un VPC requis par le service pris en charge.
  - Point de terminaison de passerelle (p. 22)
  - Point de terminaison d'interface (p. 3)
  - Point de terminaison d'équilibreur de charge de passerelle (p. 18)
- Service de point de terminaison : votre propre application ou service dans votre VPC. D'autres mandataires AWS peuvent créer un point de terminaison de leur VPC à votre service de point de terminaison.

Pour utiliser la technologie AWS PrivateLink, créez un point de terminaison de VPC pour un service dans votre VPC. Créez le type de point de terminaison d'un VPC requis par le service pris en charge. Une interface réseau Elastic est ainsi créée dans votre sous-réseau avec une adresse IP privée qui sert de point d'entrée au trafic destiné au service. Le diagramme suivant présente l'architecture de base pour connecter en toute sécurité votre VPC à un service AWS prenant en charge la technologie AWS PrivateLink.



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 — Offre une interface web que vous pouvez utiliser pour accéder à vos AWS PrivateLink ressources.
- AWS Command Line Interface (AWS CLI) — Fournit des commandes pour une large gamme de services AWS, notamment AWS PrivateLink. Pour plus d'informations sur les commandes pour AWS PrivateLink, consultez ec2 dans la Référence des commandes du AWS CLI.
- AWS CloudFormation - Créez des modèles qui décrivent vos AWS ressources. Vous utilisez les modèles pour provisionner et gérer ces ressources comme une seule unité. Pour plus d'informations, consultez les AWS PrivateLink ressources suivantes :
  - AWS::EC2::VPCEndpoint
  - AWS::EC2::VPCEndpointConnectionNotification
  - AWS::EC2::VPCEndpointService
  - AWS::EC2::VPCEndpointServicePermissions
  - AWS::ElasticLoadBalancingV2::LoadBalancer
- Kits SDK AWS — Fournissent des API spécifiques du langage. Les kits 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 Kits SDK 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.

Exemple de configurations de point de terminaison

Pour en savoir plus sur AWS PrivateLink et pour obtenir des exemples d'appairage de VPC, consultez Exemple : services utilisant la technologie AWS PrivateLink et l'appairage de VPC dans l'Amazon VPC User Guide.

Tarification des points de terminaison

Pour plus d'informations sur la tarification, consultez Tarification AWS PrivateLink.

Points de terminaison d'un VPC

Un point de terminaison de VPC permet les connexions entre un réseau cloud privé virtuel et les services pris en charge sans nécessiter de passerelle Internet, de périphérique NAT, de connexion VPN ou de connexion AWS Direct Connect. Par conséquent, vous contrôlez les points de terminaison d'API, les sites et les services spécifiques accessibles depuis votre VPC.

Les points de terminaison d'un VPC sont des appareils virtuels. Il s'agit de composants VPC mis à l'à échelle horizontalement, redondants et hautement disponibles. Voici les différents types de points de terminaison d'un VPC. Créez le type de point de terminaison d'un VPC requis par le service pris en charge.

Points de terminaison d'interface

Un point de terminaison d'interface (p. 3) est une interface réseau Elastic avec une adresse IP privée de la plage d'adresses IP de votre sous-réseau. Il sert de point d'entrée au trafic destiné à un service appartenant à AWS ou appartenant à un client ou partenaire AWS. Pour obtenir une liste des services AWS qui s'intègrent à AWS PrivateLink, consultez Services qui prennent en charge la technologie AWS PrivateLink (p. 74).

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.

Points de terminaison de l'équilibreur de charge de passerelle

Un point de terminaison d'équilibreur de charge de passerelle (p. 18) est une interface réseau Elastic à adresse IP privée provenant de la plage d'adresses IP de votre sous-réseau. Il sert de point d'entrée pour intercepter le trafic et l'acheminer vers un service de réseau ou de sécurité que vous avez configuré à l'aide d'un équilibreur de charge de passerelle. Vous spécifiez un point de terminaison d'équilibreur de charge de passerelle comme cible de route dans une table de routage. Les points de terminaison d'équilibreur de charge de passerelle sont prises en charge pour les services de point de terminaison configurés uniquement pour les équilibreurs de charge de passerelle.

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.

Points de terminaison de passerelle

Un point de terminaison de passerelle (p. 22) est une passerelle qui sert de cible pour une route dans votre table de routage pour le trafic destiné à Amazon S3 ou à DynamoDB.

Il n'y a pas de frais 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. Pour une comparaison des deux options, veuillez consulter Types de points de terminaison de VPC pour Amazon S3 dans le Guide de l'utilisateur Amazon S3.

Points de terminaison de VPC d'interface (AWS PrivateLink)

Un point de terminaison de VPC d'interface (point de terminaison d'interface) vous permet de vous connecter à des services optimisés par la technologie AWS PrivateLink. Ces services incluent certains services AWS, les services hébergés par d'autres clients et partenaires AWS dans leurs propres VPC (désignés comme services de point de terminaison) et les services partenaires AWS Marketplace pris en charge. Le propriétaire du service est le fournisseur du service, et vous, en tant que mandataire créant le point de terminaison d'interface, vous êtes le consommateur du service.

Les étapes générales suivantes permettent de configurer un point de terminaison d'interface :

1. Choisissez le VPC dans lequel créer le point de terminaison d'interface et fournissez le nom du service AWS, le service du point de terminaison ou le service AWS Marketplace auquel vous êtes connecté.
2. Choisissez un sous-réseau de votre VPC pour utiliser le point de terminaison d'interface. Nous créons une interface réseau du point de terminaison dans le sous-réseau. Une interface réseau de point de terminaison se voit attribuer une adresse IP privée à partir de la plage d'adresses IP de votre sous-réseau et conserve cette adresse IP jusqu'à ce que le point de terminaison d'interface soit supprimé. Vous pouvez spécifier plusieurs sous-réseaux dans différentes zones de disponibilité (telles que prises en charge par le service) afin de vous assurer que le point de terminaison de votre interface résiste aux défaillances des zones de disponibilité. Dans ce cas, nous créons une interface réseau du point de terminaison dans chaque sous-réseau que vous spécifiez.

   Note

   Un point de terminaison d'interface est une interface réseau gérée par demandeur. Vous pouvez l'afficher dans votre compte, mais vous ne pouvez pas la gérer vous-même. Pour de plus amples informations, veuillez consulter Interfaces réseau gérées par le demandeur.
3. Spécifiez les groupes de sécurité à associer à l'interface réseau du point de terminaison. Les règles des groupes de sécurité contrôlent le trafic en direction de l'interface réseau du point de terminaison des ressources de votre VPC. Si vous ne spécifiez pas de groupe de sécurité, nous associons le groupe de sécurité par défaut pour le VPC.
4. (Facultatif, services AWS et services partenaires AWS Marketplace uniquement) Activez le DNS privé (p. 5) pour le point de terminaison afin que vous puissiez adresser des demandes au service en utilisant son nom d'hôte DNS par défaut.

   Important

   Le DNS privé est activé par défaut pour les points de terminaison créés pour des services AWS et des services partenaires AWS Marketplace.
   Le DNS privé est activé dans les autres sous-réseaux qui se trouvent dans les mêmes VPC et zone de disponibilité (ou zone locale).
5. Lorsque le fournisseur de service et le consommateur sont dans des comptes différents, consultez the section called “Considérations sur les zones de disponibilité des points de terminaison d'interface” (p. 8) pour plus d’informations sur la façon d’utiliser les ID de zones de disponibilité pour identifier la zone de disponibilité du point de terminaison d'interface.
6. Une fois que vous avez créé le point de terminaison d'interface, celui-ci est disponible pour utilisation quand il est accepté par le fournisseur de services. Le fournisseur de service doit configurer le service pour qu'il accepte les demandes automatiquement ou manuellement. Les services AWS et les services AWS Marketplace acceptent généralement de manière automatique toutes les demandes de point de terminaison. Pour plus d'informations sur le cycle de vie d'un point de terminaison, consultez Cycle de vie du point de terminaison d'interface (p. 8).

Les services ne peuvent pas initier de demandes en direction des ressources de votre VPC via le point de terminaison. Un point de terminaison retourne uniquement les réponses au trafic initié depuis les ressources de votre VPC. Avant d'intégrer un service et un point de terminaison, consultez la documentation relative au point de terminaison de VPC spécifique au service pour prendre connaissance de toute configuration et limitation spécifiques au service.

Table des matières

DNS privé pour les points de terminaison d'interface

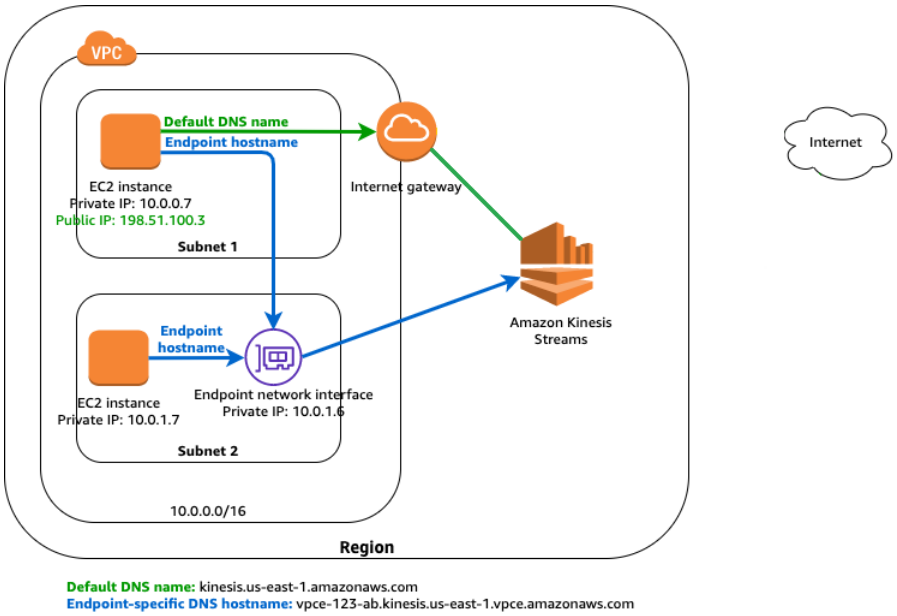
> Important
>
> Le DNS privé n'est pas pris en charge pour les points de terminaison de l'interface d'Amazon S3.

Quand vous créez un point de terminaison d'interface, nous générons des noms d'hôte DNS spécifiques au point de terminaison que vous pouvez utiliser pour communiquer avec le service. Pour les services AWS et les services partenaires AWS Marketplace, l'option de DNS privé (activée par défaut) associe une zone hébergée privée à votre VPC. La zone hébergée contient un ensemble d'enregistrements pour le nom DNS par défaut du service (par exemple, `ec2.us-east-1.amazonaws.com`) qui se résout dans les adresses IP privées des interfaces réseau de point de terminaison de votre VPC. Vous pouvez ainsi adresser des demandes au service à l'aide de son nom d'hôte DNS par défaut au lieu des noms d'hôte DNS propres au point de terminaison. Par exemple, si vos applications existantes adressent des demandes à un service AWS, elles peuvent continuer à le faire via le point de terminaison d'interface sans nécessiter de modifications de configuration.

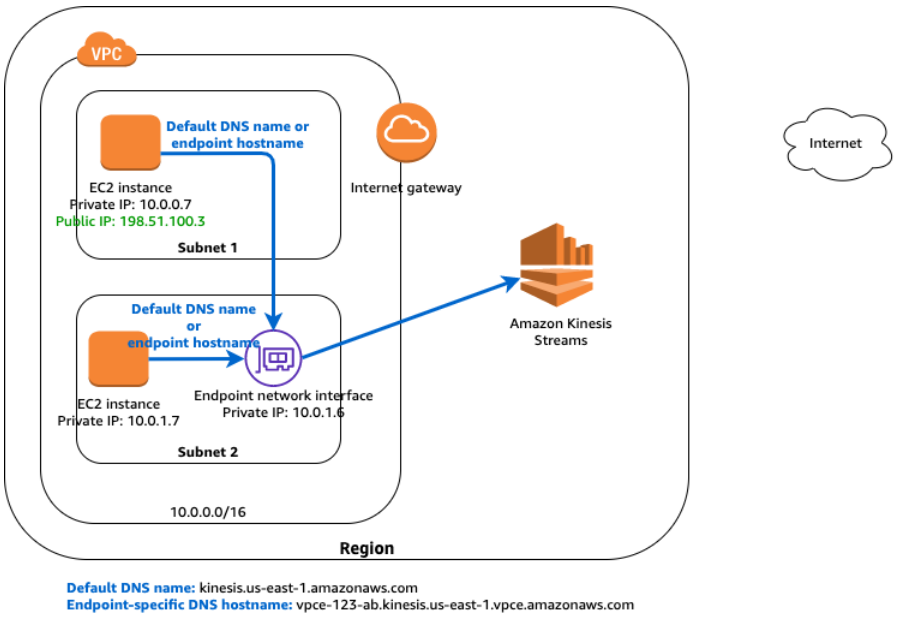
Dans l'exemple illustré par le schéma suivant, il existe un point de terminaison d'interface pour Amazon Kinesis Data Streams et une interface réseau de point de terminaison dans le sous-réseau 2. Le DNS privé pour le point de terminaison d'interface est désactivé. Les tables de routage des sous-réseaux comportent les routes suivantes.

Sous-réseau 1	
Destination (Destination	Cible
10.0.0.0/16	Locale
0.0.0.0/0	internet-gateway-id
Sous-réseau 2	
Destination (Destination	Cible
10.0.0.0/16	Locale

Les instances des deux sous-réseaux peuvent envoyer des demandes à Amazon Kinesis Data Streams par le biais du point de terminaison d'interface à l'aide d'un nom d'hôte de DNS spécifique au point de terminaison. Les instances du sous-réseau 1 peuvent communiquer avec Amazon Kinesis Data Streams sur un espace d'adressage IP public de la région AWS en utilisant son nom DNS par défaut.



Dans le diagramme suivant, le DNS privé du point de terminaison est activé. Les instances de deux sous-réseaux peuvent envoyer des demandes à Amazon Kinesis Data Streams par le biais du point de terminaison d'interface en utilisant le nom d'hôte de DNS par défaut ou celui spécifique au point de terminaison.



Important

Pour utiliser les DNS privés, vous devez définir les attributs VPC suivants sur `true` : `enableDnsHostnames` et `enableDnsSupport`. Pour de plus amples informations, veuillez consulter Affichage et mise à jour de la prise en charge de DNS pour votre VPC. Les utilisateurs IAM doivent avoir l'autorisation d'utiliser les zones hébergées. Pour de plus amples informations, veuillez consulter Authentification et contrôle d'accès pour Route 53.

Propriétés et limites des points de terminaison d'interface

Pour utiliser les points de terminaison d'interface, vous devez être conscient des propriétés et limitations actuelles :

- Pour chaque point de terminaison d'interface, vous ne pouvez choisir qu'un seul sous-réseau par zone de disponibilité.
- Certains services peuvent ne pas être disponibles dans toutes les zones de disponibilité via un point de terminaison d'interface. Pour connaître les zones de disponibilité compatibles, utilisez la commande describe-vpc-endpoint-services ou utilisez la console Amazon VPC. Pour plus d'informations, consultez Créer un point de terminaison d'interface (p. 9).
- Lorsque vous créez un point de terminaison d'interface, celui-ci est créé dans la zone de disponibilité mappée à votre compte et est indépendant des autres comptes. Lorsque le fournisseur de service et le consommateur sont dans des comptes différents, consultez the section called “Considérations sur les zones de disponibilité des points de terminaison d'interface” (p. 8) pour plus d’informations sur la façon d’utiliser les ID de zones de disponibilité pour identifier la zone de disponibilité du point de terminaison d'interface.
- Lorsque le fournisseur de services et le consommateur ont des comptes différents et utilisent plusieurs zones de disponibilité, et que le consommateur visualise les informations du service de point de terminaison VPC, la réponse inclut uniquement les zones de disponibilité communes. Par exemple, lorsque le compte du fournisseur de services utilise les régions `us-east-1a` et `us-east-1c` et le consommateur les régions `us-east-1a` et `us-east-1b`, la réponse inclut les services de point de terminaison VPC dans la zone de disponibilité commune, `us-east-1a`.
- Par défaut, chaque point de terminaison d'interface peut prendre en charge une bande passante jusqu'à 10 Gbits/s par zone de disponibilité et met à l'échelle jusqu'à 40 Gbits/s. Si votre application nécessite un débit plus élevé par zone, contactez le support AWS.
- Si la liste ACL réseau de votre sous-réseau limite le trafic, vous pourriez ne pas pouvoir envoyer du trafic via l'interface réseau du point de terminaison. Assurez-vous d'ajouter des règles appropriées qui autorisent le trafic vers et depuis le bloc d'adresse CIDR du sous-réseau.
- Assurez-vous que le groupe de sécurité associé à l'interface réseau du point de terminaison permet la communication entre l'interface réseau du point de terminaison et les ressources de votre VPC qui communiquent avec le service. Pour faire en sorte que les outils de ligne de commande, tels que la AWS CLI, puissent honorer les demandes sur HTTPS entre les ressources du VPC et un service AWS, le groupe de sécurité doit autoriser le trafic HTTPS entrant (port 443).
- Un point de terminaison d'interface prend uniquement en charge le trafic TCP.
- Quand vous créez un point de terminaison, vous pouvez lui attacher une stratégie de point de terminaison qui contrôle l'accès au service auquel vous vous connectez. Pour de plus amples informations, consultez Bonnes pratiques en matière de stratégies et the section called “Contrôler l'accès aux services” (p. 40).
- Vérifiez les limites spécifiques au service pour votre service de point de terminaison.
- Les participants ne peuvent pas créer de points de terminaison du résolveur Amazon Route53 dans un VPC qu'ils ne possèdent pas. Seul le propriétaire du VPC peut créer des ressources de niveau VPC telles que des points de terminaison entrants.
- Les points de terminaison sont uniquement pris en charge dans une même région. Vous ne pouvez pas créer un point de terminaison entre un VPC et un service situé dans une autre région.
- Les points de terminaison prennent en charge le trafic IPv4 uniquement.
- Vous ne pouvez pas transférer de point de terminaison d'un VPC à un autre, ou d'un service à un autre.
- Vous êtes soumis à un quota pour le nombre de points de terminaison que vous pouvez créer par VPC. Pour plus d'informations, consultez AWS PrivateLinkQuotas (p. 89).

Connexion aux centres de données locaux

Vous pouvez utiliser les types de connexions suivants pour établir une connexion entre un point de terminaison d'interface et votre centre de données sur site :

- AWS Direct Connect
- AWS Site-to-Site VPN

Cycle de vie du point de terminaison d'interface

Un point de terminaison d'interface passe par plusieurs étapes à partir du moment où vous le créez (la demande de connexion du point de terminaison). À chaque étape, il peut y avoir des actions que le consommateur du service et le fournisseur du service peuvent prendre.

Les règles suivantes s'appliquent :

- Un fournisseur de service peut configurer son service pour qu'il accepte les demandes de point de terminaison d'interface automatiquement ou manuellement. Les services AWS et les services AWS Marketplace acceptent généralement de manière automatique toutes les demandes de point de terminaison.
- Un fournisseur de service ne peut pas supprimer le point de terminaison d'interface de son service. Seul le consommateur du service ayant demandé la connexion du point de terminaison d'interface peut supprimer le point de terminaison d'interface.
- Un fournisseur de service peut rejeter le point de terminaison d'interface après l'avoir accepté (manuellement ou automatiquement) et qu'il se trouve dans l'état `available`.

Considérations sur les zones de disponibilité des points de terminaison d'interface

Lorsque vous créez un point de terminaison d'interface, celui-ci est créé dans la zone de disponibilité mappée à votre compte et est indépendant des autres comptes. Lorsque le fournisseur de service et le consommateur sont dans des comptes différents, utilisez l'ID de zone de disponibilité pour identifier de façon unique et cohérente la zone de disponibilité du point de terminaison d'interface. Par exemple, `use1-az1` est un ID de zone de disponibilité pour la Région `us-east-1`, qui correspond au même emplacement dans chaque compte AWS. Pour en savoir plus sur les ID de zone de disponibilité, consultez ID de zone de disponibilité pour vos ressources dans le Guide de l'utilisateur AWS RAM ou utilisez describe-availability-zones.

Certains services peuvent ne pas être disponibles dans toutes les zones de disponibilité via un point de terminaison d'interface. Vous pouvez utiliser les opérations suivantes pour déterminer quelles zones de disponibilité sont prises en charge pour un service :

- describe-vpc-endpoint-services (AWS CLI)
- DescribeVpcEndpointServices (API)
- La console Amazon VPC lorsque vous créez un point de terminaison d'interface. Pour plus d'informations, consultez the section called “Créer un point de terminaison d'interface” (p. 9).

Consultation des noms de services AWS disponibles

Lorsque vous utilisez la console Amazon VPC pour créer un point de terminaison, vous pouvez obtenir la liste des noms de services AWS disponibles.

Lorsque vous utilisez l'AWS CLI pour créer un point de terminaison, vous pouvez utiliser la commande describe-vpc-endpoint-services pour afficher les noms des services, puis créer le point de terminaison à l'aide de la commande create-vpc-endpoint.

Console

Pour afficher les services AWS disponibles 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, sélectionnez Points de terminaison, Créer un point de terminaison.
3. Dans la section Nom du service, les services disponibles sont répertoriés.

Command line

Pour consulter les services AWS disponibles à l'aide de la AWS CLI

- Utilisez la commande describe-vpc-endpoint-services pour obtenir la liste des services disponibles auxquels vous pouvez vous connecter. Le champ `ServiceType` indique si vous vous connectez au service via un point de terminaison d'interface ou un point de terminaison de passerelle. Le champ `ServiceName` fournit le nom du service. L'exemple suivant répertorie le nom et le propriétaire de tous les points de terminaison de l'interface.

```
aws ec2 describe-vpc-endpoint-services --filter "Name=service-
type,Values=Interface" --query "ServiceDetails[*].[ServiceName, Owner]" --output
 table
```

```
------------------------------------------------------------------
|                   DescribeVpcEndpointServices                  |
+--------------------------------------------------+-------------+
|  aws.sagemaker.us-west-2.notebook                |  amazon     |
|  aws.sagemaker.us-west-2.studio                  |  amazon     |
|  com.amazonaws.us-west-2.access-analyzer         |  amazon     |
|  com.amazonaws.us-west-2.acm-pca                 |  amazon     |
...
```

Pour consulter les services AWS disponibles à l'aide de la AWS Tools for Windows PowerShell

- Get-EC2VpcEndpointService

Pour consulter les services AWS disponibles à l'aide de l'API

- DescribeVpcEndpointServices

Créer un point de terminaison d'interface

Pour créer un point de terminaison d'interface, vous devez spécifier le VPC dans lequel vous voulez créer le point de terminaison d'interface et le service avec lequel vous voulez établir la connexion.

Pour les services AWS ou les services partenaires AWS Marketplace, vous pouvez éventuellement activer le DNS privé (p. 5) pour le point de terminaison afin de pouvoir adresser des demandes au service en utilisant son nom d'hôte DNS par défaut.

> **Important**
>
> Le DNS privé est activé par défaut pour les points de terminaison créés pour des services AWS et des services partenaires AWS Marketplace.

Console

Pour créer le point de terminaison d'interface d'un service AWS 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, sélectionnez Points de terminaison, Créer un point de terminaison.
3. Pour Catégorie de service, assurez-vous que l'option services AWS est sélectionnée.
4. Pour Nom du service, choisissez le service auquel vous connectez. Pour Type, assurez-vous qu'Interface soit indiqué.
5. Complétez les informations suivantes, puis choisissez Créer un point de terminaison.

   - Pour VPC, sélectionnez un VPC dans lequel créer le point de terminaison.
   - Pour Sous-réseaux, sélectionnez les sous-réseaux (zones de disponibilité) dans lesquels créer les interfaces réseau du point de terminaison.

     Certaines zones de disponibilité peuvent ne pas être prises en charge pour tous les services AWS.
   - Pour activer un DNS privé pour le point de terminaison d'interface, cochez Enable DNS Name (Activer le nom de DNS).

     > **Important**
     >
     > Le DNS privé n'est pas pris en charge pour les points de terminaison de l'interface d'Amazon S3.

     Cette option est activée par défaut. Pour utiliser l'option DNS privé, les attributs suivants de votre VPC doivent être définis sur `true` : `enableDnsHostnames` et `enableDnsSupport`. Pour de plus amples informations, veuillez consulter Affichage et mise à jour de la prise en charge de DNS pour votre VPC.
   - Pour Groupe de sécurité, sélectionnez les groupes de sécurité à associer aux interfaces réseau du point de terminaison.
   - (Facultatif) Ajoutez ou supprimez une balise.

     [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :
     - Pour Clé, saisissez le nom de la clé.
     - Pour Valeur, saisissez la valeur clé.

     [Supprimer une balise] Choisissez le bouton de suppression (« x ») situé à la droite de la clé et de la valeur de la balise.

Pour créer le point de terminaison d'interface d'un service de point de terminaison, vous devez avoir le nom du service auquel vous connectez. Le fournisseur du service peut vous fournir le nom.

Pour créer le point de terminaison d'interface d'un service de point de terminaison

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Points de terminaison, Créer un point de terminaison.
3. Pour Catégorie de service, choisissez Rechercher un service par nom.

4. Pour Nom du service, entrez le nom du service (par exemple, `com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`) et choisissez Vérifier.
5. Complétez les informations suivantes, puis choisissez Créer un point de terminaison.

   - Pour VPC, sélectionnez un VPC dans lequel créer le point de terminaison.
   - Pour Sous-réseaux, sélectionnez les sous-réseaux (zones de disponibilité) dans lesquels créer les interfaces réseau du point de terminaison.

     Certaines zones de disponibilité peuvent ne pas être prises en charge pour le service.
   - Pour Groupe de sécurité, sélectionnez les groupes de sécurité à associer aux interfaces réseau du point de terminaison.
   - (Facultatif) Ajoutez ou supprimez une balise.

     [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :
     - Pour Clé, saisissez le nom de la clé.
     - Pour Valeur, saisissez la valeur clé.

     [Supprimer une balise] Choisissez le bouton de suppression (« x ») situé à la droite de la clé et de la valeur de la balise.

Pour créer le point de terminaison d'interface d'un service partenaire AWS Marketplace

1. Accédez à la page PrivateLink sur AWS Marketplace et abonnez-vous à un service depuis un fournisseur SaaS (Software as a Service). Les services qui prennent en charge les points de terminaison d'interface incluent une option pour se connecter via un point de terminaison.
2. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
3. Dans le volet de navigation, sélectionnez Points de terminaison, Créer un point de terminaison.
4. Pour Service category (Catégorie de service), choisissez Vos services AWS Marketplace.
5. Choisissez le service AWS Marketplace auquel vous êtes inscrit.
6. Complétez les informations suivantes, puis choisissez Créer un point de terminaison.

   - Pour VPC, sélectionnez un VPC dans lequel créer le point de terminaison.
   - Pour Sous-réseaux, sélectionnez les sous-réseaux (zones de disponibilité) dans lesquels créer les interfaces réseau du point de terminaison.

     Certaines zones de disponibilité peuvent ne pas être prises en charge pour le service.
   - Pour Groupe de sécurité, sélectionnez les groupes de sécurité à associer aux interfaces réseau du point de terminaison.
   - (Facultatif) Ajoutez ou supprimez une balise.

     [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :
     - Pour Clé, saisissez le nom de la clé.
     - Pour Valeur, saisissez la valeur clé.

     [Supprimer une balise] Choisissez le bouton de suppression (« x ») situé à la droite de la clé et de la valeur de la balise.

Command line

Pour créer un point de terminaison d'interface à l'aide de l AWS CLI

1. Utilisez la commande describe-vpc-endpoint-services pour obtenir la liste des services disponibles. Dans le résultat retourné, prenez note du nom du service auquel se connecter. Le

champ `ServiceType` indique si vous vous connectez au service via un point de terminaison d'interface ou un point de terminaison de passerelle. Le champ `ServiceName` fournit le nom du service.

2. Pour créer un point de terminaison d'interface, utilisez la commande create-vpc-endpoint et indiquez l'ID du VPC, le type de point de terminaison (interface), le nom du service, les sous-réseaux qui utiliseront le point de terminaison et les groupes de sécurité à associer aux interfaces réseau de ce dernier.

   L'exemple suivant crée un point de terminaison d'interface pour le service Elastic Load Balancing.

```
aws ec2 create-vpc-endpoint --vpc-id vpc-ec43eb89 --vpc-endpoint-type Interface
 --service-name com.amazonaws.us-east-1.elasticloadbalancing --subnet-id subnet-
abababab --security-group-id sg-1a2b3c4d
```

```
{
    "VpcEndpoint": {
        "PolicyDocument": "{\n  \"Statement\": [\n    {\n      \"Action\": \"*\",
 \n      \"Effect\": \"Allow\", \n      \"Principal\": \"*\", \n      \"Resource\":
 \"*\"\n    }\n  ]\n}",
        "VpcId": "vpc-ec43eb89",
        "NetworkInterfaceIds": [
            "eni-bf8aa46b"
        ],
        "SubnetIds": [
            "subnet-abababab"
        ],
        "PrivateDnsEnabled": true,
        "State": "pending",
        "ServiceName": "com.amazonaws.us-east-1.elasticloadbalancing",
        "RouteTableIds": [],
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-1a2b3c4d"
            }
        ],
        "VpcEndpointId": "vpce-088d25a4bbf4a7abc",
        "VpcEndpointType": "Interface",
        "CreationTimestamp": "2017-09-05T20:14:41.240Z",
        "DnsEntries": [
            {
                "HostedZoneId": "Z7HUB22UULQXV",
                "DnsName": "vpce-088d25a4bbf4a7abc-
ks83awe7.elasticloadbalancing.us-east-1.vpce.amazonaws.com"
            },
            {
                "HostedZoneId": "Z7HUB22UULQXV",
                "DnsName": "vpce-088d25a4bbf4a7abc-ks83awe7-us-
east-1a.elasticloadbalancing.us-east-1.vpce.amazonaws.com"
            },
            {
                "HostedZoneId": "Z1K56Z6FNPJRR",
                "DnsName": "elasticloadbalancing.us-east-1.amazonaws.com"
            }
        ]
    }
}
```

   Sinon, l'exemple suivant crée un point de terminaison d'interface pour un service de point de terminaison d'un autre compte (le fournisseur de service vous communique le nom du service de point de terminaison).

```
aws ec2 create-vpc-endpoint --vpc-id vpc-ec43eb89 --vpc-endpoint-type Interface
 --service-name com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc --subnet-
id subnet-abababab --security-group-id sg-1a2b3c4d
```

Dans le résultat retourné, notez les champs `privateDnsNames`. Vous pouvez utiliser ces noms DNS pour accéder au service AWS.

Pour décrire les services disponibles et créer un point de terminaison VPC à l'aide des AWS Tools for Windows PowerShell

- Get-EC2VpcEndpointService
- New-EC2VpcEndpoint

Pour décrire les services disponibles et créer un point de terminaison VPC à l'aide de l'API

- DescribeVpcEndpointServices
- CreateVpcEndpoint

Afficher votre point de terminaison d'interface

Une fois que vous avez créé un point de terminaison d'interface, vous pouvez afficher des informations à son sujet.

Console

Pour afficher les informations sur 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 volet de navigation, choisissez Points de terminaison, puis sélectionnez votre point de terminaison d'interface.
3. Pour afficher les informations sur le point de terminaison d'interface, choisissez Détails. Le champ DNS affiche les noms DNS à utiliser pour accéder au service.
4. Pour afficher les sous-réseaux dans lesquels le point de terminaison d'interface a été créé, ainsi que l'ID de l'interface réseau du point de terminaison de chaque sous-réseau, choisissez Sous-réseaux.
5. Pour afficher les groupes de sécurité associés à l'interface réseau du point de terminaison, choisissez Groupe de sécurité.

Command line

Pour décrire votre point de terminaison d'interface à l'aide de l AWS CLI

- Vous pouvez décrire votre point de terminaison à l'aide de la commande describe-vpc-endpoints.

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-ids vpce-088d25a4bbf4a7abc
```

Pour décrire vos points de terminaison VPC à l'aide des AWS Tools for PowerShell ou de l'API

- Get-EC2VpcEndpoint (Tools for Windows PowerShell)
- DescribeVpcEndpoints (API de requête Amazon EC2)

Créer et gérer une notification pour un point de terminaison d'interface

Vous pouvez créer une notification pour recevoir des alertes pour les événements spécifiques qui se produisent sur le point de terminaison de votre interface. Par exemple, vous pouvez recevoir un e-mail quand le point de terminaison d'interface est accepté par le fournisseur du service. Afin de créer une notification, vous devez lui associer une rubrique Amazon SNS. Vous pouvez vous inscrire à la rubrique SNS pour recevoir une notification par e-mail quand un événement de point de terminaison se produit.

La rubrique Amazon SNS que vous utilisez pour les notifications doit avoir une stratégie de rubrique qui permet à un service de point de terminaison VPC d'Amazon de publier celles-ci en votre nom. Veillez à inclure la déclaration suivante dans votre stratégie de rubrique. Pour de plus amples informations, veuillez consulter Identity and Access Management dans Amazon SNS dans le Guide du développeur Amazon Simple Notification Service.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account:topic-name"
    }
  ]
}
```

Command line

Pour créer et gérer une notification à l'aide de l AWS CLI

1. Pour créer une notification pour un point de terminaison d'interface, utilisez la commande create-vpc-endpoint-connection-notification. Spécifiez l'ARN de la rubrique SNS, les événements à notifier et l'ID du point de terminaison, comme indiqué dans l'exemple suivant.

   ```
   aws ec2 create-vpc-endpoint-connection-notification --connection-notification-
   arn arn:aws:sns:us-east-2:123456789012:EndpointNotification --connection-events
    Accept Reject --vpc-endpoint-id vpce-123abc3420c1931d7
   ```

2. Pour afficher vos notifications, utilisez la commande describe-vpc-endpoint-connection-notifications.

   ```
   aws ec2 describe-vpc-endpoint-connection-notifications
   ```

3. Pour modifier la rubrique SNS ou les événements de point de terminaison de la notification, utilisez la commande modify-vpc-endpoint-connection-notification.

   ```
   aws ec2 modify-vpc-endpoint-connection-notification --connection-notification-
   id vpce-nfn-008776de7e03f5abc --connection-events Accept --connection-notification-
   arn arn:aws:sns:us-east-2:123456789012:mytopic
   ```

4. Pour supprimer une notification, utilisez la commande delete-vpc-endpoint-connection-notifications.

```
aws ec2 delete-vpc-endpoint-connection-notifications --connection-notification-
ids vpce-nfn-008776de7e03f5abc
```

Accéder à un service via un point de terminaison d'interface

Une fois que vous avez créé un point de terminaison d'interface, vous pouvez envoyer des demandes au service pris en charge via une URL de point de terminaison. Vous pouvez utiliser les éléments suivants :

- Si vous avez activé le DNS privé pour le point de terminaison (zone hébergée privée ; applicable aux services AWS et aux services partenaires AWS Marketplace uniquement), le nom d'hôte DNS par défaut du service AWS de la Région. Par exemple, `ec2.us-east-1.amazonaws.com`.

  Important

  Le DNS privé n'est pas pris en charge pour les points de terminaison de l'interface d'Amazon S3.
- Le nom d'hôte DNS régional propre au point de terminaison qui est généré pour le point de terminaison d'interface. Le nom d'hôte inclut un identifiant de point de terminaison unique, un identifiant de service, la région et `vpce.amazonaws.com` dans son nom.. Par exemple, `vpce-0fe5b17a0707d6abc-29p5708s.ec2.us-east-1.vpce.amazonaws.com`.
- Le nom d'hôte DNS de la zone propre au point de terminaison qui est généré pour chaque zone de disponibilité dans laquelle le point de terminaison est disponible. Le nom d'hôte inclut la zone de disponibilité dans son nom. Par exemple, `vpce-0fe5b17a0707d6abc-29p5708s-us-east-1a.ec2.us-east-1.vpce.amazonaws.com`. Vous pouvez utiliser cette option si votre architecture isole les zones de disponibilité (par exemple, pour contenir les défaillances ou réduire les coûts de transfert de données régional).

  Une demande vers un nom d'hôte DNS zonal est destiné à l'emplacement de zone de disponibilité correspondant dans le compte du fournisseur de services, qui peut ne pas avoir le même nom de zone de disponibilité que votre compte. Pour de plus amples informations, veuillez consulter Concepts de région et de zone de disponibilité.
- Adresse IP privée de l'interface réseau du point de terminaison du VPC.

Pour obtenir les noms DNS de région et de zone, veuillez consulter Afficher votre point de terminaison d'interface (p. 13).

Par exemple, dans un sous-réseau où vous avez un point de terminaison d'interface pour Elastic Load Balancing pour lequel vous n'avez pas activé l'option de DNS privé, utilisez la commande de la AWS CLI suivante à partir d'une instance pour décrire vos équilibreurs de charge. La commande utilise le nom d'hôte DNS régional propre au point de terminaison pour créer la demande via le point de terminaison d'interface.

```
aws elbv2 describe-load-balancers --endpoint-url https://vpce-0f89a33420c193abc-
bluzidnv.elasticloadbalancing.us-east-1.vpce.amazonaws.com/
```

Si vous activez l'option DNS privé, vous n'avez pas à spécifier l'URL du point de terminaison dans la demande. L'AWS CLI utilise le point de terminaison par défaut du service AWS de la région (`elasticloadbalancing.us-east-1.amazonaws.com`).

Modifier un point de terminaison d'interface

Vous pouvez modifier les attributs suivants d'un point de terminaison d'interface :

- Le sous-réseau où figure le point de terminaison d'interface
- Les groupes de sécurité associés à l'interface réseau du point de terminaison
- Les balises
- L'option de DNS privé

  Note

  Lorsque vous activez le DNS privé, il peut prendre quelques minutes pour que les adresses IP privées deviennent disponibles.
- La stratégie de point de terminaison (si elle est prise en charge par le service)

Si vous supprimez un sous-réseau du point de terminaison d'interface, l'interface réseau de point de terminaison correspondante du sous-réseau est supprimée.

Console

Pour modifier les sous-réseaux d'un point de terminaison d'interface

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 le point de terminaison d'interface.
3. Choisissez Actions, Gérer les sous-réseaux.
4. Sélectionnez les sous-réseaux ou annulez leur sélection si nécessaire, puis choisissez Modifier les sous-réseaux.

Pour ajouter ou supprimer les groupes de sécurité associés à un point de terminaison d'interface

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 le point de terminaison d'interface.
3. Choisissez Actions, Gérer les groupes de sécurité.
4. Sélectionnez les groupes de sécurité ou annulez leur sélection si nécessaire, puis choisissez Enregistrer.

Pour ajouter ou supprimer une balise de point de terminaison d’interface

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoints (Points de terminaison).
3. Sélectionnez le point de terminaison d’interface et choisissez Actions, Add/Edit Tags (Ajouter/modifier des balises).
4. Ajoutez ou supprimez une balise.

   [Ajouter une balise] Choisissez Create tag (Créer une balise) et procédez comme suit :

   - Pour Clé, saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur clé.

[Supprimer une balise] Choisissez le bouton de suppression (« x ») situé à la droite de la clé et de la valeur de la balise.

Pour modifier l'option de DNS privé

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 le point de terminaison d'interface.
3. Choisissez Actions, Modifier les noms de DNS privés.
4. Définissez l'option si nécessaire, puis choisissez Modify Private DNS names (Modifier les noms de DNS privés).

Pour mettre à jour la stratégie de point de terminaison

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 le point de terminaison d'interface.
3. Choisissez Actions, Modifier une stratégie.
4. Choisissez Accès complet pour autoriser un accès complet au service, ou choisissez Personnalisé et spécifiez une stratégie personnalisée. Choisissez Enregistrer.

Command line

Pour modifier un point de terminaison de VPC à l'aide de la AWS CLI

1. Utilisez la commande describe-vpc-endpoints pour obtenir l'ID de votre point de terminaison d'interface.

```
aws ec2 describe-vpc-endpoints
```

2. L'exemple suivant utilise la commande modify-vpc-endpoint pour ajouter le sous-réseau `subnet-aabb1122` au point de terminaison d'interface.

```
aws ec2 modify-vpc-endpoint --vpc-endpoint-id vpce-0fe5b17a0707d6abc --add-subnet-id subnet-aabb1122
```

Pour modifier un point de terminaison de VPC à l'aide de AWS Tools for Windows PowerShell ou d'une API

- Edit-EC2VpcEndpoint (AWS Tools for Windows PowerShell)
- ModifyVpcEndpoint (API de requête Amazon EC2)

Pour ajouter ou supprimer une balise de point de terminaison de VPC avec la AWS Tools for Windows PowerShell ou une API

- tag-resource (AWS CLI)
- TagResource (AWS Tools for Windows PowerShell)
- untag-resource (AWS CLI)
- TagResource (AWS Tools for Windows PowerShell)

Points de terminaison de l'équilibreur de charge de passerelle (AWS PrivateLink)

Un point de terminaison d'équilibreur de charge de passerelle vous permet d'intercepter le trafic et de l'acheminer vers un service que vous avez configuré à l'aide des équilibreurs de charge de passerelle, par exemple, pour une inspection de sécurité. Le propriétaire du service est le fournisseur du service, et vous, en tant que mandataire créant le point de terminaison d'équilibreur de charge de passerelle, vous êtes le consommateur du service.

Les étapes générales de configuration d'un point de terminaison d'équilibreur de charge de passerelle sont les suivantes :

1. Assurez-vous qu'un service de point de terminaison d'équilibreur de charge de passerelle soit configuré. Pour plus d'informations, consultez Services de point de terminaison d'un VPC pour les points de terminaison d'équilibreur de charge de passerelle (p. 47).
2. Choisissez le VPC dans lequel créer le point de terminaison d'équilibreur de charge de passerelle et indiquez le nom du service.
3. Choisissez un sous-réseau dans votre VPC pour utiliser le point de terminaison d'équilibreur de charge de passerelle. Nous créons une interface réseau du point de terminaison dans le sous-réseau. Une interface réseau de point de terminaison se voit attribuer une adresse IP privée à partir de la plage d'adresses IP de votre sous-réseau et conserve cette adresse IP jusqu'à ce que le point de terminaison d'équilibreur de charge de passerelle soit supprimé.

   Note

   Un point de terminaison d'interface est une interface réseau gérée par demandeur. Vous pouvez l'afficher dans votre compte, mais vous ne pouvez pas la gérer vous-même. Pour de plus amples informations, veuillez consulter Interfaces réseau gérées par le demandeur.
4. Une fois que vous avez créé le point de terminaison d'équilibreur de charge de passerelle, celui-ci est disponible pour utilisation quand il est accepté par le fournisseur de service. Le fournisseur de service peut configurer le service pour accepter les demandes automatiquement ou manuellement.
5. Configurez votre table de routage de sous-réseau et votre table de routage de passerelle pour diriger le trafic vers le point de terminaison d'équilibreur de charge de passerelle. Pour plus d'informations, reportez-vous à la section Routage vers un point de terminaison d'équilibreur de charge de passerelle dans le Guide de l'utilisateur Amazon VPC.

Table des matières

Propriétés et limites du point de terminaison d'équilibreur de charge de passerelle

Pour utiliser un point de terminaison d'équilibreur de charge de passerelle, tenez compte des points suivants :

- Pour chaque point de terminaison d'équilibreur de charge de passerelle, vous ne pouvez choisir qu'une seule zone de disponibilité (sous-réseau) dans votre VPC. Vous ne pouvez pas modifier le sous-réseau ultérieurement. Pour utiliser un point de terminaison d'équilibreur de charge de passerelle dans un sous-réseau différent, créez un point de terminaison d'équilibreur de charge de passerelle dans ce sous-réseau. Vous pouvez créer un point de terminaison de l'équilibreur de charge de passerelle unique par zone de disponibilité pour un service, mais uniquement pour les zones de disponibilité prises en charge par l'équilibreur de charge de passerelle.
- Chaque point de terminaison d'équilibreur de charge de passerelle prend en charge une bande passante maximale de 40 Gbit/s.
- Si la liste ACL réseau de votre sous-réseau limite le trafic, vous pourriez ne pas pouvoir envoyer du trafic via le point de terminaison d'équilibreur de charge de passerelle. Assurez-vous d'ajouter des règles appropriées qui autorisent le trafic vers et depuis le bloc d'adresse CIDR du sous-réseau.
- Les groupes de sécurité ne sont pas pris en charge.
- Les stratégies de point de terminaison ne sont pas prises en charge.
- Un service peut ne pas être disponible dans toutes les zones de disponibilité via un point de terminaison d'équilibreur de charge de passerelle. Pour connaître les zones de disponibilité compatibles, utilisez la commande describe-vpc-endpoint-services ou utilisez la console Amazon VPC. Pour plus d'informations, consultez Créer un point de terminaison d'équilibreur de charge de passerelle (p. 20).
- Lorsque vous créez un point de terminaison d'équilibreur de charge de passerelle, celui-ci est créé dans la zone de disponibilité mappée à votre compte et est indépendant des autres comptes. Lorsque le fournisseur de service et le consommateur sont dans des comptes différents, utilisez l'ID de zone de disponibilité pour identifier de façon unique et cohérente la zone de disponibilité du point de terminaison. Par exemple, `use1-az1` est un ID de zone de disponibilité pour la région `us-east-1`, qui correspond au même emplacement dans chaque compte AWS. Pour en savoir plus sur les ID de zone de disponibilité, consultez ID de zone de disponibilité pour vos ressources dans le Guide de l'utilisateur AWS RAM ou utilisez describe-availability-zones.
- Pour maintenir le trafic 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 allez envoyer 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.
- Les points de terminaison sont uniquement pris en charge dans une même région. Vous ne pouvez pas créer un point de terminaison entre un VPC et un service situé dans une autre région.
- Les points de terminaison prennent en charge le trafic IPv4 uniquement.
- Vous ne pouvez pas transférer de point de terminaison d'un VPC à un autre, ou d'un service à un autre.
- Vous êtes soumis à un quota pour le nombre de points de terminaison que vous pouvez créer par VPC. Pour plus d'informations, consultez AWS PrivateLinkQuotas (p. 89).

Cycle de vie des points de terminaison d'équilibreur de charge de passerelle

Un point de terminaison d'équilibreur de charge de passerelle passe par plusieurs étapes à partir du moment où vous le créez (la demande de connexion du point de terminaison). À chaque étape, il peut y avoir des actions que le consommateur du service et le fournisseur du service peuvent prendre.

Les règles suivantes s'appliquent :

- Un fournisseur de service peut configurer le service pour accepter les demandes de point de terminaison d'équilibreur de charge de passerelle automatiquement ou manuellement.

- Un fournisseur de service ne peut pas supprimer un point de terminaison d'équilibreur de charge de passerelle sur son service. Seul le consommateur de service qui a demandé la connexion peut supprimer le point de terminaison d'équilibreur de charge de passerelle.
- Un fournisseur de service peut rejeter le point de terminaison d'équilibreur de charge de passerelle une fois qu'il a été accepté et qu'il est dans l'état `available`.

Tarification des points de terminaison d'équilibreur de charge de passerelle

La création et l'utilisation d'un point de terminaison d'équilibreur de charge de passerelle vers un service vous sont facturées. Les tarifs d'utilisation horaire et les tarifs de traitement des données s'appliquent. Pour plus d'informations, consultez Tarification AWS PrivateLink. Vous pouvez afficher le nombre total de points de terminaison Gateway Load Balancer à l'aide de la console Amazon VPC ou de la AWS CLI.

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

Pour créer un point de terminaison d'équilibreur de charge de passerelle, vous devez spécifier le VPC dans lequel vous voulez créer le point de terminaison et le service avec lequel vous voulez établir la connexion.

Console

Pour créer 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, sélectionnez Points de terminaison, Créer un point de terminaison.
3. Pour Catégorie de service, choisissez Rechercher un service par nom.
4. Pour Service Name (Nom du service), entrez le nom du service et choisissez Verify (Vérifier).
5. Complétez les informations suivantes, puis choisissez Créer un point de terminaison.
   - Pour VPC, sélectionnez un VPC dans lequel créer le point de terminaison.
   - Pour Subnets (Sous-réseaux), sélectionnez le sous-réseau (Zone de disponibilité) dans lequel vous souhaitez créer le point de terminaison d'équilibreur de charge de passerelle.
   - (Facultatif) Pour ajouter une balise, choisissez Add tag (Ajouter une balise) et spécifiez la clé et la valeur de la balise.

Command line

Pour créer un point de terminaison Gateway Load Balancer à l'aide de la AWS CLI

Utilisez la commande create-vpc-endpoint et spécifiez l'ID du VPC, le type de point de terminaison d'un VPC (équilibreur de charge de passerelle), le nom du service et le sous-réseau dans lequel vous souhaitez créer le point de terminaison d'équilibreur de charge de passerelle.

```
aws ec2 create-vpc-endpoint --vpc-endpoint-type GatewayLoadBalancer --vpc-id vpc-id --
subnet-ids subnet-id --service-name gateway-load-balancer-service-name
```

Pour créer un point de terminaison de VPC l'aide de AWS Tools for Windows PowerShell ou de l'API

- New-EC2VpcEndpoint
- CreateVpcEndpoint

Afficher votre point de terminaison d'équilibreur de charge de passerelle

Après avoir créé un point de terminaison d'équilibreur de charge de passerelle, vous pouvez afficher les informations à son sujet.

Console

Pour afficher les informations sur 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 volet de navigation, choisissez Endpoints (Points de terminaison), puis sélectionnez votre point de terminaison d'équilibreur de charge de passerelle.
3. Sélectionnez Details (Détails).
4. Pour afficher le sous-réseau dans lequel le point de terminaison d'équilibreur de charge de passerelle a été créé, ainsi que l'ID de l'interface réseau du point de terminaison de chaque sous-réseau, choisissez Subnets (Sous-réseaux).

Command line

Pour décrire votre point de terminaison d'équilibreur de charge de passerelle à l'aide d'un outil de ligne de commande ou d'une API

- describe-vpc-endpoints (AWS CLI)
- Get-EC2VpcEndpoint (Tools for Windows PowerShell)
- DescribeVpcEndpoints (API de requête Amazon EC2)

Ajouter ou supprimer des balises pour un point de terminaison d'équilibreur de charge de passerelle

Vous pouvez ajouter ou supprimer les balises de votre point de terminaison d'équilibreur de charge de passerelle.

Console

Pour ajouter ou supprimer une balise.

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoints (Points de terminaison).
3. Sélectionnez le point de terminaison d'équilibreur de charge de passerelle et choisissez Actions, Add/Edit Tags (Ajouter/modifier des balises).
4. Ajoutez ou supprimez une balise.

   [Ajouter une balise] Choisissez Create tag (Créer une balise) et procédez comme suit :

   - Pour Clé, saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur clé.

   [Supprimer une balise] Choisissez le bouton de suppression (« x ») situé à la droite de la clé et de la valeur de la balise.

Command line

Pour ajouter ou supprimer des balises à l'aide d'un outil de ligne de commande ou d'une API

- Utilisez create-tags et delete-tags. (AWS CLI)
- Use New-EC2Tag et Remove-EC2Tag (AWS Tools for Windows PowerShell)
- Utilisez CreateTags et DeleteTags. (API de requête Amazon EC2)

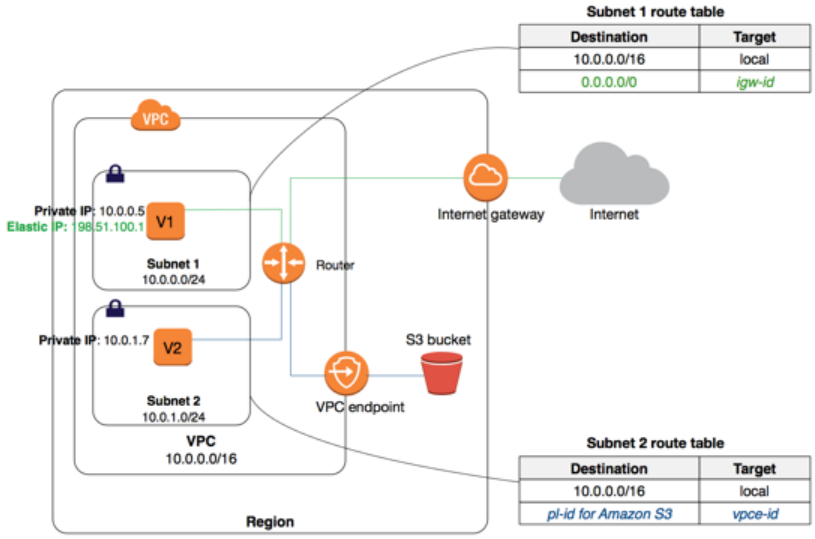
Points de terminaison d'un VPC de passerelle

Les points de terminaison 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 n'activent pas AWS PrivateLink.

Pour créer et configurer un point de terminaison de passerelle, suivez ces étapes générales :

1. Spécifiez le VPC dans lequel créer le point de terminaison et le service auquel vous souhaitez vous connecter. Un service est identifié par une liste de préfixes gérée par AWS (nom et ID d'un service pour une Région). Un ID de liste de préfixes AWS utilise le format `pl-xxxxxxxx` et un nom de liste de préfixes AWS utilise le format « com.amazonaws.*region*.*service* ». Utilisez le nom de liste de préfixes AWS (nom de service) pour créer un point de terminaison.
2. Attachez une stratégie de point de terminaison à votre point de terminaison pour autoriser l'accès à certains ou à tous les services auxquels vous vous connectez. Pour plus d'informations, consultez Utiliser les stratégies de point de terminaison d'un VPC (p. 40).
3. Spécifiez une ou plusieurs tables de routage dans lesquelles créer les itinéraires vers le service. Les tables de routage contrôlent l'acheminement du trafic entre votre VPC et l'autre service. Chaque sous-réseau associé à une de ces tables de routage a accès au point de terminaison, et le trafic entre les instances de ces sous-réseaux et le service est ensuite acheminé via le point de terminaison.

Dans le schéma suivant, les instances du sous-réseau 2 peuvent accéder à Amazon S3 par le biais du point de terminaison de passerelle.



Vous pouvez créer plusieurs points de terminaison dans un seul VPC, par exemple, pour plusieurs services. Vous pouvez aussi créer plusieurs points de terminaison pour un seul service et vous pouvez utiliser différentes tables de routage pour imposer différentes stratégies d'accès depuis plusieurs sous-réseaux vers le même service.

Après avoir créé un point de terminaison, vous pouvez modifier la stratégie du point de terminaison attachée à votre point de terminaison, et ajouter ou supprimer les tables de routage utilisées par le point de terminaison.

Table des matières

Tarification des points de terminaison de passerelle

Il n'y a pas de frais supplémentaires pour l'utilisation de points de terminaison de passerelle. Des frais standards s'appliquent pour le transfert de données et l'utilisation de ressources. Pour de plus amples informations sur la tarification, veuillez consulter Tarification d'Amazon EC2.

Routage des points de terminaison de passerelle

Quand vous créez ou modifiez un point de terminaison, vous spécifiez les tables de routage VPC qui sont utilisées pour accéder au service via le point de terminaison. Une route est automatiquement ajoutée à chacune des tables de routage avec une destination qui indique l'ID de liste de préfixes AWS du service (`pl-xxxxxxxx`) et une cible avec l'ID du point de terminaison (`vpce-xxxxxxxx`) ; par exemple :

Destination	Cible
10.0.0.0/16	Locale
pl-1a2b3c4d	vpce-11bb22cc

L'ID de liste des préfixes représente logiquement la plage d'adresses IP publiques utilisée par le service. Toutes les instances des sous-réseaux associés aux tables de routage spécifiées utilisent automatiquement le point de terminaison pour accéder au service. Les sous-réseaux qui ne sont pas associés aux tables de routage spécifiées n'utilisent pas le point de terminaison. Vous pouvez ainsi garder des ressources dans d'autres sous-réseaux séparés de votre point de terminaison.

Pour voir la plage d'adresses IP publiques actuelle d'un service, vous pouvez utiliser la commande describe-prefix-lists. .

> **Note**
>
> La plage d'adresses IP publiques pour un service peut changer de temps en temps. Prenez en compte les implications avant d'effectuer le routage ou de prendre d'autres décisions selon la plage d'adresses IP actuelle pour un service.

Les règles suivantes s'appliquent :

- Vous pouvez avoir plusieurs routes de point de terminaison pour différents services dans une table de routage, et vous pouvez avoir plusieurs routes de point de terminaison pour le même service dans

différentes tables de routage. Mais vous ne pouvez pas avoir plusieurs routes de point de terminaison pour le même service dans une seule table de routage. Par exemple, si vous créez deux points de terminaison vers Amazon S3 dans votre VPC, vous ne pouvez pas créer de routes pour les deux points de terminaison dans la même table de routage.

- Vous ne pouvez pas explicitement ajouter, modifier ou supprimer une route de point de terminaison dans votre table de routage en utilisant ses API ou la page Tables de routage de la console Amazon VPC. Vous pouvez uniquement ajouter une route de point de terminaison en associant une table de routage à un point de terminaison. Vous pouvez modifier le point de terminaison (p. 38) pour changer les tables de routage qui sont associées à votre point de terminaison.
- Une route du point de terminaison est automatiquement supprimée quand vous enlevez l'association de la table de routage depuis le point de terminaison (en modifiant le point de terminaison) ou quand vous supprimez votre point de terminaison.

Nous utilisons la route la plus spécifique qui correspond au trafic afin de déterminer comment router le trafic (correspondance de préfixe le plus long). Si vous avez un itinéraire existant dans votre table de routage pour tout le trafic Internet (`0.0.0.0/0`) qui pointe vers une passerelle Internet, l'itinéraire du point de terminaison est prioritaire sur tout le trafic destiné au service, puisque la plage d'adresses IP pour le service est plus spécifique que `0.0.0.0/0`. Tout le reste du trafic Internet va vers votre passerelle Internet, y compris le trafic destiné au service dans d'autres régions.

Cependant, si vous avez des itinéraires plus spécifiques existants vers des plages d'adresses IP qui pointent vers une passerelle Internet ou un périphérique NAT, ces itinéraires sont prioritaires. Si vous avez des routes existantes destinées à une plage d'adresses IP qui est identique à la plage d'adresses IP utilisée par le service, alors vos routes sont prioritaires.

Exemple : une route de point de terminaison dans une table de routage

Dans ce scénario, vous avez un itinéraire existant dans votre table de routage pour tout le trafic Internet (`0.0.0.0/0`) qui pointe vers une passerelle Internet. Tout trafic sortant du sous-réseau destiné à un autre service AWS utilise la passerelle Internet.

Destination	Cible
10.0.0.0/16	Locale
0.0.0.0/0	igw-1a2b3c4d

Vous pouvez créer un point de terminaison vers un service AWS pris en charge et associer votre table de routage au point de terminaison. Une route de point de terminaison est automatiquement ajoutée à la table de routage, avec comme destination `pl-1a2b3c4d` (en supposant que cela représente le service vers lequel vous avez créé le point de terminaison). Maintenant, tout trafic du sous-réseau destiné à ce service AWS dans la même région va vers le point de terminaison et non vers la passerelle Internet. Tout autre trafic Internet va vers votre passerelle Internet, y compris le trafic destiné à d'autres services et destiné au service AWS dans d'autres régions.

Destination	Cible
10.0.0.0/16	Locale
0.0.0.0/0	igw-1a2b3c4d
pl-1a2b3c4d	vpce-11bb22cc

Exemple : ajustement de vos tables de routage pour les points de terminaison

Dans ce scénario, `54.123.165.0/24` se trouve dans la plage d'adresses IP Amazon S3 et vous avez configuré votre table de routage pour permettre aux instances de votre sous-réseau de communiquer avec les compartiments Amazon S3 par le biais d'une passerelle Internet. Vous avez ajouté un itinéraire avec `54.123.165.0/24` comme destination et la passerelle Internet comme cible. Vous créez ensuite un point de terminaison et associez cette table de routage au point de terminaison. Une route de point de terminaison est automatiquement ajoutée à la table de routage. Vous utilisez ensuite la commande describe-prefix-lists afin d'afficher la plage d'adresses IP pour Amazon S3. La plage est `54.123.160.0/19`, ce qui est moins spécifique que la plage qui pointe vers votre passerelle Internet. Cela signifie que tout trafic destiné à la plage d'adresses IP `54.123.165.0/24` continue d'utiliser la passerelle Internet et n'utilise pas le point de terminaison, aussi longtemps qu'elle reste la plage d'adresses IP publiques pour Amazon S3.

Destination	Cible
10.0.0.0/16	Locale
54.123.165.0/24	igw-1a2b3c4d
pl-1a2b3c4d	vpce-11bb22cc

Pour vous assurer que tout le trafic destiné à Amazon S3 de la même région est acheminé par le biais du point de terminaison, vous devez ajuster les routes dans votre table de routage. Pour ce faire, vous pouvez supprimer l'itinéraire vers la passerelle Internet. Désormais, tout le trafic pour Amazon S3 de la même région utilise le point de terminaison et le sous-réseau associé à votre table de routage est privé.

Destination	Cible
10.0.0.0/16	Locale
pl-1a2b3c4d	vpce-11bb22cc

Limitations de point de terminaison de passerelle

Pour utiliser les points de terminaison de passerelle, vous devez être conscient des limitations actuelles :

- Vous ne pouvez pas utiliser d'ID de liste de préfixes AWS dans une règle sortante d'une liste ACL réseau pour autoriser ou refuser le trafic sortant à destination du service spécifié dans un point de terminaison. Si vos règles ACL réseau limitent le trafic, vous devez spécifier le bloc d'adresses CIDR (plage d'adresses IP) pour le service à la place. Vous pouvez toutefois utiliser un ID de liste de préfixes AWS dans une règle de groupe de sécurité de trafic sortant. Pour plus d'informations, consultez Groupes de sécurité (p. 41).
- Les points de terminaison sont uniquement pris en charge dans une même région. Vous ne pouvez pas créer un point de terminaison entre un VPC et un service situé dans une autre région.
- Les points de terminaison prennent en charge le trafic IPv4 uniquement.
- Vous ne pouvez pas transférer de point de terminaison d'un VPC à un autre, ou d'un service à un autre.
- Vous êtes soumis à un quota pour le nombre de points de terminaison que vous pouvez créer par VPC. Pour plus d'informations, consultez AWS PrivateLinkQuotas (p. 89).
- 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 de VPC, d'une passerelle de transit, d'une connexion AWS Direct Connect ou d'une connexion ClassicLink de votre VPC ne peuvent pas utiliser le point de terminaison pour communiquer avec les ressources du service de point de terminaison.

- Vous devez activer la résolution DNS dans votre VPC ou, si vous utilisez votre propre serveur DNS, vous devez veiller à ce que les demandes DNS vers le service requis (par exemple, Amazon S3) soient résolues correctement en adresses IP gérées par AWS. Pour en savoir plus, consultez Utilisation de DNS avec votre VPC dans le Guide de l'utilisateur Amazon VPC et Plages d'adresse IP AWS dans Référence générale d'Amazon Web Services.
- Vérifiez les limites spécifiques au service pour votre service de point de terminaison.

Pour de plus amples informations en ce qui concerne les règles et limitations propres à Amazon S3, veuillez consulter Points de terminaison pour Amazon S3 (p. 26).

Pour de plus amples informations en ce qui concerne les règles et limitations propres à DynamoDB, veuillez consulter Points de terminaison pour Amazon DynamoDB (p. 33).

Points de terminaison pour Amazon S3

Si vous avez déjà configuré un accès à vos ressources Amazon S3 depuis votre VPC, vous pouvez continuer à utiliser des noms de DNS Amazon S3 pour accéder à ces ressources après avoir configuré un point de terminaison. Cependant, veuillez noter ce qui suit :

- Votre point de terminaison a une stratégie qui contrôle l'utilisation du point de terminaison pour accéder aux ressources Amazon S3. La stratégie par défaut autorise tout utilisateur ou service au sein du VPC à accéder à une ressource Amazon S3 en utilisant les informations d'identification d'un compte Compte AWS quelconque, y compris à des ressources Amazon S3 pour un compte Compte AWS autre que le compte auquel le VPC est associé. Pour plus d'informations, consultez Contrôler l'accès aux services avec les points de terminaison d'un VPC (p. 40).
- 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.
- Vous ne pouvez pas utiliser de stratégie IAM ou de compartiment pour autoriser l'accès depuis une plage d'adresses CIDR IPv4 de VPC (la plage d'adresses IPv4 privées). Les blocs d'adresse CIDR du VPC peuvent se chevaucher ou être identiques, ce qui peut entraîner des résultats inattendus. Vous ne pouvez donc pas utiliser la condition `aws:SourceIp` dans vos stratégies IAM pour des demandes vers Amazon S3 par le biais d'un point de terminaison VPC. Cela s'applique aux stratégies IAM; pour les utilisateurs et les rôles, ainsi que n'importe quelle stratégie de compartiment. Si une instruction comprend la condition `aws:SourceIp`, la valeur ne correspondra à aucune adresse IP ou plage fournie. Au lieu de cela, vous pouvez effectuer les actions suivantes :
  - Utilisez vos tables de routage pour contrôler quelles instances peuvent avoir accès aux ressources dans Amazon S3 par le biais du point de terminaison.
  - Pour stratégies de compartiment, vous pouvez restreindre l'accès à un point de terminaison spécifique ou à un VPC spécifique. Pour plus d'informations, consultez Stratégies de compartiment Amazon S3 (p. 31).
- Les points de terminaison ne sont actuellement pas compatibles avec les demandes inter-régionales. Assurez-vous de créer votre point de terminaison dans la même région que votre compartiment. Vous pouvez trouver l'emplacement de votre compartiment en utilisant la console Amazon S3 ou la commande get-bucket-location. Utilisez un point de terminaison Amazon S3 spécifique à une région pour accéder à votre compartiment, par exemple, `mybucket.s3.us-west-2.amazonaws.com`. Pour de plus amples informations sur les points de terminaison spécifiques à une région pour Amazon S3, veuillez consulter Amazon Simple Storage Service (S3) dans Références générales Amazon Web Services. Si vous utilisez la AWS CLI pour adresser des demandes à Amazon S3, configurez la même région que votre compartiment en tant que région par défaut ou utilisez le paramètre `--region` dans vos demandes.

Note

Traitez la région USA Standard pour Amazon S3 comme mappée à la région `us-east-1`.

- Actuellement, les points de terminaison sont pris en charge pour le trafic IPv4 uniquement.

Avant d'utiliser les points de terminaison avec Amazon S3, veuillez prendre connaissances des limites générales suivantes : Limitations de point de terminaison de passerelle (p. 25). Pour plus d'informations sur la création et l'affichage des compartiments S3, veuillez consulter Comment créer un compartiment S3 et Comment afficher les propriétés pour un compartiment S3 dans le Guide de l'utilisateur d'Amazon Simple Storage Service.

Si vous utilisez d'autres services AWS dans votre VPC, il se peut qu'ils utilisent des compartiments S3 pour certaines tâches. Assurez-vous que votre stratégie de point de terminaison autorise un accès total à Amazon S3 (stratégie par défaut) ou qu'elle autorise l'accès aux compartiments spécifiques utilisés par ces services. Sinon, créez uniquement un point de terminaison dans un sous-réseau qui n'est utilisé par aucun de ces services, pour permettre aux services de continuer à accéder aux compartiments S3 à l'aide d'adresses IP publiques.

Le tableau suivant répertorie les services AWS susceptibles d'être affectés par un point de terminaison ainsi que des informations propres à chaque service.

Service AWS	Remarque
Amazon AppStream 2.0	Votre stratégie de point de terminaison doit autoriser l'accès aux compartiments spécifiques utilisés par AppStream 2.0 pour stocker le contenu utilisateur. Pour de plus amples d'informations, veuillez consulter Utilisation des points de terminaison VPC Amazon S3 pour les dossiers de base et la persistance des paramètres d'application dans le Guide d'administration Amazon AppStream 2.0.
AWS CloudFormation	Si vous avez des ressources dans votre VPC qui doivent répondre à une condition d'attente ou à une demande de ressource personnalisée, votre stratégie de point de terminaison doit au moins autoriser l'accès aux compartiments spécifiques qui sont utilisés par ces ressources. Pour de plus amples informations, veuillez consulter Configuration des points de terminaison d'un VPC pour AWS CloudFormation.
CodeDeploy	Votre stratégie de point de terminaison doit autoriser un accès total à Amazon S3 ou à tout compartiment S3 que vous avez créé pour vos déploiements CodeDeploy.
Elastic Beanstalk	Votre stratégie de point de terminaison doit au moins autoriser l'accès à tous les compartiments S3 utilisés pour les applications Elastic Beanstalk. Pour en savoir plus, consultez Utilisation d'Elastic Beanstalk avec Amazon S3 dans le Guide du développeur AWS Elastic Beanstalk.

Service AWS	Remarque
Amazon EMR	Votre stratégie de point de terminaison doit autoriser l'accès aux référentiels Amazon Linux et aux autres compartiments utilisés par Amazon EMR. Pour de plus amples informations, veuillez consulter Stratégie Amazon S3 minimum pour sous-réseau privé dans le Guide de gestion Amazon EMR.
AWS OpsWorks	Votre stratégie de point de terminaison doit au moins autoriser l'accès aux compartiments spécifiques utilisés par AWS OpsWorks. Pour en savoir plus, consultez Exécution d'une pile dans un VPC dans le Guide de l'utilisateur AWS OpsWorks.
AWS Systems Manager	Votre stratégie de point de terminaison doit autoriser l'accès aux compartiments Amazon S3 utilisés par le Gestionnaire de correctifs pour les opérations de référence de correctif dans votre Région AWS. Ces compartiments contiennent le code qui est extrait et exécuté sur des instances par le service de référence de correctif. Pour en savoir plus, consultez Créer un point de terminaison de VPC dans le Guide de l'utilisateur AWS Systems Manager. Pour obtenir la liste des autorisations de compartiment S3 requises par SSM agent pour ses opérations, consultez Autorisations minimales relatives aux compartiments S3 pour l'agent SSM dans le Guide de l'utilisateur AWS Systems Manager.
Amazon Elastic Container Registry	Votre stratégie de point de terminaison doit autoriser l'accès aux compartiments Amazon S3 utilisés par Amazon ECR pour stocker les couches d'image Docker. Pour de plus amples informations, veuillez consulter Autorisations minimales de compartiment Amazon S3 pour Amazon ECR dans le Guide de l'utilisateur Amazon Elastic Container Registry.
Amazon WorkDocs	Si vous utilisez un client Amazon WorkDocs dans WorkSpaces ou une instance EC2, votre stratégie de point de terminaison doit autoriser l'accès complet à Amazon S3.
WorkSpaces	WorkSpaces ne dépend pas directement d'Amazon S3. Cependant, si vous accordez un accès Internet aux utilisateurs WorkSpaces, notez que les sites web, les e-mails HTML et les services Internet d'autres sociétés peuvent dépendre d'Amazon S3. Assurez-vous que votre stratégie de point de terminaison donne un accès total à Amazon S3 pour permettre à ces services de continuer à fonctionner correctement.

Le trafic entre votre VPC et les compartiments S3 ne quitte pas le réseau Amazon.

Stratégies de point de terminaison pour Amazon S3

Voici des exemples de stratégies point de terminaison pour accéder à Amazon S3. Pour plus d'informations, consultez Utiliser les stratégies de point de terminaison d'un VPC (p. 40). Il appartient à l'utilisateur de déterminer les restrictions de stratégie répondant à ses besoins métier.

> **Important**
>
> Tous les types de stratégies doivent accorder les autorisations nécessaires pour un accès valable à Amazon S3 et notamment les stratégies d'utilisateur IAM, de point de terminaison, de compartiment S3 et de liste de contrôle d'accès (ACL) Amazon S3 (le cas échéant). AWS vous recommande d'utiliser les conditions IAM, plutôt que l'élément `Principal` IAM, dans les stratégies de point de terminaison de VPC lorsque vous limitez l'utilisation du point de terminaison à certains appelants. Les exemples de ces conditions comprennent `aws:PrincipalArn`, `aws:PrincipalAccount`, `aws:PrincipalOrgId`, et `aws:PrincipalOrgPaths`. Pour de plus amples informations sur les clés de contexte de condition globale, veuillez consulter Clés de contexte de condition globale AWS dans le Guide de l'utilisateur AWS Identity and Access Management.

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. Ce point est utile si d'autres services AWS dans votre VPC utilisent des compartiments S3. Voici un exemple de politique qui restreint l'accès au compartiment spécifié uniquement.

```
{
  "Sid": "AccessToSpecificBucket",
  "Effect": "Allow",
  "Principal": "*",
  "Action": [
     "s3:ListBucket",
     "s3:GetObject",
     "s3:PutObject"
  ],
  "Resource": [
     "arn:aws:s3:::example-bucket",
     "arn:aws:s3:::example-bucket/*"
  ]
}
```

Example Exemple : Restriction de l'utilisation de ce point de terminaison d'un VPC à un rôle IAM spécifique dans un compte

Vous pouvez créer une stratégie qui limite l'utilisation du point de terminaison d'un VPC à un rôle IAM spécifique. Voici un exemple de restriction de l'accès au rôle spécifié dans le Compte AWS spécifié.

```
{
  "Sid": "Restrict-acess-to-specific-IAM-role",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "ArnEquals": {
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/SomeRole"
    }
  }
}
```

Example Exemple : Restriction de l'utilisation de ce point de terminaison d'un VPC à un utilisateur dans un compte spécifique

Vous pouvez créer une stratégie qui limite l'utilisation du point de terminaison d'un VPC à un compte spécifique. Voici un exemple de restriction de l'accès aux utilisateurs dans le Compte AWS spécifié.

```
{
  "Sid": "AllowCallersFromAccount111122223333",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:PrincipalAccount": "111122223333"
    }
  }
}
```

Example Exemple : autorisation d'accès aux référentiels AMI Amazon Linux

Les référentiels Amazon Linux sont des compartiments Amazon S3 dans chaque région. Pour autoriser les instances de votre VPC à accéder aux référentiels via un point de terminaison, créez une stratégie de point de terminaison.

La stratégie suivante accorde aux utilisateurs l'accès aux référentiels Amazon Linux. Veillez à remplacer *région* avec votre AWS Région (par exemple, `us-east-1`).

```
{
  "Statement": [
    {
      "Sid": "AmazonLinuxAMIRepositoryAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::packages.region.amazonaws.com/*",
        "arn:aws:s3:::repo.region.amazonaws.com/*"
      ]
    }
  ]
}
```

La stratégie suivante accorde aux utilisateurs l'accès aux référentiels Amazon Linux 2. Veillez à remplacer *région* avec votre AWS Région (par exemple, `us-east-1`).

```
{
  "Statement": [
    {
      "Sid": "AmazonLinux2AMIRepositoryAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::amazonlinux.region.amazonaws.com/*"
        "arn:aws:s3:::amazonlinux-2-repos-region/*"
      ]
```

```
    }
  ]
}
```

Stratégies de compartiment Amazon S3

Vous pouvez utiliser des stratégies de compartiment pour contrôler l'accès aux compartiments à partir de points de terminaison, VPC, plages d'adresses IP ou Comptes AWS spécifiques.

Vous ne pouvez pas utiliser la condition `aws:SourceIp` dans vos stratégies de compartiment pour des demandes à Amazon S3 par le biais d'un point de terminaison VPC. La condition ne correspond à aucune adresse IP ou plage d'adresses IP spécifiée et peut avoir un effet indésirable lorsque vous adressez des demandes à un compartiment Amazon S3. Exemples :

- Vous disposez d'une stratégie de compartiment avec un effet `Deny` et une condition `NotIpAddress` qui a pour but d'octroyer l'accès à partir d'une plage d'adresses IP unique ou limitée uniquement. Pour les demandes au compartiment via un point de terminaison, la condition `NotIpAddress` est toujours remplie, et l'effet de l'instruction est appliqué, en supposant que d'autres contraintes de la stratégie correspondent. L'accès au compartiment est refusé.
- Vous disposez d'une stratégie de compartiment avec un effet `Deny` et une condition `IpAddress` qui a pour but de refuser l'accès à une plage d'adresses IP unique ou limitée uniquement. Pour les demandes au compartiment via un point de terminaison, la condition n'est pas remplie, et l'instruction n'est pas appliquée. L'accès au compartiment est autorisé, en supposant qu'il existe des autres instructions qui autorisent l'accès sans condition `IpAddress`.

Utilisez `aws:VpcSourceIp` pour contrôler l'accès à partir de plages d'adresses IP spécifiques.

Pour permettre aux utilisateurs IAM de travailler avec des stratégies de compartiment, vous devez leur accorder l'autorisation d'utiliser les actions `s3:GetBucketPolicy` et `s3:PutBucketPolicy`.

Pour plus d'informations sur les stratégies de compartiment pour Amazon S3, veuillez consulter Utilisation de stratégies de compartiment et de stratégies utilisateur dans le Guide de l'utilisateur d'Amazon Simple Storage Service.

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

Vous pouvez créer une stratégie de compartiment qui restreint l'accès à un point de terminaison spécifique en utilisant la condition `aws:sourceVpce`. Voici un exemple de stratégie de compartiment S3 qui autorise l'accès à un compartiment `example_bucket` à partir d'un point de terminaison `vpce-1a2b3c4d`. La politique refuse tout accès au compartiment si le point de terminaison spécifié n'est pas utilisé. La condition `aws:sourceVpce` ne requiert pas d'ARN pour la ressource du point de terminaison d'un VPC, uniquement l'ID point de terminaison. 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",
  "Id": "Access-to-bucket-using-specific-endpoint",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPCE-only",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": ["arn:aws:s3:::example_bucket",
                   "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
```

```
        }
      }
    }
  ]
}
```

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

Vous pouvez créer une stratégie de compartiment qui restreint l'accès à des VPC spécifiques en utilisant la condition `aws:sourceVpc`. Ce point est utile si vous avez plusieurs points de terminaison configurés pour le même VPC et si vous voulez gérer l'accès à vos compartiments S3 pour tous vos points de terminaison. Voici un exemple de stratégie qui autorise le VPC `vpc-111bbb22` à accéder à `example_bucket` et ses objets. La politique refuse tout accès au compartiment si le VPC spécifié n'est pas utilisé. La condition `aws:sourceVpc` ne requiert pas d'ARN pour la ressource du VPC, uniquement l'ID du VPC. 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",
  "Id": "Access-to-bucket-using-specific-VPC",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPC-only",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "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 stratégie qui restreint l'accès à une plage d'adresses IP spécifique en utilisant la condition `aws:VpcSourceIp`. Voici un exemple de stratégie qui autorise le `172.31.0.0/16` à accéder à `example_bucket` et à ses objets. La stratégie refuse l'accès au compartiment à partir d'autres plages d'adresses IP. 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",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-specific-VPC-CIDR-only",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": ["arn:aws:s3:::example_bucket",
                   "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "NotIpAddress": {
          "aws:VpcSourceIp": "172.31.0.0/16"
        }
      }
```

```
    }
  ]
}
```

Example Exemple : restriction de l'accès aux compartiments dans un Compte AWS spécifique

Vous pouvez créer une stratégie qui restreint l'accès aux compartiments S3 dans un Compte AWS spécifique en utilisant la condition `s3:ResourceAccount`. Ceci est utile si vous souhaitez empêcher les clients de votre VPC d'accéder aux compartiments dont vous n'êtes pas le propriétaire. Voici un exemple de stratégie qui limite l'accès à des ressources appartenant à un seul Compte AWS, avec l'ID de compte `111122223333`. 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",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Access-to-bucket-in-specific-account-only",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "s3:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

Points de terminaison pour Amazon DynamoDB

Si vous avez déjà configuré l'accès à vos tables DynamoDB depuis votre VPC, vous pouvez continuer à accéder à ces tables comme vous le feriez normalement après avoir configuré un point de terminaison de passerelle. Cependant, veuillez noter ce qui suit :

- Votre point de terminaison dispose d'une stratégie qui contrôle l'utilisation du point de terminaison pour accéder aux ressources DynamoDB. La stratégie par défaut autorise tout utilisateur ou service au sein du VPC à accéder à une ressource DynamoDB en utilisant les informations d'identification d'un compte AWS. Pour plus d'informations, consultez Contrôler l'accès aux services avec les points de terminaison d'un VPC (p. 40).
- DynamoDB n'est pas compatible avec les stratégies basées sur des ressources (par exemple, sur des tables). L'accès à DynamoDB est contrôlé par le biais des stratégie de point de terminaison et IAM pour les utilisateurs et les rôles IAM individuels.
- Les points de terminaison ne sont actuellement pas compatibles avec les demandes inter-régionales. Assurez-vous de créer votre point de terminaison dans la même région que vos tables DynamoDB.
- Si vous utilisez AWS CloudTrail pour journaliser les opérations DynamoDB, les fichiers journaux contiennent l'adresse IP privée de l'instance EC2 dans le VPC et l'ID du point de terminaison pour les actions effectuées via le point de terminaison.
- 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 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 DynamoDB après l'interruption de la connexion.

Avant d'utiliser les points de terminaison avec DynamoDB, veuillez prendre connaissances des limites générales suivantes : Limitations de point de terminaison de passerelle (p. 25).

Pour de plus amples informations sur la création d'un point de terminaison VPC de passerelle, veuillez consulter Points de terminaison d'un VPC de passerelle (p. 22).

Stratégies de point de terminaison pour DynamoDB

Une stratégie de point de terminaison est une stratégie IAM que vous attachez à un point de terminaison pour permettre l'accès à l'ensemble ou à une partie des services auxquels vous vous connectez. Voici des exemples de stratégies de point de terminaison pour accéder à DynamoDB.

> **Important**
>
> Tous les types de stratégies doivent accorder les autorisations nécessaires pour un accès valable à DynamoDB et notamment les stratégies d'utilisateur IAM et de point de terminaison.

Example Exemple : accès en lecture seule

Vous pouvez créer une stratégie qui limite les actions pour uniquement répertorier et décrire les tables DynamoDB par le biais du point de terminaison d'un VPC.

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

Example Exemple : restreindre l'accès à une table spécifique

Vous pouvez créer une stratégie qui restreint l'accès à une table DynamoDB spécifique. Dans cet exemple, la stratégie de point de terminaison autorise l'accès à `StockTable` uniquement.

```
{
  "Statement": [
    {
      "Sid": "AccessToSpecificTable",
      "Principal": "*",
      "Action": [
        "dynamodb:Batch*",
        "dynamodb:Delete*",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Update*"
      ],
```

```
      "Effect": "Allow",
      "Resource": "arn:aws:dynamodb:us-east-1:123456789012:table/StockTable"
    }
  ]
}
```

Utiliser des stratégies IAM pour contrôler l'accès à DynamoDB

Vous pouvez créer une stratégie IAM pour vos utilisateurs, groupes ou rôles IAM afin de restreindre l'accès aux tables DynamoDB à partir d'un point de terminaison VPC spécifique uniquement. Pour ce faire, vous pouvez utiliser la clé de condition `aws:sourceVpce` pour la ressource de table dans votre stratégie IAM.

Pour de plus amples informations sur la gestion de l'accès à DynamoDB, veuillez consulter Authentification et contrôle d'accès pour Amazon DynamoDB dans le Guide du développeur Amazon DynamoDB.

Example Exemple : restreindre l'accès à partir d'un point de terminaison spécifique

Dans cet exemple, les utilisateurs sont pas autorisés à utiliser des tables DynamoDB, sauf si elles sont accessibles par le biais du point de terminaison `vpce-11aa22bb`.

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

Example Exemple : Restriction de l'utilisation de ce point de terminaison d'un VPC à un rôle IAM spécifique dans un compte

Vous pouvez créer une stratégie qui limite l'utilisation du point de terminaison d'un VPC à un rôle IAM spécifique. L'exemple suivant présente la restriction de l'accès à `SomeRole` dans le compte `111122223333`.

```
{
  "Sid": "Restrict-acess-to-specific-IAM-role",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "ArnEquals": {
      "aws:PrincipalArn": "arn:aws:iam::111122223333:role/SomeRole"
    }
  }
}
```

Example Exemple : Restriction de l'utilisation de ce point de terminaison d'un VPC à un utilisateur dans un compte spécifique

Vous pouvez créer une stratégie qui limite l'utilisation du point de terminaison d'un VPC à un compte spécifique. L'exemple suivant présente la restriction de l'accès aux utilisateurs dans le compte `111122223333`.

```
{
  "Sid": "AllowCallersFromAccount111122223333",
  "Effect": "Allow",
  "Principal": "*",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "aws:PrincipalAccount": "111122223333"
    }
  }
}
```

Créer un point de terminaison de passerelle

Pour créer un point de terminaison, vous devez spécifier le VPC dans lequel vous voulez créer le point de terminaison et le service avec lequel vous voulez établir la connexion.

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 volet de navigation, sélectionnez Points de terminaison, Créer un point de terminaison.
3. Pour Nom du service, choisissez le service auquel vous connectez. Pour créer un point de terminaison de passerelle vers DynamoDB ou Amazon S3, assurez-vous que la colonne Type indique Gateway (Passerelle).
4. Complétez les informations suivantes, puis choisissez Créer un point de terminaison.

   - Pour VPC, sélectionnez un VPC dans lequel créer le point de terminaison.
   - Pour Configurer les tables de routage, sélectionnez les tables de routage à utiliser par le point de terminaison. Un itinéraire est automatiquement ajouté qui pointe le trafic destiné au service vers le point de terminaison des tables de routage sélectionnées.
   - Pour Stratégie, choisissez le type de stratégie. Vous pouvez laisser l'option par défaut, Full Access, pour autoriser un accès total au service. Vous pouvez également sélectionner Custom (Personnaliser) puis utiliser le générateur de stratégie AWS pour créer une stratégie personnalisée ou entrer votre propre stratégie dans la fenêtre de stratégie.
   - (Facultatif) Ajoutez ou supprimez une balise.

     [Ajouter une identification] Choisissez Ajouter une identification et procédez comme suit :

     - Pour Clé, saisissez le nom de la clé.
     - Pour Valeur, saisissez la valeur clé.

     [Supprimer une balise] Choisissez le bouton de suppression (« x ») situé à la droite de la clé et de la valeur de la balise.

Une fois que vous avez créé un point de terminaison d'interface, vous pouvez afficher des informations à son sujet.

Pour afficher les informations sur 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 volet de navigation, choisissez Points de terminaison, puis sélectionnez votre point de terminaison.
3. Pour afficher des informations sur le point de terminaison, choisissez Résumé. Vous pouvez obtenir le nom de la liste de préfixes AWS du service dans la zone Service.

4. Pour afficher des informations sur les tables de routage utilisées par le point de terminaison, choisissez Tables de routage.
5. Pour afficher la stratégie IAM attachée à votre point de terminaison, choisissez Policy (Stratégie).

   Note

   L'onglet Stratégie affiche uniquement la stratégie du point de terminaison. Il n'affiche aucune information sur les stratégies IAM pour les utilisateurs IAM qui sont autorisés à utiliser des points de terminaison. Il n'affiche pas non plus de stratégies spécifiques aux services ; par exemple, les stratégies de compartiment S3.

Pour créer et afficher un point de terminaison à l'aide de l AWS CLI

1. Utilisez la commande describe-vpc-endpoint-services pour obtenir la liste des services disponibles. Dans le résultat retourné, prenez note du nom du service auquel vous voulez vous connecter. Le champ `serviceType` indique si vous vous connectez au service via un point de terminaison d'interface ou un point de terminaison de passerelle.

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

```
{
    "serviceDetailSet": [
        {
            "serviceType": [
                {
                    "serviceType": "Gateway"
                }
            ...
```

2. Pour créer un point de terminaison de passerelle (par exemple, vers Amazon S3), utilisez la commande create-vpc-endpoint et spécifiez l'ID du VPC, le nom du service et les tables de routage qui utiliseront le point de terminaison. Vous pouvez, le cas échéant, utiliser le paramètre `--policy-document` pour spécifier une stratégie personnalisée afin de contrôler l'accès au service. Si le paramètre n,'est pas utilisé, nous lui attachons une stratégie par défaut pour vous qui autorise un accès total au service.

   Pour Amazon S3, vous devez définir le paramètre `--vpc-endpoint-type` sur `Gateway`.

```
aws ec2 create-vpc-endpoint --vpc-id vpc-1a2b3c4d --service-name com.amazonaws.us-east-1.s3 --route-table-ids rtb-11aa22bb --vpc-endpoint-type Gateway
```

3. Décrivez votre point de terminaison à l'aide de la commande describe-vpc-endpoints.

```
aws ec2 describe-vpc-endpoints
```

Pour décrire les services disponibles à l'aide du kit AWS Tools for Windows PowerShell ou de l'API

- Get-EC2VpcEndpointService (AWS Tools for Windows PowerShell)
- DescribeVpcEndpointServices (API de requête Amazon EC2)

Pour créer un point de terminaison de VPC l'aide de AWS Tools for Windows PowerShell ou de l'API

- New-EC2VpcEndpoint (AWS Tools for Windows PowerShell)
- CreateVpcEndpoint (API de requête Amazon EC2)

Pour décrire vos points de terminaison VPC à l'aide des AWS Tools for Windows PowerShell ou de l'API

- Get-EC2VpcEndpoint (AWS Tools for Windows PowerShell)
- DescribeVpcEndpoints (API de requête Amazon EC2)

Modifier votre groupe de sécurité

Si le groupe de sécurité du VPC associé à votre instance restreint le trafic sortant, vous devez ajouter une règle pour autoriser le trafic destiné au service AWS à quitter votre instance.

Pour ajouter une règle sortante pour un point de terminaison de passerelle

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Groupes de sécurité.
3. Sélectionnez le groupe de sécurité de votre VPC, choisissez l'onglet Règles sortantes, puis Modifier.
4. Sélectionnez le type de trafic dans la liste Type et entrez la plage de ports, si nécessaire. Par exemple, si vous utilisez votre instance pour récupérer des objets depuis Amazon S3, choisissez HTTPS dans la liste Type.
5. Pour Destination, commencez par saisir `pl-` pour afficher une liste des ID et des noms de listes de préfixes pour les services AWS disponibles. Choisissez l'ID de liste des préfixes pour le service AWS ou saisissez-le.
6. Choisissez Enregistrer.

Pour obtenir le nom de la liste des préfixes, l'ID et la plage d'adresses IP d'un service AWS à l'aide de la ligne de commande ou de l'API

- describe-prefix-lists (AWS CLI)
- Get-EC2PrefixList (AWS Tools for Windows PowerShell)
- DescribePrefixLists (API de requête Amazon EC2)

Modifier un point de terminaison de passerelle

Vous pouvez modifier un point de terminaison de passerelle en changeant ou en supprimant sa stratégie, et en ajoutant ou en supprimant les tables de routage utilisées par le point de terminaison.

Si vous souhaitez migrer un point de terminaison de passerelle Amazon S3 existant vers un point de terminaison d'interface, après avoir créé le point de terminaison de l'interface d'Amazon S3, supprimez le point de terminaison de la passerelle Amazon S3. Pour de plus amples informations, veuillez consulter the section called “Créer un point de terminaison d'interface” (p. 9) et the section called “Supprimer un point de terminaison d'un VPC” (p. 41).

Pour modifier la stratégie associée à un point de terminaison 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, Modifier une stratégie.
4. Vous pouvez choisir Accès complet pour autoriser un accès total. Vous pouvez également sélectionner Custom (Personnaliser), puis utiliser le générateur de stratégie AWS pour créer une stratégie personnalisée ou entrer votre propre stratégie dans la fenêtre de stratégie. Lorsque vous avez terminé, sélectionnez Save.

Note

Il peut se passer quelques minutes avant que les changements de stratégie prennent effet.

Pour ajouter ou supprimer des tables de routage utilisées par un point de terminaison 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, Gérer les tables de routage.
4. Sélectionnez les tables de routage requises ou annulez leur sélection, puis choisissez Modify Route Tables (Modifier les tables de routage).

Pour modifier un point de terminaison de passerelle à l'aide de l AWS CLI

1. Utilisez la commande describe-vpc-endpoints pour obtenir l'ID de votre point de terminaison de passerelle.

```
aws ec2 describe-vpc-endpoints
```

2. L'exemple suivant utilise la commande modify-vpc-endpoint pour associer la table de routage `rtb-aaa222bb` au point de terminaison de passerelle et réinitialiser le document de stratégie.

```
aws ec2 modify-vpc-endpoint --vpc-endpoint-id vpce-1a2b3c4d --add-route-table-ids rtb-aaa222bb --reset-policy
```

Pour modifier un point de terminaison de VPC à l'aide de AWS Tools for Windows PowerShell ou d'une API

- Edit-EC2VpcEndpoint (AWS Tools for Windows PowerShell)
- ModifyVpcEndpoint (API de requête Amazon EC2)

Ajouter ou supprimer des balises de point de terminaison de passerelle

Les balises permettent d'identifier le point de terminaison de passerelle. Vous pouvez ajouter ou supprimer une balise.

Pour ajouter ou supprimer une balise de point de terminaison de passerelle

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Endpoints (Points de terminaison).
3. Sélectionnez le point de terminaison de passerelle et choisissez Actions, Add/Edit Tags (Ajouter/modifier des balises).
4. Ajoutez ou supprimez une balise.

   [Ajouter une balise] Choisissez Create tag (Créer une balise) et procédez comme suit :
   - Pour Clé, saisissez le nom de la clé.
   - Pour Valeur, saisissez la valeur clé.

[Supprimer une balise] Choisissez le bouton de suppression (« x ») situé à la droite de la clé et de la valeur de la balise.

Pour ajouter ou supprimer une balise à l'aide de AWS Tools for Windows PowerShell ou d'une API

- create-tags (AWS CLI)
- CreateTags (AWS Tools for Windows PowerShell)
- delete-tags (AWS CLI)
- DeleteTags (AWS Tools for Windows PowerShell)

Contrôler l'accès aux services avec les points de terminaison d'un VPC

Quand vous créez un point de terminaison d'interface ou de passerelle, vous pouvez lui attacher une stratégie de point de terminaison qui contrôle l'accès au service auquel vous vous connectez. Les stratégies de point de terminaison doivent être écrites au format JSON. Tous les services ne prennent pas en charge les stratégies de point de terminaison.

Si vous utilisez un point de terminaison pour Amazon S3, vous pouvez également utiliser des stratégies de compartiment Amazon S3 afin de contrôler l'accès aux compartiments depuis des points de terminaison ou des VPC spécifiques. Pour plus d'informations, consultez Stratégies de compartiment Amazon S3 (p. 31).

Table des matières

Utiliser les stratégies de point de terminaison d'un VPC

Une stratégie de point de terminaison d'un VPC est une stratégie de ressource IAM que vous attachez à un point de terminaison lorsque vous le créez ou le modifiez. Si vous n'attachez pas de stratégie quand vous créez un point de terminaison, nous lui attachons une stratégie par défaut pour vous qui autorise un accès total au service. Si un service ne prend pas en charge les stratégies de point de terminaison, le point de terminaison permet un accès complet au service. Une stratégie de point de terminaison n'annule pas et ne remplace pas les stratégies utilisateur IAM ou les stratégies propres à des services comme par exemple, les stratégies de compartiment S3. Il s'agit d'une politique séparée qui contrôle l'accès depuis le point de terminaison jusqu'au service spécifié.

Vous ne pouvez pas attacher plus d'une stratégie à un point de terminaison. Toutefois, vous pouvez modifier la stratégie à tout moment. Si vous modifiez une stratégie, il peut se passer quelques minutes avant que les changements ne prennent effet. Pour de plus amples informations sur l'écriture des stratégies, veuillez consulter Présentation des stratégies IAM dans le Guide de l'utilisateur IAM.

Votre stratégie de point de terminaison peut être comme n'importe quelle autre stratégie IAM cependant, veuillez noter ce qui suit :

- Votre stratégie doit contenir un élément Principal. Pour de plus amples informations sur les points de terminaison de passerelle connexes, veuillez consulter Stratégies de point de terminaison pour les points de terminaison de passerelle (p. 41).

- La taille d'une stratégie de point de terminaison ne peut pas dépasser 20 480 caractères (espaces compris).

Pour de plus amples informations sur les services qui prennent en charge les stratégies de point de terminaison, veuillez consulter Services qui prennent en charge la technologie AWS PrivateLink (p. 74).

Stratégies de point de terminaison pour les points de terminaison de passerelle

Pour les stratégies de point de terminaison appliquées à des points de terminaison de passerelle, si vous spécifiez `Principal` au format `"AWS":"account-ID"` ou `"AWS":"arn:aws:iam::account-ID:root"`, l'accès est accordé uniquement à l'utilisateur racine du compte et non à tous les utilisateurs et rôles IAM de ce compte.

Si vous spécifiez un Amazon Resource Name (ARN) pour l'élément `Principal`, l'ARN devient un ID du mandataire unique lorsque la stratégie est enregistrée.

Pour des exemples de stratégies de point de terminaison relatif à Amazon S3 et DynamoDB, veuillez consulter les rubriques suivantes :

- Stratégies de point de terminaison pour Amazon S3 (p. 29)
- Stratégies de point de terminaison pour DynamoDB (p. 34)

Groupes de sécurité

Lorsque vous créez un point de terminaison d'interface, vous pouvez associer les groupes de sécurité à l'interface réseau de point de terminaison créée dans votre VPC. Si vous ne spécifiez pas un groupe de sécurité, le groupe de sécurité par défaut de votre VPC est automatiquement associé à l'interface réseau du point de terminaison. Vous devez vous assurer que les règles du groupe de sécurité autorisent la communication entre l'interface réseau du point de terminaison et les ressources de votre VPC qui communiquent avec le service.

Pour un point de terminaison de passerelle, si les règles sortantes de votre groupe de sécurité sont restreintes, vous devez ajouter une règle qui autorise le trafic sortant depuis votre VPC vers le service spécifié dans votre point de terminaison. Pour ce faire, vous pouvez utiliser l'ID de liste de préfixes AWS du service comme destination dans la règle de trafic sortant. Pour plus d'informations, consultez Modifier votre groupe de sécurité (p. 38).

Les groupes de sécurité ne s’appliquent pas aux points de terminaison d’équilibreur de charge de passerelle.

Supprimer un point de terminaison d'un VPC

Si vous n'avez plus besoin d'un point de terminaison, vous pouvez le supprimer. La suppression d'un point de terminaison de passerelle supprime entraîne aussi celle des itinéraires du point de terminaison dans les tables de routage qui étaient utilisées par le point de terminaison, sans affecter les groupes de sécurité associés au VPC dans lequel le point de terminaison réside. La suppression d’un point de terminaison d’interface ou d’un point de terminaison d’équilibreur de charge de passerelle supprime également les interfaces réseau des points de terminaison.

Un point de terminaison d’équilibreur de charge de passerelle ne peut pas être supprimé si des routes dans vos tables de routage dirigent vers le point de terminaison.

Supprimer un point de terminaison

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.

Suppression d'un point de terminaison VPC

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (AWS Tools for Windows PowerShell)
- DeleteVpcEndpoints (API de requête Amazon EC2 Query API)

Services de points de terminaison de VPC (AWS PrivateLink)

Vous pouvez créer votre propre application dans votre VPC et la configurer comme service à technologie AWS PrivateLink (appelé service de point de terminaison). D'autres mandataires AWS peuvent créer une connexion de leur VPC à votre service de point de terminaison à l'aide d'un point de terminaison de VPC d'interface (p. 3) ou d'un point de terminaison d'équilibreur de charge de passerelle (p. 18), selon le type de service. Vous êtes le fournisseur du service et les mandataires AWS qui créent des connexions à votre service sont les consommateurs du service.

Table des matières

Services de point de terminaison d'un VPC pour les points de terminaison d'interface

Les étapes générales suivantes permettent de créer un service de point de terminaison pour les points de terminaison d'interface.

1. Créez un Network Load Balancer (équilibreur de charge réseau) pour l'application dans votre VPC et configurez-le pour chaque sous-réseau (zone de disponibilité) dans lequel le service doit être disponible. L'équilibreur de charge reçoit les demandes des consommateurs du service et les achemine vers votre service. Vous pouvez également configurer un Application Load Balancer en tant que cible du Network Load Balancer, puis l'Application Load Balancer peut acheminer les demandes vers votre service. Pour plus d'informations, veuillez consulter le Guide de l'utilisateur pour les Network Load Balancers.

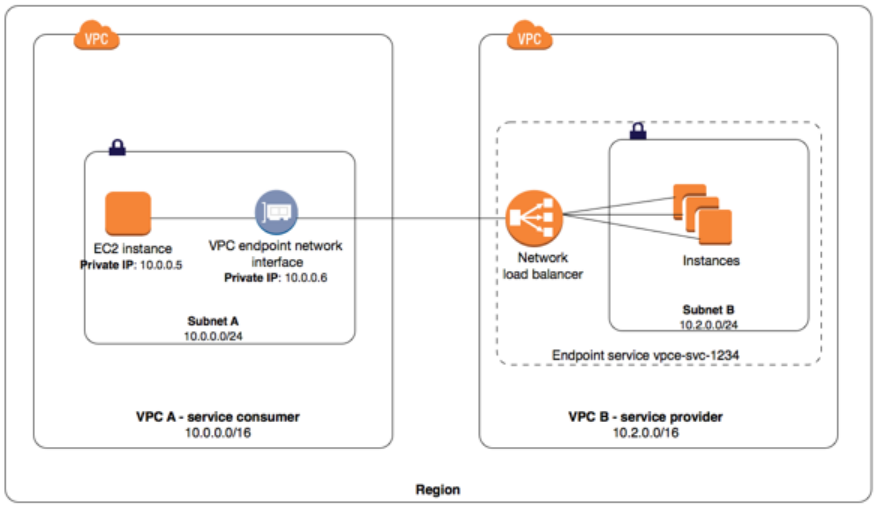
   Nous vous recommandons de configurer votre service dans toutes les zones de disponibilité de la région.
2. Créez une configuration de service de point de terminaison VPC et spécifiez votre Network Load Balancer (NLB).

La procédure générale suivante permet aux consommateurs de service de se connecter à votre service.

1. Accordez des autorisations à des consommateurs de service spécifiques (comptes AWS, utilisateurs IAM et rôles IAM) afin de créer une connexion à votre service de point de terminaison.
2. Un consommateur de service ayant les autorisations crée un point de terminaison d'interface pour votre service, le cas échéant dans chaque zone de disponibilité dans laquelle vous avez configuré votre service.
3. Pour activer la connexion, acceptez la demande de connexion de point de terminaison d'interface. Par défaut, les demandes de connexion doivent être acceptées manuellement. Toutefois, vous pouvez configurer les paramètres d'acceptation pour votre point de terminaison de façon à accepter automatiquement les demandes de connexion.

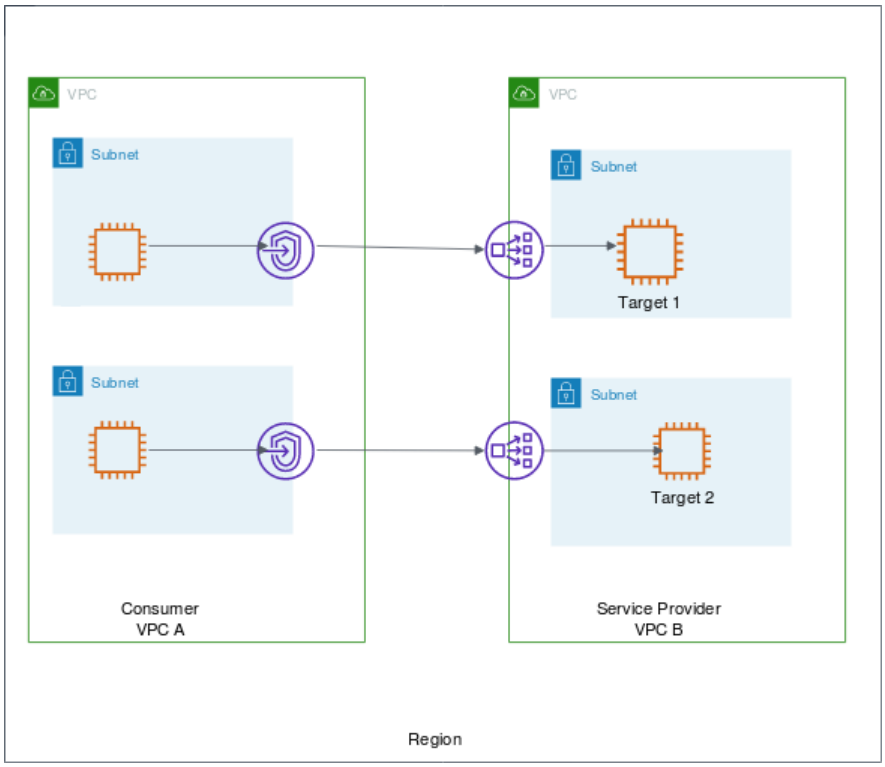
La combinaison des autorisations et des paramètres d'acceptation peut vous aider à contrôler les consommateurs de service (mandataires AWS) qui peuvent accéder à votre service. Par exemple, vous pouvez accorder des autorisations à des mandataires sélectionnés auxquels vous faites confiance et accepter automatiquement toutes les demandes de connexion, ou accorder des autorisations à un groupe plus vaste de mandataires et accepter manuellement les demandes de connexion spécifiques auxquelles vous faites confiance.

Dans le schéma suivant, le propriétaire de compte du VPC B est un fournisseur de service et dispose d'un service qui s'exécute sur les instances du sous-réseau B. Le propriétaire du VPC B a un point de terminaison de service (vpce-svc-1234) associé avec un Network Load Balancer qui pointe vers les instances du sous-réseau B comme cibles. Les instances du sous-réseau A du VPC A utilisent un point de terminaison d'interface pour accéder aux services du sous-réseau B.



Pour une faible latence et une tolérance aux pannes, nous vous recommandons d'utiliser un Network Load Balancer avec des cibles dans chaque zone de disponibilité de la Région AWS. Pour vous aider à atteindre une haute disponibilité pour les consommateurs de service qui utilisent des noms d'hôte DNS zonaux (p. 15) pour accéder au service, vous pouvez activer l'équilibrage de charge entre zones. L'équilibrage de charge entre zones permet à l'équilibreur de charge de répartir le trafic entre les cibles enregistrées dans toutes les zones de disponibilité activées. Pour de plus amples informations, consultez Équilibrage de charge entre zones dans le Guide de l'utilisateur des Network Load Balancers. Des frais de transfert de données régional peuvent être appliqués à votre compte lorsque vous activez l'équilibrage de charge entre zones.

Dans le diagramme suivant, le propriétaire du VPC B est le fournisseur de services et a configuré un Network Load Balancer avec des cibles dans deux zones de disponibilité différentes. Le consommateur du service (VPC A) a créé des points de terminaison d'interface dans les mêmes deux zones de disponibilité de son VPC. Les demandes vers le service depuis des instances du VPC A peuvent utiliser l'un ou l'autre des points de terminaison d'interface.



Considérations sur les zones de disponibilité de service de point de terminaison

Lorsque vous créez un service de point de terminaison, celui-ci est créé dans la zone de disponibilité mappée à votre compte et est indépendant des autres comptes. Lorsque le fournisseur de service et le consommateur sont dans des comptes différents, utilisez l'ID de zone de disponibilité pour identifier de façon unique et cohérente la zone de disponibilité du service de point de terminaison. Par exemple, `use1-az1` est un ID de zone de disponibilité pour la Région `us-east-1` et est mappé au même emplacement dans chaque compte AWS. Pour en savoir plus sur les ID de zone de disponibilité, consultez ID de zone de disponibilité pour vos ressources dans le Guide de l'utilisateur AWS RAM, ou utilisez describe-availability-zones.

Lorsque le fournisseur de services et le consommateur ont des comptes différents et utilisent plusieurs zones de disponibilité, et que le consommateur visualise les informations du service de point de terminaison VPC, la réponse inclut uniquement les zones de disponibilité communes. Par exemple, lorsque le compte du fournisseur de services utilise les régions `us-east-1a` et `us-east-1c` et le consommateur les régions `us-east-1a` et `us-east-1b`, la réponse inclut les services de point de terminaison VPC dans la zone de disponibilité commune, `us-east-1a`.

Noms DNS d'un service de point de terminaison

Quand vous créez un service de point de terminaison d'un VPC, AWS génère des noms d'hôte DNS spécifiques au point de terminaison que vous pouvez utiliser pour communiquer avec le service. Ces noms incluent l'ID du service de point de terminaison d'un VPC et le code de la Région. Par exemple, vpce-svc-01234567890abcdef.us-east-1.vpce.amazonaws.com. Par défaut, vos consommateurs accèdent au service avec ce nom DNS et doivent généralement modifier la configuration de l'application.

Si le service de point de terminaison est pour un service AWS ou un service disponible dans le Marketplace AWS, il existe un nom DNS par défaut. Pour les autres services, le fournisseur de services peut configurer

un nom DNS privé, afin que les consommateurs puissent accéder au service à l'aide d'un nom DNS existant sans apporter de modifications à leurs applications. Pour plus d'informations, consultez Noms DNS privés (p. 64).

Les fournisseurs de services peuvent utiliser la clé de contexte de condition ec2:VpceServicePrivateDnsName dans une déclaration de stratégie IAM pour contrôler quels noms DNS privés peuvent être créés. Pour de plus amples informations, veuillez consulter Actions définies par Amazon EC2 dans le Guide de l'utilisateur IAM.

Exigences relatives aux noms DNS privés

Les fournisseurs de services peuvent spécifier un nom DNS privé pour un service de point de terminaison nouveau ou existant. Pour utiliser un nom DNS privé, activez la fonctionnalité, puis spécifiez un nom DNS privé. Avant que les consommateurs puissent utiliser le nom DNS privé, vous devez vérifier que vous avez le contrôle du domaine/sous-domaine. Vous pouvez initier la vérification de propriété de domaine à l'aide de la console ou de l'API Amazon VPC. Une fois la propriété du domaine vérifiée, les consommateurs de services peuvent accéder à votre service en utilisant le nom DNS privé

Se connecter aux centres de données sur site

Vous pouvez utiliser les types de connexions suivants pour établir une connexion entre un point de terminaison d'interface et votre centre de données sur site :

- AWS Direct Connect
- AWS Site-to-Site VPN

Accéder aux services via une connexion d'appairage de VPC

Vous pouvez utiliser une connexion d'appairage de VPC avec un point de terminaison de VPC pour autoriser un accès privé aux consommateurs sur l'ensemble de la connexion d'appairage de VPC. Pour en savoir plus, consultez Exemple : services utilisant la technologie AWS PrivateLink et un appairage de VPC dans l'Amazon VPC User Guide.

Utiliser un protocole proxy pour les informations de connexion

Un Network Load Balancer fournit des adresses IP source à votre application (votre service). Quand les consommateurs de service envoient du trafic vers votre service par le biais d'un point de terminaison d'interface, les adresses IP source fournies à votre application sont celles des nœuds du Network Load Balancer et non celles des consommateurs de service.

Si vous avez besoin des adresses IP des consommateurs du service et de leurs ID de point de terminaison d'interface correspondants, activez le protocole proxy sur votre équilibreur de charge et obtenez les adresses IP clients 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.

Règles et limitations

Pour utiliser les services de points de terminaison, vous devez être conscient des règles et limitations actuelles :

- Un service de point de terminaison prend uniquement en charge le trafic IPv4 sur TCP.
- Les consommateurs de services peuvent utiliser les noms d'hôtes DNS spécifiques au point de terminaison pour accéder au service de point de terminaison, ou le nom DNS privé.
- Si un service de point de terminaison est associé à plusieurs Network Load Balancers, pour une zone de disponibilité spécifique, un point de terminaison d'interface établit une connexion avec un seul équilibreur de charge.
- Pour le service de point de terminaison, le Network Load Balancer associé peut prendre en charge 55 000 connexions simultanées ou environ 55 000 connexions par minute sur chaque cible unique (adresse IP et port). Si vous dépassez ce nombre de connexions, il y a plus de risque d'erreurs d'attribution de port. Pour résoudre les erreurs d'attribution de port, ajoutez davantage de cibles au groupe cible. Pour plus d'informations sur les groupes cibles du Network Load Balancer, veuillez consulter Groupes cibles pour vos Network Load Balancers et Enregistrer les cibles auprès de votre groupe cible dans le Guide de l'utilisateur des Network Load Balancers.
- Les zones de disponibilité de votre compte peuvent ne pas mapper vers les mêmes emplacements que les zones de disponibilité d'un autre compte. Par exemple, votre zone de disponibilité `us-east-1a` peut se trouver dans un emplacement différent `us-east-1a` de celui d'un autre compte. Pour de plus amples informations, veuillez consulter Régions et zones. Lorsque vous configurez un service de point de terminaison, celui-ci est configuré dans les zones de disponibilité comme mappé à votre compte.
- Un service de point de terminaison n'est disponible que dans la région où vous l'avez créé.
- Vérifiez les limites spécifiques au service pour votre service de point de terminaison.
- Examinez les bonnes pratiques en matière de sécurité et les exemples pour les services de point de terminaison. Pour de plus amples informations, veuillez consulter Bonnes pratiques en matière de stratégies et the section called "Contrôler l'accès aux services" (p. 40).

Services de point de terminaison d'un VPC pour les points de terminaison d'équilibreur de charge de passerelle

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 pouvez ensuite configurer Gateway Load Balancer en tant que service de point de terminaison de VPC pour permettre à d'autres mandataires AWS d'accéder au service via un point de terminaison Gateway Load Balancer.

Les étapes générales suivantes permettent de créer un service de point de terminaison pour un point de terminaison d'équilibreur de charge de passerelle.

1. Créez un équilibreur de charge de passerelle pour vos appliances virtuelles. Pour plus d'informations, veuillez consulter Mise en route des équilibreurs de charge de passerelle.

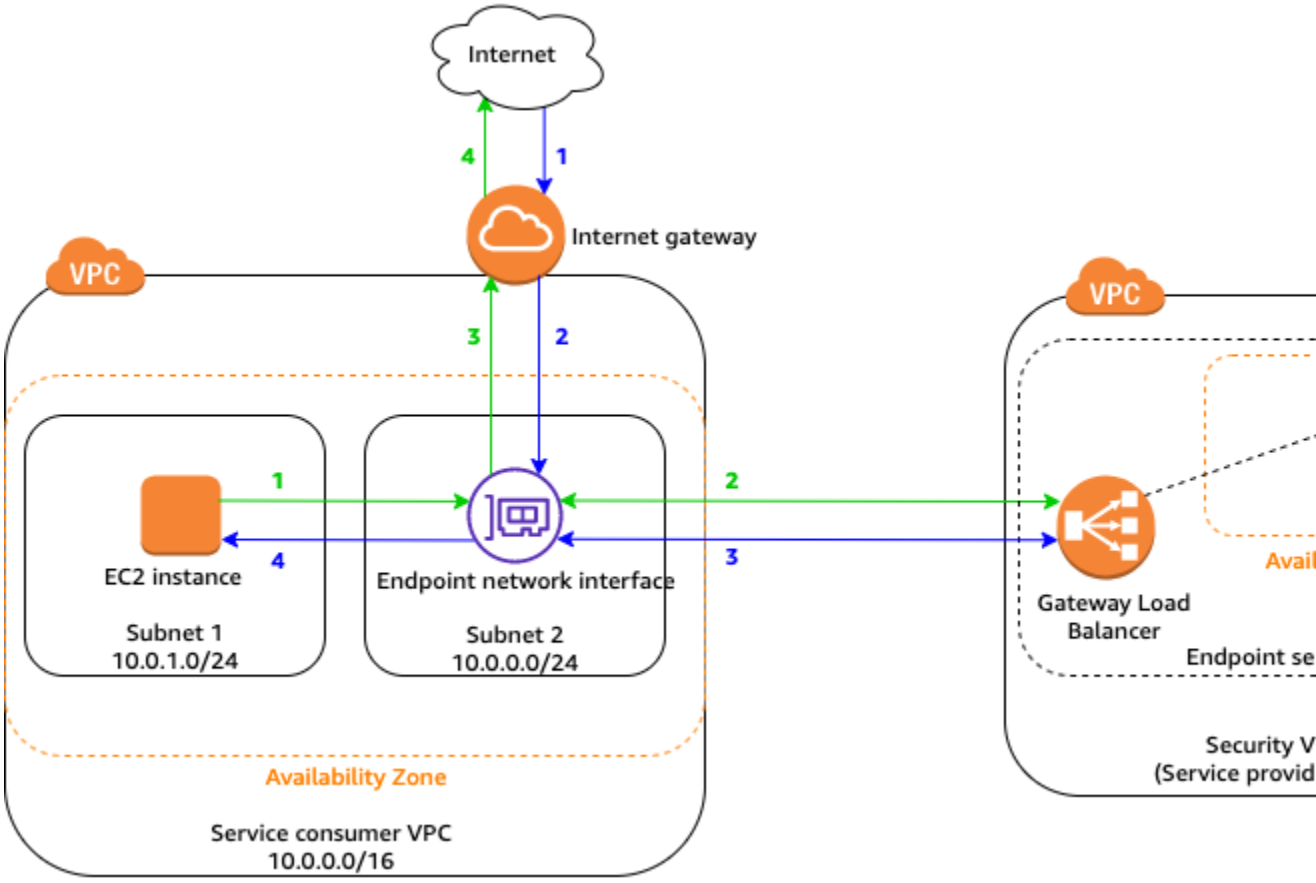
   Nous vous recommandons de configurer votre service dans toutes les zones de disponibilité de la région.
2. Créez une configuration de service de point de terminaison d'un VPC et spécifiez votre équilibreur de charge de passerelle.

La procédure générale suivante permet aux consommateurs de service de se connecter à votre service.

1. Accordez des autorisations à des consommateurs de service spécifiques (comptes AWS, utilisateurs IAM et rôles IAM) afin de créer une connexion à votre service de point de terminaison.

2. Un consommateur de service disposant d'autorisations crée un point de terminaison d'équilibreur de charge de passerelle (p. 18) pour votre service.
3. Pour activer la connexion, acceptez la demande de connexion du point de terminaison. Par défaut, les demandes de connexion doivent être acceptées manuellement. Toutefois, vous pouvez configurer les paramètres d'acceptation pour votre point de terminaison de façon à accepter automatiquement les demandes de connexion.

Dans l'exemple suivant, un parc d'appliances de sécurité est configuré derrière un équilibreur de charge de passerelle dans le VPC de sécurité. Un service de point de terminaison est configuré pour l'équilibreur de charge de passerelle. Le propriétaire du VPC de consommateur de services crée un point de terminaison d'équilibreur de charge de passerelle dans le sous-réseau 2 de son VPC (représenté par une interface réseau de point de terminaison). Tout le trafic entrant dans le VPC via la passerelle Internet est d'abord acheminé vers le point de terminaison de l'équilibreur de charge de passerelle pour inspection dans le VPC de sécurité avant d'être acheminé vers le sous-réseau de destination. De même, tout le trafic quittant l'instance EC2 dans le sous-réseau 1 est d'abord acheminé vers le point de terminaison de l'équilibreur de charge de passerelle pour inspection dans le VPC de sécurité avant d'être acheminé vers Internet.



Pour plus d'informations sur la configuration de routage pour ce scénario, reportez-vous à la section Routage vers un point de terminaison d'équilibreur de charge de passerelle dans le Guide l'utilisateur Amazon VPC.

Considérations sur les zones de disponibilité

Lorsque vous créez un service de point de terminaison, celui-ci est créé dans la zone de disponibilité mappée à votre compte et est indépendant des autres comptes. Lorsque le fournisseur de service et le consommateur sont dans des comptes différents, utilisez l'ID de zone de disponibilité pour identifier de

façon unique et cohérente la zone de disponibilité du service de point de terminaison. Par exemple, `use1-az1` est un ID de zone de disponibilité pour la Région `us-east-1` et est mappé au même emplacement dans chaque compte AWS. Pour en savoir plus sur les ID de zone de disponibilité, consultez ID de zone de disponibilité pour vos ressources dans le Guide de l'utilisateur AWS RAM, ou utilisez describe-availability-zones.

Lorsque le fournisseur de services et le consommateur ont des comptes différents et utilisent plusieurs zones de disponibilité, et que le consommateur visualise les informations du service de point de terminaison VPC, la réponse inclut uniquement les zones de disponibilité communes. Par exemple, lorsque le compte du fournisseur de services utilise les régions `us-east-1a` et `us-east-1c` et le consommateur les régions `us-east-1a` et `us-east-1b`, la réponse inclut les services de point de terminaison VPC dans la zone de disponibilité commune, `us-east-1a`.

Règles et limitations

Pour utiliser les services de point de terminaison pour les points de terminaison d'équilibreur de charge de passerelle, tenez compte des règles et limites actuelles :

- Si un service de point de terminaison est associé à plusieurs équilibreurs de charge de passerelle, pour une zone de disponibilité spécifique, un point de terminaison d'équilibreur de charge de passerelle établit une connexion avec un seul équilibreur de charge.
- Les noms DNS privés ne sont pas pris en charge.
- Les zones de disponibilité de votre compte peuvent ne pas mapper vers les mêmes emplacements que les zones de disponibilité d'un autre compte. Par exemple, votre zone de disponibilité `us-east-1a` peut se trouver dans un emplacement différent `us-east-1a` de celui d'un autre compte. Pour de plus amples informations, veuillez consulter Régions et zones. Lorsque vous configurez un service de point de terminaison, celui-ci est configuré dans les zones de disponibilité comme mappé à votre compte.

Créer une configuration de service de point de terminaison d'un VPC pour les points de terminaison d'interface

Vous pouvez créer une configuration de service de point de terminaison à l'aide de la console Amazon VPC ou de la ligne de commande. Pour de plus amples informations sur les limitations de point de terminaison de VPC, veuillez consulterLimitations dans l'Amazon VPC User Guide.

Avant de commencer, assurez-vous d'avoir créé un ou plusieurs NLB dans le VPC de votre service. Pour de plus amples informations, veuillez consulter Démarrage avec les Network Load Balancers dans le Guide de l'utilisateur pour les Network Load Balancers.

Dans votre configuration, vous pouvez éventuellement spécifier que les demandes de connexion de point de terminaison d'interface à votre service doivent être acceptées manuellement par vous. Vous pouvez créer une notification (p. 56) pour recevoir des alertes en cas de demandes de connexion. Si vous n'acceptez pas une connexion, les consommateurs de service ne peuvent pas accéder à votre service.

> Note
>
> Quels que soient les paramètres d'acceptation, les consommateurs de service doivent également disposer d'autorisations (p. 52) pour créer une connexion à votre service.

Après avoir créé une configuration de service de point de terminaison, vous devez ajouter des autorisations pour autoriser les consommateurs du service à créer des points de terminaison d'interface à votre service.

Console

Pour créer un service de point de terminaison

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Endpoint Services (Services de points de terminaison), Create endpoint service (Créer un service de point de terminaison).
3. Pour Type d'équilibreur de charge, choisissez Network (Réseau).
4. Pour Équilibreurs de charge disponibles, sélectionnez les Network Load Balancers à associer au service du point de terminaison.
5. Pour Requiert l'acceptation du point de terminaison, activez la case à cocher pour accepter manuellement les demandes de connexion à votre service. Sinon, les connexions de point de terminaison sont automatiquement acceptées.
6. Pour Activer le nom DNS privé sélectionnez la case à cocher pour associer un nom DNS privé au service, puis, saisissez le nom DNS privé.
7. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
8. Sélectionnez Créer un .

AWS CLI

Pour créer un service de point de terminaison

Utilisez la commande create-vpc-endpoint-service-configuration et spécifiez un ou plusieurs ARN pour vos NLB. Vous pouvez éventuellement spécifier si une acceptation est requise pour la connexion à votre service et si le service a un nom DNS privé.

```
aws ec2 create-vpc-endpoint-service-configuration --network-load-balancer-arns
 arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
vpce/e94221227f1ba532 --acceptance-required --privateDnsName exampleservice.com
```

Voici un exemple de sortie.

```
{
    "ServiceConfiguration": {
        "ServiceType": [
            {
                "ServiceType": "Interface"
            }
        ],
        "NetworkLoadBalancerArns": [
            "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
vpce/e94221227f1ba532"
        ],
        "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-03d5ebb7d9579a2b3",
        "ServiceState": "Available",
        "ServiceId": "vpce-svc-03d5ebb7d9579a2b3",
        "PrivateDnsName": "exampleService.com",
        "AcceptanceRequired": true,
        "AvailabilityZones": [
            "us-east-1d"
        ],
        "BaseEndpointDnsNames": [
            "vpce-svc-03d5ebb7d9579a2b3.us-east-1.vpce.amazonaws.com"
        ]
    }
}
```

Tools for Windows PowerShell

Pour créer un service de point de terminaison

Utilisez New-EC2VpcEndpointServiceConfiguration.

API

Pour créer un service de point de terminaison

Utilisez CreateVpcEndpointServiceConfiguration.

Créer une configuration de service de point de terminaison d'un VPC pour les points de terminaison de l'équilibreur de charge de passerelle

Vous pouvez créer une configuration de service de point de terminaison à l'aide de la console Amazon VPC ou de la ligne de commande. Avant de commencer, assurez-vous d'avoir créé un ou plusieurs équilibreurs de charge de passerelle dans le VPC de votre service. Pour plus d'informations, veuillez consulter Mise en route des équilibreurs de charge de passerelle.

Dans votre configuration, vous pouvez éventuellement spécifier que les demandes de connexion de point de terminaison d'équilibreur de charge de passerelle à votre service doivent être acceptées manuellement par vous. Vous pouvez créer une notification (p. 56) pour recevoir des alertes en cas de demandes de connexion. Si vous n'acceptez pas une connexion, les consommateurs de service ne peuvent pas accéder à votre service.

Après avoir créé une configuration de service de point de terminaison, vous devez ajouter des autorisations (p. 52) pour autoriser les consommateurs du service à créer des points de terminaison d'équilibreur de charge de passerelle à votre service.

Console

Pour créer un service de point de terminaison

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le panneau de navigation, choisissez Endpoint Services (Services de points de terminaison), Create endpoint service (Créer un service de point de terminaison).
3. Pour Type d'équilibreur de charge, choisissez Gateway (Passerelle).
4. Pour Équilibreurs de charge disponibles, sélectionnez les équilibreurs de charge de passerelle à associer au service du point de terminaison.
5. Pour Requiert l'acceptation du point de terminaison, activez la case à cocher pour accepter manuellement les demandes de connexion à votre service. Sinon, les connexions de point de terminaison sont automatiquement acceptées.
6. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
7. Sélectionnez Créer un .

AWS CLI

Pour créer un service de point de terminaison

Utilisez la commande create-vpc-endpoint-service-configuration et spécifiez un ou plusieurs ARN pour vos équilibreurs de charge de passerelle. Le cas échéant, vous pouvez spécifier si l'acceptation est requise pour la connexion à votre service.

```
aws ec2 create-vpc-endpoint-service-configuration --gateway-load-balancer-arns gateway-load-balancer-arn --no-acceptance-required
```

Tools for Windows PowerShell

Pour créer un service de point de terminaison

Utilisez New-EC2VpcEndpointServiceConfiguration.

API

Pour créer un service de point de terminaison

Utilisez CreateVpcEndpointServiceConfiguration.

Ajouter et supprimer des autorisations pour votre service de point de terminaison

Après avoir créé votre configuration de service de point de terminaison, vous pouvez contrôler quels consommateurs de service peuvent créer un point de terminaison d'interface ou un point de terminaison d'équilibreur de charge de passerelle pour se connecter à votre service. Les consommateurs de service sont des mandataires IAM (utilisateurs IAM, rôles IAM et comptes AWS). Pour ajouter ou supprimer des autorisations pour un principal, vous avez besoin de son Amazon Resource Name (ARN).

- Pour un compte AWS (et par conséquent tous les mandataires du compte), le format de l'ARN est `arn:aws:iam::aws-account-id:root`.
- Pour un utilisateur IAM spécifique, le format de l'ARN est `arn:aws:iam::aws-account-id:user/user-name`.
- Pour un rôle IAM spécifique, le format de l'ARN est `arn:aws:iam::aws-account-id:role/role-name`.

> **Note**
>
> Si vous définissez l'autorisation sur « tout le monde peut accéder » et que vous définissez le modèle d'acceptation sur « accepter toutes les demandes », alors vous venez de rendre votre équilibreur de charge public. Il est facile d'obtenir un compte AWS. De ce fait, il n'existe pas de restrictions pratiques quant aux personnes qui peuvent accéder à votre équilibreur de charge, même s'il ne possède pas d'adresse IP publique.

Console

Pour ajouter ou supprimer des autorisations pour votre service de point de terminaison

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Endpoint Services (Services de point de terminaison).
3. Sélectionnez votre service de point de terminaison et choisissez Actions (Actions), Allow principals (Autoriser les mandataires).
4. Spécifiez l'ARN du principal pour lequel vous ajoutez les autorisations. Pour ajouter un autre mandataire, choisissez Add principal (Ajouter un mandataire). Pour supprimer un principal, sélectionnez Remove (Supprimer) à côté de l'entrée.

   Spécifiez `*` pour ajouter des autorisations pour tous les mandataires. Cela permet à tous les mandataires de tous les comptes AWS de créer un point de terminaison pour votre service de point de terminaison.

5. Choisissez Allow principals (Autoriser les mandataires).

AWS CLI

Pour ajouter des autorisations pour votre service de point de terminaison

Utilisez la commande modify-vpc-endpoint-service-permissions. Spécifiez le paramètre `--add-allowed-principals` pour ajouter un ou plusieurs ARN pour les mandataires.

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-03d5ebb7d9579a2b3
 --add-allowed-principals '["arn:aws:iam::123456789012:root"]'
```

Pour afficher les autorisations que vous avez ajoutées pour votre service de point de terminaison

Utilisez la commande describe-vpc-endpoint-service-permissions.

```
aws ec2 describe-vpc-endpoint-service-permissions --service-id vpce-
svc-03d5ebb7d9579a2b3
```

Voici un exemple de sortie.

```
{
    "AllowedPrincipals": [
        {
            "PrincipalType": "Account",
            "Principal": "arn:aws:iam::123456789012:root"
        }
    ]
}
```

Pour supprimer des autorisations pour votre service de point de terminaison

Utilisez la commande modify-vpc-endpoint-service-permissions. Spécifiez le paramètre `--remove-allowed-principals` pour ajouter un ou plusieurs ARN pour les mandataires.

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-03d5ebb7d9579a2b3
 --remove-allowed-principals '["arn:aws:iam::123456789012:root"]'
```

Tools for Windows PowerShell

Pour ajouter ou supprimer des autorisations pour votre service de point de terminaison

Utilisez Edit-EC2EndpointServicePermission.

API

Pour ajouter ou supprimer des autorisations pour votre service de point de terminaison

Utilisez ModifyVpcEndpointServicePermissions.

Modifier la configuration du service de point de terminaison de VPC

Vous pouvez modifier votre configuration de service de point de terminaison en modifiant les équilibreurs de charge associés au service de point de terminaison et en spécifiant si l'acceptation est obligatoire ou pas en ce qui concerne les demandes de connexion à votre service de point de terminaison.

Vous ne pouvez pas dissocier un équilibreur de charge s'il y a des points de terminaison associés à votre service de point de terminaison.

Console

Pour modifier les équilibreurs de charge de votre service de point de terminaison

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Endpoint Services (Services de point de terminaison).
3. Sélectionnez votre service de point de terminaison, puis choisissezActions (Actions),Associate or disassociate load balancers (Associer ou dissocier des équilibreurs de charge).
4. Sélectionnez les équilibreurs de charge ou annulez leur sélection si nécessaire, puis choisissez Save changes (Enregistrer les modifications).

Pour modifier le paramètre d'acceptation

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Endpoint Services (Services de point de terminaison).
3. Sélectionnez votre service de point de terminaison, puis choisissezActions (Actions),Modify endpoint acceptance setting (Modifier le paramètre d'acceptation de point de terminaison).
4. Sélectionnez ou désélectionnez Acceptance required (Acceptation requise), puis Save changes(Enregistrez les modifications).

AWS CLI

Pour modifier les équilibreurs de charge de votre service de point de terminaison

Utilisez la commande modify-vpc-endpoint-service-configuration. L'exemple suivant utilise le paramètre `--remove-network-load-balancer-arn` pour supprimer un Network Load Balancer.

```
aws ec2 modify-vpc-endpoint-service-configuration --service-
id vpce-svc-09222513e6e77dc86 --remove-network-load-balancer-arn
 arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/nlb-
vpce/e94221227f1ba532
```

Pour spécifier si l'acceptation est obligatoire ou non

Utilisez la commande modify-vpc-endpoint-service-configuration et spécifiez `--acceptance-required` ou `--no-acceptance-required`.

```
aws ec2 modify-vpc-endpoint-service-configuration --service-id vpce-
svc-09222513e6e77dc86 --no-acceptance-required
```

Tools for Windows PowerShell

Pour modifier la configuration du service de point de terminaison

Utilisez Edit-EC2VpcEndpointServiceConfiguration.

API

Pour modifier la configuration du service de point de terminaison

Utilisez ModifyVpcEndpointServiceConfiguration.

Accepter et rejeter les demandes de connexion de point de terminaison

Après avoir créé un service de point de terminaison, les consommateurs de service auxquels vous avez ajouté une autorisation peuvent créer un point de terminaison d'interface ou un point de terminaison d'équilibreur de charge de passerelle pour se connecter à votre service. Pour de plus amples informations, veuillez consulter Points de terminaison de VPC d'interface (AWS PrivateLink) (p. 3) et Points de terminaison de l'équilibreur de charge de passerelle (AWS PrivateLink) (p. 18).

Si vous avez spécifié que l'acceptation est obligatoire pour les demandes de connexion, vous devez accepter ou rejeter manuellement les demandes de connexion de point de terminaison adressées à votre service de point de terminaison. Une fois qu'un point de terminaison est accepté, il devient `available`. Sachez qu'un changement d'état de validation peut prendre du temps, de même pour que l'état devienne `available`.

Vous pouvez rejeter une connexion de point de terminaison une fois qu'il est dans l'état `available`.

Console

Pour accepter ou refuser une demande de connexion

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Endpoint Services (Services de point de terminaison).
3. Sélectionnez votre service de point de terminaison.
4. À partir de Connexions de point de terminaison, sélectionnez le point de terminaison. Pour accepter une demande de connexion, choisissezActions (Actions),Accept endpoint connection request (Accepter la demande de connexion de point de terminaison). Pour rejeter la demande de connexion, choisissezActions (Actions),Reject endpoint connection request (Rejeter la demande de connexion de point de terminaison).

AWS CLI

Pour afficher les connexions de points de terminaison en attente d'acceptation

Utilisez la commande describe-vpc-endpoint-connections et filtrez par l'état `pendingAcceptance`.

```
aws ec2 describe-vpc-endpoint-connections --filters Name=vpc-endpoint-
state,Values=pendingAcceptance
```

Voici un exemple de sortie.

```
{
    "VpcEndpointConnections": [
        {
            "VpcEndpointId": "vpce-0c1308d7312217abc",
            "ServiceId": "vpce-svc-03d5ebb7d9579a2b3",
            "CreationTimestamp": "2017-11-30T10:00:24.350Z",
            "VpcEndpointState": "pendingAcceptance",
            "VpcEndpointOwner": "123456789012"
        }
    ]
}
```

Pour accepter une demande de connexion de point de terminaison

Utilisez la commande accept-vpc-endpoint-connections et spécifiez les ID de point de terminaison et de service de point de terminaison.

```
aws ec2 accept-vpc-endpoint-connections --service-id vpce-svc-03d5ebb7d9579a2b3 --vpc-endpoint-ids vpce-0c1308d7312217abc
```

Pour rejeter les demandes de connexion de point de terminaison

Utilisez la commande reject-vpc-endpoint-connections.

```
aws ec2 reject-vpc-endpoint-connections --service-id vpce-svc-03d5ebb7d9579a2b3 --vpc-endpoint-ids vpce-0c1308d7312217abc
```

Tools for Windows PowerShell

Pour accepter ou refuser une demande de connexion

Utilisez Confirm-EC2EndpointConnection et Deny-EC2EndpointConnection.

API

Pour accepter ou refuser une demande de connexion

Utilisez AcceptVpcEndpointConnections et RejectVpcEndpointConnections.

Créer et gérer une notification pour un service de point de terminaison

Vous pouvez créer une notification pour recevoir des alertes pour les événements spécifiques qui se produisent sur les points de terminaison attachés à votre service de point de terminaison. Par exemple, vous pouvez recevoir un e-mail quand une demande de point de terminaison est acceptée ou rejetée pour votre service de point de terminaison. Pour créer une notification, vous devez associer une rubrique Amazon SNS à celle-ci. Vous pouvez vous inscrire à la rubrique SNS pour recevoir une notification par e-mail quand un événement de point de terminaison se produit. Pour de plus amples informations, veuillez consulter dans le Guide du développeur Amazon Simple Notification Service.

La rubrique Amazon SNS que vous utilisez pour les notifications doit avoir une stratégie de rubrique qui permet au service de point de terminaison Amazon VPC de publier des notifications en votre nom. Veillez à inclure la déclaration suivante dans votre stratégie de rubrique. Pour de plus amples informations, veuillez consulter Gestion de l'accès à vos rubriques Amazon SNS dans le Guide du développeur Amazon Simple Notification Service.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account:topic-name"
    }
  ]
}
```

Console

Pour créer une notification pour un service de point de terminaison

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Endpoint Services (Services de point de terminaison).
3. Sélectionnez votre service de point de terminaison, puis choisissez l'onglet Notifications (Notifications).
4. Choisissez Create notification (Créer une notification).
5. Pour Notification d'ARN choisissez l'ARN de la rubrique SNS à associer à la notification.
6. Pour Événements, sélectionnez les événements de point de terminaison pour les notifications que vous voulez recevoir.
7. Choisissez Create notification (Créer une notification).

Après la création d'une notification, vous pouvez modifier ses paramètres.

Pour modifier une notification pour un service de point de terminaison

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Endpoint Services (Services de point de terminaison).
3. Sélectionnez votre service de point de terminaison, puis choisissez l'onglet Notifications (Notifications).
4. Sélectionnez la notification et choisissez Actions(Actions), Modify notification (Modifier la notification).
5. Modifiez la rubrique SNS ou les événements de point de terminaison comme requis.
6. Choisissez Enregistrer les modifications.

Si vous n'avez plus besoin d'une notification, vous pouvez la supprimer.

Pour supprimer une notification

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

AWS CLI

Pour créer une notification pour un service de point de terminaison

Utilisez la commande create-vpc-endpoint-connection-notification . Spécifiez l'ARN de la rubrique SNS, les événements à notifier et l'ID du point de terminaison.

```
aws ec2 create-vpc-endpoint-connection-notification --connection-notification-
arn arn:aws:sns:us-east-2:123456789012:VpceNotification --connection-events Connect
 Accept Delete Reject --service-id vpce-svc-1237881c0d25a3abc
```

Voici un exemple de sortie.

```
{
    "ConnectionNotification": {
        "ConnectionNotificationState": "Enabled",
        "ConnectionNotificationType": "Topic",
        "ServiceId": "vpce-svc-1237881c0d25a3abc",
        "ConnectionEvents": [
            "Reject",
            "Accept",
            "Delete",
            "Connect"
        ],
        "ConnectionNotificationId": "vpce-nfn-008776de7e03f5abc",
        "ConnectionNotificationArn": "arn:aws:sns:us-
east-2:123456789012:VpceNotification"
    }
}
```

Pour afficher vos notifications

Utilisez la commande describe-vpc-endpoint-connection-notifications.

```
aws ec2 describe-vpc-endpoint-connection-notifications
```

Pour modifier la rubrique SNS ou les événements de point de terminaison pour une notification

Utilisez la commande modify-vpc-endpoint-connection-notification.

```
aws ec2 modify-vpc-endpoint-connection-notification --connection-notification-id vpce-
nfn-008776de7e03f5abc --connection-events Accept Reject --connection-notification-
arn arn:aws:sns:us-east-2:123456789012:mytopic
```

Pour supprimer une notification

Utilisez la commande delete-vpc-endpoint-connection-notifications.

```
aws ec2 delete-vpc-endpoint-connection-notifications --connection-notification-
ids vpce-nfn-008776de7e03f5abc
```

Tools for Windows PowerShell

Pour créer et gérer une notification

Utilisez ce qui suit :

- New-EC2VpcEndpointConnectionNotification
- Get-EC2EndpointConnectionNotification
- Edit-EC2VpcEndpointConnectionNotification
- Remove-EC2EndpointConnectionNotification

API

Pour créer et gérer une notification

Utilisez ce qui suit :

- CreateVpcEndpointConnectionNotification
- DescribeVpcEndpointConnectionNotifications

- ModifyVpcEndpointConnectionNotification
- DeleteVpcEndpointConnectionNotifications

Ajouter ou supprimer des balises d'un service de point de terminaison d'un VPC

Les balises permettent d'identifier un service de point de terminaison de VPC. Vous pouvez ajouter ou supprimer une balise.

Console

Pour ajouter ou supprimer une balise d'un service de point de terminaison de VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison de VPC et choisissez Actions (Actions), Manage tags (Gerer des indetifications).
4. Ajoutez ou supprimez des indetifications.

   [Add a tag] Choisissez Add new tag (Ajouter une identification), puis saisissez la clé et la valeur de l'identification.

   [Remove a tag] Choisissez Remove (Supprimer) à la droite de la clé et de la valeur de l'identification.

AWS CLI

Utilisez create-tags et delete-tags.

API

Utilisez CreateTags et DeleteTags.

Supprimer une configuration de service de point de terminaison.

Vous pouvez supprimer une configuration de service de point de terminaison. La suppression d'une configuration ne supprime pas l'application hébergée dans votre VPC ou les équilibreurs de charge associés.

Avant de supprimer la configuration du service de point de terminaison, vous devez refuser les points de terminaison VPC `available` ou `pending-acceptance` qui sont attachés au service. Pour plus d'informations, consultez Accepter et rejeter les demandes de connexion de point de terminaison (p. 55).

Console

Pour supprimer une configuration de service de point de terminaison

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez 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).

AWS CLI

Pour supprimer une configuration de service de point de terminaison

Utilisez la commande delete-vpc-endpoint-service-configurations. Specifiez l'ID du service.

```
aws ec2 delete-vpc-endpoint-service-configurations --service-ids vpce-
svc-03d5ebb7d9579a2b3
```

Tools for Windows PowerShell

Pour supprimer une configuration de service de point de terminaison

Utilisez Remove-EC2EndpointServiceConfiguration.

API

Pour supprimer une configuration de service de point de terminaison

Utilisez DeleteVpcEndpointServiceConfigurations.

Identity and Access Management (Gestion des identités et des accès - IAM) pour les points de terminaison de VPC et les services de points de terminaison de VPC

Utilisez IAM pour gérer l'accès aux points de terminaison de VPC et aux services de point de terminaison de VPC.

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

Par défaut, les utilisateurs IAM ne sont pas autorisés à utiliser des points de terminaison. Vous pouvez créer une stratégie d'utilisateur IAM qui autorise les utilisateurs à créer, modifier, décrire et supprimer des points de terminaison. En 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 “Contrôler l'accès aux services” (p. 40).

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 de 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 de VPC

Vous pouvez utiliser la clé de condition `ec2:VpceServicePrivateDnsName` pour contrôler quel service de point de terminaison de 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 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 de VPC

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

Noms DNS privés pour les services de point de terminaison

Quand vous créez un service de point de terminaison d'un VPC, nous générons des noms d'hôte DNS spécifiques au point de terminaison que vous pouvez utiliser pour communiquer avec le service. Ces noms incluent l'ID du service du point de terminaison d'un VPC et le code de la Région. Par exemple, vpce-svc-01234567890abcdef.us-east-1.vpce.amazonaws.com. Par défaut, vos consommateurs accèdent au service avec ce nom DNS et doivent généralement modifier la configuration de l'application.

Si le service de point de terminaison est pour un service AWS ou un service disponible dans le Marketplace AWS, il existe un nom DNS par défaut. Pour les autres services, le fournisseur de services peut configurer un nom DNS privé, afin que les consommateurs puissent accéder au service à l'aide d'un nom DNS existant sans apporter de modifications à leurs applications. Pour de plus amples informations, veuillez consulter Services de points de terminaison de VPC (p. 43).

Les fournisseurs de services peuvent spécifier un nom DNS privé pour un service de point de terminaison nouveau ou existant. Pour utiliser un nom DNS privé, activez la fonctionnalité, puis spécifiez un nom DNS privé. Avant que les consommateurs puissent utiliser le nom DNS privé, vous devez vérifier que vous avez le contrôle du domaine/sous-domaine. Vous pouvez lancer une vérification de propriété de domaine. Une fois la propriété du domaine vérifiée, les consommateurs de services peuvent accéder à votre service en utilisant le nom DNS privé.

Pour vérifier le domaine, vous devez disposer d'un nom hébergé public ou d'un fournisseur DNS public.

Les noms DNS privés ne sont pas pris en charge pour les services de point de terminaison que vous créez pour les points de terminaison de l’équilibreur de charge de passerelle.

La procédure de haut niveau est la suivante :

1. Ajoutez un nom DNS privé. Pour plus d'informations, consultez the section called “Créer une configuration de service de point de terminaison d'un VPC pour les points de terminaison d'interface” (p. 49) ou the section called “Modifier un nom DNS privé d'un service de point de terminaison existant” (p. 67).
2. Notez la Domain verification value (Valeur de vérification de domaine) et le Domain verification name (Nom de vérification de domaine) dont vous avez besoin pour les enregistrements du serveur DNS. Pour de plus amples informations, veuillez consulter the section called “Afficher la configuration du nom DNS privé du service de point de terminaison” (p. 68).
3. Ajoutez un enregistrement au serveur DNS. Pour de plus amples informations, veuillez consulter the section called “Vérification du nom DNS privé du service de point de terminaison d’un VPC” (p. 65).
4. Vérifiez le nom DNS privé. Pour de plus amples informations, veuillez consulter the section called “Lancer manuellement la vérification du domaine de nom DNS privé du service de point de terminaison” (p. 68).

Vous pouvez gérer le processus de vérification à l'aide de la console ou de l’API Amazon VPC.

- the section called “Vérification du nom DNS privé du service de point de terminaison d’un VPC” (p. 65)
- the section called “Modifier un nom DNS privé d'un service de point de terminaison existant” (p. 67)
- the section called “Supprimer un nom DNS privé du service de point de terminaison” (p. 69)

- the section called “Afficher la configuration du nom DNS privé du service de point de terminaison” (p. 68)
- Enregistrements TXT de vérification de nom de domaine DNS privé Amazon VPC (p. 70)

Observations relatives à la vérification du nom de domaine

Notez les points importants suivants concernant la vérification de propriété de domaine :

- Un consommateur peut uniquement utiliser le nom DNS privé pour accéder au service de point de terminaison lorsque l'état de la vérification est verified (vérifié).
- Si le statut de vérification passe de verified (vérifié) à pendingVerification (vérification en attente), ou failed (échec), les connexions consommateur existantes sont maintenues, mais toute nouvelle demande de connexion est refusée.

  Pour les fournisseurs de services qui sont soucieux des connexions vers les services de point de terminaison qui ne sont plus dans l'état verified (vérifié), nous recommandons d'utiliser DescribeVpcEndpointServices afin de vérifier l'état de vérification au moins une fois par jour.
- Un service de point de terminaison ne peut avoir qu'un seul nom DNS privé.
- Vous pouvez spécifier un nom DNS privé pour un service de point de terminaison nouveau ou existant.
- Vous pouvez utiliser uniquement des serveurs de noms de domaine public.
- Vous pouvez utiliser des caractères génériques dans les noms de domaine, par exemple « *.myexampleservice.com ».
- Vous devez effectuer une vérification de propriété de domaine séparée pour chaque service de point de terminaison.
- Vous pouvez vérifier le domaine d'un sous-domaine. Par exemple, vous pouvez vérifier example.com, au lieu de a.example.com. Comme indiqué dans la spécification RFC 1034, chaque étiquette DNS peut comporter jusqu'à 63 caractères et l'ensemble du nom de domaine ne doit pas dépasser une longueur totale de 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 avant que vos consommateurs puissent utiliser ce nom.
- Les noms de domaine doivent être en minuscules.

Vérification du nom DNS privé du service de point de terminaison d’un VPC

Votre domaine est associé à un ensemble d'enregistrements de système de noms de domaine (DNS) que vous gérez via votre fournisseur DNS. Un enregistrement TXT est un type d'enregistrement DNS qui fournit des informations supplémentaires sur votre domaine. Chaque enregistrement TXT est constitué d'un nom et d'une valeur.

Lorsque vous lancez la vérification de propriété de domaine, nous vous fournissons le nom et la valeur à utiliser pour l'enregistrement TXT. Par exemple, si votre domaine est myexampleservice.com, les paramètres d'enregistrement TXT que nous générons seront similaires à l'exemple suivant :

Enregistrement TXT du nom DNS privé du point de terminaison

Nom de vérification de domaine	Type de vérification de domaine	Valeur de vérification de domaine
_aksldja21i1	TXT	vpce:asjdakjshd78126eu21

Ajoutez un enregistrement TXT au serveur DNS de votre domaine en utilisant le Domain verification name (Nom de vérification de domaine) et la Domain verification value (Valeur de vérification de domaine)spécifiés. La vérification de propriété de domaine est terminée lorsque nous détectons l'existence de l'enregistrement TXT dans les paramètres DNS de votre domaine.

Si votre fournisseur DNS n'autorise pas les traits de soulignement dans les noms d'enregistrements DNS, vous pouvez omettre _aksldja21i1 du Domain verification name (Nom de vérification de domaine). Dans ce cas, pour l'exemple précédent, le nom de l'enregistrement TXT serait myexampleservice.com au lieu de _aksldja21i1.myexampleservice.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. Cette section fournit les procédures pour l'ajout d'un enregistrement TXT à Route 53, ainsi que les procédures génériques qui s'appliquent à d'autres fournisseurs DNS.

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison.
4. Dans l'onglet Details (Détails), notez les valeurs affichées en regard de Domain verification value (Valeur de vérification de domaine) et Domain verification name (Nom de vérification de domaine).
5. Si Route 53 fournit le service DNS pour le domaine que vous vérifiez et que vous êtes connecté à AWS Management Console avec le même compte que celui que vous utilisez pour Route 53, nous vous offrons la possibilité de mettre à jour immédiatement votre serveur DNS à partir de la console Amazon VPC.

   Si vous utilisez un autre fournisseur DNS, les procédures de mise à jour des enregistrements DNS varient en fonction du DNS ou du fournisseur d'hébergement web que vous utilisez. Le tableau ci-dessous répertorie les liens menant à la documentation proposée pour plusieurs fournisseurs courants. Cette liste n'est pas exhaustive et l'inclusion dans cette liste ne constitue ni une approbation ni une recommandation vis-à-vis des produits ou services de l'entreprise. Si votre fournisseur n'est pas répertorié dans le tableau, vous pouvez probablement utiliser le domaine avec des points de terminaison.

Fournisseur DNS/d'hébergement	Lien vers la documentation
GoDaddy	Ajout d'un registre TXT (lien externe)
Dreamhost	How do I add custom DNS records? (Comment ajouter des registres DNS personnalisés ?) (lien externe)

Fournisseur DNS/d'hébergement	Lien vers la documentation
Cloudflare	Gestion des enregistrements DNS dans CloudFlare (lien externe)
HostGator	Manage DNS Records with HostGator/eNom (Gérer des registres DNS avec HostGator/eNom) (lien externe)
Namecheap	How do I add TXT/SPF/DKIM/DMARC records for my domain? (Comment ajouter des registres TXT/SPF/DKIM/DMARC pour mon domaine ?) (lien externe)
Names.co.uk	Changing your domains DNS Settings (Modifier vos paramètres DNS de domaine) (lien externe)
Wix	Ajout ou mise à jour des enregistrements TXT dans votre compte Wix (lien externe)

Lorsque la vérification est terminée, l'état du domaine dans la console Amazon VPC passe de Pending (En attente) à Verified (Vérifié).

6. Vous pouvez désormais utiliser le nom de domaine privé pour le service de point de terminaison du VPC.

Si les paramètres DNS ne sont pas correctement mis à jour, le domaine affiche l'état failed (échec) sous l'onglet Details (Détails). Si cela se produit, effectuez les étapes indiquées sur la page de dépannage de the section called "Résoudre les problèmes courants de vérification de domaine" (p. 71). Après avoir vérifié que votre enregistrement TXT a été créé correctement, relancez l'opération.

Modifier un nom DNS privé d'un service de point de terminaison existant

Vous pouvez modifier le nom DNS privé du service de point de terminaison pour un service de point de terminaison nouveau ou existant.

Après avoir mis à jour le nom, faites de même pour l'entrée pour le domaine sur votre serveur DNS. Nous interrogeons automatiquement le serveur DNS pour vérifier que l'enregistrement existe sur le serveur. Les mises à jour d'enregistrement DNS peuvent prendre jusqu'à 48 heures, mais sont souvent appliquées beaucoup plus rapidement. Pour de plus amples informations, veuillez consulter the section called "Enregistrements TXT de vérification de nom de domaine DNS privé" (p. 70) et the section called "Vérification du nom DNS privé du service de point de terminaison d'un VPC" (p. 65).

Console

Pour modifier un nom DNS privé d'un service de point de terminaison existant

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison, puis choisissez Actions, Modifiy private DNS name (Modifier le nom DNS privé).
4. Sélectionnez Associate a private DNS name with the service (Associer un nom de DNS privé au service) puis saisissez le nom DNS privé.

5. Choisissez Save changes (Enregistrer les modifications).

AWS CLI

Pour modifier un nom DNS privé d'un service de point de terminaison

Utilisez modify-vpc-endpoint-service-configuration.

API

Pour modifier un nom DNS privé d'un service de point de terminaison

Utilisez ModifyVpcEndpointServiceConfiguration.

Afficher la configuration du nom DNS privé du service de point de terminaison

Vous pouvez afficher le nom DNS privé du service de point de terminaison pour un service de point de terminaison.

Console

Pour afficher la configuration du nom DNS privé du service de point de terminaison

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 points de terminaison), puis sélectionnez le service de point de terminaison.
3. L'onglet Détails (Détails) affiche les informations suivantes pour la vérification de propriété de domaine DNS privé :
   - Domain verification status (Statut de vérification du domaine) : état de la vérification.
   - Domain verification type (Type de vérification du domaine) : type de vérification.
   - Domain verification value (Valeur de vérification du domaine) : valeur DNS.
   - Domain verification name (Nom de vérification de domaine) : nom du sous-domaine d'enregistrement.

AWS CLI

Pour afficher la configuration du nom DNS privé du service de point de terminaison

Utilisez describe-vpc-endpoint-service-configurations.

API

Pour afficher la configuration du nom DNS privé du service de point de terminaison

Utilisez DescribeVpcEndpointServiceConfigurations.

Lancer manuellement la vérification du domaine de nom DNS privé du service de point de terminaison

Le fournisseur de services doit prouver qu'il est le propriétaire du domaine de nom DNS privé pour que les consommateurs puissent utiliser le nom DNS privé.

Console

Pour lancer le processus de vérification du domaine de nom DNS privé

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

   Si les paramètres DNS ne sont pas correctement mis à jour, le statut de vérification du domaine est échoué. Si cela se produit, effectuez les étapes indiquées sur la page de dépannage de the section called “Résoudre les problèmes courants de vérification de domaine” (p. 71).

AWS CLI

Pour lancer le processus de vérification du domaine de nom DNS privé

Utilisez start-vpc-endpoint-service-private-dns-verification.

API

Pour lancer le processus de vérification du domaine de nom DNS privé

Utilisez StartVpcEndpointServicePrivateDnsVerification.

Supprimer un nom DNS privé du service de point de terminaison

Vous pouvez supprimer le nom DNS privé du service de point de terminaison uniquement lorsqu’il n'y a aucune connexion au service.

Console

Pour supprimer un nom DNS privé du service de point de terminaison

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sélectionnez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison, puis choisissez Actions, Modifiy private DNS name (Modifier le nom DNS privé).
4. Effacer Associate a private DNS name with the service (Associer un nom de DNS privé au service).
5. Choisissez Save changes (Enregistrer les modifications).

AWS CLI

Pour supprimer un nom DNS privé du service de point de terminaison

Utilisez modify-vpc-endpoint-service-configuration.

API

Pour supprimer un nom DNS privé du service de point de terminaison

Utilisez ModifyVpcEndpointServiceConfiguration.

Enregistrements TXT de vérification de nom de domaine DNS privé Amazon VPC

Votre domaine est associé à un ensemble d'enregistrements de système de noms de domaine (DNS) que vous gérez via votre fournisseur DNS. Un enregistrement TXT est un type d'enregistrement DNS qui fournit des informations supplémentaires sur votre domaine. Chaque enregistrement TXT est constitué d'un nom et d'une valeur.

Lorsque vous lancez la vérification de propriété de domaine à l'aide de la console ou de l'API Amazon VPC, nous vous fournissons le nom et la valeur à utiliser pour l'enregistrement TXT. Par exemple, si votre domaine est myexampleservice.com, les paramètres d'enregistrement TXT que génère Amazon VPC seront similaires à l'exemple suivant :

Enregistrement TXT du nom DNS privé du point de terminaison

Nom de vérification de domaine	Type de vérification de domaine	Valeur de vérification de domaine
_aksldja21i1.myexampleservice.com	TXT	vpce:asjdakjshd78126eu21

Ajoutez un enregistrement TXT au serveur DNS de votre domaine en utilisant le Domain verification name (Nom de vérification de domaine) et la Domain verification value (Valeur de vérification de domaine)spécifiés. La vérification de propriété de domaine Amazon VPC est terminée lorsque Amazon VPC détecte l'existence de l'enregistrement TXT dans les paramètres DNS de votre domaine.

Si votre fournisseur DNS n'autorise pas l'utilisation de traits de soulignement dans les noms d'enregistrements DNS, vous pouvez utiliser le nom de domaine comme nom de vérification de domaine. Dans ce cas, pour l'exemple précédent, le nom de l'enregistrement TXT serait myexampleservice.com.

Vous trouverez des informations de résolution de problèmes et des instructions sur la manière de contrôler vos paramètres de vérification de propriété de domaine dans Résoudre les problèmes courants de vérification de domaine DNS privé (p. 71).

Amazon Route 53

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. Cette section fournit les procédures pour l'ajout d'un enregistrement TXT à Route 53, ainsi que les procédures génériques qui s'appliquent à d'autres fournisseurs DNS.

Pour ajouter un enregistrement TXT à l'enregistrement DNS de votre domaine géré par Route 53.

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison.
4. Dans l'onglet Details (Détails), notez les valeurs affichées en regard de Domain verification value (Valeur de vérification de domaine) et Domain verification name (Nom de vérification de domaine).
5. Dans la console Amazon Route 53, créez un enregistrement pour votre zone hébergée. Pour plus d'informations sur la création d'un enregistrement, reportez-vous à la section Création

d'enregistrements à l'aide de la console Amazon Route 53 dans le Manuel du développeur Amazon Route 53. 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 Value/Route traffic to (Valeur/Acheminer le trafic vers), saisissez la Domain verification value (Valeur de vérification de domaine) à partir de la console Amazon VPC.

6. Sous l'onglet Details (Détails) de la page Endpoint Services (Services de point de terminaison) de la console Amazon VPC, vérifiez la valeur dans la colonne Domain verification status (État de vérification de domaine) à côté du point de terminaison. Si le statut est « pending verification » (vérification en attente), patientez quelques minutes, puis choisissez refresh (actualiser). Répétez ce processus jusqu'à ce que la valeur de la colonne d'état soit « verified ». Vous pouvez lancer manuellement le processus de vérification. Pour plus d'informations, consultez the section called “Lancer manuellement la vérification du domaine de nom DNS privé du service de point de terminaison” (p. 68).

Generic procedures for other DNS providers

La procédure d'ajout d'enregistrements TXT aux configurations DNS varie d'un fournisseur à l'autre. Pour les étapes spécifiques, consultez la documentation de votre fournisseur DNS. La procédure de cette section donne une vue d'ensemble élémentaire des mesures que vous prenez lors de l'ajout d'un enregistrement TXT à la configuration DNS de votre domaine.

Pour ajouter un enregistrement TXT au serveur DNS de votre domaine (procédure générale)

1. Accédez au site web de votre fournisseur DNS. Si vous n'êtes pas certain du fournisseur DNS qui sert votre domaine, essayez de le rechercher à l'aide d'un service Whois gratuit.
2. Sur le site web du fournisseur, connectez-vous à votre compte.
3. Recherchez la page permettant de mettre à jour les enregistrements DNS de votre domaine. Cette page contient souvent un nom comme DNS Records, DNS Zone File ou Advanced DNS. En cas de doute, consultez la documentation du fournisseur.
4. Ajoutez un enregistrement TXT avec le nom et la valeur fournis par AWS.

   Important

   Certains fournisseurs DNS ajoutent automatiquement le nom de domaine à la fin des enregistrements DNS. L'ajout d'un enregistrement contenant déjà le nom de domaine (par exemple, _pmBGN/7Mjnf.example.com) peut entraîner la duplication du nom de domaine (par exemple, _pmBGN/7Mjnfexample.com.example.com). Pour éviter la duplication du nom de domaine, ajoutez un point à la fin du nom de domaine dans l'enregistrement DNS. Cela permettra d'indiquer à votre fournisseur DNS que le nom d'enregistrements est complet (autrement dit, qu'il ne dépend plus du nom de domaine) et de l'empêcher d'ajouter un nom de domaine supplémentaire.
5. Enregistrez vos modifications. Les mises à jour d'enregistrement DNS peuvent prendre jusqu'à 48 heures, mais sont souvent appliquées beaucoup plus rapidement.

Résoudre les problèmes courants de vérification de domaine DNS privé

Pour vérifier un nom de domaine DNS privé du service de point de terminaison avec Amazon VPC, vous lancez le processus à l'aide de la console ou de l'API Amazon VPC. Cette section contient des informations qui peuvent vous aider à résoudre les problèmes liés au processus de vérification.

Problèmes courants de vérification de domaine

Si vous tentez de vérifier un domaine et que vous rencontrez des problèmes, étudiez les causes possibles et les solutions ci-dessous.

- Vous essayez de vérifier un domaine dont vous n'êtes pas le propriétaire. Vous ne pouvez pas vérifier un domaine à moins d'en être le propriétaire.
- Votre fournisseur DNS n'autorise pas les traits de soulignement dans les noms d'enregistrements TXT. Certains fournisseurs DNS ne vous permettent pas d'inclure le caractère de soulignement dans les noms d'enregistrements DNS de votre domaine. Si c'est le cas de votre fournisseur, vous pouvez omettre _amazonvpc du nom de l'enregistrement TXT.
- 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. Par exemple, si vous créez un enregistrement où le nom d'attribut est _amazonvpc.example.com, le fournisseur peut ajouter le nom de domaine, ce qui donne _amazonvpc.example.com.example.com. Pour éviter la duplication du nom de domaine, ajoutez un point à la fin du nom de domaine lorsque vous créez l'enregistrement TXT. Cette étape indique à votre fournisseur DNS qu'il n'est pas nécessaire d'ajouter le nom de domaine à l'enregistrement TXT.
- Votre fournisseur DNS a modifié la valeur d'enregistrement DNS. Certains fournisseurs modifient automatiquement les valeurs d'enregistrement DNS pour n'utiliser que des lettres minuscules. Nous vérifions uniquement votre domaine lorsqu'il détecte un enregistrement de vérification dont la valeur d'attribut correspond exactement à celle que nous avons fournie lorsque vous avez lancé le processus de vérification de propriété de domaine. Si le fournisseur DNS pour votre domaine modifie les valeurs de votre enregistrement TXT pour utiliser uniquement des lettres minuscules, contactez le fournisseur DNS pour obtenir plus d'aide.
- Vous souhaitez vérifier plusieurs fois le même domaine. Vous serez peut-être amené à vérifier votre domaine plusieurs fois, soit parce que vous effectuez un envoi dans différentes régions, soit parce que vous utilisez le même domaine pour envoyer à partir de plusieurs comptes AWS. Si votre fournisseur DNS ne vous autorise pas à avoir plusieurs enregistrements TXT avec le même nom d'attribut, vous pouvez quand-même vérifier deux domaines. Si votre fournisseur DNS le permet, vous pouvez affecter plusieurs valeurs d'attribut au même enregistrement TXT. Par exemple, si votre DNS est géré par Amazon Route 53, vous pouvez définir plusieurs valeurs pour le même enregistrement TXT, en respectant les étapes suivantes :

  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. Dans la zoneValue (Valeur), allez à la fin de la valeur d'attribut existante, 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'affecter plusieurs valeurs au même enregistrement TXT, vous pouvez vérifier le domaine une fois avec la valeur dans le nom d'attribut de l'enregistrement TXT et une autre fois avec la valeur supprimée du nom d'attribut. Par exemple, vous vérifiez avec « _asnbcdasd », puis avec « asnbcdasd ». L'inconvénient de cette solution est que vous ne pouvez vérifier le même domaine que deux fois.

Comment vérifier les paramètres de vérification de domaine

Vous pouvez vérifier que l'enregistrement TXT de vérification de propriété de votre domaine DNS privé est publié correctement sur votre serveur DNS selon la procédure suivante. Cette procédure utilise l'outil nslookup, disponible pour Windows et Linux. Sous Linux, vous pouvez également utiliser dig.

Les commandes dans ces instructions sont exécutées sous Windows 7, et le domaine que nous utilisons comme exemple est example.com.

Dans cette procédure, vous trouvez d'abord les serveurs DNS qui servent votre domaine, puis interrogez ces serveurs pour afficher les enregistrements TXT. Vous interrogez les serveurs DNS qui servent votre domaine, car ces serveurs contiennent les dernières informations concernant votre domaine et qui peuvent prendre du temps à être propagées vers d'autres serveurs DNS.

Pour vérifier que votre enregistrement TXT de vérification de propriété de domaine est publié sur votre serveur DNS

1. Trouvez les serveurs de noms de votre domaine en effectuant les étapes suivantes.

   a. Accédez à la ligne de commande. Pour obtenir la ligne de commande sur Windows 7, choisissez Start (Démarrer), puis saisissez cmd. Sur les systèmes d'exploitation Linux, ouvrez une fenêtre de terminal.

   b. Dans l'invite de commande, saisissez ce qui suit, où **<**domain**>** est votre domaine.

   ```
   nslookup -type=NS <domain>
   ```

   Par exemple, si votre domaine était example.com, la commande ressemblerait à la suivante.

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

   Le résultat de la commande présente les serveurs de noms qui servent votre domaine. Vous interrogerez l'un de ces serveurs à l'étape suivante.

2. Vérifiez que l'enregistrement TXT est correctement publié en effectuant les étapes suivantes.

   a. Dans l'invite de commande, saisissez ce qui suit, où **<**domain**>** est votre domaine, et **<**name server**>** est l'un des serveurs de noms que vous avez trouvé à l'étape 1.

   ```
   nslookup -type=TXT  _aksldja21i1.<domain> <name server>
   ```

   Dans notre exemple _aksldja21i1.example.com, si nous trouvions un serveur de noms appelé ns1.name-server.net à l'étape 1, nous saisirions ce qui suit.

   ```
   nslookup -type=TXT  _aksldja21i1.example.com ns1.name-server.net
   ```

   b. Dans le résultat de la commande, vérifiez que la chaîne qui suit `text =` correspond à la valeur TXT qui s'affiche lorsque vous choisissez le domaine dans la liste des identités de la console Amazon VPC.

   Dans notre exemple, nous recherchons un enregistrement TXT sous _aksldja21i1.example.com avec la valeur `asjdakjshd78126eu21`. Si l'enregistrement est correctement publié, la commande doit générer le résultat suivant.

   ```
   _aksldja21i1.example.com text = "asjdakjshd78126eu21"
   ```

Services AWS qui s'intègrent avec AWS PrivateLink

Ce qui suit Services AWS s'intègre avec AWS PrivateLink. Vous pouvez vous connecter à ces services en privé, comme s'ils étaient exécutés dans votre propre VPC.

Cliquez sur le lien dans la colonne AWS service pour consulter la documentation des services qui s'intègrent à AWS PrivateLink. La colonne politique de point de terminaison d'un VPC indique si le service prend en charge les politiques de point de terminaison d'un VPC. Le Service name (Nom du service) contient le nom de service que vous spécifiez lorsque vous créez le point de terminaison d'un VPC de l'interface.

AWSService	Stratégies de point de terminaison d'un VPC	Nom du service
Analyseur d'accès	Oui	com.amazonaws.region.access-analyzer
AWS Account Management	Oui	com.amazonaws.region.account
Amazon API Gateway	Oui	com.amazonaws.region.execute-api
Amazon AppIntegrations	Oui	com.amazonaws.region.app-integrations
AWS App Mesh	Non	com.amazonaws.region.appmesh-envoy-management
AWS App Runner	Oui	com.amazonaws.region.apprunner
Application Auto Scaling	Oui	com.amazonaws.region.application-autoscaling
AWS Application Migration Service	Oui	com.amazonaws.region.mgn
Amazon AppStream 2.0	Non	com.amazonaws.region.appstream.api
		com.amazonaws.region.appstream.streaming
Amazon Athena	Oui	com.amazonaws.region.athena
AWS Audit Manager	Oui	com.amazonaws.region.auditmanager
Amazon Aurora	Oui	com.amazonaws.region.rds
AWS Auto Scaling	Oui	com.amazonaws.region.autoscaling-plans
AWS Backup	Oui	com.amazonaws.region.backup
AWS Batch	Oui	com.amazonaws.region.batch
AWS Conducteur de facturation	Oui	com.amazonaws.region.billingconductor

AWSService	Stratégies de point de terminaison d'un VPC	Nom du service
Amazon Braket	Oui	com.amazonaws.region.braket
AWS Certificate Manager Private Certificate Authority	Oui	com.amazonaws.region.acm-pca
Amazon Cloud Directory	Oui	com.amazonaws.region.clouddirectory
AWS CloudFormation	Oui	com.amazonaws.region.cloudformation
AWS CloudHSM	Oui	com.amazonaws.region.cloudhsmv2
AWS CloudTrail	Non	com.amazonaws.region.cloudtrail
Amazon CloudWatch	Oui	com.amazonaws.region.evidently
		com.amazonaws.region.evidently-dataplane
		com.amazonaws.region.monitoring
		com.amazonaws.region.rhum
		com.amazonaws.region.rum-dataplane
		com.amazonaws.region.synthetics
Amazon CloudWatch Events	Oui	com.amazonaws.region.events
Amazon CloudWatch Logs	Oui	com.amazonaws.region.logs
AWS CodeArtifact	Oui	com.amazonaws.region.codeartifact.api
		com.amazonaws.region.codeartifact.repositories
AWS CodeBuild	Oui	com.amazonaws.region.codebuild
		com.amazonaws.region.codebuild-fips
AWS CodeCommit	Oui	com.amazonaws.region.codecommit
		com.amazonaws.region.codecommit-fips
		com.amazonaws.region.git-codecommit
		com.amazonaws.region.git-codecommit-fips
AWS CodeDeploy	Oui	com.amazonaws.region.codedeploy
		com.amazonaws.region.codedeploy-commands-secure
Amazon CodeGuru Profiler	Non	com.amazonaws.region.codeguru-profiler

AWSService	Stratégies de point de terminaison d'un VPC	Nom du service
Amazon CodeGuru Reviewer	Non	com.amazonaws.region.codeguru-reviewer
AWS CodePipeline	Non	com.amazonaws.region.codePipeline
Connexions AWS CodeStar	Oui	com.amazonaws.region.codestar-connections.api
Amazon Comprehend	Oui	com.amazonaws.region.comprehend
Amazon Comprehend Medical	Oui	com.amazonaws.region.comprenehendmedical
AWS Config	Oui	com.amazonaws.region.config
Amazon Connect Customer Profiles	Oui	com.amazonaws.region.profile
Amazon Connect Voice ID	Oui	com.amazonaws.region.voiceid
Amazon Connect Wisdom	Oui	com.amazonaws.region.wisdom
AWS Database Migration Service	Oui	com.amazonaws.region.dms
		com.amazonaws.region.dms-fips
AWS Data Exchange	Oui	com.amazonaws.region.dataexchange
AWS DataSync	Non	com.amazonaws.region.datasync
AWS Device Farm	Non	
Amazon DevOps Guru	Oui	com.amazonaws.region.devops-guru
API directes Amazon EBS	Non	com.amazonaws.region.ebs
Amazon EC2	Oui	com.amazonaws.region.ec2
EC2 Image Builder	Oui	com.amazonaws.region.imagebuilder
Amazon EC2 Auto Scaling	Oui	com.amazonaws.region.autoscaling
AWS Elastic Beanstalk	Oui	com.amazonaws.region.elasticbeanstalk
		com.amazonaws.region.elasticbeanstalk-health
Amazon Elastic File System	Oui	com.amazonaws.region.elasticfilesystem
		com.amazonaws.region.elasticfilesystem-fips
Elastic Load Balancing	Oui	com.amazonaws.region.elasticloadbalancing
Amazon Elastic Container Registry	Oui	com.amazonaws.region.ecr.api

AWSService	Stratégies de point de terminaison d'un VPC	Nom du service
		com.amazonaws.region.ecr.dkr
Amazon Elastic Container Service	Oui	com.amazonaws.region.ecs
		com.amazonaws.region.ecs-agent
		com.amazonaws.region.ecs-telemetry
AWS Elastic Disaster Recovery	Oui	com.amazonaws.region.drs
AWS Elastic Inference	Non	com.amazonaws.region.elastic-inference.runtime
Amazon ElastiCache	Oui	com.amazonaws.region.elasticache
Amazon EMR	Oui	com.amazonaws.region.elasticmapreduce
Amazon EMR on EKS	Oui	com.amazonaws.region.emr-containers
Amazon EventBridge	Oui	com.amazonaws.region.events
AWS Fault Injection Simulator	Oui	com.amazonaws.region.fis
Amazon FinSpace	Oui	com.amazonaws.region.finspace
		com.amazonaws.region.finspace-api
Amazon Forecast	Oui	com.amazonaws.region.forecast
		com.amazonaws.region.forecastquery
		com.amazonaws.region.forecast-fips
		com.amazonaws.region.forecastquery-fips
Amazon Fraud Detector	Oui	com.amazonaws.region.frauddetector
AWS Glue	Oui	com.amazonaws.region.glue
AWS Glue DataBrew	Oui	com.amazonaws.region.databrew
Amazon Managed Grafana	Oui	com.amazonaws.region.grafana
AWS Ground Station	Oui	com.amazonaws.region.groundstation
Amazon HealthLake	Oui	com.amazonaws.region.healthlake
Amazon Inspector	Oui	com.amazonaws.regionInspector2
AWS IoT Core	Non	com.amazonaws.region.iot.data
AWS IoT Core for LoRaWAN	Non	com.amazonaws.region.iotwireless.api

AWSService	Stratégies de point de terminaison d'un VPC	Nom du service
		com.amazonaws.region.lorawan.cups
		com.amazonaws.region.lorawan.lns
AWS IoT Greengrass	Oui	com.amazonaws.region.greengrass
AWS IoT SiteWise	Non	com.amazonaws.region.iotsitewise.api
		com.amazonaws.region.iotsitewise.data
Amazon Kendra	Oui	com.amazonaws.region.kendra
AWS Key Management Service	Oui	com.amazonaws.region.kms
Amazon Keyspaces (for Apache Cassandra)	Oui	com.amazonaws.region.cassandra
		com.amazonaws.region.cassandra-fips
Amazon Kinesis Data Firehose	Oui	com.amazonaws.region.kinesis-firehose
Amazon Kinesis Data Streams	Oui	com.amazonaws.region.kinesis-streams
AWS Lake Formation	Oui	com.amazonaws.region.lakeformation
AWS Lambda	Oui	com.amazonaws.region.lambda
Amazon Lex	Oui	com.amazonaws.region.models-v2-lex
		com.amazonaws.region.runtime-v2-lex
AWS License Manager	Oui	com.amazonaws.region.license-manager
		com.amazonaws.region.license-manager-fips
Amazon Lookout for Equipment	Oui	com.amazonaws.region.lookoutequipment
Amazon Lookout for Metrics	Oui	com.amazonaws.region.lookoutmetrics
Amazon Lookout for Vision	Oui	com.amazonaws.region.lookoutvision
Amazon Macie	Non	com.amazonaws.region.macie2
Amazon Managed Blockchain	Non	
Amazon MemoryDB pour Redis	Oui	com.amazonaws.region.memory-db
		com.amazonaws.region.memorydb-fips
Amazon Managed Service for Prometheus	Non	com.amazonaws.region.aps
		com.amazonaws.region.aps-workspaces

AWSService	Stratégies de point de terminaison d'un VPC	Nom du service
Amazon Managed Workflows for Apache Airflow	Oui	com.amazonaws.region.airflow.api
		com.amazonaws.region.airflow.env
		com.amazonaws.region.airflow.ops
Migration Hub Strategy Recommendations	Oui	com.amazonaws.region.migrationhub-strategy
Amazon Nimble Studio	Oui	com.amazonaws.region.nimble
AWS Proton	Oui	com.amazonaws.region.proton
Amazon QLDB	Oui	com.amazonaws.region.qldb.session
Amazon RDS	Oui	com.amazonaws.region.rds
Amazon RDS Data API	Oui	com.amazonaws.region.rds-data
Amazon Redshift	Oui	com.amazonaws.region.redshift
		com.amazonaws.region.redshift-data
		com.amazonaws.region.redshift-fips
Amazon Rekognition	Oui	com.amazonaws.region.rekognition
		com.amazonaws.region.rekognition-fips
AWS RoboMaker	Oui	com.amazonaws.region.robomaker
Amazon S3	Oui	com.amazonaws.region.s3
Amazon S3 Multi-Region Access Points	Oui	com.amazonaws.s3-global.accesspoint
Amazon SageMaker	Oui	aws.sagemaker.region.notebook
		aws.sagemaker.region.studio
		com.amazonaws.region.sagemaker.api
		com.amazonaws.region.sagemaker.featurestore-runtime
		com.amazonaws.region.sagemaker.runtime
		com.amazonaws.region.sagemaker.runtime-fips
AWS Secrets Manager	Oui	com.amazonaws.region.secretsmanager
AWS Security Hub	Oui	com.amazonaws.region.securityhub
AWS Security Token Service	Oui	com.amazonaws.région.sts

AWSService	Stratégies de point de terminaison d'un VPC	Nom du service
AWS Server Migration Service	Non	com.amazonaws.region.awsconnector
		com.amazonaws.region.sms
		com.amazonaws.region.sms-fips
AWS Service Catalog	Oui	com.amazonaws.region.servicecatalog
		com.amazonaws.region.servicecatalog-appregistry
Amazon SES	Non	com.amazonaws.region.email-smtp
Amazon SNS	Oui	com.amazonaws.region.sns
Amazon SQS	Oui	com.amazonaws.region.sqs
AWS Snow Device Management	Oui	com.amazonaws.region.snow-device-management
AWS Step Functions	Oui	com.amazonaws.region.states
		com.amazonaws.region.sync-states
AWS Systems Manager	Oui	com.amazonaws.region.ec2messages
		com.amazonaws.region.ssm-contacts
		com.amazonaws.region ssm-incidents
		com.amazonaws.region.ssm
		com.amazonaws.region.ssmmessages
AWS Storage Gateway	Non	com.amazonaws.region.storagegateway
Amazon Textract	Oui	com.amazonaws.region.textract
		com.amazonaws.region.textract-fips
Amazon Transcribe	Oui	com.amazonaws.region.transcribe
		com.amazonaws.region.transcribestreaming
Amazon Transcribe Medical	Oui	com.amazonaws.region.transcribe
		com.amazonaws.region.transcribestreaming
AWS Transfer for SFTP	Non	com.amazonaws.region.transfer
		com.amazonaws.region.transfer.server
Amazon Translate	Oui	com.amazonaws.region.translate
Amazon WorkSpaces	Oui	com.amazonaws.region.workspaces

AWSService	Stratégies de point de terminaison d'un VPC	Nom du service
AWS X-Ray	Oui	com.amazonaws.region.xray

Consultation des noms de services 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.

Vous pouvez exécuter la commande suivante pour obtenir une liste des noms de service pour les points de terminaison de passerelle ou d'interface. Les valeurs possibles pour le filtre `service-type` sont `Interface` et `Gateway`. L'option `--query` limite la sortie aux noms de services.

```
aws ec2 describe-vpc-endpoint-services --filter Name=service-type,Values=service-type --
query ServiceNames
```

L'exemple suivant montre les services qui prennent en charge les points de terminaison de l'interface.

```
aws ec2 describe-vpc-endpoint-services --filter Name=service-type,Values=Interface --query
 ServiceNames
```

Voici un exemple de sortie :

```
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.acm-pca",
    "com.amazonaws.us-east-1.airflow.api",
    "com.amazonaws.us-east-1.airflow.env",
    "com.amazonaws.us-east-1.airflow.ops",
    "com.amazonaws.us-east-1.application-autoscaling",
    "com.amazonaws.us-east-1.appmesh-envoy-management",
    "com.amazonaws.us-east-1.appstream.api",
    "com.amazonaws.us-east-1.appstream.streaming",
    "com.amazonaws.us-east-1.aps-workspaces",
    "com.amazonaws.us-east-1.athena",
...
```

Une fois que vous avez le nom du service, vous pouvez afficher des informations détaillées à l'aide de la commande suivante.

```
aws ec2 describe-vpc-endpoint-services --service-name service-name
```

L'exemple suivant affiche des informations sur le point de terminaison de l'interface Amazon S3 dans la région `us-east-1`. Le filtre `service-type` exclut le point de terminaison de la passerelle Amazon S3 de la sortie.

```
aws ec2 describe-vpc-endpoint-services --service-name "com.amazonaws.us-east-1.s3" --filter
 Name=service-type,Values=Interface --region us-east-1
```

Voici un exemple de sortie :


```
{
    "ServiceDetails": [
        {
            "ServiceName": "com.amazonaws.us-east-1.s3",
            "ServiceId": "vpce-svc-081d84efcdc7bac15",
            "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": [
                "s3.us-east-1.vpce.amazonaws.com"
            ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": []
        }
    ],
    "ServiceNames": [
        "com.amazonaws.us-east-1.s3"
    ]
}
```

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. 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

Métrique	Description
	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`
`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`

Métrique	Description
	• `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. 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` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint 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, sélectionnez Endpoint Services (Services de point de terminaison). Sélectionnez le service de votre point de terminaison, puis choisissez l'onglet Monitoring (Surveillance).

Pour afficher les métriques à l'aide de la 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
```

AWS PrivateLinkQuotas

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 de plus amples 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 VPC de passerelle par région	20	Oui	Il y a une limite de 255 points de terminaison de passerelle par VPC
Points de terminaison d'équilibreur de charge d'interface et de passerelle par VPC	50	Oui	Il s'agit du quota combiné pour les points de terminaison d'interface et les points de terminaison d'équilibreur de charge de passerelle pour un VPC.
Taille de politique de point de terminaison de VPC	20 480 caractères	Non	La taille d'une stratégie de point de terminaison VPC inclut des espaces blancs

Les règles suivantes s'appliquent au trafic qui passe par un point de terminaison de VPC.

- Par défaut, chaque point de terminaison d'interface peut prendre en charge une bande passante jusqu'à 10 Gbits/s par zone de disponibilité et met à l'échelle jusqu'à 40 Gbits/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 le point de terminaison de VPC. Plus la MTU est grande, plus la quantité de données pouvant être transmises dans un seul paquet est importante. Un point de terminaison de 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 de VPC sont supprimés.
- Le point de terminaison de VPC ne génère pas le paquet FRAG_NEEDEDIMP ;, la détection de MTU de chemin (PMTUD) n'est donc pas prise en charge.
- Le point de terminaison de VPC applique 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 toutes les versions des AWS PrivateLink.

update-history-change	update-history-description	update-history-date
mesures CloudWatch	AWS PrivateLink publie les métriques CloudWatch pour vos points de terminaison d'interface, vos points de terminaison de Gateway Load Balancer et vos 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'interface pour un service AWS afin de contrôler l'accès au service.	23 mars 2020
Clés de condition pour les points de terminaison de VPC et les services de point de terminaison	Vous pouvez utiliser des clés de condition EC2 pour contrôler l'accès aux points de terminaison de VPC et aux services de point de terminaison.	6 mars 2020
Identification des points de terminaison de VPC et des services de point de terminaison lors de la création (p. 90)	Vous pouvez ajouter des identifications lorsque vous créez des points de terminaison de VPC et des services de points de terminaison.	5 février 2020
Noms DNS privés	Vous pouvez accéder aux services basés sur AWS PrivateLink depuis votre VPC en utilisant des noms DNS privés.	6 janvier 2020
Services de points de terminaison de VPC	Vous pouvez créer vos propres services de points de terminaison et permettre à d'autres comptes et utilisateurs AWS de se connecter à votre service via un point de terminaison d'un	28 novembre 2017

	VPC d'interface. Vous pouvez proposer vos services de point de terminaison à l'abonnement sur AWS Marketplace.	
Points de terminaison d'un VPC d'interface pour les services AWS	Vous pouvez créer un point de terminaison d'interface pour vous connecter aux services AWS qui s'intègrent à AWS PrivateLink sans utiliser de passerelle Internet ou de dispositif NAT.	8 novembre 2017
Points de terminaison de 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.	11 mai 2015