



AWS PrivateLink

Amazon Virtual Private Cloud



Amazon Virtual Private Cloud: AWS PrivateLink

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Qu'est-ce que AWS PrivateLink?	1
Cas d'utilisation	1
Utiliser des points de terminaison d'un VPC	3
Tarification	3
Concepts	4
Diagramme d'architecture	4
Prestataires	5
Consommateurs de services ou de ressources	7
AWS PrivateLink connections	9
Zones privées hébergées	10
Prise en main	11
Étape 1 : Créer un VPC et des sous-réseaux	12
Étape 2 : Lancer les instances	12
Étape 3 : Tester CloudWatch l'accès	14
Étape 4 : créer un point de terminaison VPC auquel accéder CloudWatch	15
Étape 5 : Test du point de terminaison d'un VPC	16
Étape 6 : Nettoyage	16
Accès à Services AWS	18
Vue d'ensemble	19
Noms d'hôte DNS	20
Résolution DNS	22
DNS privé	22
Sous-réseaux et zones de disponibilité	23
Types d'adresses IP	26
Type d'adresse IP de l'enregistrement DNS	27
Services qui s'intègrent	28
Afficher disponible Service AWS names	54
Afficher les informations sur un service	54
Afficher la prise en charge de stratégie de point de terminaison	56
Afficher la prise charge d'IPv6	57
Cross-region activé Services AWS	58
Afficher disponible Service AWS names	54
Autorisations et considérations	60
Créez un point de terminaison d'interface vers un Service AWS dans une autre région	61

Création d'un point de terminaison d'interface	61
Conditions préalables	62
Création d'un point de terminaison de VPC	63
Sous-réseaux partagés	65
ICMP	65
Configuration d'un point de terminaison d'interface	65
Ajouter ou supprimer des sous-réseaux	65
Association de groupes de sécurité	66
Pour modifier la politique de point de terminaison de VPC	67
Activation de noms DNS privés	67
Gestion des balises	68
Réception d'alertes pour les événements relatifs aux points de terminaison d'interface	69
Création d'une notification SNS	69
Ajout d'une stratégie d'accès	70
Ajout d'une stratégie de clé	71
Suppression d'un point de terminaison d'interface	72
Points de terminaison de passerelle	72
Présentation de	73
Routage	75
Sécurité	76
Type d'adresse IP	77
Type d'adresse IP de l'enregistrement DNS	77
Points de terminaison pour Amazon S3	79
Points de terminaison pour DynamoDB	91
Accès aux produits SaaS	100
Présentation de	100
Création d'un point de terminaison d'interface	101
Partage des services	103
Présentation de	103
Noms d'hôte DNS	104
DNS privé	105
Sous-réseaux et zones de disponibilité	105
Cross-Region accès	106
Types d'adresses IP	107
Création d'un service de point de terminaison	109
Considérations	109

Conditions préalables	110
Création d'un service de point de terminaison	111
Mettre le service de point de terminaison à la disposition des consommateurs du service	113
Connexion à un service de point de terminaison en tant que consommateur du service	113
Configuration d'un service de point de terminaison	115
Gestion des autorisations	115
Acceptation ou refus des demandes de connexion	117
Gérer les équilibres de charge	118
Association d'un nom DNS privé	120
Modifier les régions prises en charge	121
Modification des types d'adresses IP pris en charge	121
Gestion des balises	122
Gestion des noms DNS	124
Vérification de la propriété du domaine	125
Obtention du nom et de la valeur	126
Ajout d'un enregistrement TXT au serveur DNS de votre domaine	127
Vérification de la publication de l'enregistrement TXT	128
Résolution des problèmes de vérification de domaine	129
Réception d'alertes pour les événements relatifs au service de point de terminaison	130
Création d'une notification SNS	130
Ajout d'une stratégie d'accès	131
Ajout d'une stratégie de clé	132
Suppression d'un service de point de terminaison	133
Accès à des dispositifs virtuels	134
Présentation de	134
Types d'adresses IP	136
Routage	137
Création d'un service de point de terminaison d'équilibreur de charge de passerelle	139
Considérations	139
Conditions préalables	140
Création du service de point de terminaison	140
Assurer la disponibilité de votre service de point de terminaison	141
Créer un point de terminaison d'équilibreur de charge de passerelle	142
Considérations	142
Conditions préalables	143
Créer le point de terminaison	144

Configurer le routage	145
Gestion des balises	146
Suppression du point de terminaison	147
Accédez aux ressources VPC	148
Vue d'ensemble	149
Considérations	149
Noms d'hôte DNS	150
Résolution DNS	151
DNS privé	151
Sous-réseaux et zones de disponibilité	152
Types d'adresses IP	152
Création d'un point de terminaison de ressources	153
Conditions préalables	153
Création d'un point de terminaison de ressources VPC	153
Gérer les points de terminaison des ressources	155
Supprimer un point de terminaison	155
Mettre à jour un point de terminaison	155
Accédez à des segments de réseau	157
Vue d'ensemble	157
Considérations	158
Encapsulation GENEVE	158
Noms d'hôte DNS	158
Résolution DNS	158
DNS privé	159
Sous-réseaux et Zones de disponibilité	159
Types d'adresses IP	159
Création d'un point de terminaison de tunnel	160
Conditions préalables	160
Création d'un point de terminaison VPC tunnel	161
Réseaux de services d'accès	163
Présentation de	164
Noms d'hôte DNS	165
Résolution DNS	165
DNS privé	166
Sous-réseaux et zones de disponibilité	166
Types d'adresses IP	167

Création d'un point de terminaison de réseau de services	168
Conditions préalables	168
Création d'un point de terminaison de réseau de service	169
Gérer les points de terminaison des réseaux de services	170
Supprimer un point de terminaison	170
Mettre à jour un point de terminaison de réseau de service	170
Configuration des ressources	172
Types de configurations de ressources	172
Passerelle de ressources	173
Noms de domaine personnalisés pour les fournisseurs de ressources	173
Noms de domaine personnalisés pour les consommateurs de ressources	174
Noms de domaine personnalisés pour les propriétaires de réseaux de service	176
Définition de la ressource	177
Protocole	177
Gammes de ports	178
Accès aux ressources	178
Association avec le type de réseau de service	179
Types de réseaux de services	179
Partage de configurations de ressources via AWS RAM	180
Contrôle	180
Création d'une configuration de ressources	181
Gérer les associations	183
Gérer les associations de ressources du réseau de services	183
Gérer les associations de points de terminaison VPC de ressources	184
Passerelle de ressources	173
Considérations	186
Groupes de sécurité	187
Types d'adresses IP	187
Adresses IPv4 par ENI	188
Configuration des ressources et résolution DNS	188
Création d'une passerelle de ressources	189
Supprimer une passerelle de ressources	190
Gestion des identités et des accès	191
Public ciblé	191
Authentification par des identités	192
Compte AWS utilisateur root	192

Identité fédérée	192
Utilisateurs et groupes IAM	193
Rôles IAM	193
Gestion de l'accès à l'aide de politiques	193
Identity-based politiques	194
Resource-based politiques	194
Autres types de politique	194
Plusieurs types de politique	195
Comment AWS PrivateLink fonctionne avec IAM	195
Identity-based politiques	196
Resource-based politiques	196
Actions de politique	197
Ressources de politique	198
Clés de condition de politique	198
ACL	199
ABAC	199
Informations d'identification temporaires	199
Autorisations de principal	200
Rôles du service	200
Rôles Service-linked	200
Identity-based exemples de politiques	200
Contrôler l'utilisation de points de terminaison d'un VPC	201
Contrôler la création de points de terminaison d'un VPC en fonction du propriétaire du service	202
Contrôle des noms DNS privés pouvant être spécifiés pour les services de point de terminaison d'un VPC	203
Contrôle des noms de services pouvant être spécifiés pour les services de point de terminaison d'un VPC	203
Politiques de point de terminaison	205
Considérations	205
Politique de point de terminaison par défaut	206
Politiques relatives aux points de terminaison d'interface	206
Principaux pour les points de terminaison de passerelle	207
Mise à jour d'une politique de point de terminaison d'un VPC	207
AWS politiques gérées	208
Mises à jour des politiques	208

CloudWatch métriques	210
Métriques et dimensions des points de terminaison	210
Métriques et dimensions de point de terminaison de service	213
Afficher les CloudWatch indicateurs	216
Utilisation des règles intégrées de Contributor Insights	217
Activez les règles Contributor Insights	218
Désactivez les règles Contributor Insights	219
Supprimer les règles Contributor Insights	220
Quotas	221
Historique de la documentation	223
.....	ccxxvii

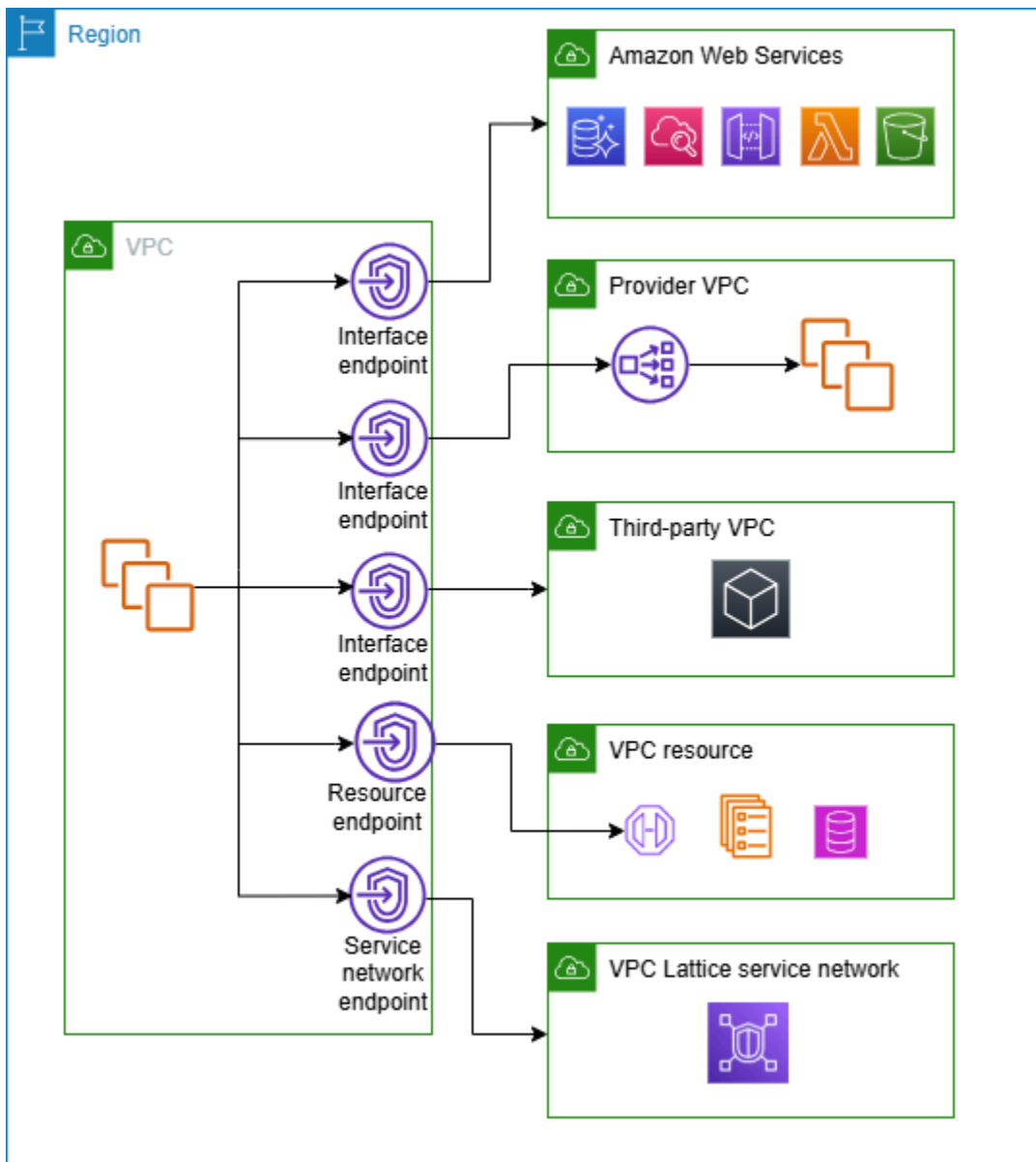
Qu'est-ce que AWS PrivateLink?

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

Cas d'utilisation

Vous pouvez créer des points de terminaison VPC AWS PrivateLink basés pour accéder aux services, aux ressources et aux segments de réseau au-delà des limites des VPC et des comptes. Vous pouvez créer votre propre service de point de terminaison VPC et le mettre à la disposition d'autres AWS clients. Pour plus d'informations, consultez [the section called "Concepts"](#).

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



En savoir plus

- [Concepts](#)
- [Accès à Services AWS](#)
- [Accès aux produits SaaS](#)
- [Accès à des dispositifs virtuels](#)
- [Partage des services](#)

Utiliser des points de terminaison d'un VPC

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

- Console de gestion AWS— Fournit une interface Web que vous pouvez utiliser pour accéder à vos AWS PrivateLink ressources. Ouvrez la console Amazon VPC et choisissez Endpoints ou Endpoint services.
- AWS Command Line Interface (AWS CLI) — Fournit des commandes pour un large éventail de Services AWS, notamment AWS PrivateLink. Pour plus d'informations sur les commandes pour AWS PrivateLink, consultez [ec2](#) dans la référence des AWS CLI commandes.
- 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](#)
- AWS SDK : fournissent des API spécifiques à chaque langue. Les kits de développement (SDK) prennent en charge la plupart des détails de connexion, notamment le calcul des signatures, le traitement des nouvelles tentatives de demande et le traitement des erreurs. Pour de plus amples informations, veuillez consulter [Outils pour créer sur AWS](#).
- API de requête : Fournit des actions d'API de bas niveau appelées à l'aide de demandes HTTPS. L'utilisation de l'API de requête est le moyen le plus direct d'accéder à Amazon VPC. Toutefois, il faut alors que votre application gère les détails de bas niveau, notamment la génération du hachage pour signer la demande et la gestion des erreurs. Pour plus d'informations, consultez les [AWS PrivateLink actions](#) dans la Référence API d'Amazon EC2.

Tarification

Pour en savoir plus sur la tarification des points de terminaison d'un VPC, voir [Tarification AWS PrivateLink](#).

AWS PrivateLink concepts

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

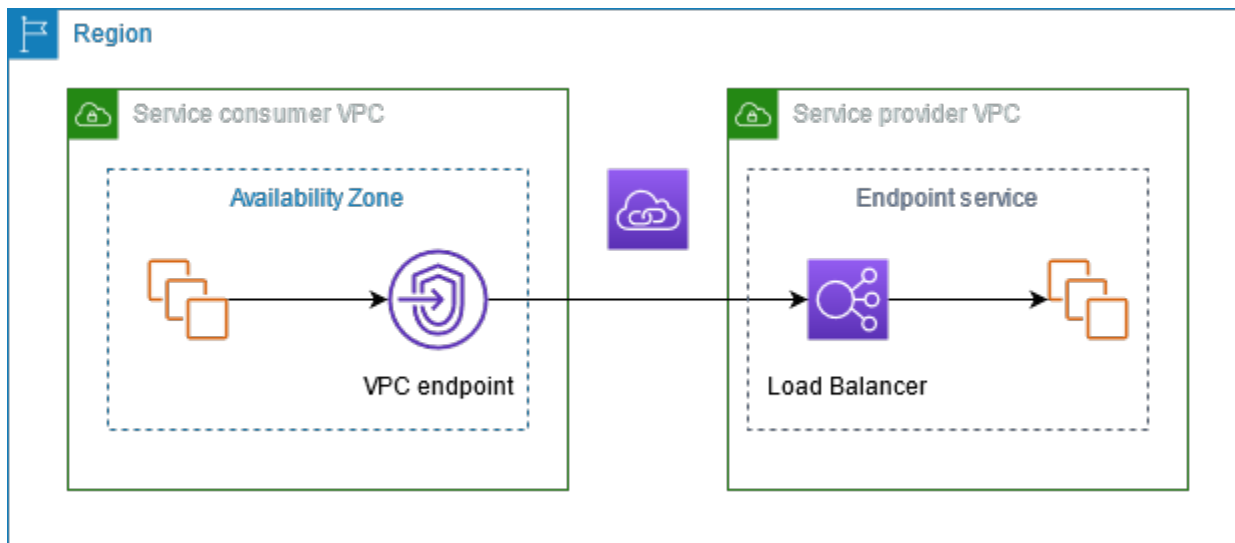
Les concepts suivants sont importants à comprendre lorsque vous commencez à utiliser AWS PrivateLink.

Table des matières

- [Diagramme d'architecture](#)
- [Prestataires](#)
- [Consommateurs de services ou de ressources](#)
- [AWS PrivateLink connections](#)
- [Zones privées hébergées](#)

Diagramme d'architecture

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



Prestataires

Comprenez les concepts liés à un fournisseur.

Prestataire de services

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

Fournisseur de ressources

Le propriétaire d'une ressource, par exemple une base de données ou une instance Amazon EC2, est le fournisseur de ressources. Les fournisseurs de ressources incluent AWS, les services, les partenaires et d'autres Comptes AWS. Les fournisseurs de ressources peuvent héberger leurs ressources dans des VPC ou sur site.

Concepts

- [Services de point de terminaison](#)
- [Noms de service](#)
- [États de service](#)
- [Configuration des ressources](#)
- [Passerelle de ressources](#)

Services de point de terminaison

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

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

Noms de service

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

États de service

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

- En attente : le service Endpoint est en cours de création.
- Disponible : le service Endpoint est disponible.
- Échec : le service Endpoint n'a pas pu être créé.
- Suppression : le fournisseur de services a supprimé le service de point de terminaison et la suppression est en cours.
- Supprimé : le service Endpoint est supprimé.

Configuration des ressources

Le fournisseur de ressources crée une configuration de ressources pour partager une ressource. Une configuration de ressources est un objet logique qui représente une ressource unique telle qu'une base de données, un groupe de ressources ou un segment de réseau (un ensemble de plages CIDR). Une ressource peut être une adresse IP, un nom de domaine cible ou une base de données [Amazon Relational Database Service](#) (Amazon RDS).

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

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

Passerelle de ressources

Une passerelle de ressources est un point d'entrée dans un VPC à partir duquel une ressource est partagée. Le fournisseur crée une passerelle de ressources pour partager les ressources du VPC.

Consommateurs de services ou de ressources

L'utilisateur d'un service ou d'une ressource est un consommateur. Les consommateurs peuvent accéder aux services et aux ressources des terminaux depuis leurs VPC ou depuis leurs locaux.

Concepts

- [Points de terminaison d'un VPC](#)
- [Interfaces réseau de point de terminaison](#)
- [Politiques de point de terminaison](#)
- [États de point de terminaison](#)

Points de terminaison d'un VPC

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

- **Interface-** Créez un point de terminaison d'interface pour envoyer du trafic TCP ou UDP à un service de point de terminaison. Le trafic destiné au service de point de terminaison est résolu à l'aide du DNS.
- **GatewayLoadBalancer** – Créer un Point de terminaison d'équilibreur de charge de passerelle pour envoyer le trafic vers une flotte de dispositifs virtuels en utilisant des adresses IP privées. Vous acheminez le trafic de votre VPC vers le point de terminaison d'équilibreur de charge de

passerelle à l'aide de tables de routage. L'équilibreur de charge de passerelle distribue le trafic vers les dispositifs virtuels et peut s'adapter à la demande.

- **Resource**- Créez un point de terminaison de ressource pour accéder à une ressource qui a été partagée avec vous et qui se trouve dans un autre VPC. Un point de terminaison de ressources vous permet d'accéder de manière privée et sécurisée à des ressources telles qu'une base de données, une instance Amazon EC2, un point de terminaison d'application, une cible de nom de domaine ou une adresse IP qui peut se trouver dans un sous-réseau privé d'un autre VPC ou dans un environnement sur site. Les points de terminaison des ressources ne nécessitent pas d'équilibreur de charge et vous permettent d'accéder directement à la ressource.
- **Tunnel**- Créez un point de terminaison de tunnel pour accéder à un segment de réseau qui a été partagé avec vous depuis un autre VPC ou compte. Un point de terminaison de tunnel vous permet d'accéder de manière privée et sécurisée à un segment de réseau (une liste de plages CIDR) et d'accéder à n'importe quelle ressource située dans ce segment. Les points de terminaison des tunnels nécessitent que vous encapsuliez le trafic des applications dans GENEVE.
- **Service network**- Créez un point de terminaison de réseau de service pour accéder à un réseau de service que vous avez créé ou que vous avez partagé avec vous. Vous pouvez utiliser un seul point de terminaison de réseau de service pour accéder de manière privée et sécurisée à plusieurs ressources et services associés à un réseau de services.

Il existe un autre type de point de terminaison d'un VPC, Gateway, qui crée un point de terminaison de passerelle pour envoyer le trafic vers Amazon S3 ou DynamoDB. Les points de terminaison de passerelle n'utilisent pas AWS PrivateLink, contrairement aux autres types de points de terminaison VPC. Pour plus d'informations, consultez [the section called "Points de terminaison de passerelle"](#).

Interfaces réseau de point de terminaison

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

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

Politiques de point de terminaison

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

États de point de terminaison

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

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

- PendingAcceptance - La demande de connexion est en attente. Il s'agit de l'état initial si les demandes sont acceptées manuellement.
- En attente : le fournisseur de services a accepté la demande de connexion. Il s'agit de l'état initial si les demandes sont acceptées automatiquement. Le point de terminaison d'un VPC revient à cet état si le consommateur du service modifie le point de terminaison d'un VPC.
- Disponible : le point de terminaison VPC est disponible pour utilisation.
- Rejeté : le fournisseur de services a rejeté la demande de connexion. Le fournisseur du service peut également refuser une connexion lorsqu'elle est disponible pour utilisation.
- Expiré : la demande de connexion a expiré.
- Échec : le point de terminaison du VPC n'a pas pu être mis à disposition.
- Suppression : le client du service a supprimé le point de terminaison VPC et la suppression est en cours.
- Supprimé : le point de terminaison du VPC est supprimé.

L' AWS PrivateLink API renvoie les états possibles en utilisant Camel Case.

AWS PrivateLink connections

Le trafic provenant de votre VPC est envoyé vers un service ou une ressource de point de terminaison via une connexion entre le point de terminaison du VPC et le service ou la ressource de

point de terminaison. Le trafic entre un point de terminaison VPC et un service ou une ressource de point de terminaison reste sur le AWS réseau, sans passer par l'Internet public.

Un fournisseur de services ajoute des [autorisations](#) afin que les consommateurs puissent accéder au service de point de terminaison. Les consommateurs de services initient la connexion et le fournisseur de services accepte ou rejette les demandes de connexion. Le propriétaire d'une ressource ou d'un réseau de services partage une configuration de ressources ou un réseau de services avec les consommateurs AWS Resource Access Manager afin que ceux-ci puissent accéder à la ressource ou au réseau de services.

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

Zones privées hébergées

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

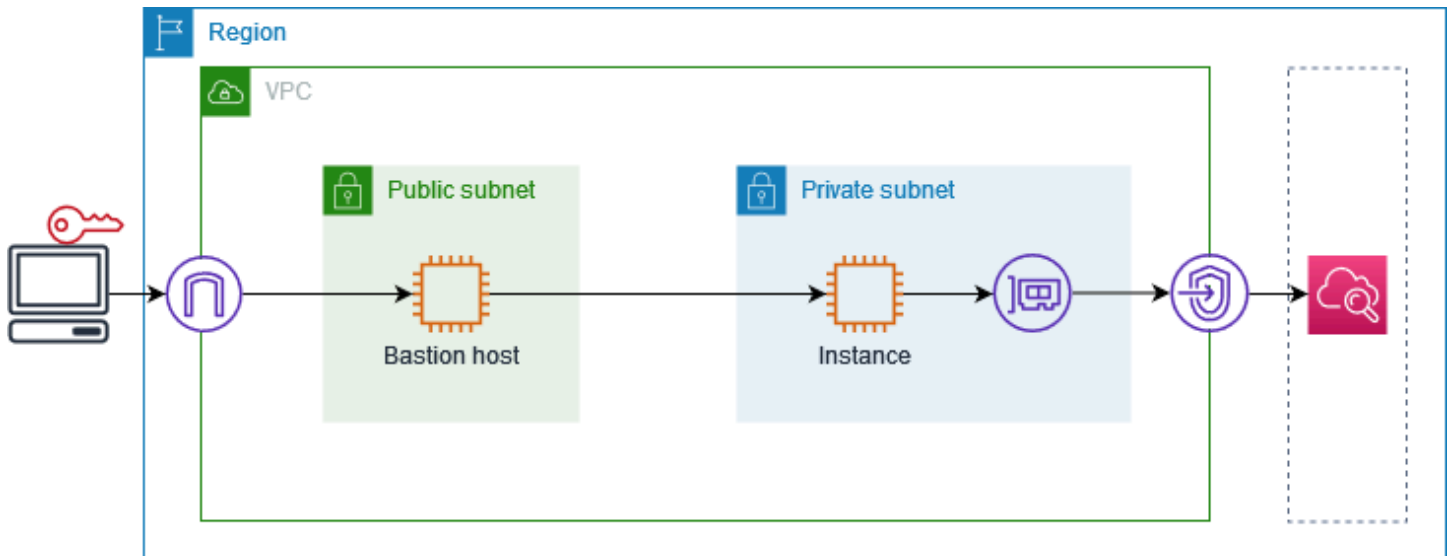
Vous pouvez configurer Amazon Route 53 pour acheminer le trafic du domaine vers un point de terminaison de VPC. Pour plus d'informations, voir [Acheminement du trafic vers un point de terminaison de VPC en utilisant votre nom de domaine](#).

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

Commencez avec AWS PrivateLink

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

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



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

Tâches

- [Étape 1 : Créer un VPC et des sous-réseaux](#)
- [Étape 2 : Lancer les instances](#)
- [Étape 3 : Tester CloudWatch l'accès](#)
- [Étape 4 : créer un point de terminaison VPC auquel accéder CloudWatch](#)

- [Étape 5 : Test du point de terminaison d'un VPC](#)
- [Étape 6 : Nettoyage](#)

Étape 1 : Créer un VPC et des sous-réseaux

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

Pour créer le VPC

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Sélectionnez Create VPC (Créer un VPC).
3. Sous Resources to create (Ressources à créer), choisissez VPC and more (VPC et autres).
4. Pour Name tag auto-generation (Génération automatique de balises de nom), saisissez un nom pour le VPC.
5. Pour configurer les sous-réseaux, procédez comme suit :
 - a. Pour Number of Availability Zones (Nombre de zones de disponibilité), choisissez 1 ou 2, selon vos besoins.
 - b. Pour Number of public subnets (Nombre de sous-réseaux publics), assurez-vous de disposer d'un sous-réseau public par zone de disponibilité.
 - c. Pour Number of private subnets (Nombre de sous-réseaux privés), assurez-vous de disposer d'un sous-réseau privé par zone de disponibilité.
6. Sélectionnez Create VPC (Créer un VPC).

Étape 2 : Lancer les instances

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

Conditions préalables

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

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

Pour lancer l'hôte bastion

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

Pour lancer l'instance

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

7. Développez Advanced Details (Détails avancés). Pour IAM instance profile (Profil d'instance IAM), choisissez votre nom de profil d'instance IAM.
8. Choisissez Launch Instance.

Étape 3 : Tester CloudWatch l'accès

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

Pour tester CloudWatch l'accès

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

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

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

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

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

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

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

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

4. Exécutez la [commande CloudWatch](#) list-metrics sur l'instance comme suit. Pour l'option --region, spécifiez la région dans laquelle vous avez créé le VPC.

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

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

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

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

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

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

Prérequis

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

Pour créer un point de terminaison VPC pour CloudWatch

- Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
- Dans le panneau de navigation, choisissez Points de terminaison.
- Choisissez Créer un point de terminaison.
- Sous Name (Nom), saisissez un nom pour le point de terminaison.
- Pour Service category (Catégorie de service), choisissez Services AWS.
- Pour Service, sélectionnez `com.amazonaws.region.surveillance`.
- Pour VPC, sélectionnez votre VPC.
- Pour Subnets (Sous-réseaux), sélectionnez la zone de disponibilité puis le sous-réseau privé.
- Pour Security group (Groupe de sécurité), sélectionnez le groupe de sécurité du point de terminaison d'un VPC.
- Pour Policy (Politique), sélectionnez Full access (Accès complet) pour autoriser toutes les opérations de tous les principaux sur toutes les ressources via le point de terminaison d'un VPC.
- (Facultatif) Pour ajouter une balise, choisissez Ajouter une nouvelle balise et entrez la clé et la valeur de la balise.
- Choisissez Créer un point de terminaison. Le statut initial est Pending (En attente). Avant de passer à l'étape suivante, attendez que le statut soit Disponible. Cette opération peut prendre quelques minutes.

Étape 5 : Test du point de terminaison d'un VPC

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

Pour tester le point de terminaison d'un VPC

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

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

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

Si vous obtenez un `UnauthorizedOperation` message d'erreur, assurez-vous que l'instance possède un rôle IAM qui autorise l'accès à CloudWatch.

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

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

Étape 6 : Nettoyage

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

Pour résilier les instances

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

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

Pour supprimer le point de terminaison d'un VPC

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

Accès Services AWS à travers AWS PrivateLink

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

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

Tarification

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

Table des matières

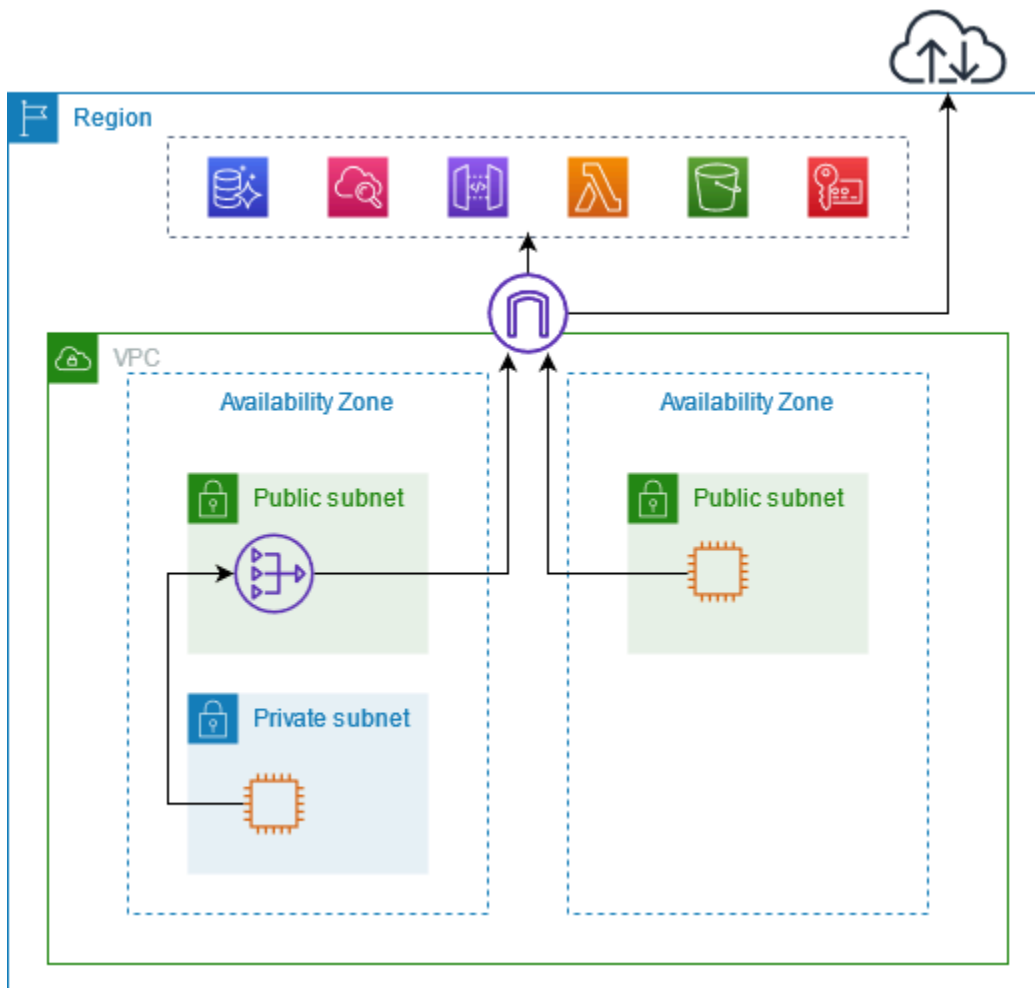
- [Vue d'ensemble](#)
- [Noms d'hôte DNS](#)
- [Résolution DNS](#)
- [DNS privé](#)
- [Sous-réseaux et zones de disponibilité](#)
- [Types d'adresses IP](#)
- [Type d'adresse IP de l'enregistrement DNS](#)
- [Services AWS qui s'intègrent à AWS PrivateLink](#)
- [Cross-region enabled Services AWS](#)
- [Accédez à Service AWS à l'aide d'un point de terminaison VPC d'interface](#)
- [Configuration d'un point de terminaison d'interface](#)
- [Réception d'alertes pour les événements relatifs aux points de terminaison d'interface](#)
- [Suppression d'un point de terminaison d'interface](#)
- [Points de terminaison de passerelle](#)

Vue d'ensemble

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

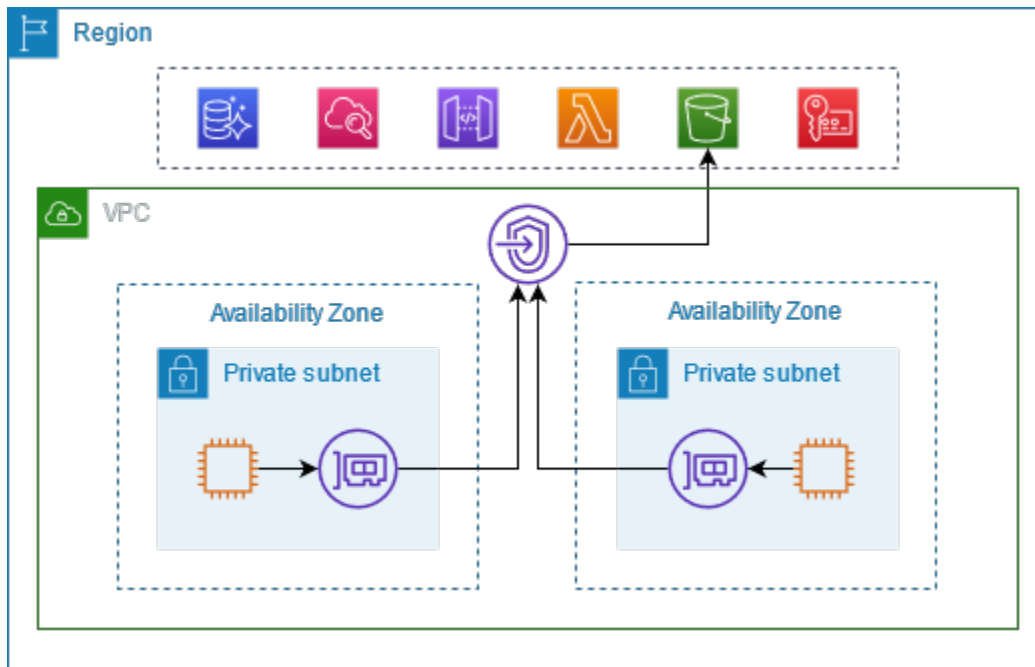
Accès via des points de terminaison de service public

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



Connectez-vous via AWS PrivateLink

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



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

Noms d'hôte DNS

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

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

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

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

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

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

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

Les noms DNS zonaux ont la syntaxe suivante :

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

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

La commande [describe-vpc-endpoints](#) suivante affiche les entrées DNS d'un point de terminaison d'interface.

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

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

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

```

        "HostedZoneId": "ZC8PG0KIFKBRI"
    },
    {
        "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2a.monitoring.us-
east-2.vpce.amazonaws.com",
        "HostedZoneId": "ZC8PG0KIFKBRI"
    },
    {
        "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2b.monitoring.us-
east-2.vpce.amazonaws.com",
        "HostedZoneId": "ZC8PG0KIFKBRI"
    },
    {
        "DnsName": "monitoring.us-east-2.amazonaws.com",
        "HostedZoneId": "Z06320943MM0WYG6MAVL9"
    }
]
]

```

Résolution DNS

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

DNS privé

Si vous activez le DNS privé pour le point de terminaison VPC de votre interface et que les noms d'hôte [DNS et la résolution DNS sont](#) activés sur votre VPC, nous créons pour vous une zone hébergée privée cachée et AWS gérée. La zone hébergée contient un ensemble d'enregistrements pour le nom DNS par défaut du service qui se résout en adresses IP privées des interfaces réseau du point de terminaison de votre VPC. Par conséquent, si vous avez des applications existantes qui envoient des demandes à l' Service AWS aide d'un point de terminaison régional public, ces demandes passent désormais par les interfaces réseau du point de terminaison, sans que vous n'ayez à apporter de modifications à ces applications.

Nous vous recommandons d'activer des noms d'hôtes DNS privés pour votre point de terminaison de VPC pour les Services AWS. Cela garantit que les demandes qui utilisent les points de terminaison

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

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

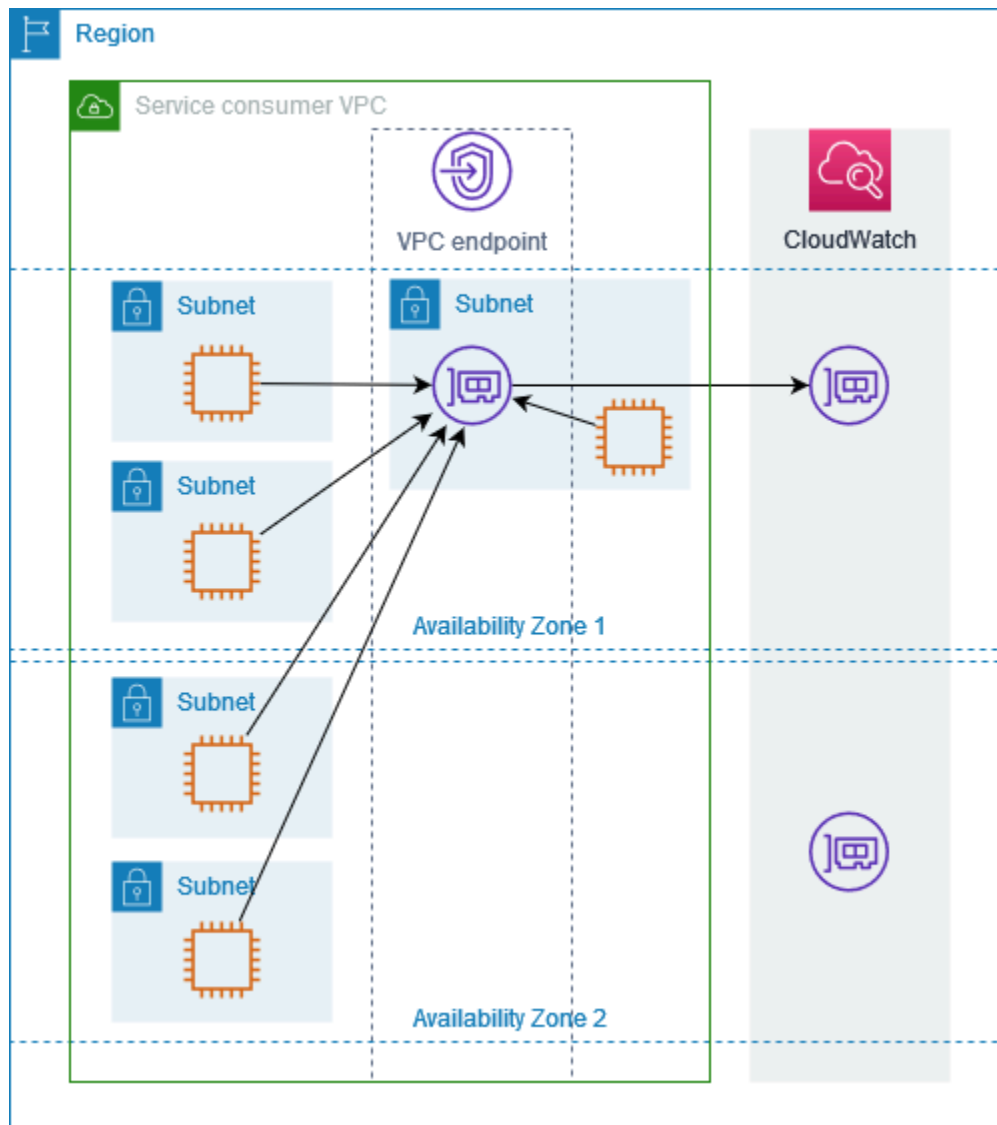
Sous-réseaux et zones de disponibilité

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

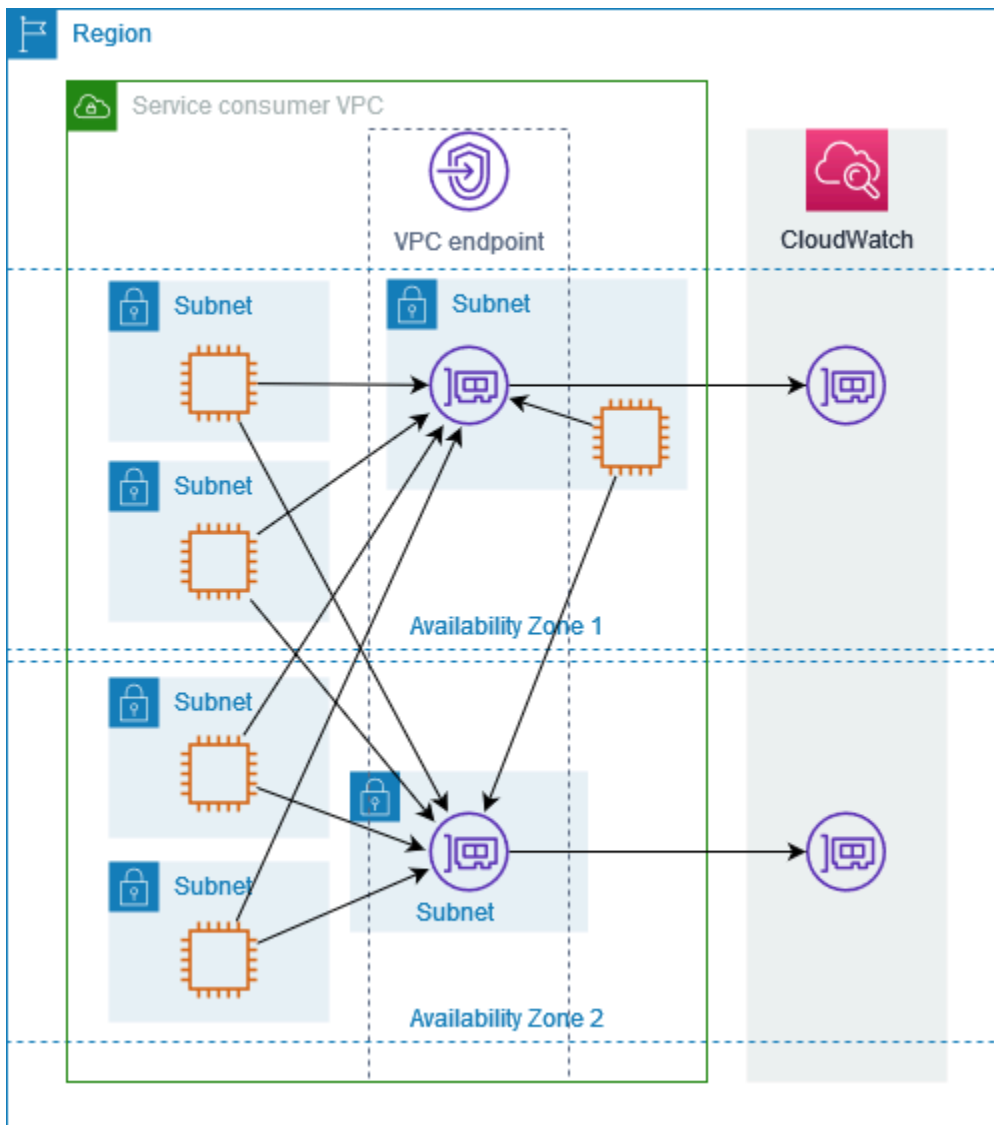
Dans un environnement de production, pour assurer une disponibilité et une résilience élevées, nous recommandons ce qui suit :

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

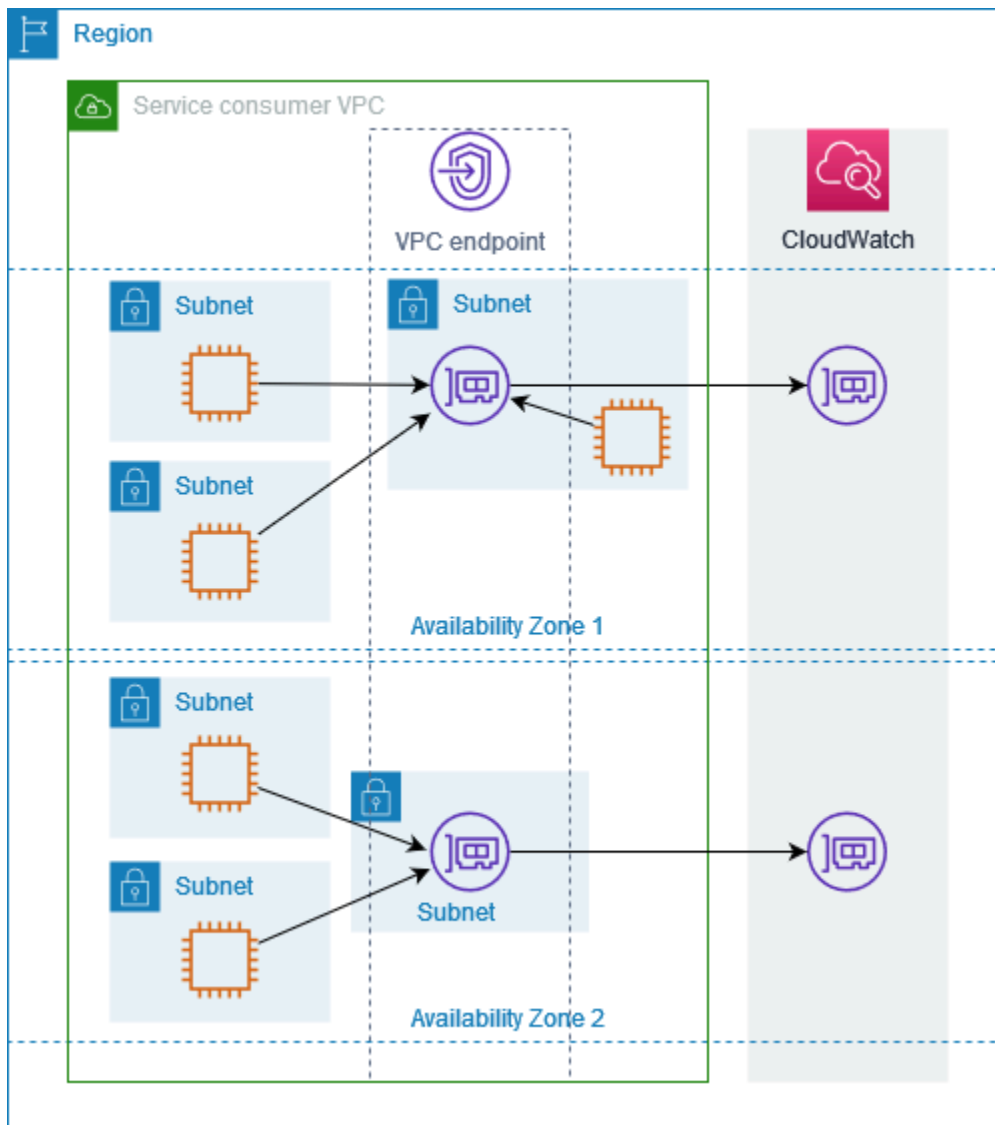
Le schéma suivant montre un point de terminaison VPC pour Amazon CloudWatch avec une interface réseau de point de terminaison dans une seule zone de disponibilité. Lorsqu'une ressource d'un sous-réseau du VPC accède à Amazon CloudWatch via son point de terminaison public, nous résolvons le trafic vers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



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



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



Types d'adresses IP

Services AWS peuvent prendre en charge IPv6 via leurs points de terminaison privés même s'ils ne prennent pas en charge IPv6 via leurs points de terminaison publics. Les points de terminaison qui prennent en charge IPv6 peuvent répondre aux requêtes DNS avec des enregistrements AAAA.

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

- Service AWS Il doit rendre ses points de terminaison de service disponibles via IPv6. Pour plus d'informations, consultez [the section called "Afficher la prise charge d'IPv6"](#).
- Le type d'adresse IP d'un point de terminaison d'interface doit être compatible avec les sous-réseaux du point de terminaison d'interface, comme décrit ici :

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

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

Type d'adresse IP de l'enregistrement DNS

En fonction de votre type d'adresse IP, lorsque vous appelez un point de terminaison VPC, le AWS service peut renvoyer des enregistrements A, des enregistrements AAAA ou à la fois des enregistrements A et AAAA. Vous pouvez personnaliser les types d'enregistrement renvoyés par votre AWS service en modifiant le type IP de l'enregistrement DNS. Le tableau suivant indique les types d'adresses IP d'enregistrement DNS pris en charge et les types d'enregistrements renvoyés :

Type d'adresse IP de l'enregistrement DNS	Types d'enregistrements renvoyés
IPv4	A
IPv6	AAAA
Double pile	A et AAAA

Par défaut, le type d'enregistrement DNS est le même que le type d'adresse IP. Vous pouvez choisir un autre type d'adresse IP d'enregistrement DNS, mais vous devez utiliser un type d'adresse IP compatible pour le service de point de terminaison. Le tableau suivant indique le type d'adresse IP

d'enregistrement DNS pris en charge pour chaque type d'adresse IP pour les points de terminaison de l'interface :

Type d'adresse IP	Types d'adresses IP d'enregistrement DNS pris en charge
IPv4	IPv4
IPv6	IPv6
Double pile	Dualstack*, IPv4, IPv6, défini par le service

* Représente le type d'adresse IP d'enregistrement DNS par défaut.

Un type d'adresse IP d'enregistrement DNS défini par un service renvoie des enregistrements DNS en fonction du point de terminaison de service que vous appelez. Si vous utilisez un type d'adresse IP d'enregistrement DNS défini par un service, assurez-vous que votre service peut gérer les appels variables provenant des points de terminaison du service. Pour voir les enregistrements DNS pris en charge par le point de terminaison de votre interface, consultez les noms DNS de votre point de terminaison VPC dans le Console de gestion AWS, ou utilisez [DescribeVpcEndpoints](#).

Le comportement du type d'adresse IP de l'enregistrement DNS est différent pour les points de terminaison de la passerelle. Pour plus d'informations, consultez la section Type d'adresse IP d'enregistrement [DNS pour les points de terminaison](#) de passerelle.

Services AWS qui s'intègrent à AWS PrivateLink

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

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

Service AWS	Nom du service
Gestion de compte AWS	com.amazonaws. <i>region</i> .compte
Amazon API Gateway	com.amazonaws. <i>region</i> .exécuter-api
	com.amazonaws. <i>region</i> . une passerelle
AWS AppConfig	com.amazonaws. <i>region</i> .appconfig
	com.amazonaws. <i>region</i> .appconfig-fips
	com.amazonaws. <i>region</i> .appconfigdata
	com.amazonaws. <i>region</i> .appconfigdata-fips
AWS App Mesh	com.amazonaws. <i>region</i> .appmesh
	com.amazonaws. <i>region</i> .appmesh-envoy-management
AWS App Runner	com.amazonaws. <i>region</i> .apprunner
Services AWS App Runner	com.amazonaws. <i>region</i> .apprunner.requests
Application Autoscaling	com.amazonaws. <i>region</i> .mise à l'échelle automatique des applications
AWS Application Discovery Service	com.amazonaws. <i>region</i> .découverte
	com.amazonaws. <i>region</i> .découverte de l'arsenal
AWS Service de migration des applications	com.amazonaws. <i>region</i> .mgn
WorkSpaces Applications Amazon	com.amazonaws. <i>region</i> .appstream.api
	com.amazonaws. <i>region</i> .appstream.streaming
AWS AppSync	com.amazonaws. <i>region</i> .appsync api
Amazon Athena	com.amazonaws. <i>region</i> .athéna

Service AWS	Nom du service
AWS Audit Manager	com.amazonaws. <i>region</i> . responsable de l'audit
Amazon Aurora	com.amazonaws. <i>region</i> .rds
	com.amazonaws. <i>region</i> .rds-fips
Amazon Aurora DSQL	com.amazonaws. <i>region</i> .dsq
AWS Auto Scaling	com.amazonaws. <i>region</i> .plans de mise à l'échelle automatique
AWS Échange de données B2B	com.amazonaws. <i>region</i> .b2bi
AWS Backup	com.amazonaws. <i>region</i> .sauvegarde
	com.amazonaws. <i>region</i> .passerelle de sauvegarde
AWS Batch	com.amazonaws. <i>region</i> .lot
Amazon Bedrock	com.amazonaws. <i>region</i> . socle
	com.amazonaws. <i>region</i> .agent de base
	com.amazonaws. <i>region</i> .bedrock-agent-runtime
	com.amazonaws. <i>region</i> .bedrock-data-automation
	com.amazonaws. <i>region</i> .conseils sur l'automatisation des données Bedrock
	com.amazonaws. <i>region</i> .bedrock-data-automation-runtime
	com.amazonaws. <i>region</i> .bedrock-data-automation-runtime-fips
	com.amazonaws. <i>region</i> .bedrock-runtime
Amazon Bedrock AgentCore	com.amazonaws. <i>region</i> . bedrock-agentcore-control

Service AWS	Nom du service
AWS Billing and Cost Management	com.amazonaws. <i>region</i> .bedrock-agentcore
	com.amazonaws. <i>region</i> .facturation
	com.amazonaws. <i>region</i> .plus gratuit
	com.amazonaws. <i>region</i> .taxe
AWS Billing Conductor	com.amazonaws. <i>region</i> . responsable de la facturation
Amazon Braket	com.amazonaws. <i>region</i> . support
AWS Certificate Manager	com.amazonaws. <i>region</i> .acm
	com.amazonaws. <i>region</i> .acm-fips
Kit SDK Amazon Chime	com.amazonaws. <i>region</i> .chime-sdk-voice
	com.amazonaws. <i>region</i> .carillon de réunion
	com.amazonaws. <i>region</i> .carillon de messagerie
	com.amazonaws. <i>region</i> .carillon de messagerie fips
	com.amazonaws. <i>region</i> .carillon d'identité
	com.amazonaws. <i>region</i> .carillon d'identité
	com.amazonaws. <i>region</i> .media-pipelines-carillon
	com.amazonaws. <i>region</i> .media-pipelines-chime-fips
AWS Clean Rooms	com.amazonaws. <i>region</i> . salles blanches
	com.amazonaws. <i>region</i> .conseils sur les salles blanches
AWS Salles propres ML	com.amazonaws. <i>region</i> .cleanrooms-ml
API de commande du Cloud AWS	com.amazonaws. <i>region</i> .cloudcontrol api

Service AWS	Nom du service
	com.amazonaws. <i>region</i> .cloudcontrol api-fips
Amazon Cloud Directory	com.amazonaws. <i>region</i> répertoire .cloud
AWS CloudFormation	com.amazonaws. <i>region</i> . formation des nuages
	com.amazonaws. <i>region</i> .cloudformation-fips
Amazon CloudFront	com.amazonaws.cloudfront
Plans CloudFront Flat-Rate tarifaires Amazon	com.amazonaws.us-east-1.pricingplanmanager
AWS CloudHSM	com.amazonaws. <i>region</i> .cloudhsmv2
AWS Cloud Map	com.amazonaws. <i>region</i> .découverte de services
	com.amazonaws. <i>region</i> .servicediscovery-fips
	com.amazonaws. <i>region</i> .data-servicediscovery
	com.amazonaws. <i>region</i> .data-servicediscovery-fips
AWS CloudTrail	com.amazonaws. <i>region</i> .cloudtrail
AWS Réseau WAN dans le cloud	com.amazonaws. <i>region</i> .gestionnaire de réseau
Amazon CloudWatch	com.amazonaws. <i>region</i> .signaux-d'application
	com.amazonaws. <i>region</i> . aperçus des applications
	com.amazonaws. <i>region</i> . moniteur Internet
	com.amazonaws. <i>region</i> .internetmonitor fips
	com.amazonaws. <i>region</i> .surveillance
	com.amazonaws. <i>region</i> . moniteur de flux réseau

Service AWS	Nom du service
	com.amazonaws. <i>region</i> . rapports de surveillance des flux réseau
	com.amazonaws. <i>region</i> . moniteur réseau
	com.amazonaws. <i>region</i> .observabilityadmin
	com.amazonaws. <i>region</i> .rhum
	com.amazonaws. <i>region</i> plan-données .rum
	com.amazonaws. <i>region</i> . synthétiques
	com.amazonaws. <i>region</i> .embouts synthétiques
	com.amazonaws. <i>region</i> .oam
CloudWatch Journaux Amazon	com.amazonaws. <i>region</i> .journaux
AWS CodeArtifact	com.amazonaws. <i>region</i> .codeartifact.api
	com.amazonaws. <i>region</i> .codeartifact.repositories
AWS CodeBuild	com.amazonaws. <i>region</i> .codebuild
	com.amazonaws. <i>region</i> .codebuild-fips
AWS CodeCommit	com.amazonaws. <i>region</i> .code commit
	com.amazonaws. <i>region</i> .codecommit-fips
	com.amazonaws. <i>region</i> .git-code commit
	com.amazonaws. <i>region</i> .git-codecommit-fips
AWS CodeConnections	com.amazonaws. <i>region</i> .codeconnections.api
	com.amazonaws. <i>region</i> .codestar-connections.api
AWS CodeDeploy	com.amazonaws. <i>region</i> .codedeploy

Service AWS	Nom du service
	com.amazonaws. <i>region</i> .codedeploy-commands-secure
	com.amazonaws. <i>region</i> .codedeploy-fips
CodeGuru Profileur Amazon	com.amazonaws. <i>region</i> .codeguru - profileur
CodeGuru Réviseur Amazon	com.amazonaws. <i>region</i> .codeguru-reviewer
AWS CodePipeline	com.amazonaws. <i>region</i> .codepipeline
Amazon Comprehend	com.amazonaws. <i>region</i> .comprendre
	com.amazonaws. <i>region</i> .comprendre les astuces
Amazon Comprehend Medical	com.amazonaws. <i>region</i> . comprendre la médecine
Optimiseur de calcul AWS	com.amazonaws. <i>region</i> .optimiseur de calcul
AWS Config	com.amazonaws. <i>region</i> .config
	com.amazonaws. <i>region</i> .config-fips
Connecter le client	com.amazonaws. <i>region</i> Intégrations .app
	com.amazonaws. <i>region</i> . étuis
	com.amazonaws. <i>region</i> .connecter
	com.amazonaws. <i>region</i> .connect-fips
	com.amazonaws. <i>region</i> Campagnes .connect
	com.amazonaws. <i>region</i> .profil
	com.amazonaws. <i>region</i> .identifiant vocal
	com.amazonaws. <i>region</i> .sagesse
AWS Connector Service	com.amazonaws. <i>region</i> connecteur .aws

Service AWS	Nom du service
AWS Control Catalog	com.amazonaws. <i>region</i> .catalogue de contrôle
AWS Cost Explorer	com.amazonaws. <i>region</i> .ce
Hub d'optimisation des coûts AWS	com.amazonaws. <i>region</i> .hub d'optimisation des coûts
AWS Control Tower	com.amazonaws. <i>region</i> . tour de contrôle
	com.amazonaws. <i>region</i> .controlltower-fips
AWS Data Exchange	com.amazonaws. <i>region</i> . échange de données
Exportations de données AWS	aws.api. <i>region</i> Exportations de données .bcm
	com.amazonaws. <i>region</i> Calculateur de prix .bcm
Amazon Data Firehose	com.amazonaws. <i>region</i> .kinesis-firehose
Amazon Data Lifecycle Manager	com.amazonaws. <i>region</i> .dlm
	com.amazonaws. <i>region</i> .dlm-fips
AWS Database Migration Service	com.amazonaws. <i>region</i> .dms
	com.amazonaws. <i>region</i> .dms-fips
AWS DataSync	com.amazonaws. <i>region</i> .datasync
Amazon DataZone	com.amazonaws. <i>region</i> .zone de données
	com.amazonaws. <i>region</i> .datazone-fips
AWS Deadline Cloud	com.amazonaws. <i>region</i> .échéance.gestion
	com.amazonaws. <i>region</i> .deadline .planification
Amazon Detective	com.amazonaws. <i>region</i> .détective
	com.amazonaws. <i>region</i> .détective-fips

Service AWS	Nom du service
Le DevOps gourou d'Amazon	com.amazonaws. <i>region</i> .devops-gourou
AWS Direct Connect	com.amazonaws. <i>region</i> .connexion directe
	com.amazonaws. <i>region</i> .directconnect-fips
AWS Directory Service	com.amazonaws. <i>region</i> .ds
	com.amazonaws. <i>region</i> .ds-données
	com.amazonaws. <i>region</i> .ds-data-fips
Amazon DocumentDB	com.amazonaws. <i>region</i> .rds
Amazon DynamoDB	com.amazonaws. <i>region</i> .dynamodb
	com.amazonaws. <i>region</i> .dynamodb-fips
	com.amazonaws. <i>region</i> .flux dynamodb
API directes Amazon EBS	com.amazonaws. <i>region</i> .ebs
	com.amazonaws. <i>region</i> .ebs-fips
Amazon EC2	com.amazonaws. <i>region</i> .ec2
	com.amazonaws. <i>region</i> .ec2-fips
Amazon EC2 Auto Scaling	com.amazonaws. <i>region</i> .mise à l'échelle automatique
	com.amazonaws. <i>region</i> .autoscaling-fips
EC2 Image Builder	com.amazonaws. <i>region</i> .créateur d'images
Amazon ECR	com.amazonaws. <i>region</i> .ecr.api
	com.amazonaws. <i>region</i> .ecr.dkr
Amazon ECS	com.amazonaws. <i>region</i> .ecs

Service AWS	Nom du service
	com.amazonaws. <i>region</i> .ecs-agent
	com.amazonaws. <i>region</i> .ecs-télémétrie
Amazon EKS	com.amazonaws. <i>region</i> .eks
	com.amazonaws. <i>region</i> .eks-auth
	com.amazonaws. <i>region</i> .eks-fips
	com.amazonaws. <i>region</i> .eks-mcp
	com.amazonaws. <i>region</i> .eks-proxy
	com.amazonaws. <i>region</i> .oid-eks
AWS Elastic Beanstalk	com.amazonaws. <i>region</i> . tige de haricot élastique
	com.amazonaws. <i>region</i> . tige de haricot élastique - santé
Reprise après sinistre AWS Elastic	com.amazonaws. <i>region</i> .drs
Amazon Elastic File System	com.amazonaws. <i>region</i> système de fichiers .elastic
	com.amazonaws. <i>region</i> Système de fichiers .elastic-fips
Elastic Load Balancing	com.amazonaws. <i>region</i> . équilibrage de charge élastique
Service Amazon Elastic VMware	com.amazonaws. <i>region</i> .evs
	com.amazonaws. <i>region</i> .evs-fips
Amazon ElastiCache	com.amazonaws. <i>region</i> . cache élastique
	com.amazonaws. <i>region</i> .attaches élastiques
AWS Elemental MediaConnect	com.amazonaws. <i>region</i> .mediaconnect

Service AWS	Nom du service
AWS Elemental MediaConvert	com.amazonaws. <i>region</i> .media convertit
	com.amazonaws. <i>region</i> .mediaconvert-fips
Amazon EMR	com.amazonaws. <i>region</i> .elasticmapreduce
	com.amazonaws. <i>region</i> .elasticmapreduce-fips
	com.amazonaws. <i>region</i> .Tableau de bord .emr
Amazon EMR on EKS	com.amazonaws. <i>region</i> .Conteneurs .emr
Amazon EMR sans serveur	com.amazonaws. <i>region</i> .emr sans serveur
	com.amazonaws. <i>region</i> .emr-serverless-services.livy
	com.amazonaws. <i>region</i> .emr-serverless.dashboard
Amazon EMR WAL	com.amazonaws. <i>region</i> .merwal.prod
AWS Messagerie à l'utilisateur final : réseaux sociaux	com.amazonaws. <i>region</i> .messagerie sociale
	com.amazonaws. <i>region</i> .fips de messagerie sociale
Résolution des entités AWS	com.amazonaws. <i>region</i> . résolution de l'entité
	com.amazonaws. <i>region</i> .entityresolution - fips
Amazon EventBridge	com.amazonaws. <i>region</i> .événements
	com.amazonaws. <i>region</i> .infos-événements
	com.amazonaws. <i>region</i> . tuyaux
	com.amazonaws. <i>region</i> .pipes-data
	com.amazonaws. <i>region</i> .pipes-fips
	com.amazonaws. <i>region</i> .schémas

Service AWS	Nom du service
EventBridge Planificateur Amazon	com.amazonaws. <i>region</i> .planificateur
AWS Fault Injection Service	com.amazonaws. <i>region</i> .fisc
	com.amazonaws. <i>region</i> .fis-fips
Amazon FinSpace	com.amazonaws. <i>region</i> .finspace
	com.amazonaws. <i>region</i> .finspace api
AWS Firewall Manager	com.amazonaws. <i>region</i> .fms
	com.amazonaws. <i>region</i> .fms-fips
Amazon Forecast	com.amazonaws. <i>region</i> .prévision
	com.amazonaws. <i>region</i> .requête de prévision
	com.amazonaws. <i>region</i> .conseils sur les prévisions
	com.amazonaws. <i>region</i> .forecastquery-fips
Amazon Fraud Detector	com.amazonaws. <i>region</i> .détecteur de fraude
Amazon FSx	com.amazonaws. <i>region</i> .fsx
	com.amazonaws. <i>region</i> .fsx-fips
GameLift Serveurs Amazon	com.amazonaws. <i>region</i> .gamelift
Amazon GameLift Streams	com.amazonaws. <i>region</i> .gameliftstreams
Réseaux mondiaux AWS pour les passerelles de transit	com.amazonaws. <i>region</i> .gestionnaire de réseau
AWS Glue	com.amazonaws. <i>region</i> .colle
	com.amazonaws. <i>region</i> .glue.dashboard
AWS Glue DataBrew	com.amazonaws. <i>region</i> . base de données

Service AWS	Nom du service
	com.amazonaws. <i>region</i> .databrew-fips
Amazon Managed Grafana	com.amazonaws. <i>region</i> .grafana
	com.amazonaws. <i>region</i> .grafana-workspace
AWS Ground Station	com.amazonaws. <i>region</i> .station au sol
	com.amazonaws. <i>region</i> .groundstations-fips
Amazon GuardDuty	com.amazonaws. <i>region</i> .devoir de garde
	com.amazonaws. <i>region</i> .guardduty-data
	com.amazonaws. <i>region</i> .guardduty-data-fips
	com.amazonaws. <i>region</i> .guardduty-tips
AWS HealthImaging	com.amazonaws. <i>region</i> .dicom-imagerie médicale
	com.amazonaws. <i>region</i> .imagerie médicale
	com.amazonaws. <i>region</i> .imagerie médicale d'exécution
AWS HealthLake	com.amazonaws. <i>region</i> .lac de santé
AWS HealthOmics	com.amazonaws. <i>region</i> .analytique-omique
	com.amazonaws. <i>region</i> .analytics-omics-fips
	com.amazonaws. <i>region</i> .control-storage-omics
	com.amazonaws. <i>region</i> .control-storage-omics-fips
	com.amazonaws. <i>region</i> .storage-omics
	com.amazonaws. <i>region</i> .tags-omics
	com.amazonaws. <i>region</i> .tags-omics-fips

Service AWS	Nom du service
	com.amazonaws. <i>region</i> .workflows-omics
	com.amazonaws. <i>region</i> .workflows-omics-fips
Gestion des identités et des accès AWS (IAM)	com.amazonaws.iam
Analyseur d'accès IAM	com.amazonaws. <i>region</i> .analyseur d'accès
	com.amazonaws. <i>region</i> .access-analyzer-fips
IAM Identity Center	com.amazonaws. <i>region</i> .boutique d'identité
	com.amazonaws. <i>region</i> .sso
	com.amazonaws. <i>region</i> .sso-oauth
Rôles Anywhere IAM	com.amazonaws. <i>region</i> . des rôles n'importe où
	com.amazonaws. <i>region</i> .rolesanywhere - fips
Amazon Inspector	com.amazonaws. <i>region</i> .inspecteur 2
	com.amazonaws. <i>region</i> .inspector2-fips
	com.amazonaws. <i>region</i> .inspector-scan
	com.amazonaws. <i>region</i> .inspector-scan-fips
Amazon Interactive Video Service	com.amazonaws. <i>region</i> .ivs.contribute
AWS IoT Core	com.amazonaws. <i>region</i> .iot.api
	com.amazonaws. <i>region</i> .iot-fips.api
	com.amazonaws. <i>region</i> .iot.data
	com.amazonaws. <i>region</i> .iot.informations d'identification

Service AWS	Nom du service
AWS IoT Device Management tunneling sécurisé	com.amazonaws. <i>region</i> .iot.tunneling.api
	com.amazonaws. <i>region</i> .iot-fips.tunneling.api
	com.amazonaws. <i>region</i> .iot.tunneling.data
	com.amazonaws. <i>region</i> .iot-fips.tunneling.data
AWS IoT Core Device Advisor	com.amazonaws. <i>region</i> .deviceadvisor.iot
Intégrations gérées pour AWS IoT Device Management	com.amazonaws. <i>region</i> .iotmanagedintegrations.api
	com.amazonaws. <i>region</i> .Intégrations gérées .iot - fips.api
AWS IoT Core for LoRaWAN	com.amazonaws. <i>region</i> .iot-wireless.api
	com.amazonaws. <i>region</i> .gobelets.lorawan
	com.amazonaws. <i>region</i> .lorawan.lns
AWS IoT FleetWise	com.amazonaws. <i>region</i> .iotfleetwise
AWS IoT Greengrass	com.amazonaws. <i>region</i> .herbe verte
AWS IoT RoboRunner	com.amazonaws. <i>region</i> .iotroborunner
AWS IoT SiteWise	com.amazonaws. <i>region</i> .iot-sitewise.api
	com.amazonaws. <i>region</i> .iot sitewise.data
AWS IoT TwinMaker	com.amazonaws. <i>region</i> .iottwinmaker.api
	com.amazonaws. <i>region</i> .iottwinmaker.data
Amazon Kendra	com.amazonaws. <i>region</i> .kendra
	aws.api. <i>region</i> .kendra - classement
AWS Key Management Service	com.amazonaws. <i>region</i> .km

Service AWS	Nom du service
	com.amazonaws. <i>region</i> .kms-fips
Amazon Keyspaces (pour Apache Cassandra)	com.amazonaws. <i>region</i> .cassandra
	com.amazonaws. <i>region</i> .cassandra-fips
Amazon Kinesis Data Streams	com.amazonaws. <i>region</i> .kinesis-streams
	com.amazonaws. <i>region</i> .kinesis-streams-fips
AWS Lake Formation	com.amazonaws. <i>region</i> . formation du lac
AWS Lambda	com.amazonaws. <i>region</i> .lambda
	com.amazonaws. <i>region</i> .lambda microvm
AWS Launch Wizard	com.amazonaws. <i>region</i> .assistant de lancement
Amazon Lex V2	com.amazonaws. <i>region</i> .modèles-v2-lex
	com.amazonaws. <i>region</i> .runtime-v2-lex
AWS License Manager	com.amazonaws. <i>region</i> .gestionnaire de licences
	com.amazonaws. <i>region</i> .license-manager-fips
	com.amazonaws. <i>region</i> .license-manager-linux-subscriptions
	com.amazonaws. <i>region</i> .license-manager-linux-subscriptions-fips
	com.amazonaws. <i>region</i> .license-manager-user-subscriptions
	com.amazonaws. <i>region</i> .license-manager-user-subscriptions-fips
Amazon Lightsail	com.amazonaws. <i>region</i> . voile légère

Service AWS	Nom du service
Amazon Location Service	com.amazonaws. <i>region</i> .geo.maps
	com.amazonaws. <i>region</i> .geo.lieux
	com.amazonaws. <i>region</i> .geo.routes
	com.amazonaws. <i>region</i> .geo.geofencing
	com.amazonaws. <i>region</i> .geo.tracking
	com.amazonaws. <i>region</i> .geo.métadonnées
Amazon Lookout for Equipment	com.amazonaws. <i>region</i> . équipement d'observation
Amazon Lookout for Vision	com.amazonaws. <i>region</i> . belvédère
Amazon Macie	com.amazonaws. <i>region</i> .macie 2
	com.amazonaws. <i>region</i> .macie2-fips
AWS Mainframe Modernization	com.amazonaws. <i>region</i> .test d'application
	com.amazonaws. <i>region</i> m2
Amazon Managed Blockchain	com.amazonaws. <i>region</i> .requête blockchain gérée
	com.amazonaws. <i>region</i> .chaîne de blocs gérée .bitcoin. mainnet
	com.amazonaws. <i>region</i> .chaîne de blocs gérée .bitcoin. testnet
AWS Accord relatif au marché	com.amazonaws. <i>region</i> . marché des accords
AWS Découverte du marché	com.amazonaws. <i>region</i> .discovery-marketplace
AWS Marketplace Metering Service	com.amazonaws. <i>region</i> .marché des compteurs
Amazon Managed Service for Prometheus	com.amazonaws. <i>region</i> .aps

Service AWS	Nom du service
	com.amazonaws. <i>region</i> .aps-espaces de travail
Amazon Managed Streaming for Apache Kafka (MSK)	com.amazonaws. <i>region</i> .kafka
	com.amazonaws. <i>region</i> .kafka-fips
Amazon Managed Workflows for Apache Airflow	com.amazonaws. <i>region</i> .airflow.api
	com.amazonaws. <i>region</i> .airflow.api-fips
	com.amazonaws. <i>region</i> .airflow.env
	com.amazonaws. <i>region</i> .airflow.env-fips
	com.amazonaws. <i>region</i> .airflow.ops
Amazon Route 53	com.amazonaws.route53
Amazon Route 53 Global Resolver	résolveur global aws.api.us-east-2.route53
	résolveur global aws.api.us-east-2.route53 - fips
Profils Amazon Route 53	com.amazonaws. <i>region</i> Profils .route 53
Console de gestion AWS	com.amazonaws. <i>region</i> .console
	com.amazonaws. <i>region</i> .connexion
Amazon MemoryDB	com.amazonaws. <i>region</i> .mémoire-base de données
	com.amazonaws. <i>region</i> .memorydb-fips
Orchestrateur de l'AWS Migration Hub	com.amazonaws. <i>region</i> .migrationhub-orchestrateur
AWS Migration Hub Refactor Spaces	com.amazonaws. <i>region</i> .espaces de refactorisation
Migration Hub Strategy Recommendations	com.amazonaws. <i>region</i> .stratégie de hub de migration

Service AWS	Nom du service
Amazon MQ	com.amazonaws. <i>region</i> .mq
	com.amazonaws. <i>region</i> .mq-fips
Amazon Neptune Analytics	com.amazonaws. <i>region</i> .graphe Neptune
	com.amazonaws. <i>region</i> .neptune-graphe-data
	com.amazonaws. <i>region</i> .neptune-graphe-fips
AWS Network Firewall	com.amazonaws. <i>region</i> .pare-feu-réseau
	com.amazonaws. <i>region</i> .network-firewall-fips
OpenSearch Service Amazon	Ces points de terminaison sont gérés par des services
OpenSearch Ingestion par Amazon	com.amazonaws. <i>region</i> .osis
AWS Organizations	com.amazonaws. <i>region</i> .organisations
	com.amazonaws. <i>region</i> .organisations-fips
AWS Outposts	com.amazonaws. <i>region</i> . avant-postes
AWS Panorama	com.amazonaws. <i>region</i> .panorama
AWS Cryptographie des paiements	com.amazonaws. <i>region</i> .cryptographie de paiement. plan de contrôle
	com.amazonaws. <i>region</i> .cryptographie de paiement. dataplane
AWS PC	com.amazonaws. <i>region</i> .pièces
	com.amazonaws. <i>region</i> .pcs-fips
Amazon Personalize	com.amazonaws. <i>region</i> .personnaliser
	com.amazonaws. <i>region</i> .personnalisez vos événements

Service AWS	Nom du service
	com.amazonaws. <i>region</i> .personnaliser-runtime
Amazon Pinpoint	com.amazonaws. <i>region</i> .identifier
	com.amazonaws. <i>region</i> .pinpoint-sms-voix-v2
Amazon Polly	com.amazonaws. <i>region</i> .polly
	com.amazonaws. <i>region</i> .polly-fips
AWS Price List	com.amazonaws. <i>region</i> .tarification.api
Autorité de certification privée AWS	com.amazonaws. <i>region</i> .acm-pca
	com.amazonaws. <i>region</i> .acm-pca-fips
	com.amazonaws. <i>region</i> .pca-connecteur-ad
	com.amazonaws. <i>region</i> .Connecteur-pca-scep
AWS Proton	com.amazonaws. <i>region</i> .proton
Amazon Q Business	aws.api. <i>region</i> .qentreprise
Amazon Q Developer	com.amazonaws. <i>region</i> .codewhisperer
	com.amazonaws. <i>region</i> .q.
	com.amazonaws. <i>region</i> .applications
Abonnements utilisateur Amazon Q	com.amazonaws. <i>region</i> .service.abonnements utilisateur
Rapide	com.amazonaws. <i>region</i> .site web .quicksight
Amazon RDS	com.amazonaws. <i>region</i> .rds
	com.amazonaws. <i>region</i> .rds-fips
Amazon RDS Data API	com.amazonaws. <i>region</i> .données RDS

Service AWS	Nom du service
Analyse des performances d'Amazon RDS	com.amazonaws. <i>region</i> .pi
	com.amazonaws. <i>region</i> .pi-fips
AWS Re : Publier en privé	com.amazonaws. <i>region</i> .espace de republication
Corbeille	com.amazonaws. <i>region</i> .bin
	com.amazonaws. <i>region</i> .rbin-fips
Amazon Redshift	com.amazonaws. <i>region</i> . décalage vers le rouge
	com.amazonaws. <i>region</i> .redshift-fips
	com.amazonaws. <i>region</i> .redshift sans serveur
	com.amazonaws. <i>region</i> .redshift-serverless-fips
API de données Amazon Redshift	com.amazonaws. <i>region</i> .redshift data
	com.amazonaws. <i>region</i> .redshift-data-fips
Amazon Rekognition	com.amazonaws. <i>region</i> .reconnaissance
	com.amazonaws. <i>region</i> .conseils de reconnaissance
	com.amazonaws. <i>region</i> .streaming - reconnaissance
	com.amazonaws. <i>region</i> .streaming-rekognition-tips
AWS Resource Access Manager	com.amazonaws. <i>region</i> .ram
	com.amazonaws. <i>region</i> .ram-fips
Explorateur de ressources AWS	com.amazonaws. <i>region</i> .explorateur-de-ressource-2
	com.amazonaws. <i>region</i> .resource-explorer-2-fips
Groupes de ressources AWS	com.amazonaws. <i>region</i> .groupes-ressources

Service AWS	Nom du service
	com.amazonaws. <i>region</i> .ressource-groups-fips
AWS Resource Groups Tagging API	com.amazonaws. <i>region</i> .balisage
Amazon S3	com.amazonaws. <i>region</i> .s3
	com.amazonaws. <i>region</i> .s3-fips
	com.amazonaws. <i>region</i> tableaux .s3
Points d' Multi-Region accès Amazon S3	com.amazonaws.s3-global.accesspoint
Amazon S3 sur Outposts	com.amazonaws. <i>region</i> .s3-avant-postes
Amazon SageMaker AI	aws.sagemaker. <i>region</i> .expériences
	aws.sagemaker. <i>region</i> .bloc-notes
	aws.sagemaker. <i>region</i> .app-partenaire
	aws.sagemaker. <i>region</i> .studio
	com.amazonaws. <i>region</i> .sagemaker-assistant-des-sciences des données
	com.amazonaws. <i>region</i> .sagemaker.api
	com.amazonaws. <i>region</i> .sagemaker.api-fips
	com.amazonaws. <i>region</i> .sagemaker.featurestore-runtime
	com.amazonaws. <i>region</i> .sagemaker.featurestore-astuces d'exécution
	com.amazonaws. <i>region</i> .sagemaker.metrics
	com.amazonaws. <i>region</i> .sagemaker.runtime

Service AWS	Nom du service
	com.amazonaws. <i>region</i> .sagemaker.astuces d'exécution
Savings Plans	com.amazonaws.savingsplans
AWS Secrets Manager	com.amazonaws. <i>region</i> . gestionnaire de secrets
AWS Agent de sécurité	com.amazonaws. <i>region</i> .agent de sécurité
AWS Security Hub CSPM	com.amazonaws. <i>region</i> .hub de sécurité
	com.amazonaws. <i>region</i> .securityhub-fips
Amazon Security Lake	com.amazonaws. <i>region</i> . lac de sécurité
	com.amazonaws. <i>region</i> .securitylake-fips
AWS Security Token Service	com.amazonaws. <i>region</i> .sts
	com.amazonaws. <i>region</i> .sts-fips
AWS Serverless Application Repository	com.amazonaws. <i>region</i> .dépôt sans serveur
Service Catalog	com.amazonaws. <i>region</i> .catalogue de services
	com.amazonaws. <i>region</i> .servicecatalog-app registry
Service Quotas	com.amazonaws. <i>region</i> . quotas de service
Amazon SES	com.amazonaws. <i>region</i> .courriel-smtp
	com.amazonaws. <i>region</i> .gestionnaire de courrier
	com.amazonaws. <i>region</i> .mail-manager-fips
	com.amazonaws. <i>region</i> .mail-manager-smtp.auth.fips
	com.amazonaws. <i>region</i> .mail-manager-smtp.open.fips

Service AWS	Nom du service
AWS Snowball Edge Device Management	com.amazonaws. <i>region</i> .snow-device-management
Amazon SNS	com.amazonaws. <i>region</i> .sns
Amazon SQS	com.amazonaws. <i>region</i> .sqs
	com.amazonaws. <i>region</i> .sqs-fips
Amazon SWF	com.amazonaws. <i>region</i> .swf
	com.amazonaws. <i>region</i> .swf-fips
AWS Step Functions	com.amazonaws. <i>region</i> .états
	com.amazonaws. <i>region</i> .états de synchronisation
AWS Storage Gateway	com.amazonaws. <i>region</i> . passerelle de stockage
AWS Supply Chain	com.amazonaws. <i>region</i> .scn
AWS Systems Manager	com.amazonaws. <i>region</i> Messages .ec2
	com.amazonaws. <i>region</i> .ssm
	com.amazonaws. <i>region</i> .ssm-contacts
	com.amazonaws. <i>region</i> .ssm-incidents
	com.amazonaws. <i>region</i> .ssm-incidents-tips
	com.amazonaws. <i>region</i> Configuration rapide du fichier .ssm
	com.amazonaws. <i>region</i> Messages .sms
Gestionnaire de systèmes AWS pour SAP	com.amazonaws. <i>region</i> .ssm-sap
	com.amazonaws. <i>region</i> .ssm-sap-fips

Service AWS	Nom du service
AWS Constructeur de réseaux de télécommunications	com.amazonaws. <i>region</i> .tnb
Amazon Textract	com.amazonaws. <i>region</i> . extrait
	com.amazonaws. <i>region</i> .textract-fips
Amazon Timestream	com.amazonaws. <i>region</i> .timestream.ingest- <i>cell</i>
	com.amazonaws. <i>region</i> .timestream.query- <i>cell</i>
Amazon Timestream pour InfluxDB	com.amazonaws. <i>region</i> .timestream-influxdb
	com.amazonaws. <i>region</i> .timestream-influxdb-fips
Amazon Transcribe	com.amazonaws. <i>region</i> .transcrire
	com.amazonaws. <i>region</i> .transcrire des fips
	com.amazonaws. <i>region</i> . transcrire en streaming
com.amazonaws. <i>region</i> .transcrire les fips en streaming	
Amazon Transcribe Medical	com.amazonaws. <i>region</i> .transcrire
	com.amazonaws. <i>region</i> . transcrire en streaming
AWS Transfer Family	com.amazonaws. <i>region</i> .transfert
AWS Transform	com.amazonaws. <i>region</i> .transformer
AWS Transform personnalisé	com.amazonaws. <i>region</i> .transform-personnalisé
Amazon Translate	com.amazonaws. <i>region</i> .traduire
AWS Trusted Advisor	com.amazonaws. <i>region</i> . conseiller de confiance
Notifications des utilisateurs AWS	com.amazonaws. <i>region</i> . notifications

Service AWS	Nom du service
	com.amazonaws. <i>region</i> .notifications/contacts
Amazon Verified Permissions	com.amazonaws. <i>region</i> . autorisations vérifiées
	com.amazonaws. <i>region</i> . autorisations vérifiées - fips
Amazon VPC Lattice	com.amazonaws. <i>region</i> Réseau .vpc
AWS WAFV2	com.amazonaws. <i>region</i> .wafv2
	com.amazonaws. <i>region</i> .wafv2-fips
AWS Well-Architected Tool	com.amazonaws. <i>region</i> . bien architecturé
Amazon WorkMail	com.amazonaws. <i>region</i> .workmail
	com.amazonaws. <i>region</i> flux de messages .workmail
Amazon WorkSpaces	com.amazonaws. <i>region</i> .espaces de travail
Navigateur Amazon WorkSpaces Secure	com.amazonaws. <i>region</i> .espaces-de-travail-web
	com.amazonaws. <i>region</i> .workspaces-web-fips
WorkSpaces streaming	com.amazonaws. <i>region</i> . highlander
Client WorkSpaces léger Amazon	com.amazonaws. <i>region</i> .thinclient.api
aws.api. <i>region</i> fichiers .s3	
aws.api. <i>region</i> Fichiers .s3 - fips	
AWS X-Ray	com.amazonaws. <i>region</i> .xray
Service géré Amazon pour Apache Flink	com.amazonaws. <i>region</i> .kinesis analytics
	com.amazonaws. <i>region</i> .kinesisanalytics-fips

Afficher disponible Service AWS names

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

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

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

Voici un exemple de sortie. La sortie complète n'est pas affichée.

```
[
  "api.aws.us-east-1.cassandra-streams",
  "aws.api.us-east-1.bcm-data-exports",
  "aws.api.us-east-1.emr-service-cell01",
  "aws.api.us-east-1.freetier",
  "aws.api.us-east-1.kendra-ranking",
  "aws.api.us-east-1.qbusiness",
  . . .
  "com.amazonaws.us-east-1.xray"
]
```

Afficher les informations sur un service

Une fois que vous avez le nom du service, vous pouvez utiliser la commande [describe-vpc-endpoint-services](#) pour afficher des informations détaillées sur chaque service de point de terminaison.

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

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

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

```
{
  "ServiceDetails": [
    {
      "ServiceName": "com.amazonaws.us-east-1.monitoring",
      "ServiceId": "vpce-svc-0fc975f3e7e5beba4",
      "ServiceType": [
        {
          "ServiceType": "Interface"
        }
      ],
      "AvailabilityZones": [
        "us-east-1a",
        "us-east-1b",
        "us-east-1c",
        "us-east-1d",
        "us-east-1e",
        "us-east-1f"
      ],
      "Owner": "amazon",
      "BaseEndpointDnsNames": [
        "monitoring.us-east-1.vpce.amazonaws.com"
      ],
      "PrivateDnsName": "monitoring.us-east-1.amazonaws.com",
      "PrivateDnsNames": [
        {
          "PrivateDnsName": "monitoring.us-east-1.amazonaws.com"
        },
        {
          "PrivateDnsName": "monitoring.us-east-1.api.aws"
        },
        {
          "PrivateDnsName": "monitoring-fips.us-east-1.amazonaws.com"
        },
        {
          "PrivateDnsName": "monitoring-fips.us-east-1.api.aws"
        }
      ],
      "VpcEndpointPolicySupported": true,
      "AcceptanceRequired": false,
      "ManagesVpcEndpoints": false,
      "Tags": [],
      "PrivateDnsNameVerificationState": "verified",
      "SupportedIpAddressTypes": [
        "ipv6",
```

```
        "ipv4"  
      ]  
    },  
    "ServiceNames": [  
      "com.amazonaws.us-east-1.monitoring"  
    ]  
  }  
}
```

Afficher la prise en charge de stratégie de point de terminaison

Pour vérifier si un service prend en charge [les stratégies de point de terminaison](#), appelez la commande [describe-vpc-endpoint-services](#) et vérifiez la valeur de `VpcEndpointPolicySupported`. Les valeurs possibles sont `true` et `false`.

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

```
aws ec2 describe-vpc-endpoint-services \  
  --service-name "com.amazonaws.us-east-1.s3" \  
  --region us-east-1 \  
  --query ServiceDetails[*].VpcEndpointPolicySupported \  
  --output text
```

Voici un exemple de sortie.

```
True
```

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

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

Voici un exemple de sortie. La sortie complète n'est pas affichée.

```
[
  "api.aws.us-east-1.cassandra-streams",
  "aws.api.us-east-1.bcm-data-exports",
  "aws.api.us-east-1.emr-service-cell01",
  "aws.api.us-east-1.freetier",
  "aws.api.us-east-1.kendra-ranking",
  . . .
  "com.amazonaws.us-east-1.xray"
]
```

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

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

Voici un exemple de sortie. La sortie complète n'est pas affichée.

```
[
  "com.amazonaws.us-east-1.appmesh-envoy-management",
  "com.amazonaws.us-east-1.apprunner.requests",
  "com.amazonaws.us-east-1.appstream.api",
  "com.amazonaws.us-east-1.appstream.streaming",
  "com.amazonaws.us-east-1.awsconnector",
  . . .
]
```

Afficher la prise charge d'IPv6

Pour consulter la prise en charge d'IPv6 pour les AWS services, consultez les [AWS services qui prennent en charge IPv6](#). Vous pouvez également utiliser la [commande](#) `describe-vpc-endpoint-services` suivante pour afficher les informations Services AWS auxquelles vous pouvez accéder via IPv6 dans la région spécifiée. L'option `--query` limite la sortie aux noms de services.

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

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

Voici un exemple de sortie. La sortie complète n'est pas affichée.

```
[
  "api.aws.us-east-1.cassandra-streams",
  "aws.api.us-east-1.bcm-data-exports",
  "aws.api.us-east-1.freetier",
  "aws.api.us-east-1.kendra-ranking",
  "aws.api.us-east-1.qbusiness",
  "aws.api.us-east-1.resource-explorer-2",
  "aws.api.us-east-1.resource-explorer-2-fips",
  "aws.sagemaker.us-east-1.experiments",
  "aws.sagemaker.us-east-1.partner-app",
  "com.amazonaws.iam",
  "com.amazonaws.us-east-1.access-analyzer",
  "com.amazonaws.us-east-1.account",
  . . .
  "com.amazonaws.us-east-1.xray"
]
```

Cross-region enabled Services AWS

Les éléments suivants Services AWS s'intègrent à l'ensemble des régions AWS PrivateLink. Vous pouvez créer un point de terminaison d'interface pour vous connecter à ces services dans une autre AWS région, en privé, comme s'ils s'exécutaient dans votre propre VPC.

Cliquez sur le lien dans la Service AWS colonne pour consulter la documentation du service. La colonne Nom du service contient le nom du service que vous spécifiez lorsque vous créez le point de terminaison de l'interface.

Service AWS	Nom du service
Amazon S3	com.amazonaws. <i>region</i> .s3
Gestion des identités et des accès AWS (IAM)	com.amazonaws.iam

Service AWS	Nom du service
Amazon ECR	com.amazonaws. <i>region</i> .ecr.api
	com.amazonaws. <i>region</i> .ecr.dkr
AWS Key Management Service	com.amazonaws. <i>region</i> .km
	com.amazonaws. <i>region</i> .kms-fips
Amazon ECS	com.amazonaws. <i>region</i> .ecs
AWS Lambda	com.amazonaws. <i>region</i> .lambda
Amazon Data Firehose	com.amazonaws. <i>region</i> .kinesis-firehose
Service géré Amazon pour Apache Flink	com.amazonaws. <i>region</i> .kinesis analytics
	com.amazonaws. <i>region</i> .kinesisanalytics-fips
Amazon Route 53	com.amazonaws.route53

Afficher disponible Service AWS names

Vous pouvez utiliser la commande [describe-vpc-endpoint-services](#) pour afficher les services activés entre régions.

L'exemple suivant montre Services AWS ce à quoi un utilisateur de la us-east-1 Région peut accéder via les points de terminaison de l'interface, à la Région de service spécifiée (us-west-2). L'option `--query` limite la sortie aux noms de services.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --service-region us-west-2 \
  --query ServiceNames
```

Voici un exemple de sortie. La sortie complète n'est pas affichée.

```
[
```

```
"com.amazonaws.us-west-2.ecr.api",  
"com.amazonaws.us-west-2.ecr.dkr",  
"com.amazonaws.us-west-2.ecs",  
"com.amazonaws.us-west-2.ecs-fips",  
...  
"com.amazonaws.us-west-2.s3"
```

```
]
```

Note

Vous devez utiliser un DNS régional. Le DNS zonal n'est pas pris en charge lors de l'accès Services AWS dans une autre région. Pour plus d'informations, consultez [Afficher et mettre à jour les attributs DNS](#) dans le guide de l'utilisateur Amazon VPC.

Autorisations et considérations

- Par défaut, les entités IAM ne sont pas autorisées à accéder à une entité située Service AWS dans une autre région. Pour accorder les autorisations requises pour l'accès entre régions, un administrateur IAM peut créer des politiques IAM qui autorisent l'action uniquement avec `vpce:AllowMultiRegion` autorisation.
- Assurez-vous que votre politique de contrôle des services (SCP) ne refuse pas les actions nécessitant uniquement des `vpce:AllowMultiRegion` autorisations. Pour utiliser AWS PrivateLink la fonctionnalité de connectivité interrégionale, votre politique d'identité et votre SCP doivent autoriser cette action.
- Pour contrôler les régions qu'une entité IAM peut spécifier en tant que région de service lors de la création d'un point de terminaison VPC, utilisez la clé de `ec2:VpceServiceRegion` condition.
- Un consommateur de services doit accéder à une région optionnelle avant de la sélectionner comme région de service pour un point de terminaison. Dans la mesure du possible, nous recommandons aux consommateurs de services d'accéder à un service en utilisant la connectivité intra-régionale plutôt que la connectivité interrégionale. Intra-Region la connectivité permet de réduire la latence et les coûts.
- Vous pouvez utiliser la nouvelle clé de condition `aws:SourceVpcArn` globale d'IAM pour sécuriser les régions Comptes AWS et les VPC depuis lesquels vos ressources sont accessibles. Cette clé permet de mettre en œuvre la résidence des données et le contrôle d'accès basé sur la région.

- Pour une haute disponibilité, créez un point de terminaison d'interface multirégional dans au moins deux zones de disponibilité. Dans ce cas, les fournisseurs et les consommateurs ne sont pas tenus d'utiliser les mêmes zones de disponibilité.
- Avec un accès interrégional, AWS PrivateLink gère le basculement entre les zones de disponibilité dans les régions de service et de consommation. Il ne gère pas le basculement entre les régions.
- L'accès interrégional n'est pas pris en charge pour les zones de disponibilité suivantes : use1-az3, usw1-az2, apne1-az3, apne2-az2, et apne2-az4.
- Vous pouvez l'utiliser AWS Fault Injection Service pour simuler des événements régionaux et modéliser des scénarios de défaillance pour les points de terminaison d'interface activés au sein et entre les régions. Pour en savoir plus, consultez [AWS FIS la documentation](#).

Créez un point de terminaison d'interface vers un Service AWS dans une autre région

Pour créer un point de terminaison d'interface à l'aide de la console, consultez la [section](#) Créer un point de terminaison VPC.

Dans la CLI, vous pouvez utiliser la [commande](#) `create-vpc-endpoint` pour créer un point de terminaison VPC vers un Service AWS autre région. L'exemple suivant crée un point de terminaison d'interface vers Amazon S3 us-west-2 depuis un VPC. us-east-1

```
aws ec2 create-vpc-endpoint \  
  --vpc-id vpc-id \  
  --service-name com.amazonaws.us-west-2.s3 \  
  --vpc-endpoint-type Interface \  
  --subnet-ids subnet-id-1 subnet-id-2 \  
  --region us-east-1 \  
  --service-region us-west-2
```

Accédez à Service AWS à l'aide d'un point de terminaison VPC d'interface

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

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

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

Table des matières

- [Conditions préalables](#)
- [Création d'un point de terminaison de VPC](#)
- [Sous-réseaux partagés](#)
- [ICMP](#)

Conditions préalables

- Déployez les ressources qui y accéderont Service AWS dans votre VPC.
- Pour utiliser le système DNS privé, vous devez activer les noms d'hôte DNS et la résolution DNS pour votre VPC. Pour plus d'informations, voir [Affichage et mise à jour des attributs DNS](#) dans le Guide de l'utilisateur Amazon VPC.
- Pour activer IPv6 pour un point de terminaison d'interface, celui-ci Service AWS doit prendre en charge l'accès via IPv6. Pour plus d'informations, consultez [the section called "Types d'adresses IP"](#).
- Créez un groupe de sécurité pour l'interface réseau des terminaux qui autorise le trafic attendu en provenance des ressources de votre VPC. Par exemple, pour s'assurer qu'il AWS CLI peut envoyer des requêtes HTTPS au Service AWS, le groupe de sécurité doit autoriser le trafic HTTPS entrant.
- Si vos ressources se trouvent dans un sous-réseau doté d'une ACL réseau, vérifiez que celle-ci autorise le trafic entre les ressources de votre VPC et les interfaces réseau des terminaux.
- Vos AWS PrivateLink ressources sont soumises à des quotas. Pour plus d'informations, consultez [AWS PrivateLink quotas](#).

Création d'un point de terminaison de VPC

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

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

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Dans Type, sélectionnez Services AWS .
5. (Facultatif) Si vous créez un point de terminaison vers un point de terminaison situé Service AWS dans une autre région, cochez la case Activer le point de terminaison interrégional, puis sélectionnez la région de service dans la liste déroulante.
6. Pour Service name (Nom du service), sélectionnez le service. Pour plus d'informations, consultez [the section called "Services qui s'intègrent"](#).
7. Pour VPC, sélectionnez le VPC à partir duquel vous allez accéder au Service AWS.
8. Si, à l'étape 5, vous avez sélectionné le nom de service pour Amazon S3 et si vous souhaitez configurer la [prise en charge du DNS privé](#), sélectionnez Paramètres supplémentaires, Activer le nom DNS. Lorsque vous effectuez cette sélection, elle sélectionne également automatiquement Activer le DNS privé uniquement pour un point de terminaison entrant. Vous pouvez configurer un DNS privé avec un point de terminaison Resolver entrant uniquement pour les points de terminaison d'interface pour Amazon S3. Si vous ne disposez pas d'un point de terminaison de passerelle pour Amazon S3 et que vous sélectionnez Activer le DNS privé uniquement pour le point de terminaison entrant, vous recevrez un message d'erreur lorsque vous tenterez la dernière étape de cette procédure.

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

9. Pour Sous-réseaux, sélectionnez les sous-réseaux dans lesquels vous souhaitez créer des interfaces réseau de terminaux. Vous pouvez sélectionner un sous-réseau par zone de disponibilité. Il n'est pas possible de sélectionner plusieurs sous-réseaux dans la même zone de

disponibilité. Pour plus d'informations, consultez [the section called "Sous-réseaux et zones de disponibilité"](#).

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

10. Pour IP address type (Type d'adresse IP), choisissez l'une des options suivantes :
 - IPv4 — Attribuez des adresses IPv4 aux interfaces réseau des terminaux. Cette option est prise en charge uniquement si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4 et que le service accepte les requêtes IPv4.
 - IPv6 — Attribuez des adresses IPv6 aux interfaces réseau des terminaux. Cette option est prise en charge uniquement si tous les sous-réseaux sélectionnés sont des sous-réseaux IPv6 et que le service accepte les requêtes IPv6.
 - Dualstack : attribuez des adresses IPv4 et IPv6 aux interfaces réseau des terminaux. Cette option est prise en charge uniquement si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4 et IPv6 et que le service accepte les requêtes IPv4 et IPv6.
11. Pour Security groups (Groupes de sécurité), sélectionnez les groupes de sécurité à associer aux interfaces réseau du point de terminaison. Par défaut, nous associons le groupe de sécurité par défaut pour le VPC.
12. Dans Politique, pour autoriser toutes les opérations effectuées par tous les principaux sur toutes les ressources via le point de terminaison de l'interface, sélectionnez Accès complet. Pour restreindre l'accès, sélectionnez Personnalisé et entrez une politique. Cette option n'est disponible que si le service prend en charge les politiques de points de terminaison de VPC. Pour plus d'informations, consultez [Politiques de point de terminaison](#).
13. (Facultatif) Pour ajouter une balise, choisissez Ajouter une nouvelle balise et entrez la clé et la valeur de la balise.
14. Choisissez Créer un point de terminaison.

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

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

Sous-réseaux partagés

Vous ne pouvez pas créer, décrire, modifier ou supprimer des points de terminaison d'un VPC dans des sous-réseaux qui sont partagés avec vous. Les points de terminaison VPC gérés par un AWS service (points de terminaison VPC gérés par un service) peuvent être créés par le service dans un sous-réseau partagé.

ICMP

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

Configuration d'un point de terminaison d'interface

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

Tâches

- [Ajouter ou supprimer des sous-réseaux](#)
- [Association de groupes de sécurité](#)
- [Pour modifier la politique de point de terminaison de VPC](#)
- [Activation de noms DNS privés](#)
- [Gestion des balises](#)

Ajouter ou supprimer des sous-réseaux

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

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

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

3. Sélectionnez le point de terminaison d'interface.
4. Choisissez Actions, Manage subnets (Gérer les sous-réseaux).
5. Sélectionnez ou désélectionnez les zones de disponibilité selon vos besoins. Pour chaque zone de disponibilité, sélectionnez un sous-réseau. Par défaut, nous sélectionnons les adresses IP dans les plages d'adresses IP des sous-réseaux et les attribuons aux interfaces réseau des points de terminaison. Pour choisir les adresses IP d'une interface réseau de point de terminaison, sélectionnez Designate IP addresses et entrez une adresse IPv4 à partir de la plage d'adresses de sous-réseau. Si le service de point de terminaison prend en charge le protocole IPv6, vous pouvez également saisir une adresse IPv6 à partir de la plage d'adresses de sous-réseau.

Si vous spécifiez une adresse IP pour un sous-réseau qui possède déjà une interface réseau de point de terminaison pour ce point de terminaison d'un VPC, nous remplaçons l'interface réseau de point de terminaison par une nouvelle. Ce processus déconnecte temporairement le sous-réseau et le point de terminaison d'un VPC.

6. Choisissez Modify subnets (Modifier les sous-réseaux).

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

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

Association de groupes de sécurité

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

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

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison d'interface.
4. Choisissez Actions, Gérer les groupes de sécurité.
5. Activez ou désactivez des groupes de sécurité si nécessaire.

6. Choisissez Modify security groups (Modifier les groupes de sécurité).

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

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

Pour modifier la politique de point de terminaison de VPC

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

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

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

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

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

Activation de noms DNS privés

Nous vous recommandons d'activer des noms d'hôtes DNS privés pour votre point de terminaison de VPC pour les Services AWS. Cela garantit que les demandes qui utilisent les points de terminaison du service public, telles que les demandes effectuées via un AWS SDK, sont résolues vers votre point de terminaison VPC.

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

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

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

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

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

Gestion des balises

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

Pour gérer les balises à l'aide de la console

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

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

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

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

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

Tâches

- [Création d'une notification SNS](#)
- [Ajout d'une stratégie d'accès](#)
- [Ajout d'une stratégie de clé](#)

Création d'une notification SNS

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

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

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

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

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

Ajout d'une stratégie d'accès

Ajoutez une politique d'accès à la rubrique Amazon SNS qui permet AWS PrivateLink de publier des notifications en votre nom, comme les suivantes. Pour plus d'informations, voir [Comment modifier la stratégie d'accès à ma rubrique Amazon SNS ?](#) Utilisez les clés de condition globale `aws:SourceArn` et `aws:SourceAccount` pour vous protéger contre le [problème du député confus](#).

JSON

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

```

```

    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-east-1:111111111111:topic-name",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint/endpoint-id"
        },
        "StringEquals": {
          "aws:SourceAccount": "111111111111"
        }
      }
    }
  ]
}

```

Ajout d'une stratégie de clé

Si vous utilisez des rubriques SNS chiffrées, la politique de ressources pour la clé KMS doit être fiable AWS PrivateLink pour appeler les opérations d' AWS KMS API. Voici un exemple de stratégie de clé.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:us-east-1:111111111111:key/key-id",
    }
  ]
}

```

```

        "Condition": {
            "ArnLike": {
                "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint/endpoint-id"
            },
            "StringEquals": {
                "aws:SourceAccount": "111111111111"
            }
        }
    }
}
]
}

```

Suppression d'un point de terminaison d'interface

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

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

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

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

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

Points de terminaison de passerelle

Les points de terminaison d'un VPC de passerelle fournissent une connectivité fiable à Amazon S3 et DynamoDB sans nécessiter de passerelle Internet ou d'appareil NAT pour votre VPC. Contrairement

aux autres types de points de terminaison VPC AWS PrivateLink, les points de terminaison Gateway ne sont pas utilisés.

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

- [Types de points de terminaison VPC pour Amazon S3](#)
- [Types de points de terminaison VPC pour Amazon DynamoDB](#)

Tarification

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

Table des matières

- [Présentation de](#)
- [Routage](#)
- [Sécurité](#)
- [Type d'adresse IP](#)
- [Type d'adresse IP de l'enregistrement DNS](#)
- [Points de terminaison de passerelle pour Amazon S3](#)
- [Points de terminaison de passerelle pour Amazon DynamoDB](#)

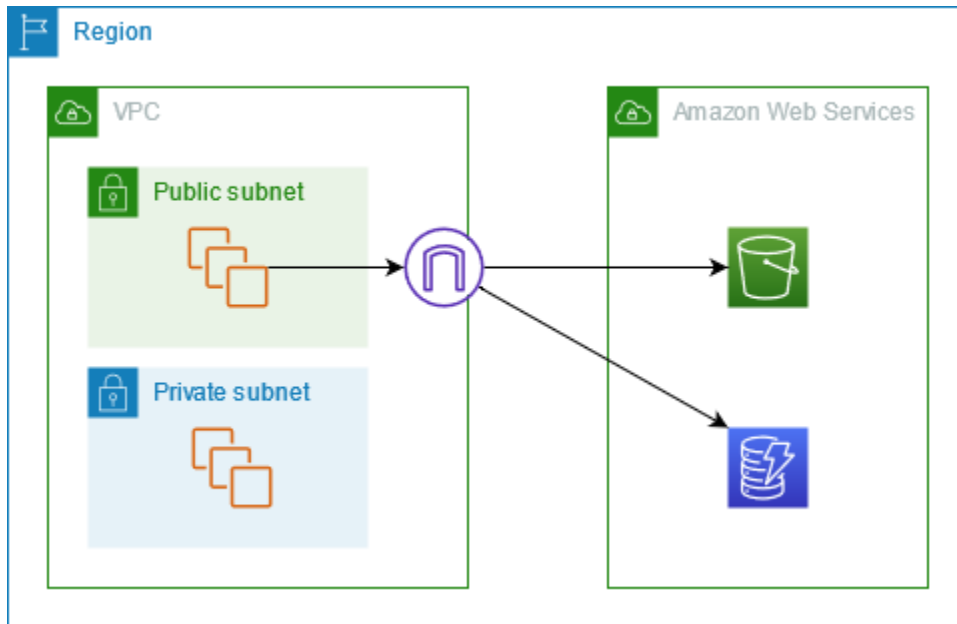
Présentation de

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

Accès via une passerelle Internet

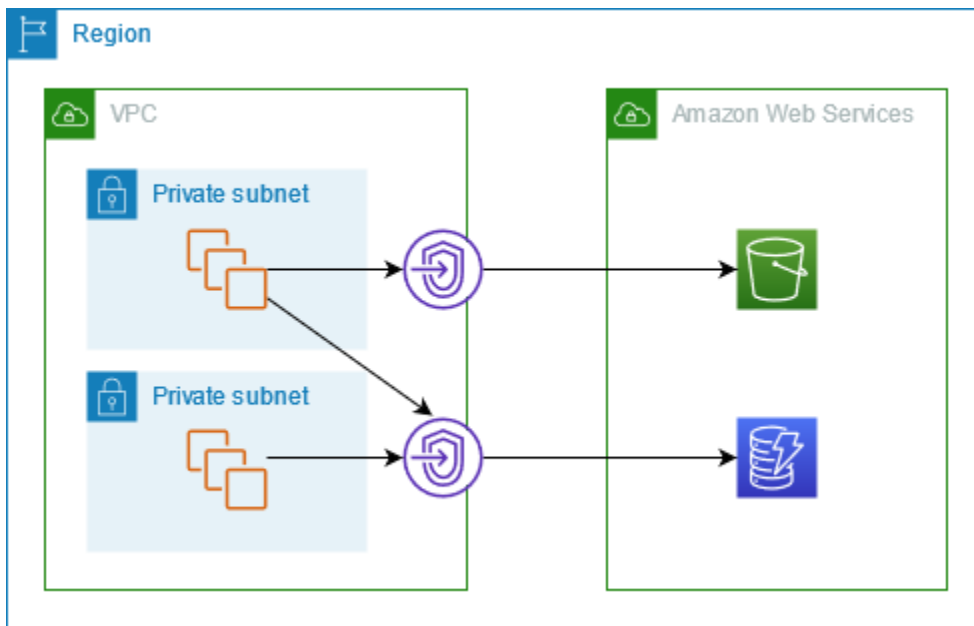
Le schéma suivant montre comment les instances accèdent à Amazon S3 et DynamoDB via leurs points de terminaison de service public. Le trafic vers Amazon S3 ou DynamoDB à partir d'une instance d'un sous-réseau public est acheminé vers la passerelle Internet du VPC, puis vers le service. Les instances d'un sous-réseau privé ne peuvent pas envoyer de trafic vers Amazon S3 ou DynamoDB, car par définition les sous-réseaux privés ne disposent pas d'itinéraires vers une

passerelle Internet. Pour permettre aux instances du sous-réseau privé d'envoyer du trafic vers Amazon S3 ou DynamoDB, vous devez ajouter un appareil NAT au sous-réseau public et acheminer le trafic du sous-réseau privé vers l'appareil NAT. Lorsque le trafic vers Amazon S3 ou DynamoDB passe par la passerelle Internet, il ne quitte pas le réseau. AWS



Accès via un point de terminaison de passerelle

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



Routage

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

Destination	Cible
<i>prefix_list_id</i>	<i>gateway_endpoint_id</i>

Considérations

- Vous pouvez consulter les itinéraires de point de terminaison que nous ajoutons à votre table de routage, mais vous ne pouvez pas les modifier ni les supprimer. Pour ajouter un itinéraire de point de terminaison à une table de routage, associez-le au point de terminaison de passerelle. Nous supprimons l'itinéraire du point de terminaison lorsque vous dissociez la table de routage du point de terminaison de passerelle ou lorsque vous supprimez le point de terminaison de passerelle.
- Toutes les instances des sous-réseaux associés à une table de routage associée à un point de terminaison de passerelle utilisent automatiquement le point de terminaison de passerelle pour accéder au service. Les instances des sous-réseaux qui ne sont pas associées à ces tables de

routage utilisent le point de terminaison du service public, et non le point de terminaison de la passerelle.

- Une table de routage peut avoir à la fois un itinéraire de point de terminaison vers Amazon S3 et un itinéraire de point de terminaison vers DynamoDB. Vous pouvez avoir des itinéraires de points de terminaison vers le même service (Amazon S3 ou DynamoDB) dans plusieurs tables de routage. Vous ne pouvez pas avoir plusieurs itinéraires de point de terminaison vers le même service (Amazon S3 ou DynamoDB) dans une seule table de routage.
- Nous utilisons la route la plus spécifique qui correspond au trafic afin de déterminer comment router le trafic (correspondance de préfixe le plus long). Pour les tables de routage avec un itinéraire de point de terminaison, cela signifie ce qui suit :
 - S'il existe un itinéraire qui envoie tout le trafic Internet (0.0.0. 0/0) vers une passerelle Internet, l'itinéraire du point de terminaison est prioritaire pour le trafic destiné au service (Amazon S3 ou DynamoDB) dans la région actuelle. Le trafic destiné à un autre Service AWS utilise la passerelle Internet.
 - Le trafic destiné au service (Amazon S3 ou DynamoDB) dans une autre région est dirigé vers la passerelle Internet, car les listes de préfixes sont spécifiques à une Région.
 - S'il existe un itinéraire qui spécifie la plage d'adresses IP exacte du service (Amazon S3 ou DynamoDB) dans la même Région, cet itinéraire a la priorité sur l'itinéraire du point de terminaison.

Sécurité

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

Destination	Protocole	Plage de ports
<i>prefix_list_id</i>	TCP	443

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

Destination	Protocole	Plage de ports
<i>service_cidr_block_1</i>	TCP	443
<i>service_cidr_block_2</i>	TCP	443
<i>service_cidr_block_3</i>	TCP	443

Type d'adresse IP

Le type d'adresse IP détermine la liste de préfixes associée à votre table de routage.

Conditions requises pour activer IPv6 pour un point de terminaison de passerelle

- Le type d'adresse IP d'un point de terminaison de passerelle doit être compatible avec les sous-réseaux du point de terminaison de passerelle, comme décrit ici :
 - IPv4 — Ajoutez la liste des préfixes IPv4 du service à votre table de routage.
 - IPv6 : ajoutez la liste des préfixes IPv6 du service à votre table de routage. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés sont des sous-réseaux IPv6 uniquement.
 - Dualstack : ajoutez la liste des préfixes IPv4 du service à votre table de routage et ajoutez la liste des préfixes IPv6 du service à votre table de routage. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4 et IPv6.

Type d'adresse IP de l'enregistrement DNS

Par défaut, un point de terminaison de passerelle renvoie des enregistrements DNS en fonction du point de terminaison de service que vous appelez. Si vous créez votre point de terminaison de passerelle à l'aide du point de terminaison du service `IPv4s3.us-east-2.amazonaws.com`, par exemple, Amazon S3 renvoie des enregistrements A à vos clients et tous les sous-réseaux de votre table de routage utilisent IPv4.

En revanche, si vous créez votre point de terminaison de passerelle à l'aide du point de terminaison de service Dualstack, par exemples `s3.dualstack.us-east-2.amazonaws.com`, Amazon S3 renvoie à la fois des enregistrements A et AAAA à vos clients, et les sous-réseaux de votre table de routage utilisent IPv4 et IPv6.

 Note

Pour les compartiments de répertoires ou S3 Express One Zone, les points de terminaison de la passerelle pour le plan de données seraient respectivement `s3express-use2-az1.us-east-2.amazonaws.com` et `s3express-use2-az1.dualstack.us-east-2.amazonaws.com`.

Le type d'adresse IP de l'enregistrement DNS influe sur la façon dont le trafic est acheminé vers vos clients. Si vous créez un point de terminaison de passerelle à l'aide du point de terminaison du service IPv4, puis que vous appelez le point de terminaison du service Dualstack, le trafic qui utilise des enregistrements AAAA ne sera pas acheminé via le point de terminaison de la passerelle. Le trafic sera interrompu ou acheminé sur un IPv6-compatible chemin s'il y en a un. Si vous utilisez un type d'adresse IP d'enregistrement DNS défini par un service, assurez-vous que votre service peut gérer des appels variables provenant de plusieurs points de terminaison de service.

Au lieu de définir le type d'adresse IP d'enregistrement DNS par défaut [comme défini par le service](#), vous pouvez personnaliser le type d'adresse IP de l'enregistrement DNS pour choisir les enregistrements renvoyés pour un point de terminaison spécifique. Le tableau suivant indique les types d'adresses IP d'enregistrement DNS pris en charge et les types d'enregistrements renvoyés :

Type d'adresse IP de l'enregistrement DNS	Types d'enregistrements renvoyés
IPv4	A
IPv6	AAAA
Double pile	A et AAAA
défini par le service	Les enregistrements dépendent du point de terminaison du service

Pour choisir un type d'adresse IP d'enregistrement DNS, vous devez utiliser un type d'adresse IP compatible pour le service Endpoint. Le tableau suivant indique le type d'adresse IP d'enregistrement DNS pris en charge pour chaque type d'adresse IP pour les points de terminaison de passerelle :

Type d'adresse IP	Types d'adresses IP d'enregistrement DNS pris en charge
IPv4	IPv4, défini par le service*
IPv6	IPv6, défini par le service*
Double pile	IPv4, IPv6, Dualstack, défini par le service*

* Représente le type d'adresse IP d'enregistrement DNS par défaut.

 Note

Pour utiliser des types d'adresses IP d'enregistrement DNS autres que ceux définis par le service pour votre point de terminaison Gateway, vous devez autoriser `enableDnsSupport` et attribuer des `enableDnsHostnames` attributs dans les paramètres de votre VPC.

Vous ne pouvez pas modifier le type d'adresse IP d'enregistrement DNS pour un point de terminaison de passerelle DynamoDB. DynamoDB prend uniquement en charge le type d'adresse IP d'enregistrement DNS défini par le service.

Le comportement du type d'adresse IP des enregistrements DNS est différent pour les points de terminaison de l'interface. Pour plus d'informations, consultez la section [Type d'adresse IP d'enregistrement DNS pour les points de terminaison](#) de l'interface.

Points de terminaison de passerelle pour Amazon S3

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

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

Amazon S3 prend en charge les points de terminaison de passerelle et les points de terminaison d'interface. Avec un point de terminaison d'une passerelle, vous pouvez accéder à Amazon S3 à partir de votre VPC sans avoir besoin d'une passerelle Internet ou d'un périphérique NAT pour votre VPC et sans frais supplémentaires. Cependant, les points de terminaison de passerelle

n'autorisent pas l'accès depuis des réseaux locaux, depuis des VPC homologues dans d'autres AWS régions ou via une passerelle de transit. Pour ces scénarios, vous devez utiliser un point de terminaison d'interface qui est disponible moyennant des frais supplémentaires. Pour de plus amples informations, veuillez consulter [Types de points de terminaison d'un VPC pour Amazon S3](#) dans le Guide de l'utilisateur Amazon S3.

Table des matières

- [Considérations](#)
- [DNS privé](#)
- [Créer un point de terminaison de passerelle](#)
- [Contrôle de l'accès à l'aide de politiques de compartiment](#)
- [Association de tables de routage](#)
- [Pour modifier la politique de point de terminaison de VPC](#)
- [Suppression d'un point de terminaison de passerelle](#)

Considérations

- Le point de terminaison de passerelle est disponible uniquement dans la Région où vous l'avez créé. Veillez à créer votre point de terminaison de passerelle dans la même Région que vos compartiments S3.
- Si vous utilisez les serveurs DNS d'Amazon, vous devez activer à la fois [les noms d'hôte DNS et la résolution DNS](#) pour votre VPC. Si vous utilisez votre propre serveur DNS, assurez-vous que les requêtes vers Amazon S3 se résolvent correctement en adresses IP gérées par AWS.
- Les règles des groupes de sécurité pour les instances qui accèdent à Amazon S3 par le point de terminaison de passerelle doivent autoriser le trafic en provenance et à destination d'Amazon S3. Vous pouvez faire référence à l'ID de la [liste de préfixes](#) pour Amazon S3 dans les règles du groupe de sécurité.
- L'ACL réseau du sous-réseau pour vos instances qui accèdent à Amazon S3 par le point de terminaison de passerelle doivent autoriser le trafic en provenance et à destination d'Amazon S3. Vous ne pouvez pas référencer les listes de préfixes dans les règles ACL réseau, mais vous pouvez obtenir les plages d'adresses IP pour Amazon S3 à partir de la [liste de préfixes](#) pour Amazon S3.
- Vérifiez si vous utilisez un compartiment S3 Service AWS qui nécessite l'accès à un compartiment S3. Par exemple, un service peut avoir besoin d'accéder à des compartiments contenant des

fichiers journaux ou vous demander de télécharger des pilotes ou des agents sur vos instances EC2. Si tel est le cas, assurez-vous que votre politique relative aux terminaux autorise la ressource Service AWS ou à accéder à ces compartiments à l'aide de `aws:VpcSourceIp`.

- Vous ne pouvez pas utiliser la condition `aws:SourceIp` dans une stratégie d'identité ou une stratégie de compartiment pour les demandes adressées à Amazon S3 qui traversent un point de terminaison d'un VPC. Utilisez à la place la condition `aws:VpcSourceIp`. Vous pouvez également utiliser des tables de routage pour contrôler quelles instances EC2 peuvent accéder à Amazon S3 via le point de terminaison d'un VPC.
- Les adresses IPv4 ou IPv6 sources des instances de vos sous-réseaux concernés reçues par Amazon S3 passent des adresses publiques aux adresses 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 publiques ne sont pas reprises. Nous vous recommandons de ne pas avoir de tâches importantes en cours d'exécution lorsque vous créez ou modifiez un point de terminaison ou de réaliser un test pour vous assurer que votre logiciel puisse automatiquement se reconnecter à Amazon S3 ; après l'interruption de la connexion.
- Les connexions de point de terminaison ne peuvent être étendues à l'extérieur d'un VPC. Les ressources situées de l'autre côté d'une connexion VPN, d'une connexion d'appairage VPC, d'une passerelle de transit ou d'une Direct Connect connexion dans votre VPC ne peuvent pas utiliser de point de terminaison de passerelle pour communiquer avec Amazon S3.
- Votre compte dispose d'un quota par défaut de 20 points de terminaison de passerelle par Région, qui est réglable. Il y a également une limite de 255 points de terminaison de passerelle par VPC.

DNS privé

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

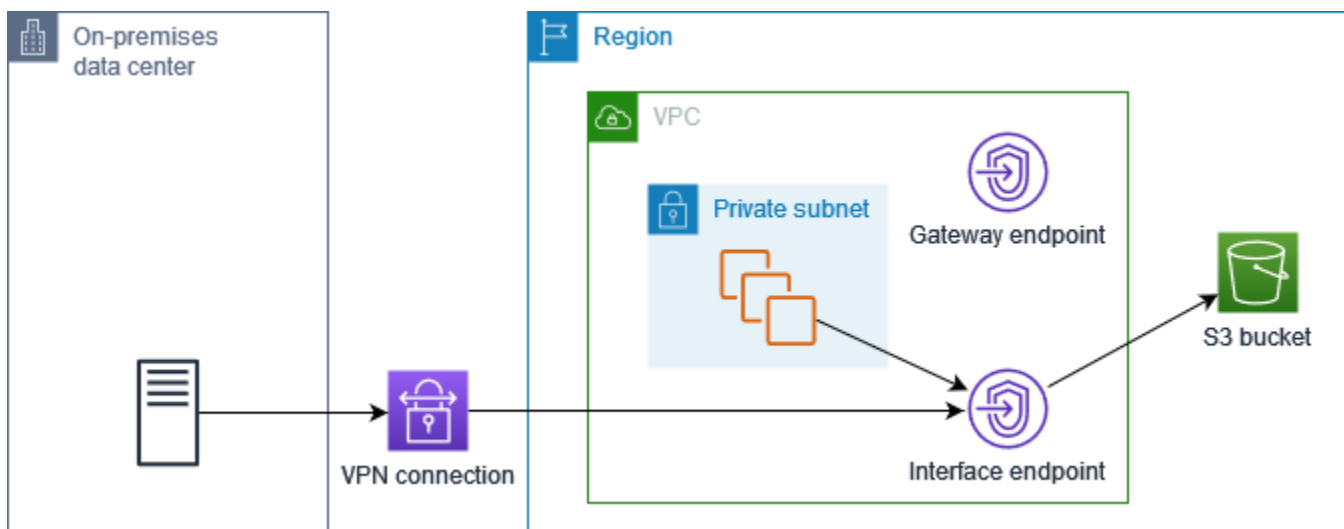
Résolveur Route 53

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

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

DNS privé

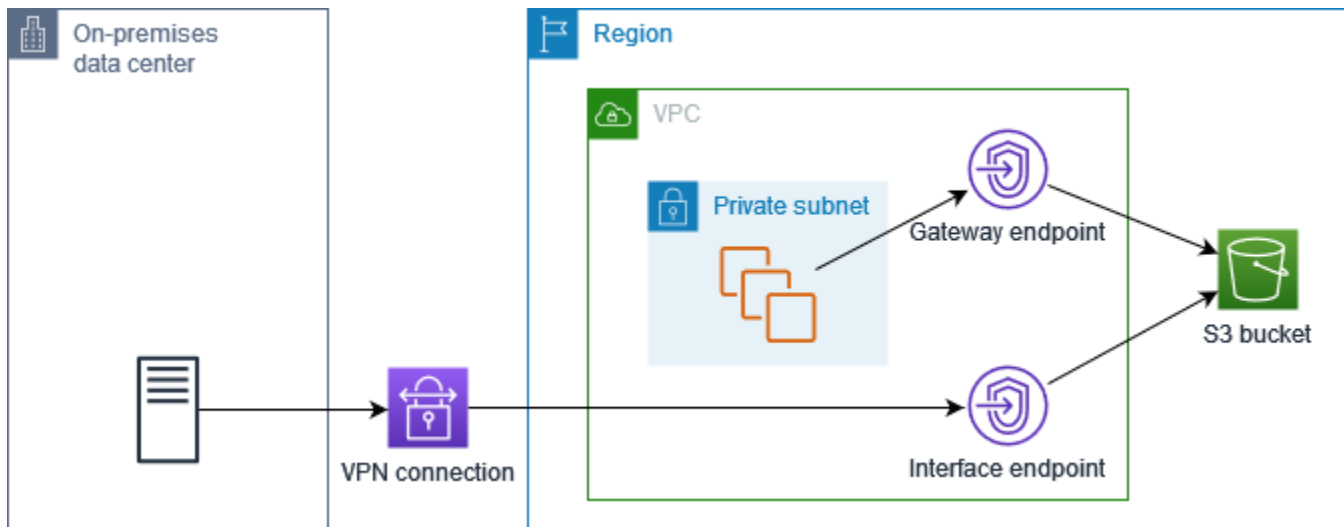
Si vous configurez un DNS privé pour votre point de terminaison d'interface pour Amazon S3 mais que vous ne configurez pas un DNS privé uniquement pour le point de terminaison Resolver entrant, les demandes provenant de votre réseau sur site et de votre VPC utilisent le point de terminaison d'interface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



DNS privé uniquement pour le point de terminaison Resolver entrant

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

Pour configurer cela, le type IP d'enregistrement DNS du point de terminaison de la passerelle doit correspondre au point de terminaison de l'interface ou être `service-defined`. AWS PrivateLink ne prend en charge aucune autre combinaison. Pour de plus amples informations, veuillez consulter [the section called “Type d'adresse IP de l'enregistrement DNS”](#).



Configurer un DNS privé

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

Créer un point de terminaison de passerelle

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

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

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

Si vos données Amazon S3 sont stockées dans des compartiments à usage général, sélectionnez `com.amazonaws.region.s3`.

Si vos données Amazon S3 sont stockées dans des compartiments de répertoires, sélectionnez `com.amazonaws.region.s3` express.

6. Pour VPC, sélectionnez le VPC dans lequel créer le point de terminaison.
7. Pour IP address type (Type d'adresse IP), choisissez l'une des options suivantes :
 - IPv4 — Attribuez des adresses IPv4 aux interfaces réseau des terminaux. Cette option est prise en charge uniquement si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4 et que le service accepte les requêtes IPv4.
 - IPv6 — Attribuez des adresses IPv6 aux interfaces réseau des terminaux. Cette option est prise en charge uniquement si tous les sous-réseaux sélectionnés sont des sous-réseaux IPv6 et que le service accepte les requêtes IPv6.
 - Dualstack : attribuez des adresses IPv4 et IPv6 aux interfaces réseau des terminaux. Cette option est prise en charge uniquement si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4 et IPv6 et que le service accepte les requêtes IPv4 et IPv6.
8. Pour Configure route tables (Configurer les tables de routage), sélectionnez les tables de routage qui seront utilisées par le point de terminaison. Nous ajoutons automatiquement un itinéraire qui dirige le trafic destiné au service vers l'interface réseau de point de terminaison.
9. Pour Policy (Politique), sélectionnez Full access (Accès complet) pour autoriser toutes les opérations de tous les principaux sur toutes les ressources via le point de terminaison de VPC. Sinon, sélectionnez Custom (Personnalisé) pour joindre une politique de point de terminaison de VPC qui contrôle les autorisations dont disposent les principaux pour effectuer des actions sur les ressources via le point de terminaison de VPC.
10. (Facultatif) Pour ajouter une balise, choisissez Ajouter une nouvelle balise et entrez la clé et la valeur de la balise.
11. Choisissez Créer un point de terminaison.

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

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

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

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

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

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

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPCE",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
        "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

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

Vous pouvez créer une politique de compartiment qui restreint l'accès à des VPC spécifiques en utilisant la clé de condition [aws:sourceVpc](#). Ceci est utile si vous avez plusieurs points de terminaison

configurés dans le même VPC. La politique suivante refuse l'accès au compartiment spécifié à l'aide des actions spécifiées à moins que la demande ne provienne du VPC spécifié. Notez que cette politique bloque l'accès au compartiment spécifié à l'aide des actions spécifiées via la Console de gestion AWS.

JSON

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

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

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

JSON

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

```

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

```

Exemple Exemple : Restreindre l'accès à des buckets dans une zone spécifique Compte AWS

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

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-bucket-in-specific-account",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:GetObject", "s3:PutObject", "s3:DeleteObject"],
      "Resource": "arn:aws:s3::*",
      "Condition": {
        "StringNotEquals": {
          "s3:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}

```

```
}
```

Association de tables de routage

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

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

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

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

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

Pour modifier la politique de point de terminaison de VPC

Vous pouvez modifier la politique de point de terminaison pour un point de terminaison de passerelle, qui contrôle l'accès à Amazon S3 depuis le VPC via le point de terminaison. Après avoir mis à jour une politique de point de terminaison, il faut parfois quelques minutes pour que les changements prennent effet. La politique par défaut permet un accès complet. Pour de plus amples informations, veuillez consulter [Politiques de point de terminaison](#).

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

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

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

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

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

Vous pouvez créer une stratégie qui restreint l'accès uniquement à des compartiments S3 spécifiques. Cela est utile si d'autres utilisateurs Services AWS de votre VPC utilisent des compartiments S3.

JSON

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

Exemple Exemple : restriction de l'accès à un rôle IAM spécifique

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

JSON

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

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

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

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-callers-from-specific-account",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
```

```
"Condition": {  
  "StringEquals": {  
    "aws:PrincipalAccount": "111122223333"  
  }  
}  
]  
}
```

Suppression d'un point de terminaison de passerelle

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

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

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

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

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

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

Points de terminaison de passerelle pour Amazon DynamoDB

Vous pouvez accéder à Amazon DynamoDB à partir de votre VPC à l'aide de points de terminaison de VPC de passerelle. Après avoir créé le point de terminaison de passerelle, vous pouvez l'ajouter comme cible dans votre table de routage pour le trafic destiné à DynamoDB depuis votre VPC.

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

DynamoDB prend en charge à la fois les points de terminaison de passerelle et les points de terminaison d'interface. Avec un point de terminaison de passerelle, vous pouvez accéder à DynamoDB depuis votre VPC, sans avoir besoin d'une passerelle Internet ou d'un périphérique NAT pour votre VPC, et sans frais supplémentaires. Cependant, les points de terminaison de passerelle n'autorisent pas l'accès depuis des réseaux locaux, depuis des VPC homologues dans d'autres AWS régions ou via une passerelle de transit. Pour ces scénarios, vous devez utiliser un point de terminaison d'interface qui est disponible moyennant des frais supplémentaires. Pour plus d'informations, consultez la section [Types de points de terminaison VPC pour DynamoDB](#) dans le manuel Amazon DynamoDB Developer Guide.

Table des matières

- [Considérations](#)
- [Créer un point de terminaison de passerelle](#)
- [Contrôle de l'accès à l'aide de politiques IAM](#)
- [Association de tables de routage](#)
- [Pour modifier la politique de point de terminaison de VPC](#)
- [Suppression d'un point de terminaison de passerelle](#)

Considérations

- Le point de terminaison de passerelle est disponible uniquement dans la Région où vous l'avez créé. Veillez à créer votre point de terminaison de passerelle dans la même Région que vos tables DynamoDB.
- Si vous utilisez les serveurs DNS d'Amazon, vous devez activer à la fois [les noms d'hôte DNS et la résolution DNS](#) pour votre VPC. Si vous utilisez votre propre serveur DNS, assurez-vous que les requêtes vers DynamoDB se résolvent correctement en adresses IP gérées par AWS.
- Les règles des groupes de sécurité pour les instances qui accèdent à DynamoDB par le point de terminaison de passerelle doivent autoriser le trafic en provenance et à destination de DynamoDB. Vous pouvez faire référence à l'ID de la [liste de préfixes](#) pour DynamoDB dans les règles du groupe de sécurité.
- L'ACL réseau du sous-réseau pour vos instances qui accèdent à DynamoDB par le point de terminaison de passerelle doivent autoriser le trafic en provenance et à destination de DynamoDB. Vous ne pouvez pas référencer les listes de préfixes dans les règles ACL réseau, mais vous

pouvez obtenir les plages d'adresses IP pour DynamoDB à partir de la [liste de préfixes](#) pour DynamoDB.

- Si vous l'utilisez AWS CloudTrail pour enregistrer les opérations DynamoDB, les fichiers journaux contiennent les adresses IP privées des instances EC2 du VPC consommateur de services et l'ID du point de terminaison de la passerelle pour toutes les demandes effectuées via le point de terminaison.
- Les points de terminaison de passerelle ne prennent en charge que le trafic IPv4.
- Les adresses IPv4 source des instances de vos sous-réseaux concernés passent d'adresses IPv4 publiques à adresses IPv4 privées de votre VPC. Un point de terminaison change de routes réseau et déconnecte les connexions TCP ouvertes. Les connexions précédentes qui utilisaient des adresses IPv4 publiques ne sont pas reprises. Nous vous recommandons de ne pas exécuter de tâches importantes lorsque vous créez ou modifiez un point de terminaison de passerelle. Vous pouvez également vérifier que votre logiciel peut se reconnecter automatiquement à DynamoDB en cas de rupture de connexion.
- Les connexions de point de terminaison ne peuvent être étendues à l'extérieur d'un VPC. Les ressources situées de l'autre côté d'une connexion VPN, d'une connexion d'appairage VPC, d'une passerelle de transit ou d'une Direct Connect connexion dans votre VPC ne peuvent pas utiliser de point de terminaison de passerelle pour communiquer avec DynamoDB.
- Votre compte dispose d'un quota par défaut de 20 points de terminaison de passerelle par Région, qui est réglable. Il y a également une limite de 255 points de terminaison de passerelle par VPC.

Créer un point de terminaison de passerelle

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

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

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

7. Pour Configurer route tables (Configurer les tables de routage), sélectionnez les tables de routage qui seront utilisées par le point de terminaison. Nous ajoutons automatiquement un itinéraire qui dirige le trafic destiné au service vers l'interface réseau de point de terminaison.
8. Pour Policy (Politique), sélectionnez Full access (Accès complet) pour autoriser toutes les opérations de tous les principaux sur toutes les ressources via le point de terminaison de VPC. Sinon, sélectionnez Custom (Personnalisé) pour joindre une politique de point de terminaison de VPC qui contrôle les autorisations dont disposent les principaux pour effectuer des actions sur les ressources via le point de terminaison de VPC.
9. (Facultatif) Pour ajouter une balise, choisissez Ajouter une nouvelle balise et entrez la clé et la valeur de la balise.
10. Choisissez Créer un point de terminaison.

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

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

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

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

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

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

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-from-specific-endpoint",
```

```

    "Effect": "Deny",
    "Principal": "*",
    "Action": "dynamodb:*",
    "Resource": "arn:aws:dynamodb:us-east-1:111111111111:table/*",
    "Condition": {
      "StringNotEquals" : {
        "aws:sourceVpce": "vpce-11aa22bb"
      }
    }
  }
]
}

```

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

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

JSON

```

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

```

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

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

JSON

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

Association de tables de routage

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

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

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Sélectionnez le point de terminaison de passerelle.
4. Choisissez Actions, Gérer les tables de routage.

5. Sélectionnez ou désélectionnez les tables de routage si nécessaire.
6. Choisissez Modify route tables (Modifier les tables de routage).

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

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

Pour modifier la politique de point de terminaison de VPC

Vous pouvez modifier la politique de point de terminaison pour un point de terminaison de passerelle, qui contrôle l'accès à DynamoDB depuis le VPC via le point de terminaison. Après avoir mis à jour une politique de point de terminaison, il faut parfois quelques minutes pour que les changements prennent effet. La politique par défaut permet un accès complet. Pour de plus amples informations, veuillez consulter [Politiques de point de terminaison](#).

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

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

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

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

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

Exemple Exemple : autorisation d'accès en lecture seule

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

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

Exemple Exemple : restreindre l'accès à une table spécifique

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

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

```
}
```

Suppression d'un point de terminaison de passerelle

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

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

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

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

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

Accédez aux produits SaaS via AWS PrivateLink

En utilisant AWS PrivateLink, vous pouvez accéder aux produits SaaS en privé, comme s'ils s'exécutaient dans votre propre VPC.

Table des matières

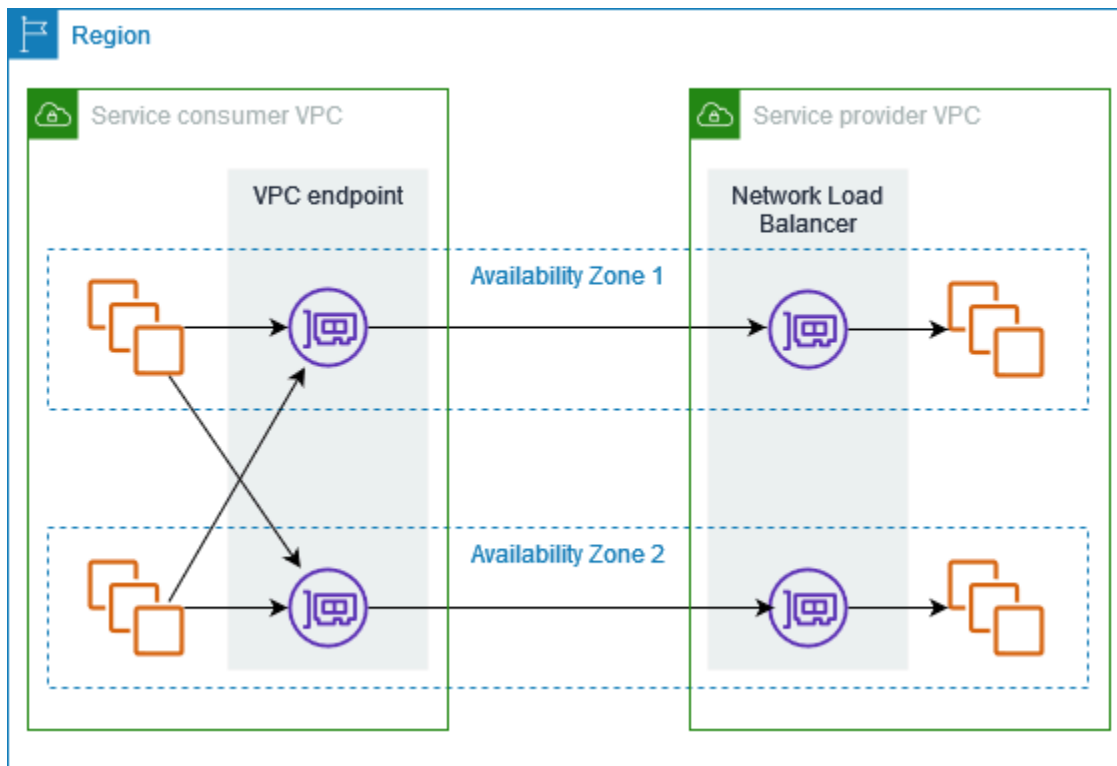
- [Présentation de](#)
- [Création d'un point de terminaison d'interface](#)

Présentation de

Vous pouvez découvrir, acheter et approvisionner des produits SaaS optimisés AWS PrivateLink par AWS Marketplace. Pour plus d'informations, voir [Accès sécurisé et privé aux applications SaaS AWS PrivateLink](#).

Vous pouvez également trouver des produits SaaS fournis par AWS PrivateLink des AWS partenaires. Pour plus d'informations, voir [Partenaires AWS PrivateLink](#).

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



Création d'un point de terminaison d'interface

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

Exigence

Abonnez-vous au service.

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

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

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

Pour configurer un point de terminaison d'interface

Pour plus d'informations sur la configuration du point de terminaison de votre interface, voir [the section called "Configuration d'un point de terminaison d'interface"](#).

Partagez vos services via AWS PrivateLink

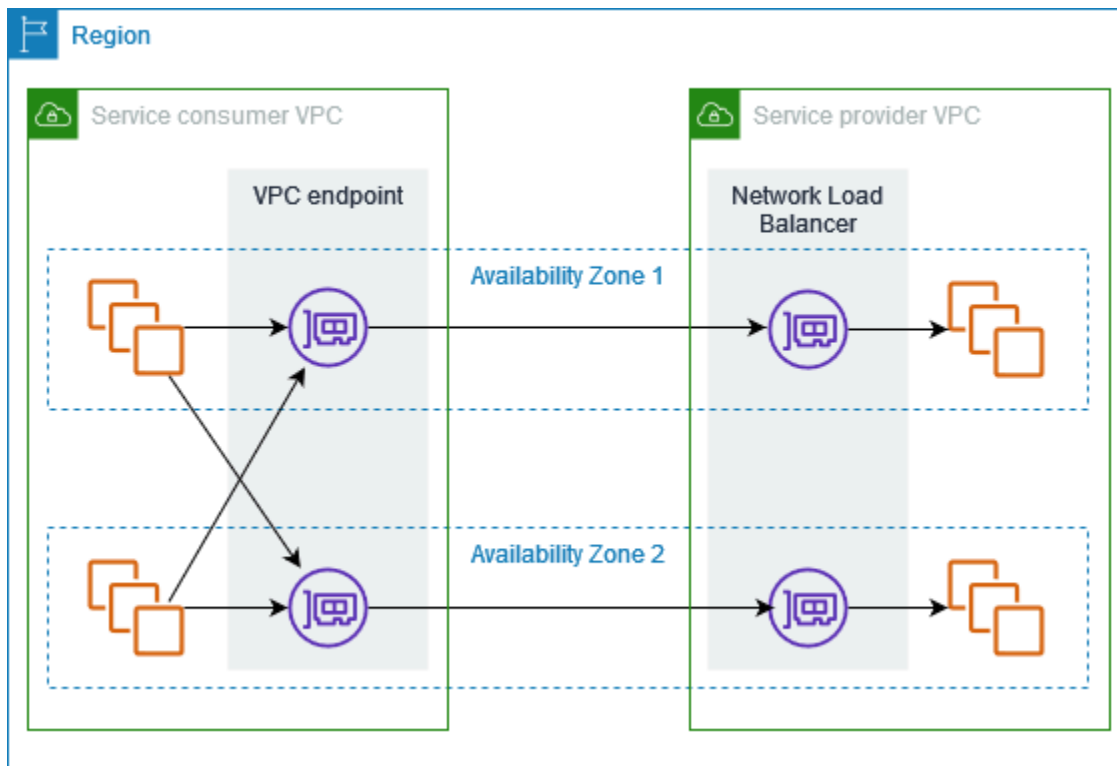
Vous pouvez héberger votre propre service AWS PrivateLink optimisé, appelé service de point de terminaison, et le partager avec d'autres AWS clients.

Table des matières

- [Présentation de](#)
- [Noms d'hôte DNS](#)
- [DNS privé](#)
- [Sous-réseaux et zones de disponibilité](#)
- [Cross-Region accès](#)
- [Types d'adresses IP](#)
- [Créez un service propulsé par AWS PrivateLink](#)
- [Configuration d'un service de point de terminaison](#)
- [Gestion des noms DNS privés pour les services de point de terminaison de VPC](#)
- [Réception d'alertes pour les événements relatifs au service de point de terminaison](#)
- [Suppression d'un service de point de terminaison](#)

Présentation de

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



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

Noms d'hôte DNS

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

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

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

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

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

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

Les noms zonaux ont la syntaxe suivante :

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

DNS privé

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

Sous-réseaux et zones de disponibilité

Votre service de point de terminaison est disponible dans les zones de disponibilité que vous activez pour votre équilibreur de charge réseau. Pour des raisons de haute disponibilité et de résilience, nous vous recommandons d'activer votre équilibreur de charge dans au moins deux zones de disponibilité, de déployer des instances EC2 dans chaque zone activée et d'enregistrer ces instances auprès du groupe cible de votre équilibreur de charge.

Vous pouvez activer l'équilibrage de charge entre zones comme alternative à l'hébergement de votre service de terminaux dans plusieurs zones de disponibilité. Toutefois, les consommateurs perdront l'accès au service de point de terminaison depuis les deux zones en cas de défaillance de la zone qui héberge le service de point de terminaison. Sachez également que lorsque vous activez l'équilibrage de charge entre zones pour un équilibreur de charge réseau, des frais de transfert de données EC2 s'appliquent.

Le consommateur peut créer des points de terminaison VPC d'interface dans les zones de disponibilité dans lesquelles votre service de point de terminaison est disponible. Nous créons une interface réseau de point de terminaison dans chaque sous-réseau que le consommateur configure pour le point de terminaison VPC. Nous attribuons des adresses IP à chaque interface réseau

de point de terminaison à partir de son sous-réseau, en fonction du type d'adresse IP du point de terminaison d'un VPC. Lorsqu'une demande utilise le point de terminaison régional pour le service de point de terminaison VPC, nous sélectionnons une interface réseau de point de terminaison saine, en utilisant l'algorithme Round Robin pour alterner entre les interfaces réseau des différentes zones de disponibilité. Nous résolvons ensuite le trafic vers l'adresse IP de l'interface réseau du point de terminaison sélectionné.

Le consommateur peut utiliser les points de terminaison zonaux pour le point de terminaison VPC s'il est préférable pour son cas d'utilisation de maintenir le trafic dans la même zone de disponibilité.

Cross-Region accès

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

Permissions

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

Considérations

- Un fournisseur de services doit adhérer à une région optionnelle avant de l'ajouter en tant que région prise en charge pour un service de point de terminaison.
- Votre service de point de terminaison doit être accessible depuis sa région hôte. Vous ne pouvez pas supprimer la région hôte de l'ensemble des régions prises en charge. À des fins de redondance, vous pouvez déployer votre service de point de terminaison dans plusieurs régions et activer l'accès interrégional pour chaque service de point de terminaison.

- Un consommateur de services doit accéder à une région optionnelle avant de la sélectionner comme région de service pour un point de terminaison. Dans la mesure du possible, nous recommandons aux consommateurs de services d'accéder à un service en utilisant la connectivité intra-régionale plutôt que la connectivité interrégionale. Intra-Region la connectivité permet de réduire la latence et les coûts.
- Si un fournisseur de services supprime une région de l'ensemble des régions prises en charge, les consommateurs de services ne peuvent pas sélectionner cette région comme région de service lorsqu'ils créent de nouveaux points de terminaison. Notez que cela n'affecte pas l'accès au service des terminaux à partir des terminaux existants qui utilisent cette région comme région de service.
- Pour une haute disponibilité, les fournisseurs doivent utiliser au moins deux zones de disponibilité. Cross-Region l'accès ne nécessite pas que les fournisseurs et les consommateurs utilisent les mêmes zones de disponibilité.
- Cross-Region l'accès n'est pas pris en charge pour les zones de disponibilité suivantes : use1-az3 usw1-az2 apne1-az3, apne2-az2, etapne2-az4.
- Avec l'accès interrégional, AWS PrivateLink gère le basculement entre les zones de disponibilité. Il ne gère pas le basculement entre les régions.
- Cross-Region l'accès n'est pas pris en charge pour les équilibreurs de charge réseau dont une valeur personnalisée est configurée pour le délai d'inactivité TCP.
- Cross-Region l'accès n'est pas pris en charge avec la fragmentation UDP.
- Cross-Region l'accès n'est pris en charge que pour les services que vous partagez AWS PrivateLink.

Types d'adresses IP

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

Si le point de terminaison d'un VPC d'interface prend en charge le protocole IPv4, les interfaces réseau du point de terminaison possèdent des adresses IPv4. Si le point de terminaison d'un VPC d'interface prend en charge le protocole IPv6, les interfaces réseau du point de terminaison possèdent des adresses IPv6. L'adresse IPv6 d'une interface réseau de point de terminaison est

inaccessible depuis Internet. Si vous décrivez une interface réseau de point de terminaison avec une adresse IPv6, remarquez que `denyAllIgwTraffic` est activé.

Exigences pour activer IPv6 pour un service de point de terminaison

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

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

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

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

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

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

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

Créez un service propulsé par AWS PrivateLink

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

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

Table des matières

- [Considérations](#)
- [Conditions préalables](#)
- [Création d'un service de point de terminaison](#)
- [Mettre le service de point de terminaison à la disposition des consommateurs du service](#)
- [Connexion à un service de point de terminaison en tant que consommateur du service](#)

Considérations

- Le service de point de terminaison n'est disponible que dans la Région où vous l'avez créé. Les consommateurs peuvent accéder à votre service depuis d'autres régions si vous activez l'accès [interrégional](#), ou s'ils utilisent le peering VPC ou une passerelle de transit.
- Lorsque les consommateurs du service extraient des informations sur un service de point de terminaison, ils ne peuvent voir que les zones de disponibilité qu'ils ont en commun avec le fournisseur du service. Lorsque le fournisseur du service et le consommateur du service se trouvent dans des comptes différents, un nom de zone de disponibilité, tel que us-east-1a, peut être mappé à une zone de disponibilité physique différente dans chaque Compte AWS. Vous

pouvez utiliser les identifiants AZ pour identifier de manière cohérente les zones de disponibilité de votre service. Pour plus d'informations, consultez la section [Identifiants AZ](#) dans le guide de l'utilisateur Amazon EC2.

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

Conditions préalables

- Créez un VPC pour votre service de point de terminaison avec au moins un sous-réseau dans chaque zone de disponibilité dans laquelle le service doit être disponible.
- Pour permettre aux consommateurs du service de créer des points de terminaison de VPC d'interface IPv6 pour votre service de terminaison, le VPC et les sous-réseaux doivent être associés à des blocs CIDR IPv6.
- Créez un équilibreur de charge de réseau Network Load Balancer dans votre VPC. Sélectionnez un sous-réseau par zone de disponibilité dans lequel le service doit être disponible pour les consommateurs. Pour une faible latence et tolérance aux pannes, nous vous recommandons de rendre votre service disponible dans toutes les zones de disponibilité de la région.

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

Si vous traitez les adresses IP sources à partir de l'en-tête du protocole de proxy version 2, vérifiez que vous pouvez traiter les adresses IPv6.

- Lancez des instances dans chaque zone de disponibilité dans laquelle le service doit être disponible et enregistrez-les dans un groupe cible d'équilibreurs de charge. Si vous ne lancez pas d'instances dans toutes les zones de disponibilité activées, vous pouvez activer l'équilibrage de charge entre zones pour prendre en charge les consommateurs du service qui utilisent des noms d'hôte DNS zonaux pour accéder au service. Des frais de transfert régional de données s'appliquent lorsque vous activez l'équilibrage de charge entre zones. Pour plus d'informations, consultez la section sur l'équilibrage de [Cross-zone charge](#) dans le Guide de l'utilisateur des Network Load Balancers.

Création d'un service de point de terminaison

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

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

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

de disponibilité incluses. Votre service de point de terminaison sera disponible dans ces zones de disponibilité.

6. (Facultatif) Pour rendre votre service de point de terminaison disponible depuis des régions autres que celle dans laquelle il est hébergé, sélectionnez les régions dans les régions de service. Pour de plus amples informations, veuillez consulter [the section called “Cross-Region accès”](#).
7. Dans la section Require acceptance for endpoint (Acceptation requise pour le point de terminaison), sélectionnez Acceptance required (Acceptation requise) pour exiger que les demandes de connexion à votre service de point de terminaison soient acceptées manuellement. Sinon, ces requêtes sont acceptées automatiquement.
8. Pour Enable private DNS name (Activer le nom DNS privé), sélectionnez Associate a private DNS name with the service (Associer un nom DNS privé au service) pour associer un nom DNS privé que les consommateurs du service peuvent utiliser pour accéder à votre service, puis saisissez le nom DNS privé. Dans le cas contraire, les utilisateurs de services peuvent utiliser le nom DNS spécifique au point de terminaison fourni par AWS. Le fournisseur du service doit vérifier qu'il est le propriétaire du domaine de nom DNS privé pour que les consommateurs puissent utiliser le nom DNS privé. Pour de plus amples informations, veuillez consulter [Gestion des noms DNS](#).
9. Pour Supported IP address types (Types d'adresse IP pris en charge), effectuez l'une des opérations suivantes :
 - Sélectionnez IPv4 – Permettez au service de point de terminaison d'accepter les requêtes IPv4.
 - Sélectionnez IPv6 – Permettez au service de point de terminaison d'accepter les requêtes IPv6.
 - Sélectionnez IPv4 et IPv6 – Permettez au service de point de terminaison d'accepter tant les requêtes IPv4 que les requêtes IPv6.
10. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
11. Choisissez Créer.

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

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

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

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

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

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

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

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

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

terminaison interrégional, puis sélectionnez la région. Pour de plus amples informations, veuillez consulter [the section called “Cross-Region accès”](#).

7. Pour VPC, sélectionnez le VPC à partir duquel vous accéderez au service Endpoint.
8. Pour Sous-réseaux, sélectionnez les sous-réseaux dans lesquels vous souhaitez créer des interfaces réseau de points de terminaison.
9. Pour IP address type (Type d'adresse IP), choisissez l'une des options suivantes :
 - IPv4 — Attribuez des adresses IPv4 aux interfaces réseau des terminaux. Cette option est prise en charge uniquement si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4 et que le service de point de terminaison accepte les requêtes IPv4.
 - IPv6 — Attribuez des adresses IPv6 aux interfaces réseau des terminaux. Cette option est prise en charge uniquement si tous les sous-réseaux sélectionnés sont des sous-réseaux IPv6 et que le service de point de terminaison accepte les requêtes IPv6.
 - Dualstack : attribuez des adresses IPv4 et IPv6 aux interfaces réseau des terminaux. Cette option est prise en charge uniquement si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4 et IPv6 et que le service de point de terminaison accepte les requêtes IPv4 et IPv6.
10. Dans DNS record IP type (Type d'IP d'enregistrement DNS), choisissez l'une des options suivantes :
 - IPv4 – Créez des enregistrements A pour les noms DNS privés, régionaux et zonaux. Le type d'adresse IP doit être IPv4 ou Dualstack.
 - IPv6 – Créez des enregistrements AAAA pour les noms DNS privés, régionaux et zonaux. Le type d'adresse IP doit être IPv6 ou Dualstack.
 - Dualstack – Créez des enregistrements A et AAAA pour les noms DNS privés, régionaux et zonaux. Le type d'adresse IP doit être Dualstack.
 - Service défini – Créez des enregistrements A pour les noms DNS privés, régionaux et zonaux et des enregistrements AAAA pour les noms DNS régionaux et zonaux. Le type d'adresse IP doit être Dualstack.
11. Pour Groupe de sécurité, sélectionnez les groupes de sécurité à associer aux interfaces réseau du point de terminaison.
12. Choisissez Créer un point de terminaison.

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

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

Configuration d'un service de point de terminaison

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

Tâches

- [Gestion des autorisations](#)
- [Acceptation ou refus des demandes de connexion](#)
- [Gérer les équilibres de charge](#)
- [Association d'un nom DNS privé](#)
- [Modifier les régions prises en charge](#)
- [Modification des types d'adresses IP pris en charge](#)
- [Gestion des balises](#)

Gestion des autorisations

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

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

ARN pour AWS principals

Compte AWS (inclut tous les mandants du compte)

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

Role

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

Utilisateur

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

Tous les directeurs en tout Comptes AWS

*

Considérations

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

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

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

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

- [modify-vpc-endpoint-service-permissions](#) (AWS CLI)
- [Edit-EC2EndpointServicePermission](#) (Outils pour Windows PowerShell)

Acceptation ou refus des demandes de connexion

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

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

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

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

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

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

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

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

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

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

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

- [accept-vpc-endpoint-connections](#) ou [reject-vpc-endpoint-connections](#) (AWS CLI)
- [Approve-EC2EndpointConnection](#) ou [Deny-EC2EndpointConnection](#) (Outils pour Windows PowerShell)

Gérer les équilibreurs de charge

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

Si vous activez une autre zone de disponibilité pour vos équilibreurs de charge, la zone de disponibilité apparaîtra sous l'onglet Load Balancers de la page des services Endpoint. Cependant, il ne sera pas activé pour le service de point de terminaison ni répertorié dans l'onglet Détails de votre service de point de terminaison sur le Console de gestion AWS. Vous devez activer le service Endpoint pour la nouvelle zone de disponibilité.

La zone de disponibilité de l'équilibreur de charge peut prendre quelques minutes pour être prête pour votre service de point de terminaison. Si vous utilisez une automatisation, nous vous recommandons d'ajouter une attente à votre processus d'automatisation avant d'activer le service Endpoint pour la nouvelle zone de disponibilité.

Pour gérer les équilibreurs de charge pour votre service Endpoint à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison.
4. Choisissez Actions, Associate or disassociate load balancers (Associer des équilibreurs de charge).
5. Modifiez la configuration du service Endpoint si nécessaire. Par exemple :
 - Cochez la case correspondant à un équilibreur de charge pour l'associer au service Endpoint.
 - Décochez la case correspondant à un équilibreur de charge pour le dissocier du service Endpoint. Vous devez conserver au moins un équilibreur de charge sélectionné.
6. Choisissez Enregistrer les modifications

Le service Endpoint sera activé pour toutes les nouvelles zones de disponibilité que vous avez ajoutées à votre équilibreur de charge. La nouvelle zone de disponibilité est répertoriée sous l'onglet Load Balancers et l'onglet Details du service Endpoint.

Après avoir activé une zone de disponibilité pour le service de point de terminaison, les consommateurs de services peuvent ajouter un sous-réseau de cette zone de disponibilité aux points de terminaison VPC de leur interface.

Pour gérer les équilibreurs de charge pour votre service Endpoint à l'aide de la ligne de commande

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

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

Association d'un nom DNS privé

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

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

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

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

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

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

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison.

4. Choisissez Actions, Verify domain ownership for private DNS name (Vérifier la propriété du domaine pour le nom DNS privé).
5. Lorsque vous êtes invité à confirmer, saisissez **verify**, puis choisissez Delete (Supprimer).

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

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

Modifier les régions prises en charge

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

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

Pour modifier les régions prises en charge pour votre service de terminaux

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

Modification des types d'adresses IP pris en charge

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

Considération

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

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

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison de VPC.
4. Choisissez Actions, Modify supported IP address types (Modifier les types d'adresses IP pris en charge).
5. Pour Supported IP address types (Types d'adresse IP pris en charge), effectuez l'une des opérations suivantes :
 - Sélectionnez IPv4 – Permettez au service de point de terminaison d'accepter les requêtes IPv4.
 - Sélectionnez IPv6 – Permettez au service de point de terminaison d'accepter les requêtes IPv6.
 - Sélectionnez IPv4 et IPv6 – Permettez au service de point de terminaison d'accepter tant les requêtes IPv4 que les requêtes IPv6.
6. Sélectionnez Enregistrer les modifications.

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

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

Gestion des balises

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

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

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

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

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

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

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez le service de point de terminaison d'un VPC, puis choisissez l'onglet Autoriser les principaux.

4. Sélectionnez le principal puis choisissez Actions (Actions), Gérer les balises.
5. Pour chaque balise à ajouter, sélectionnez Add new tag (Ajouter une nouvelle balise) et saisissez la clé et la valeur de la balise.
6. Pour supprimer une balise, choisissez Remove (Supprimer) à droite de la clé et de la valeur de la balise.
7. Choisissez Enregistrer.

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

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

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

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

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

Considérations

- Un service de point de terminaison ne peut avoir qu'un seul nom DNS privé.
- Lorsque le client crée un point de terminaison d'interface pour se connecter à votre service, nous créons une zone hébergée privée et l'associons au VPC du consommateur de services. Nous créons un enregistrement CNAME dans la zone hébergée privée qui associe le nom DNS privé

du service de point de terminaison au nom DNS régional du point de terminaison VPC. Lorsqu'un consommateur envoie une demande au nom DNS public du service, les serveurs DNS privés résolvent la demande aux adresses IP des interfaces réseau des terminaux.

- Pour vérifier un domaine, vous devez avoir un nom d'hôte public ou un fournisseur DNS public.
- Vous pouvez vérifier le domaine d'un sous-domaine. Par exemple, vous pouvez vérifier `example.com`, au lieu de `a.example.com`. Chaque étiquette DNS peut comporter jusqu'à 63 caractères et la longueur totale du nom de domaine ne doit pas dépasser 255 caractères.

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

- Les noms DNS privés ne sont pas pris en charge pour les points de terminaison d'équilibreur de charge de passerelle.

Vérification de la propriété du domaine

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

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

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

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

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

Obtention du nom et de la valeur

Nous vous fournissons le nom et la valeur que vous utilisez dans l'enregistrement TXT. Par exemple, les informations sont disponibles dans la Console de gestion AWS. Sélectionnez le service de point de terminaison et consultez Domain verification name (Nom de vérification du domaine) et Domain verification value (Valeur de vérification du domaine) dans l'onglet Details (Détails) pour le service de point de terminaison. Vous pouvez également utiliser la [AWS CLI commande](#) `describe-vpc-endpoint-service-configurations` suivante pour récupérer des informations sur la configuration du nom DNS privé pour le service de point de terminaison spécifié.

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

Voici un exemple de sortie. Vous utiliserez `Value` et `Name` lorsque vous créez l'enregistrement TXT.

```
[
  {
    "State": "pendingVerification",
    "Type": "TXT",
    "Value": "vpce:l6p0ERxITt45jevFw0Cp",
    "Name": "_6e86v84tggqubxbwii1m"
  }
]
```

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

Nom	Type	Value
_6e86v84tggqubxbwii1m.example.com	TXT	vpce : l6p0 ERxITt45jevFwOCp

Nous vous suggérons d'utiliser `Name` comme sous-domaine d'enregistrement, car il se peut que le nom de domaine de base soit déjà utilisé. Toutefois, si votre fournisseur DNS ne permet pas

aux noms d'enregistrement DNS de contenir des traits de soulignement, vous pouvez omettre le « _6e86v84tggqubxbwii1m » et utiliser simplement « exemple.com » dans l'enregistrement TXT.

Après avoir vérifié « _6e86v84tggqubxbwii1m.example.com », les consommateurs du service peuvent utiliser « exemple.com » ou un sous-domaine (par exemple, « service.example.com » ou « my.service.example.com »).

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

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

Amazon Route 53

Créez un enregistrement pour votre zone hébergée publique à l'aide d'une politique de routage simple. Utilisez les valeurs suivantes :

- Pour Record name (Nom d'enregistrement), saisissez le domaine ou le sous-domaine.
- Sous Record type (Type d'enregistrement), choisissez TXT.
- Pour le Value/Route trafic à destination de, entrez la valeur de vérification du domaine.
- Pour TTL (seconds) (TTL [secondes]), saisissez **1800**.

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

Procédure générale

Accédez au site Web de votre fournisseur DNS et connectez-vous à votre compte. Recherchez la page permettant de mettre à jour les enregistrements DNS de votre domaine. Ajoutez un enregistrement TXT avec le nom et la valeur que nous avons fournis. La mise à jour d'un enregistrement DNS peut prendre jusqu'à 48 heures, mais elle est souvent effective bien plus tôt.

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

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

Vérification de la publication de l'enregistrement TXT

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

Vous interrogerez les serveurs DNS qui desservent votre domaine, car ce sont ces serveurs qui contiennent les informations les plus récentes sur votre domaine. La propagation des informations de votre domaine aux autres serveurs DNS prend du temps.

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

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

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

Le résultat liste les serveurs de noms qui desservent votre domaine. Vous interrogerez l'un de ces serveurs à l'étape suivante.

2. Vérifiez que l'enregistrement TXT est correctement publié à l'aide de la commande suivante, où se *name_server* trouve l'un des serveurs de noms que vous avez trouvés à l'étape précédente.

```
nslookup -type=TXT _6e86v84tqqqubxbwii1m.example.com name_server
```

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

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

```
_6e86v84tqqqubxbwii1m.example.com text = "vpce:l6p0ERx1Tt45jevFw0Cp"
```

Résolution des problèmes de vérification de domaine

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

- Vérifiez si votre fournisseur DNS autorise les traits de soulignement dans les noms d'enregistrements TXT. Si votre fournisseur DNS n'autorise pas les traits de soulignement, vous pouvez omettre le nom de vérification du domaine (par exemple, « `_6e86v84tqqqubxbwii1m` ») dans l'enregistrement TXT.
- Vérifiez si votre fournisseur DNS a ajouté le nom de domaine à la fin de l'enregistrement TXT. Certains fournisseurs DNS ajoutent automatiquement le nom de votre domaine au nom d'attribut de l'enregistrement TXT. Pour éviter cette duplication du nom de domaine, ajoutez un point à la fin du nom de domaine lorsque vous créez l'enregistrement TXT. Cela indique à votre fournisseur DNS qu'il n'est pas nécessaire d'ajouter le nom de domaine à l'enregistrement TXT.
- Vérifiez si votre fournisseur DNS a modifié la valeur de l'enregistrement DNS pour n'utiliser que des lettres minuscules. Nous vérifions votre domaine uniquement lorsqu'il existe un enregistrement de vérification dont la valeur d'attribut correspond exactement à la valeur que nous avons fournie. Si le fournisseur DNS a modifié les valeurs de votre enregistrement TXT pour n'utiliser que des lettres minuscules, contactez-le pour obtenir de l'aide.
- Vous devrez peut-être vérifier votre domaine plus d'une fois parce que vous prenez en charge plusieurs Régions ou plusieurs Comptes AWS. Si votre fournisseur DNS ne vous permet pas d'avoir plus d'un enregistrement TXT avec le même nom d'attribut, vérifiez si votre fournisseur DNS vous permet d'attribuer plusieurs valeurs d'attribut au même enregistrement TXT. Par exemple, si votre DNS est géré par Amazon Route 53, vous pouvez utiliser la procédure suivante.

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

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

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

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

Tâches

- [Création d'une notification SNS](#)
- [Ajout d'une stratégie d'accès](#)
- [Ajout d'une stratégie de clé](#)

Création d'une notification SNS

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

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

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

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

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

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

Ajout d'une stratégie d'accès

Ajoutez une politique d'accès à la rubrique SNS qui permet AWS PrivateLink de publier des notifications en votre nom, comme les suivantes. Pour plus d'informations, voir [Comment modifier la stratégie d'accès à ma rubrique Amazon SNS ?](#) Utilisez les clés de condition globale `aws:SourceArn` et `aws:SourceAccount` pour vous protéger contre le [problème du député confus](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:us-east-1:111111111111:topic-name",
      "Condition": {
```

```

        "ArnLike": {
            "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint-service/service-id"
        },
        "StringEquals": {
            "aws:SourceAccount": "111111111111"
        }
    }
}
]
}

```

Ajout d'une stratégie de clé

Si vous utilisez des rubriques SNS chiffrées, la politique de ressources pour la clé KMS doit être fiable AWS PrivateLink pour appeler les opérations d' AWS KMS API. Voici un exemple de stratégie de clé.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpce.amazonaws.com"
      },
      "Action": [
        "kms:GenerateDataKey*",
        "kms:Decrypt"
      ],
      "Resource": "arn:aws:kms:us-east-1:111111111111:key/key-id",
      "Condition": {
        "ArnLike": {
            "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint-service/service-id"
        },
        "StringEquals": {
            "aws:SourceAccount": "111111111111"
        }
      }
    }
  ]
}

```

```
}  
  }  
    ]  
      }
```

Suppression d'un service de point de terminaison

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

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

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

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

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

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

Accédez aux appareils virtuels via AWS PrivateLink

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

Tarification

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

Table des matières

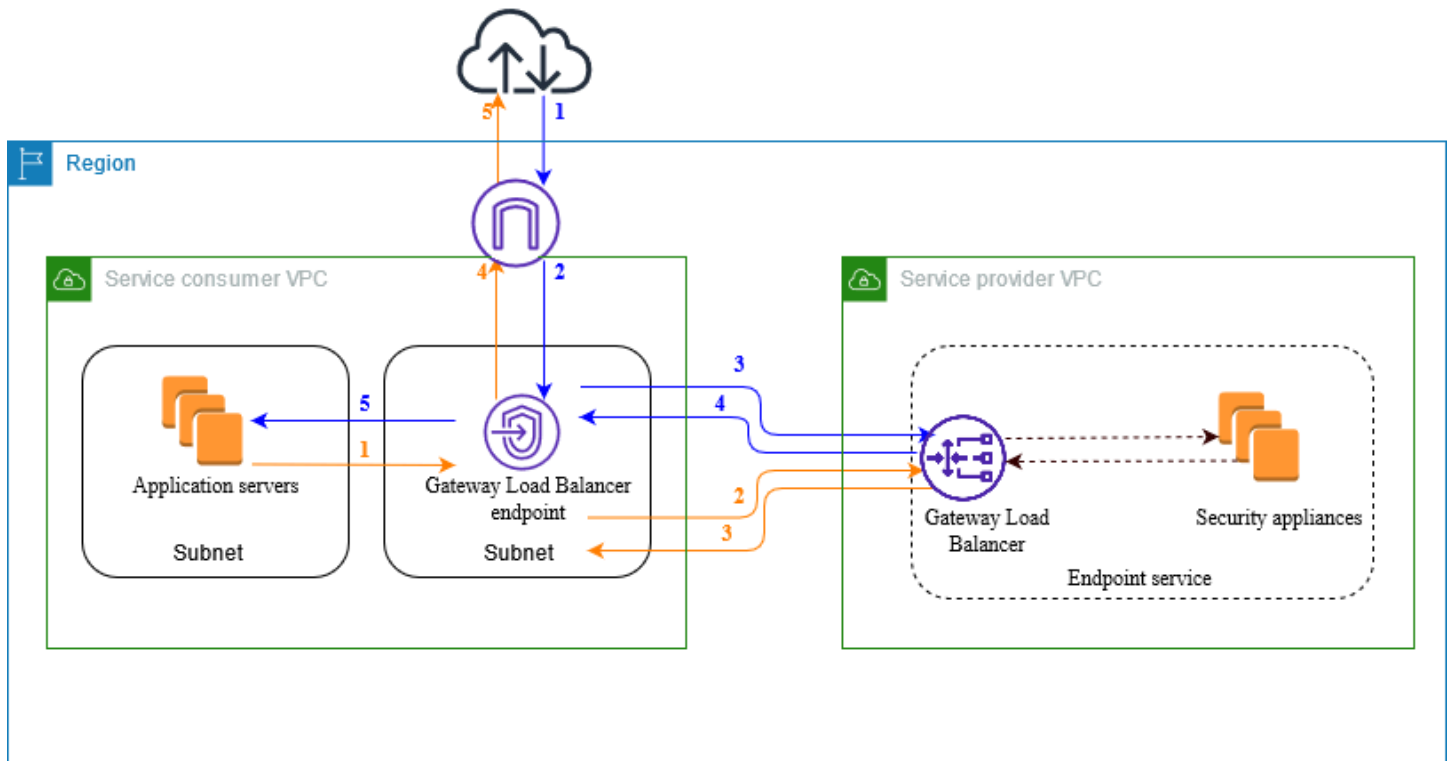
- [Présentation de](#)
- [Types d'adresses IP](#)
- [Routage](#)
- [Création d'un système d'inspection en tant que service de point de terminaison d'équilibreur de charge de passerelle](#)
- [Accès à un système d'inspection à l'aide d'un point de terminaison d'équilibreur de charge de passerelle](#)

Pour plus d'informations, consultez [Gateway Load Balancers](#).

Présentation de

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

d'équilibreur de charge de passerelle pour être inspecté avant d'être réacheminé par la passerelle Internet.



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

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

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

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

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

Types d'adresses IP

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

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

Exigences pour activer IPv6 pour un service de point de terminaison

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

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

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

- Le type d'adresse IP d'un point de terminaison d'interface équilibreur de charge de la Passerelle doit être compatible avec le sous-réseau du point de terminaison équilibreur de charge de la Passerelle, comme décrit ici :
 - IPv4 – Attribuez des adresses IPv4 aux interfaces réseau de vos points de terminaison. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4.
 - IPv6 – Attribuez des adresses IPv6 aux interfaces réseau de vos points de terminaison. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés sont des sous-réseaux IPv6 uniquement.
 - Dualstack – Attribuez à la fois des adresses IPv4 et IPv6 aux interfaces réseau de vos points de terminaison. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'adresses IPv4 et IPv6.
- Les tables de routage des sous-réseaux du VPC consommateur de services doivent acheminer le trafic IPv6 et les ACL réseau de ces sous-réseaux doivent autoriser le trafic IPv6.

Routage

Pour acheminer le trafic vers le service de point de terminaison, spécifiez le point de terminaison d'équilibreur de charge de passerelle comme cible dans vos tables de routage, à l'aide de son ID. Pour le schéma ci-dessus, ajoutez des itinéraires aux tables de routage comme suit. Lorsque votre cible est un point de terminaison GWLB, vous ne pouvez pas spécifier de liste de préfixes comme destination. Dans ces tableaux, les routes IPv6 sont incluses pour une configuration à double pile.

Table de routage pour la passerelle Internet

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

Destination	Target
<i>VPC IPv4 CIDR</i>	Local
<i>VPC IPv6 CIDR</i>	Local
<i>Application subnet IPv4 CIDR</i>	<i>vpc-endpoint-id</i>
<i>Application subnet IPv6 CIDR</i>	<i>vpc-endpoint-id</i>

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

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

Destination	Target
<i>VPC IPv4 CIDR</i>	Local
<i>VPC IPv6 CIDR</i>	Local
0,0,0. 0/0	<i>vpc-endpoint-id</i>
::/0	<i>vpc-endpoint-id</i>

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

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

Destination	Target
<i>VPC IPv4 CIDR</i>	Local
<i>VPC IPv6 CIDR</i>	Local
0,0,0. 0/0	<i>internet-gateway-id</i>
::/0	<i>internet-gateway-id</i>

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

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

Les services de point de terminaison nécessitent un Network Load Balancer (équilibreur de charge de réseau) ou un Gateway Load Balancer (équilibreur de charge de passerelle). Dans ce cas, vous allez créer un service de point de terminaison à l'aide de l'équilibreur de charge de passerelle. Pour plus d'informations sur la création d'un service de point de terminaison à l'aide d'un Network Load Balancer (équilibreur de charge de réseau), voir [Création d'un service de point de terminaison](#).

Table des matières

- [Considérations](#)
- [Conditions préalables](#)
- [Création du service de point de terminaison](#)
- [Assurer la disponibilité de votre service de point de terminaison](#)

Considérations

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

Conditions préalables

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

Création du service de point de terminaison

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

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

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Choisissez Create endpoint service (Créer un service de point de terminaison).
4. Pour Load balancer type (Type d'équilibreur de charge), choisissez Gateway (Passerelle).
5. Pour Available load balancers (Équilibreurs de charge disponibles), sélectionnez l'équilibreur de charge de passerelle.
6. Dans la section Require acceptance for endpoint (Acceptation requise pour le point de terminaison), sélectionnez Acceptance required (Acceptation requise) pour exiger que les demandes de connexion à votre service de point de terminaison soient acceptées manuellement. Sinon, ils sont acceptés automatiquement.
7. Pour Supported IP address types (Types d'adresse IP pris en charge), effectuez l'une des opérations suivantes :
 - Sélectionnez IPv4 – Permettez au service de point de terminaison d'accepter les requêtes IPv4.

- Sélectionnez IPv6 – Permettez au service de point de terminaison d'accepter les requêtes IPv6.
 - Sélectionnez IPv4 et IPv6 – Permettez au service de point de terminaison d'accepter tant les requêtes IPv4 que les requêtes IPv6.
8. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
 9. Choisissez Créer.

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

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

Assurer la disponibilité de votre service de point de terminaison

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

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

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

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

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

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

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

Table des matières

- [Considérations](#)
- [Conditions préalables](#)
- [Créer le point de terminaison](#)
- [Configurer le routage](#)
- [Gestion des balises](#)
- [Suppression d'un point de terminaison d'équilibreur de charge de passerelle](#)

Considérations

- Vous ne pouvez choisir qu'une seule zone de disponibilité dans le VPC du consommateur du service. Vous ne pourrez plus changer ce sous-réseau par la suite. Pour utiliser un point de terminaison d'équilibreur de charge de passerelle dans un sous-réseau différent, vous devez créer un point de terminaison d'équilibreur de charge de passerelle.
- Vous pouvez créer un seul point de terminaison d'équilibreur de charge de passerelle par zone de disponibilité et par service, et vous devez sélectionner la zone de disponibilité que l'équilibreur de charge de passerelle prend en charge. Lorsque le fournisseur du service et le consommateur du service se trouvent dans des comptes différents, un nom de zone de disponibilité, tel que `us-east-1a`, peut être mappé à une zone de disponibilité physique différente dans chaque Compte AWS. Vous pouvez utiliser les identifiants AZ pour identifier de manière cohérente les

zones de disponibilité de votre service. Pour plus d'informations, consultez la section [Identifiants AZ](#) dans le guide de l'utilisateur Amazon EC2.

- Pour pouvoir utiliser le service de point de terminaison, le fournisseur du service doit accepter les demandes de connexion. Le service ne peut pas lancer de requêtes vers les ressources de votre VPC via le point de terminaison de VPC. Le point de terminaison ne renvoie que les réponses au trafic initié par les ressources de votre VPC.
- Chaque point de terminaison de l'équilibreur de charge Passerelle peut prendre en charge une bande passante allant jusqu'à 10 Gbit/s par zone de disponibilité et augmente automatiquement jusqu'à 100 Gbit/s.
- Si un service de point de terminaison est associé à plusieurs équilibreurs de charge de passerelle, un point de terminaison d'équilibreur de charge de passerelle établit une connexion avec un seul équilibreur de charge par zone de disponibilité.
- Pour que le trafic reste dans la même zone de disponibilité, nous vous recommandons de créer un point de terminaison d'équilibreur de charge de passerelle dans chaque zone de disponibilité vers laquelle vous enverrez du trafic.
- La préservation de l'adresse IP du client Network Load Balancer n'est pas prise en charge lorsque le trafic est acheminé via un point de terminaison d'équilibreur de charge de passerelle, même si la cible se trouve dans le même VPC que le Network Load Balancer.
- Si les serveurs d'applications et le point de terminaison Gateway Load Balancer se trouvent dans le même sous-réseau, les règles NACL sont évaluées pour le trafic entre les serveurs d'applications et le point de terminaison Gateway Load Balancer.
- Si vous utilisez un équilibreur de charge de passerelle avec une passerelle Internet de sortie uniquement, le trafic IPv6 est interrompu. Utilisez plutôt une passerelle Internet et des règles de pare-feu entrant.
- Vos AWS PrivateLink ressources sont soumises à des quotas. Pour de plus amples informations, veuillez consulter [AWS PrivateLink quotas](#).

Conditions préalables

- Créez un VPC de consommateur du service avec au moins deux sous-réseaux dans la zone de disponibilité à partir de laquelle vous accéderez au service. Un sous-réseau est destiné aux serveurs d'applications et l'autre au point de terminaison d'équilibreur de charge de passerelle.

- Pour vérifier les zones de disponibilité prises en charge par le service de point de terminaison, décrivez le service de point de terminaison à l'aide de la console ou de la commande [describe-vpc-endpoint-services](#).
- Si vos ressources se trouvent dans un sous-réseau doté d'une liste de contrôle d'accès (ACL, Access Control List) réseau, vérifiez que cette dernière autorise le trafic entre les interfaces réseau du point de terminaison et les ressources du VPC.

Créer le point de terminaison

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

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

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Pour Type, choisissez les services Endpoint qui utilisent des NLB et des GWLB.
5. Pour Service Name (Nom du service), saisissez le nom du service et choisissez Verify service (Vérifier le service).
6. Pour VPC, sélectionnez le VPC à partir duquel vous accéderez au service Endpoint.
7. Pour Sous-réseaux, sélectionnez un sous-réseau dans lequel vous souhaitez créer une interface réseau de point de terminaison.
8. Pour IP address type (Type d'adresse IP), choisissez l'une des options suivantes :
 - IPv4 — Attribuez des adresses IPv4 à l'interface réseau du terminal. Cette option n'est prise en charge que si le sous-réseau sélectionné possède une plage d'adresses IPv4.
 - IPv6 — Attribuez des adresses IPv6 à l'interface réseau du point de terminaison. Cette option n'est prise en charge que si le sous-réseau sélectionné est un sous-réseau IPv6 uniquement.
 - Dualstack : attribuez des adresses IPv4 et IPv6 à l'interface réseau du point de terminaison. Cette option n'est prise en charge que si le sous-réseau sélectionné possède à la fois des plages d'adresses IPv4 et IPv6.
9. (Facultatif) Pour ajouter une balise, choisissez Ajouter une nouvelle balise et entrez la clé et la valeur de la balise.
10. Choisissez Créer un point de terminaison. L'état initial est pending acceptance.

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

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

Configurer le routage

Utilisez la procédure suivante pour configurer les tables de routage pour le VPC du consommateur du service. Cela permet aux dispositifs de sécurité d'effectuer une inspection de sécurité du trafic entrant destiné aux serveurs d'applications. Pour de plus amples informations, veuillez consulter [the section called "Routing"](#).

Pour configurer le routage à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Tables de routage.
3. Sélectionnez la table de routage pour la passerelle Internet et procédez comme suit :
 - a. Choisissez Actions, Modifier les routes.
 - b. Si vous êtes compatible avec IPv4, choisissez Add route (Ajouter un itinéraire). Pour Destination, entrez le bloc CIDR IPv4 du sous-réseau pour les serveurs d'applications. Pour Target (Cible), sélectionnez le point de terminaison d'un VPC.
 - c. Si vous prenez en charge IPv6, choisissez Add route (Ajouter un itinéraire). Pour Destination, entrez le bloc CIDR IPv6 du sous-réseau pour les serveurs d'applications. Pour Target (Cible), sélectionnez le point de terminaison d'un VPC.
 - d. Sélectionnez Enregistrer les modifications.
4. Sélectionnez la table de routage pour le sous-réseau avec les serveurs d'applications et procédez comme suit :
 - a. Choisissez Actions, Modifier les routes.
 - b. Si vous prenez en charge IPv4, choisissez Add route (Ajouter un itinéraire). En regard de Destination, entrez `0.0.0.0/0`. Pour Target (Cible), sélectionnez le point de terminaison d'un VPC.
 - c. Si vous prenez en charge IPv6, choisissez Add route (Ajouter un itinéraire). En regard de Destination, entrez `::/0`. Pour Target (Cible), sélectionnez le point de terminaison de VPC.

- d. Sélectionnez Enregistrer les modifications.
5. Sélectionnez la table de routage pour le sous-réseau avec le point de terminaison d'équilibreur de charge de passerelle, puis procédez comme suit :
 - a. Choisissez Actions, Modifier les routes.
 - b. Si vous prenez en charge IPv4, choisissez Add route (Ajouter un itinéraire). En regard de Destination, entrez **0.0.0.0/0**. Pour Target (Cible), sélectionnez la passerelle Internet.
 - c. Si vous prenez en charge IPv6, choisissez Add route (Ajouter un itinéraire). En regard de Destination, entrez **::/0**. Pour Target (Cible), sélectionnez la passerelle Internet.
 - d. Sélectionnez Enregistrer les modifications.

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

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

Gestion des balises

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

Pour gérer les balises à l'aide de la console

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

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

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

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

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

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

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

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

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

Accédez aux ressources VPC via AWS PrivateLink

Vous pouvez accéder en privé à une ressource VPC dans un autre VPC à l'aide d'un point de terminaison VPC de ressource (point de terminaison de ressource). Un point de terminaison de ressources vous permet d'accéder de manière privée et sécurisée à des ressources VPC telles qu'une base de données, une instance Amazon EC2, un point de terminaison d'application, une cible de nom de domaine ou une adresse IP qui peut se trouver dans un sous-réseau privé d'un autre VPC ou dans un environnement sur site. Sans points de terminaison de ressources, vous devez soit ajouter une passerelle Internet à votre VPC, soit accéder à la ressource à l'aide d'un point de terminaison d' AWS PrivateLink interface et d'un équilibreur de charge réseau. Les points de terminaison des ressources ne nécessitent pas d'[équilibreur de charge](#), vous pouvez donc accéder directement à la ressource VPC. Une ressource VPC est représentée par une configuration de ressources. Une configuration de ressources est associée à une passerelle de ressources.

Tarification

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

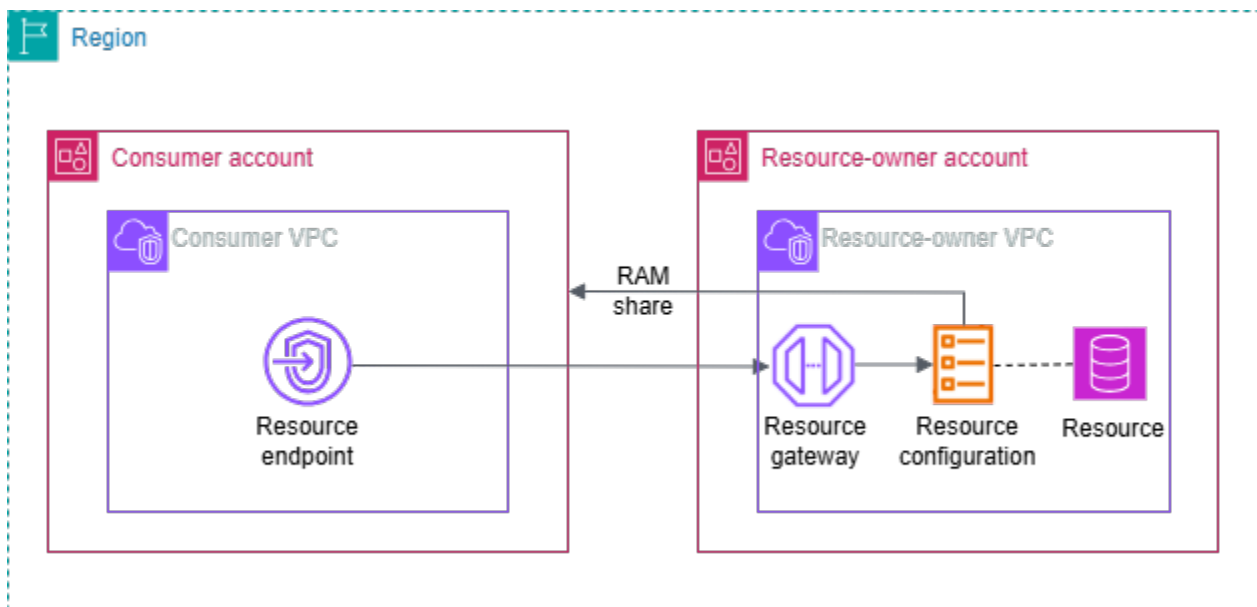
Table des matières

- [Vue d'ensemble](#)
- [Noms d'hôte DNS](#)
- [Résolution DNS](#)
- [DNS privé](#)
- [Sous-réseaux et zones de disponibilité](#)
- [Types d'adresses IP](#)
- [Accès à une ressource via un point de terminaison VPC](#)
- [Gérer les points de terminaison des ressources](#)

Vue d'ensemble

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

L'image suivante montre le point de terminaison d'une ressource dans un compte client accédant à une ressource détenue par un autre compte et partagée via AWS RAM :



Considérations

- Le trafic TCP est pris en charge. Le trafic UDP n'est pas pris en charge.
- Les connexions réseau doivent être initiées depuis le VPC qui contient le point de terminaison de la ressource, et non depuis le VPC qui possède la ressource. Le VPC de la ressource ne peut pas établir de connexions réseau avec le VPC du point de terminaison.
- Les seules ARN-based ressources prises en charge sont les ressources Amazon RDS.
- Au moins une zone de disponibilité du point de terminaison du VPC et de la passerelle de ressources doit se chevaucher.

Noms d'hôte DNS

Avec AWS PrivateLink, vous envoyez du trafic vers des ressources à l'aide de points de terminaison privés. Lorsque vous créez un point de terminaison VPC de ressource, nous créons des noms DNS régionaux (appelés nom DNS par défaut) que vous pouvez utiliser pour communiquer avec la ressource depuis votre VPC et depuis vos locaux. Nous vous recommandons d'utiliser le DNS au lieu des adresses IP des terminaux pour vous connecter à vos ressources. Le nom DNS par défaut de votre point de terminaison VPC de ressource a la syntaxe suivante :

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

Lorsque vous créez un point de terminaison VPC de ressources pour certaines configurations de ressources qui utilisent des ARN, vous pouvez activer le DNS [privé](#). Avec le DNS privé, vous pouvez continuer à envoyer des requêtes à la ressource en utilisant le nom DNS fourni pour la ressource par le AWS service, tout en tirant parti de la connectivité privée via le point de terminaison VPC de la ressource. Pour plus d'informations, consultez [the section called "Résolution DNS"](#).

La [commande](#) `describe-vpc-endpoint-associations` suivante affiche les entrées DNS pour un point de terminaison de ressource.

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

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

```
[  
  [  
    "vpce-rsc-asc-abcd1234abcd",  
    "vpce-123456789abcdefgh",  
    "Accessible",  
    {  
      "DnsName": "vpce-1234567890abcdefg-  
snra-1234567890abcdefg.rcfg-abcdefgh123456789.4232ccc.vpc-lattice-rsc.us-  
east-1.on.aws",  
      "HostedZoneId": "ABCDEFGH123456789000"  
    },  
  ],  
]
```

```
{
  "DnsName": "database-5-test.cluster-ro-example.us-east-1.rds.amazonaws.com",
  "HostedZoneId": "A1B2CD3E4F5G6H8I91234"
},
"arn:aws:vpc-lattice:us-east-1:111122223333:resourceconfiguration/rcfg-1234567890abcdefg",
"arn:aws:vpc-lattice:us-east-1:111122223333:resourceconfiguration/rcfg-1234567890xyz"
]
```

Résolution DNS

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

DNS privé

Si vous activez le DNS privé pour votre point de terminaison VPC de ressources pour certaines configurations de ressources qui utilisent des ARN, et que les noms d'hôte [DNS et la résolution DNS de votre VPC sont](#) activés, nous créons des zones hébergées privées masquées et AWS gérées pour les configurations de ressources avec un nom DNS personnalisé. La zone hébergée contient un enregistrement défini pour le nom DNS par défaut de la ressource qui le résout en adresses IP privées des interfaces réseau du point de terminaison de la ressource dans votre VPC.

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

Sous-réseaux et zones de disponibilité

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

Types d'adresses IP

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

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

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

Accès à une ressource via un point de terminaison VPC

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

Conditions préalables

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

- Vous devez disposer d'une configuration de ressources que vous avez créée ou d'un autre compte créé et partagé avec vous via AWS RAM.
- Si une configuration de ressources est partagée avec vous à partir d'un autre compte, vous devez vérifier et accepter le partage de ressources qui contient la configuration des ressources. Pour plus d'informations, consultez [Acceptation et refus des invitations](#) dans le Guide de l'utilisateur AWS RAM .

VPC Lattice ne crée pas de point de terminaison de ressource si les conditions suivantes sont remplies :

- La passerelle de ressources se trouve dans le même VPC que le point de terminaison des ressources.
- Pour les cibles de noms de domaine
 - La résolution DNS est définie sur IN_VPC sur la passerelle de ressources.
 - Le nom de domaine personnalisé ou le domaine de groupe est le même domaine de niveau ou d'un niveau supérieur que le nom de domaine cible.

Création d'un point de terminaison de ressources VPC

Suivez la procédure suivante pour créer un point de terminaison de ressource VPC. Après avoir créé un point de terminaison de ressource, vous pouvez uniquement modifier ses groupes de sécurité ou ses balises.

Pour créer un point de terminaison de ressources VPC

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Vous pouvez spécifier un nom pour faciliter la recherche et la gestion du point de terminaison.
5. Pour Type, choisissez Ressources.
6. Pour Configurations des ressources, sélectionnez la configuration des ressources.
7. Pour les paramètres réseau, sélectionnez le VPC à partir duquel vous allez accéder à la ressource.
8. Si vous souhaitez configurer la prise en charge du DNS privé pour les configurations de ressources, sélectionnez Paramètres supplémentaires, Activer le nom DNS. Pour utiliser cette fonctionnalité, assurez-vous que les attributs Activer les noms d'hôte DNS et Activer le support DNS sont activés pour votre VPC. Pour plus d'informations, consultez [the section called "Noms de domaine personnalisés pour les consommateurs de ressources"](#).
9. Pour Sous-réseaux, sélectionnez un sous-réseau dans lequel créer l'interface réseau du point de terminaison.

Dans un environnement de production, pour des raisons de haute disponibilité et de résilience, nous vous recommandons de configurer au moins deux zones de disponibilité pour chaque point de terminaison VPC.

10. Pour Groupes de sécurité, sélectionnez un groupe de sécurité.

Si vous ne spécifiez pas de groupe de sécurité, nous associons le groupe de sécurité par défaut pour le VPC.

11. Choisissez Créer un point de terminaison.

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

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

Gérer les points de terminaison des ressources

Après avoir créé un point de terminaison de ressource, vous pouvez gérer ses groupes de sécurité ou ses balises.

Tâches

- [Supprimer un point de terminaison](#)
- [Mettre à jour un point de terminaison](#)

Supprimer un point de terminaison

Lorsque vous avez terminé avec un point de terminaison de VPC, vous pouvez le supprimer.

Pour supprimer un terminal à l'aide de la console

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

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

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

Mettre à jour un point de terminaison

Vous pouvez mettre à jour un point de terminaison VPC.

Pour mettre à jour un terminal à l'aide de la console

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

4. Choisissez Actions, puis l'option appropriée.
5. Suivez les étapes de la console pour soumettre la mise à jour.

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

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

Accédez à des segments de réseau via AWS PrivateLink

Vous pouvez accéder en privé à un segment de réseau dans un autre VPC à l'aide d'un point de terminaison VPC tunnel (point de terminaison de tunnel). Un point de terminaison de tunnel vous permet d'accéder de manière privée et sécurisée aux ressources situées dans un ensemble de plages CIDR sur un autre réseau. Une plage CIDR représente un segment de réseau, de sorte qu'une application client peut accéder à n'importe quelle ressource de ce segment de réseau, sans que le fournisseur ait à énumérer chaque ressource. Ceci est utile lorsque les ressources sont éphémères ou ne sont pas connues à l'avance. Les points de terminaison du tunnel nécessitent que vous effectuiez un tunnel vers un autre VPC à l'aide de l'encapsulation GENEVE.

Tarification

Lorsque vous accédez à un segment de réseau à l'aide d'un point de terminaison de tunnel, vous êtes facturé pour chaque heure pendant laquelle votre point de terminaison de tunnel est provisionné. Vous êtes également facturé par Go de données traitées lorsque vous accédez au segment de réseau. Pour en savoir plus, consultez [Pricing AWS PrivateLink](#) (Tarification). Lorsque vous partagez votre segment de réseau à l'aide de configurations de ressources et de passerelles de ressources, vous êtes facturé par Go de données traitées par vos passerelles de ressources. Pour en savoir plus, consultez [Pricing Amazon VPC Lattice](#) (Tarification).

Table des matières

- [Vue d'ensemble](#)
- [Encapsulation GENEVE](#)
- [Noms d'hôte DNS](#)
- [Résolution DNS](#)
- [DNS privé](#)
- [Sous-réseaux et Zones de disponibilité](#)
- [Types d'adresses IP](#)
- [Accédez à un segment de réseau via un point de terminaison VPC tunnel](#)

Vue d'ensemble

Vous pouvez accéder aux segments de réseau de votre compte ou à ceux qui ont été partagés avec vous depuis un autre compte. Pour accéder à un segment de réseau, vous devez d'abord créer

un point de terminaison de tunnel, qui établit une connexion entre votre VPC et une passerelle de ressources dans le VPC à partir duquel le segment de réseau est partagé. Vous encapsulez ensuite le trafic des applications à l'aide de GENEVE et vous l'envoyez au point de terminaison du tunnel. Le point de terminaison supprime l'en-tête GENEVE et envoie le paquet interne à sa destination dans l'autre VPC. Ce faisant, il vérifie si la destination se trouve dans le segment de réseau qui a été partagé avec vous depuis l'autre VPC. S'il se trouve à l'extérieur, le terminal n'autorise pas l'accès à celui-ci.

Considérations

- Les sous-réseaux du point de terminaison du tunnel doivent Zones de disponibilité se chevaucher avec ceux Zones de disponibilité des sous-réseaux dans lesquels se trouve la passerelle de ressources.
- Les connexions réseau ne peuvent être initiées qu'à partir du VPC qui possède le point de terminaison du tunnel, et non du VPC qui partage les segments de réseau. Le VPC de segment de réseau ne peut pas établir de connexions réseau avec le VPC de point de terminaison.

Encapsulation GENEVE

Le trafic applicatif doit être encapsulé dans GENEVE. Le trafic GENEVE doit utiliser UDP et le port 6081 sur le point de terminaison du tunnel. Le VNI doit être réglé sur 0. Le paquet interne doit être un paquet IP de couche 3. Dans le paquet interne, le protocole UDP n'est pris en charge que pour les requêtes DNS. Le trafic d'application normal dans le paquet interne doit être TCP.

Noms d'hôte DNS

Un point de terminaison de tunnel possède un nom DNS régional. Il se résout en adresses IP dans les sous-réseaux où le point de terminaison du tunnel est créé. Ces adresses IP doivent être la cible de votre GENEVE-encapsulated trafic, et non du trafic des applications. Les noms DNS privés ne sont pas pris en charge pour les points de terminaison des tunnels.

Résolution DNS

Un point de terminaison de tunnel vous permet de résoudre le DNS dans le contexte du VPC qui partage le segment de réseau. Vous pouvez résoudre un domaine via le point de terminaison du tunnel par rapport au résolveur DNS du VPC distant. Pour ce faire, vous l'utilisez 169.254.168.253

comme serveur de noms. Vous le définissez comme destination de la requête DNS dans le paquet interne et vous l'encapsulez dans GENEVE comme vous le faites pour le trafic des applications. La résolution DNS est identique à celle d'un client dans le VPC distant. Il est basé sur le jeu d'options DHCP configuré par le VPC distant. Il respecte les zones hébergées privées Route 53 ou les résolveurs personnalisés configurés dans le VPC distant.

DNS privé

Les noms DNS privés ne sont pas pris en charge pour les points de terminaison des tunnels.

Sous-réseaux et Zones de disponibilité

Vous pouvez configurer votre point de terminaison de tunnel avec un sous-réseau par zone de disponibilité. Des interfaces réseau élastiques sont créées pour le point de terminaison de ces sous-réseaux. Une adresse IP est attribuée à chaque ENI à partir de son sous-réseau, en fonction du type d'adresse IP du point de terminaison. Dans un environnement de production, pour des raisons de haute disponibilité et de résilience, nous vous recommandons d'en configurer au moins deux Zones de disponibilité pour chaque point de terminaison. Les sous-réseaux du point de terminaison doivent Zones de disponibilité se chevaucher avec ceux Zones de disponibilité des sous-réseaux dans lesquels se trouve la passerelle de ressources.

Types d'adresses IP

Les paquets externes et internes peuvent avoir différents types d'adresses IP. Les combinaisons suivantes sont prises en charge : IPv4 sur IPv4, IPv6 sur IPv4, IPv4 sur IPv6 et IPv6 sur IPv6.

Le type IP du point de terminaison du tunnel détermine le type IP du paquet GENEVE externe. Le type IP du VPC distant détermine le type IP du paquet interne. Un segment de réseau partagé peut avoir à la fois des plages IPv4 et IPv6.

Les points de terminaison du tunnel prennent en charge les adresses IPv4, IPv6 ou Dualstack. Le type d'adresse IP d'un point de terminaison de tunnel doit être compatible avec les sous-réseaux du point de terminaison du tunnel, comme décrit ici :

- IPv4 — Assigne des adresses IPv4 au point de terminaison du tunnel. Pris en charge uniquement si tous les sous-réseaux du terminal ont des plages IPv4.
- IPv6 : attribue des adresses IPv6 au point de terminaison du tunnel. Pris en charge uniquement si tous les sous-réseaux du terminal possèdent des plages IPv6.

- Dualstack : attribue des adresses IPv4 et IPv6 au point de terminaison du tunnel. Pris en charge uniquement si tous les sous-réseaux du terminal possèdent à la fois des plages IPv4 et IPv6.

Les adresses IPv6 du terminal sont inaccessibles depuis Internet. `denyAllIgwTraffic` est activé sur ses interfaces réseau.

Accédez à un segment de réseau via un point de terminaison VPC tunnel

Vous pouvez accéder à un segment de réseau via un point de terminaison de tunnel. Un segment de réseau est un ensemble de plages CIDR. Elle est partagée en tant que configuration de ressource de type CIDR. Un point de terminaison de tunnel est associé à une seule configuration de CIDR-type ressources.

Conditions préalables

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

- Vous devez disposer d'une configuration de CIDR-type ressources que vous avez créée ou qu'un autre compte a créée et partagée avec vous via AWS RAM.
- Si une configuration de ressources est partagée avec vous à partir d'un autre compte, vous devez vérifier et accepter le partage de ressources qui contient la configuration des ressources. Pour plus d'informations, consultez [Acceptation et refus des invitations](#) dans le Guide de l'utilisateur AWS RAM .
- La configuration des ressources doit être attachée à une passerelle de ressources dont l'indicateur de résolution DNS est défini sur `IN_VPC`.
- Votre VPC client doit comporter des sous-réseaux Zones de disponibilité qui chevauchent ceux de la passerelle de ressources du fournisseur. Zones de disponibilité
- Votre ordinateur grand public doit être capable d'encapsuler le trafic applicatif dans GENEVE. Le VNI doit être réglé sur. 0 Le paquet interne doit être un paquet IP de couche 3. Cela devrait idéalement être effectué dans son propre contexte de routage ou espace de noms réseau.
- Les groupes de sécurité sur le terminal et sur le calcul doivent autoriser le port UDP 6081.

Création d'un point de terminaison VPC tunnel

Après avoir créé un point de terminaison de tunnel, vous devez décrire son association pour obtenir les adresses IP des points de terminaison par zone de disponibilité, puis configurer le périphérique GENEVE et le serveur de noms du tunnel sur votre ordinateur.

Pour créer un point de terminaison de tunnel (console)

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. (Facultatif) Entrez un nom pour faciliter la recherche et la gestion du terminal.
5. Pour Type, choisissez le type d'extrémité du tunnel.
6. Pour les configurations de ressources, sélectionnez la configuration des ressources CIDR.
7. Pour les paramètres réseau, sélectionnez le VPC à partir duquel vous allez accéder à la gamme.
8. Pour Sous-réseaux, sélectionnez un sous-réseau dans chaque zone de disponibilité qui chevauche celui de la passerelle de ressources. Zones de disponibilité
9. Pour Groupes de sécurité, sélectionnez un groupe de sécurité qui autorise le port UDP 6081. Si vous ne spécifiez pas de groupe de sécurité, nous associons le groupe de sécurité par défaut pour le VPC.
10. Choisissez Créer un point de terminaison.

La [commande](#) `create-vpc-endpoint` suivante crée un point de terminaison de tunnel pour une configuration de ressource CIDR :

```
aws ec2 create-vpc-endpoint \  
  --vpc-endpoint-type Tunnel \  
  --vpc-id vpc-1a2b3c4d \  
  --subnet-ids subnet-1a2b3c4d \  
  --ip-address-type ipv4 \  
  --resource-configuration-arn arn:aws:vpc-lattice:us-  
east-1:111122223333:resourceconfiguration/rcfg-1234567890abcdefg
```

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

- [create-vpc-endpoint](#) (AWS CLI)

- [New-EC2VpcEndpoint](#)(Outils pour Windows PowerShell)

Accédez aux réseaux de services via AWS PrivateLink

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

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

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

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

Tarification

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

Table des matières

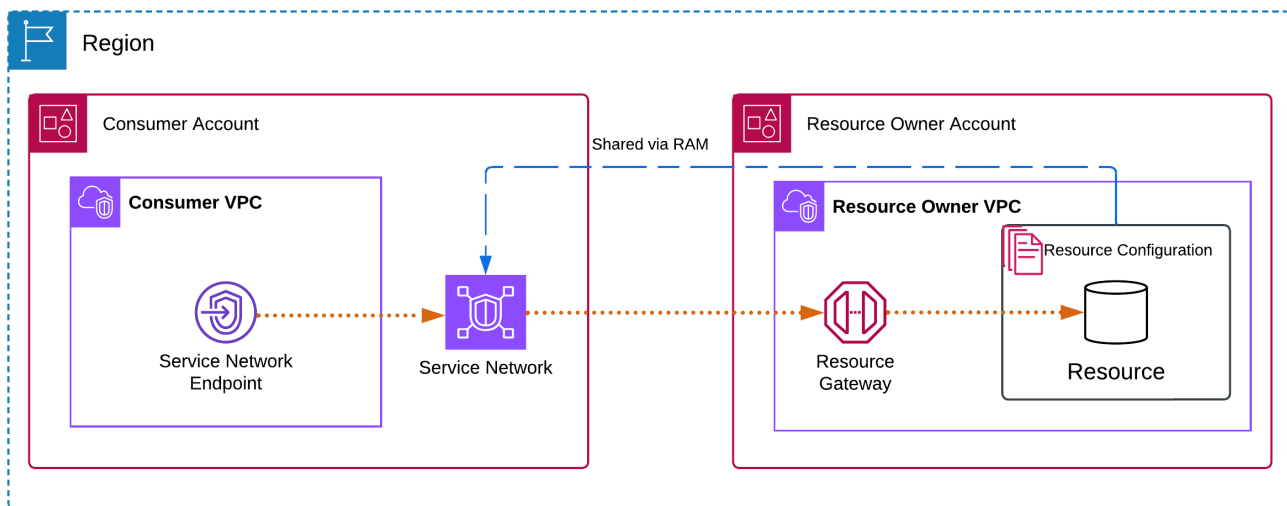
- [Présentation de](#)

- [Noms d'hôte DNS](#)
- [Résolution DNS](#)
- [DNS privé](#)
- [Sous-réseaux et zones de disponibilité](#)
- [Types d'adresses IP](#)
- [Accédez à un réseau de service via un point de terminaison de réseau de service](#)
- [Gérer les points de terminaison des réseaux de services](#)

Présentation de

Vous pouvez soit créer votre propre réseau de service, soit partager un réseau de service avec vous à partir d'un autre compte. Dans les deux cas, vous pouvez créer un point de terminaison de réseau de services pour vous y connecter depuis votre VPC. Pour plus d'informations sur la façon de créer un réseau de services et d'y associer des configurations de ressources, consultez le guide de l'utilisateur [Amazon VPC Lattice](#).

Le schéma suivant montre comment un point de terminaison de réseau de service de votre VPC accède à un réseau de service.



Les connexions réseau peuvent uniquement être initiées depuis le VPC qui possède le point de terminaison du réseau de services vers les ressources et les services du réseau de service. Le VPC doté des ressources et des services ne peut pas établir de connexions réseau avec le VPC de point de terminaison.

Noms d'hôte DNS

Avec AWS PrivateLink, vous envoyez du trafic vers des réseaux de service à l'aide de points de terminaison privés. Lorsque vous créez un point de terminaison VPC de réseau de services, nous créons des noms DNS régionaux (appelés nom DNS par défaut) pour chaque ressource et service que vous pouvez utiliser pour communiquer avec la ressource et le service depuis votre VPC et depuis vos locaux. Les adresses IP associées au terminal peuvent changer. Nous vous recommandons d'utiliser le DNS au lieu des adresses IP des terminaux pour vous connecter à vos réseaux de service.

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

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

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

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

Si vous utilisez le Console de gestion AWS, vous trouverez le nom DNS dans l'onglet **Associations**. Si vous utilisez le AWS CLI, utilisez la commande <https://docs.aws.amazon.com/cli/latest/reference/ec2/describe-vpc-endpoint-associations.html> `describe-vpc-endpoint-associations`.

Vous ne pouvez activer le DNS privé que lorsque votre réseau de service possède une configuration de ARN-type ressources pour un service de base de données Amazon RDS. Avec le DNS privé, vous pouvez continuer à adresser des requêtes à la ressource en utilisant le nom DNS fourni pour la ressource par le AWS service, tout en tirant parti de la connectivité privée via le point de terminaison VPC du réseau de services. Pour de plus amples informations, veuillez consulter [the section called "Résolution DNS"](#).

Résolution DNS

Lorsque vous créez un point de terminaison de réseau de service, nous créons des noms DNS pour chaque configuration de ressource et chaque service Lattice associé au réseau de service. Ces enregistrements DNS sont publics. Par conséquent, ces noms DNS peuvent être résolus publiquement. Cependant, les requêtes DNS provenant de l'extérieur du VPC renvoient toujours les adresses IP privées des interfaces réseau du point de terminaison du réseau de service. Vous pouvez utiliser ces noms DNS pour accéder à la ressource et aux services depuis votre site, tant que

vous avez accès au VPC dans lequel se trouve le point de terminaison du réseau de services, via VPN ou Direct Connect.

DNS privé

Si vous activez le DNS privé pour le point de terminaison VPC de votre réseau de services et que les noms d'hôte [DNS et la résolution DNS sont](#) activés sur votre VPC, nous créons des zones hébergées privées masquées et AWS gérées pour les configurations de ressources qui ont des noms DNS personnalisés. La zone hébergée contient un enregistrement défini pour le nom DNS par défaut de la ressource qui le résout en adresses IP privées des interfaces réseau du point de terminaison du réseau de services dans votre VPC.

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

Sous-réseaux et zones de disponibilité

Vous pouvez configurer le point de terminaison de votre réseau de service avec un sous-réseau par zone de disponibilité. Nous créons une interface réseau élastique pour le point de terminaison VPC de chaque sous-réseau que vous spécifiez. Nous attribuons des adresses IP à chaque interface réseau élastique à partir de son sous-réseau comme suit :

- Services VPC Lattice (couche 7) — Nous attribuons un bloc /28 (16 adresses IPv4 contiguës) par zone de disponibilité pour tous les services VPC Lattice associés au réseau de services. Ce bloc /28 est alloué lors de la création du point de terminaison du réseau de services, même s'il n'y a aucun service actuellement sur le réseau de service. Le bloc /28 doit être composé de 16 adresses IPv4 contiguës et inoccupées et il ne peut pas chevaucher les cinq adresses AWS réservées (les quatre premières et la dernière adresse IP). Assurez-vous qu'un espace d'adressage contigu libre suffisant est disponible. Pour IPv6, nous attribuons également un bloc /80 par zone de disponibilité pour les services VPC Lattice.
- Ressources VPC Lattice (couche 4/TCP) : nous attribuons une adresse IPv4 par configuration de ressource et par zone de disponibilité. Un espace d'adressage contigu n'est pas requis pour les

ressources VPC Lattice. Nous attribuons jusqu'à 63 adresses IP par interface réseau élastique. Lorsque des configurations de ressources supplémentaires dépassent cette limite, nous créons une autre interface réseau élastique dans le même sous-réseau. Pour IPv6, nous attribuons un bloc /80 à la première interface réseau élastique créée pour les ressources ; aucune interface réseau élastique supplémentaire n'est créée lors de l'utilisation d'IPv6. Lorsque vous supprimez une configuration de ressource du réseau de service, nous libérons son adresse IP associée. Lorsque toutes les adresses IPv4 d'une interface réseau élastique sont libérées, nous supprimons l'interface réseau élastique.

Dans un environnement de production, pour des raisons de haute disponibilité et de résilience, nous vous recommandons de configurer au moins deux zones de disponibilité pour chaque point de terminaison du réseau de service et de vous assurer que chaque sous-réseau dispose d'un nombre suffisant d'adresses IPv4 disponibles.

Types d'adresses IP

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

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

Si un point de terminaison VPC de réseau de services prend en charge le protocole IPv4, les interfaces réseau du point de terminaison possèdent des adresses IPv4. Si un point de terminaison VPC de réseau de services prend en charge le protocole IPv6, les interfaces réseau du point de terminaison possèdent des adresses IPv6. L'adresse IPv6 d'une interface réseau de point de

terminaison est inaccessible depuis Internet. Si vous décrivez une interface réseau de point de terminaison avec une adresse IPv6, remarquez que `denyAllIgwTraffic` est activé.

Accédez à un réseau de service via un point de terminaison de réseau de service

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

Conditions préalables

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

- Vous devez disposer d'un réseau de service créé par vous ou partagé avec vous à partir d'un autre compte via AWS RAM.
- Si un réseau de service est partagé avec vous à partir d'un autre compte, vous devez vérifier et accepter le partage de ressources qui contient le réseau de service. Pour plus d'informations, consultez [Acceptation et refus des invitations](#) dans le Guide de l'utilisateur AWS RAM .
- Pour les services VPC Lattice associés au réseau de service, le point de terminaison du réseau de services nécessite un bloc /28 contigu (16 adresses IPv4) par zone de disponibilité. Ce bloc /28 est alloué lors de la création du point de terminaison, même si aucun service n'est actuellement présent sur le réseau de services. Le bloc /28 doit être composé de 16 adresses IPv4 contiguës et inoccupées et ne peut pas chevaucher les cinq adresses AWS réservées (les quatre premières et la dernière adresse IP du sous-réseau). Pour IPv6, un bloc /80 par zone de disponibilité est alloué aux services VPC Lattice. Assurez-vous qu'un espace d'adressage contigu libre suffisant est disponible dans chaque sous-réseau que vous sélectionnez.
- Pour les ressources VPC Lattice (couche 4/TCP) associées au réseau de service, une adresse IPv4 par configuration de ressource et par zone de disponibilité est requise. Un espace d'adressage contigu n'est pas nécessaire. Jusqu'à 63 adresses IP peuvent être attribuées par interface réseau élastique. Lorsque des configurations de ressources supplémentaires dépassent cette limite, une interface réseau élastique supplémentaire est créée dans le même sous-réseau. Pour IPv6, un bloc /80 est attribué à la première interface réseau élastique créée pour les ressources ; aucune interface réseau élastique supplémentaire n'est créée lors de l'utilisation d'IPv6.

Si vous devez éviter de consommer des adresses IP CIDR VPC ou anticiper un grand nombre de configurations de ressources associées au réseau de service, envisagez plutôt d'utiliser une association VPC de réseau de service. Pour plus d'informations, consultez [Gérer les associations de points de terminaison VPC](#) dans le guide de l'utilisateur Amazon VPC Lattice.

Création d'un point de terminaison de réseau de service

Créez un point de terminaison de réseau de service pour accéder au réseau de service qui a été partagé avec vous. Après avoir créé un point de terminaison de réseau de services, vous pouvez uniquement modifier ses groupes de sécurité ou ses balises.

Pour créer un point de terminaison de réseau de services

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, sous PrivateLink Lattice, choisissez Endpoints.
3. Choisissez Créer un point de terminaison.
4. Vous pouvez spécifier un nom pour faciliter la recherche et la gestion du point de terminaison.
5. Pour Type, choisissez Réseaux de service.
6. Pour Réseaux de service, sélectionnez le réseau de service.
7. Pour les paramètres réseau, sélectionnez le VPC à partir duquel vous allez accéder au réseau de service.
8. Si vous souhaitez configurer la prise en charge du DNS privé, sélectionnez Paramètres supplémentaires, Activer le nom DNS privé. Pour utiliser cette fonctionnalité, assurez-vous que les attributs Activer les noms d'hôte DNS et Activer le support DNS sont activés pour votre VPC.
9. Pour Sous-réseaux, sélectionnez un sous-réseau dans lequel créer l'interface réseau du point de terminaison.

Dans un environnement de production, pour des raisons de haute disponibilité et de résilience, nous vous recommandons de configurer au moins deux zones de disponibilité pour chaque point de terminaison VPC.

10. Pour Groupes de sécurité, sélectionnez un groupe de sécurité.

Si vous ne spécifiez pas de groupe de sécurité, nous associons le groupe de sécurité par défaut pour le VPC.

11. Choisissez Créer un point de terminaison.

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

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

Gérer les points de terminaison des réseaux de services

Après avoir créé un point de terminaison de réseau de services, vous pouvez mettre à jour ses groupes de sécurité ou ses balises.

Tâches

- [Supprimer un point de terminaison](#)
- [Mettre à jour un point de terminaison de réseau de service](#)

Supprimer un point de terminaison

Lorsque vous avez terminé avec un point de terminaison de VPC, vous pouvez le supprimer.

Pour supprimer un terminal à l'aide de la console

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

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

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

Mettre à jour un point de terminaison de réseau de service

Vous pouvez mettre à jour un point de terminaison VPC.

Pour mettre à jour un terminal à l'aide de la console

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

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

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

Configuration des ressources pour les ressources VPC

Une configuration de ressources représente une ressource individuelle, un groupe de ressources ou une liste de plages d'adresses CIDR que vous souhaitez rendre accessibles aux clients d'autres VPC et comptes. En définissant une configuration de ressources, vous pouvez autoriser une connectivité réseau privée, sécurisée et unidirectionnelle aux ressources de votre VPC à partir de clients d'autres VPC et comptes. Une configuration de ressources est associée à une passerelle de ressources via laquelle elle reçoit le trafic.

Table des matières

- [Types de configurations de ressources](#)
- [Passerelle de ressources](#)
- [Noms de domaine personnalisés pour les fournisseurs de ressources](#)
- [Noms de domaine personnalisés pour les consommateurs de ressources](#)
- [Noms de domaine personnalisés pour les propriétaires de réseaux de service](#)
- [Définition de la ressource](#)
- [Protocole](#)
- [Gammes de ports](#)
- [Accès aux ressources](#)
- [Association avec le type de réseau de service](#)
- [Types de réseaux de services](#)
- [Partage de configurations de ressources via AWS RAM](#)
- [Contrôle](#)
- [Création d'une configuration de ressources dans VPC Lattice](#)
- [Gestion des associations pour une configuration de ressources VPC Lattice](#)

Types de configurations de ressources

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

- Configuration de ressource unique : adresse IP ou nom de domaine. Il peut être partagé indépendamment.

- Configuration des ressources du groupe : collection de configurations de ressources pour enfants. Il peut être partagé indépendamment.
- Configuration des ressources enfants : membre d'une configuration de ressources de groupe. Il représente une adresse IP ou un nom de domaine. Il ne peut pas être partagé indépendamment et ne peut être partagé que dans le cadre d'un groupe. Il peut être ajouté et supprimé d'un groupe en toute simplicité. Une fois ajouté, il est automatiquement accessible à ceux qui peuvent accéder au groupe.
- Configuration des ressources ARN : type de ressource pris en charge qui est provisionné par un AWS service. Par exemple, une base de données Amazon RDS. Les configurations des ressources pour enfants sont gérées automatiquement par AWS. Il peut être partagé indépendamment.
- Configuration des ressources CIDR : liste des plages CIDR. Il peut être partagé indépendamment.

Passerelle de ressources

Une configuration de ressources est associée à une passerelle de ressources. Une passerelle de ressources est un ensemble d'ENI qui servent de point d'entrée dans le VPC dans lequel se trouve la ressource. Plusieurs configurations de ressources peuvent être associées à la même passerelle de ressources. Lorsque les clients d'autres VPC ou comptes accèdent à une ressource de votre VPC, le trafic provient localement de la passerelle de ressources de ce VPC.

Noms de domaine personnalisés pour les fournisseurs de ressources

Les fournisseurs de ressources peuvent associer un nom de domaine personnalisé à une configuration de ressources, par exemple `example.com`, que les consommateurs de ressources peuvent utiliser pour accéder à la configuration des ressources. Le nom de domaine personnalisé peut être détenu et vérifié par le fournisseur de ressources, ou il peut s'agir d'un tiers ou d'un AWS domaine. Les fournisseurs de ressources peuvent utiliser des configurations de ressources pour partager des clusters de cache et des clusters Kafka, TLS-based des applications ou d'autres AWS ressources.

Les considérations suivantes s'appliquent aux fournisseurs de configurations de ressources :

- Une configuration de ressources ne peut avoir qu'un seul domaine personnalisé.

- Le nom de domaine personnalisé d'une configuration de ressources ne peut pas être modifié.
- Le nom de domaine personnalisé est visible pour tous les utilisateurs de configuration de ressources.
- Vous pouvez vérifier votre nom de domaine personnalisé à l'aide du processus de vérification du nom de domaine dans VPC Lattice. Pour plus d'informations, consultez <https://docs.aws.amazon.com/vpc-lattice/latest/ug/create-and-verify.html>.
- Pour les configurations de ressources de type groupe et enfant, vous devez d'abord spécifier un domaine de groupe dans la configuration des ressources de groupe. Ensuite, les configurations de ressources enfants peuvent avoir des domaines personnalisés qui sont des sous-domaines du domaine de groupe. Si le groupe ne possède pas de domaine de groupe, vous pouvez utiliser n'importe quel nom de domaine personnalisé pour l'enfant, mais VPC Lattice ne provisionnera aucune zone hébergée pour les noms de domaine enfants dans le VPC du consommateur de ressources.
- Les noms de domaine personnalisés ne sont pas pris en charge pour les configurations de ressources CIDR.

Noms de domaine personnalisés pour les consommateurs de ressources

Lorsque les consommateurs de ressources activent la connectivité à une configuration de ressources dotée d'un nom de domaine personnalisé, ils peuvent autoriser VPC Lattice à gérer une zone hébergée privée Route 53 dans leur VPC. Les consommateurs de ressources disposent d'options précises pour les domaines pour lesquels ils souhaitent autoriser VPC Lattice à gérer des zones hébergées privées.

Les consommateurs de ressources peuvent définir le `private-dns-enabled` paramètre lors de l'activation de la connectivité à des configurations de ressources via un point de terminaison de ressources, un point de terminaison de réseau de service ou une association VPC de réseau de services. Outre le `private-dns-enabled` paramètre, les consommateurs peuvent utiliser les options DNS pour spécifier les domaines pour lesquels ils souhaitent que VPC Lattice gère les zones hébergées privées pour lesquels ils souhaitent que VPC Lattice gère les zones hébergées privées. Les consommateurs peuvent choisir entre les préférences DNS privées suivantes :

ALL_DOMAINS

VPC Lattice fournit des zones hébergées privées pour tous les noms de domaine personnalisés.

VERIFIED_DOMAINS_ONLY

VPC Lattice fournit une zone hébergée privée uniquement si le nom de domaine personnalisé a été vérifié par le fournisseur.

VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS

VPC Lattice fournit des zones hébergées privées pour tous les noms de domaine personnalisés vérifiés et les autres noms de domaine spécifiés par le consommateur de ressources. Le consommateur de ressources spécifie les noms de domaine dans le `private DNS specified domains` paramètre.

SPECIFIED_DOMAINS_ONLY

VPC Lattice fournit une zone hébergée privée pour les noms de domaine spécifiés par le consommateur de ressources. Le consommateur de ressources spécifie les noms de domaine dans le `private DNS specified domains` paramètre.

Lorsque vous activez le DNS privé, VPC Lattice crée une zone hébergée privée dans votre VPC pour le nom de domaine personnalisé associé à la configuration des ressources. Par défaut, la préférence DNS privée est définie sur `VERIFIED_DOMAINS_ONLY`. Cela signifie que les zones hébergées privées ne sont créées que si le nom de domaine personnalisé a été vérifié par le fournisseur de ressources. Si vous définissez votre préférence DNS privée sur `ALL_DOMAINS` ou `SPECIFIED_DOMAINS_ONLY` si VPC Lattice crée des zones hébergées privées quel que soit l'état de vérification du nom de domaine personnalisé. Lorsqu'une zone hébergée privée est créée pour un domaine donné, tout le trafic vers ce domaine depuis votre VPC est acheminé via VPC Lattice. Nous vous recommandons d'utiliser les `SPECIFIED_DOMAINS_ONLY` préférences `ALL_DOMAINS`, `VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS`, ou uniquement lorsque vous souhaitez que le trafic vers ces noms de domaine personnalisés passe par VPC Lattice.

Nous recommandons aux utilisateurs de ressources de définir leur préférence DNS privé sur `VERIFIED_DOMAINS_ONLY`. Cela permet aux consommateurs de renforcer leur périmètre de sécurité en autorisant uniquement VPC Lattice à fournir des zones hébergées privées pour les domaines vérifiés sur le compte du consommateur de ressources.

Pour sélectionner des domaines dans les domaines spécifiés par le DNS privé, les consommateurs de ressources peuvent saisir un nom de domaine complet, tel que, `my.example.com` ou utiliser un caractère générique tel que `*.example.com`.

Les considérations suivantes s'appliquent aux utilisateurs de configurations de ressources :

- Le paramètre DNS privé activé ne peut pas être modifié.
- Le DNS privé doit être activé sur une association de ressources de réseau de service pour les zones hébergées privées à créer dans un VPC. Pour une configuration de ressources, l'état d'activation du DNS privé de l'association de ressources du réseau de service remplace l'état d'activation du DNS privé du point de terminaison du réseau de service ou de l'association VPC du réseau de service.

Pour les configurations de ressources qui sont des cibles de nom de domaine, aucune entrée de zone hébergée privée n'est créée si les conditions suivantes sont remplies :

- La passerelle de ressources se trouve dans le même VPC que l'association VPC du endpoint/service réseau de services.
- La résolution DNS est définie sur IN_VPC sur la passerelle de ressources.
- Le nom de domaine personnalisé ou le domaine de groupe est le même domaine de niveau ou d'un niveau supérieur que le nom de domaine cible.

Pour les configurations de ressources de type ARN, VPC Lattice ne crée pas d'entrée de zone hébergée privée si les conditions suivantes sont remplies :

- La passerelle de ressources se trouve dans le même VPC que l'association VPC du endpoint/service réseau de services.

Noms de domaine personnalisés pour les propriétaires de réseaux de service

La propriété privée activée par le DNS de l'association de ressources du réseau de service remplace la propriété privée activée du point de terminaison du réseau de service et l'association VPC du réseau de service.

Si le propriétaire d'un réseau de service crée une association de ressources de réseau de service et n'active pas le DNS privé, VPC Lattice ne provisionnera pas de zones hébergées privées pour cette configuration de ressources dans les VPC auxquels le réseau de service est connecté, même si le DNS privé est activé sur le point de terminaison du réseau de service ou les associations VPC du réseau de service.

Pour les configurations de ressources de type ARN, l'indicateur DNS privé est vrai et immuable. Par conséquent, VPC Lattice fournit des zones hébergées privées pour les types de ressources ARN indépendamment du paramètre de propriété DNS privé du point de terminaison du réseau de service et de l'association VPC du réseau de service, sauf lorsque la passerelle de ressources se trouve également dans le même VPC. En d'autres termes, lorsqu'un VPC est à la fois un consommateur et un fournisseur pour une configuration de ressources de type ARN, VPC Lattice ignore la création des zones hébergées privées dans un tel VPC.

Définition de la ressource

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

- Par un Amazon Resource Name (ARN) : les types de ressources pris en charge qui sont provisionnés par AWS les services peuvent être identifiés par leur ARN. Seules les bases de données Amazon RDS sont prises en charge. Vous ne pouvez pas créer de configuration de ressources pour un cluster accessible au public.
- Par une cible de nom de domaine : vous pouvez utiliser n'importe quel nom de domaine. Si vous utilisez un serveur DNS privé ou si votre domaine se trouve dans une zone hébergée privée Route 53, la résolution DNS de la passerelle de ressources doit être définie sur IN_VPC. Si votre nom de domaine pointe vers une adresse IP extérieure à votre VPC, vous devez disposer d'une passerelle NAT dans votre VPC. Domain-name les cibles qui renvoient à des adresses IPv6 publiques ne sont pas prises en charge.
- Par une adresse IP : pour IPv4, spécifiez une adresse IP privée parmi les plages suivantes : 10.0.0. 0/8, 100,64,0. 0/10, 172,16,0. 0/12, 192.168.0. 0/16. Pour IPv6, spécifiez une adresse IP depuis le VPC. Les adresses IP publiques ne sont pas prises en charge.
- Par plage d'adresses CIDR : pour une configuration de ressource de type CIDR, spécifiez la liste des CIDR que vous souhaitez partager (par exemple, 10.0.0). 0/24). Les CIDR doivent être accessibles depuis la passerelle de ressources. Pour fournir un accès complet au réseau, spécifiez 0.0.0. 0/0 si vous utilisez IPv4 ou : :0 si vous utilisez IPv6.

Protocole

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

Pour les configurations de ressources CIDR, le protocole doit être le suivant TCP_UDP : seul le protocole TCP est pris en charge pour le trafic des applications, le protocole UDP est uniquement pris en charge pour les requêtes DNS.

Gammes de ports

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

Accès aux ressources

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

- Accès direct à une configuration de ressources

Vous pouvez accéder aux configurations de ressources directement via des points de terminaison de ressources AWS PrivateLink basés et des points de terminaison de tunnel. Vous pouvez créer un point de terminaison de ressources dans votre VPC pour accéder à des configurations de ressources de type ARN, Single et Group, et vous pouvez créer un point de terminaison de tunnel pour accéder à des configurations de ressources de type CIDR. Pour plus d'informations sur la création de points de terminaison de ressources et de tunnels, consultez les rubriques [Accès aux ressources VPC](#) et [Accès aux segments réseau](#) dans le guide de l'AWS PrivateLink utilisateur.

- Accès à une configuration de ressources via un réseau de service

Vous pouvez associer une configuration de ressources à un réseau de service et connecter votre VPC au réseau de service. Vous pouvez connecter votre VPC au réseau de service via une association ou à l'aide d'un point de terminaison de réseau de service AWS PrivateLink basé. Les configurations de ressources CIDR ne peuvent pas être associées à un réseau de service.

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

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

Lorsque le DNS privé est activé pour votre VPC, vous ne pouvez pas créer de point de terminaison de ressources et de point de terminaison de réseau de services pour la même configuration de ressources.

Association avec le type de réseau de service

Lorsque vous partagez une configuration de ressources avec un compte client, par exemple, via Account-B AWS RAM, vous Account-B pouvez accéder à la configuration des ressources soit directement via un point de terminaison de ressource ou un point de terminaison de tunnel, soit via un réseau de service. Les configurations de ressources CIDR ne sont pas accessibles via un réseau de service. Ils ne sont accessibles que directement via un point de terminaison de tunnel.

Pour accéder à une configuration de ressources via un réseau de service, Account-B il faudrait associer la configuration de ressources à un réseau de service. Les réseaux de services peuvent être partagés entre les comptes. Account-B Vous pouvez donc partager leur réseau de service (auquel la configuration des ressources est associée) Account-C, rendant ainsi votre ressource accessible Account-C.

Pour empêcher un tel partage transitif, vous pouvez spécifier que la configuration de vos ressources ne peut pas être ajoutée aux réseaux de services qui peuvent être partagés entre comptes. Si vous le spécifiez, vous Account-B ne pourrez pas ajouter votre configuration de ressources aux réseaux de service partagés ou pouvant être partagés avec un autre compte ultérieurement.

Types de réseaux de services

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

- Utilisation d'un point de terminaison de ressource AWS PrivateLink basé (pour les configurations de ressources uniques, de groupe et ARN).
- Utilisation d'un point de terminaison de tunnel AWS PrivateLink basé (pour les configurations de ressources CIDR).
- Utilisation d'un point de terminaison de réseau de services AWS PrivateLink basé.
- Utilisation d'une association VPC de réseau de service.

Lorsque vous utilisez une association de réseau de service, chaque ressource se voit attribuer une adresse IP par sous-réseau à partir du 129.224.0. 0/17 bloc, qui est AWS détenu et non routable. Cela s'ajoute à la liste de [préfixes gérés](#) que VPC Lattice utilise pour acheminer le trafic vers les services via le réseau VPC Lattice. Ces deux adresses IP sont mises à jour dans la table de routage de votre VPC.

Pour l'association du point de terminaison du réseau de service et de l'association VPC du réseau de service, la configuration des ressources devrait être placée dans un réseau de service dans Account-B. Les réseaux de services peuvent être partagés entre les comptes. Account-B Vous pouvez donc partager leur réseau de service (qui contient la configuration des ressources) avec Account-C, rendant votre ressource accessible depuis Account-C. Pour empêcher un tel partage transitif, vous pouvez interdire l'ajout de votre configuration de ressources aux réseaux de services qui peuvent être partagés entre comptes. Si vous ne l'autorisez pas, vous Account-B ne pourrez pas ajouter votre configuration de ressources à un réseau de service partagé ou pouvant être partagé avec un autre compte.

Partage de configurations de ressources via AWS RAM

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

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

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

Contrôle

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

Création d'une configuration de ressources dans VPC Lattice

Créez une configuration de ressources.

Console de gestion AWS

Pour créer une configuration de ressources 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, sous PrivateLink Lattice, choisissez Resource Configurations.
3. Choisissez Créer une configuration de ressources.
4. Entrez un nom unique dans votre AWS compte. Vous ne pouvez pas modifier ce nom une fois la configuration des ressources créée.
5. Pour Type de configuration, choisissez Ressource pour une ressource unique ou enfant ou Groupe de ressources pour un groupe de ressources pour un groupe de ressources enfants.
6. Choisissez une passerelle de ressources que vous avez créée précédemment ou créez-en une maintenant.
7. (Facultatif) Pour saisir un nom de domaine personnalisé, effectuez l'une des opérations suivantes :
 - Si vous avez une configuration de ressources de type unique, vous pouvez saisir un nom de domaine personnalisé. Les consommateurs de ressources peuvent utiliser ce nom de domaine pour accéder à vos configurations de ressources.
 - Si vous avez une configuration de ressources de type groupe et enfant, vous devez d'abord spécifier un domaine de groupe dans la configuration des ressources de groupe. Ensuite, les configurations de ressources enfants peuvent avoir des domaines personnalisés qui sont des sous-domaines du domaine de groupe.
8. (Facultatif) Entrez le numéro de vérification.

Fournissez un identifiant de vérification si vous souhaitez que votre nom de domaine soit vérifié. Cela permet aux consommateurs de ressources de savoir que vous êtes propriétaire du nom de domaine.

9. Choisissez l'identifiant de la ressource que vous souhaitez que cette configuration de ressource représente.
10. Choisissez les plages de ports via lesquelles vous souhaitez partager la ressource.

11. Pour les paramètres d'association, indiquez si cette configuration de ressources peut être associée à des réseaux de services partageables.
12. Pour la configuration des ressources de partage, choisissez les partages de ressources qui identifient les principaux utilisateurs autorisés à accéder à cette ressource.
13. (Facultatif) Pour la surveillance, activez les journaux d'accès aux ressources et la destination de livraison si vous souhaitez surveiller les demandes et les réponses depuis et vers la configuration des ressources.
14. (Facultatif) Pour ajouter une balise, choisissez Ajouter une nouvelle balise et entrez la clé et la valeur de la balise.
15. Choisissez Créer une configuration de ressources.

AWS CLI

La [commande](#) `create-resource-configuration` suivante crée une configuration de ressource unique et l'associe au nom de domaine personnalisé. `example.com`

```
aws vpc-lattice create-resource-configuration \
  --name my-resource-config \
  --type SINGLE \
  --resource-gateway-identifiant rgw-0bba03f3d56060135 \
  --resource-configuration-definition 'ipResource={ipAddress=10.0.14.85}' \
  --custom-domain-name example.com \
  --verification-id dv-aaaa000000011111
```

La [commande](#) `create-resource-configuration` suivante crée une configuration de ressources de groupe et l'associe au nom de domaine personnalisé. `example.com`

```
aws vpc-lattice-custom-dns create-resource-configuration \
  --name my-custom-dns-resource-config-group \
  --type GROUP \
  --resource-gateway-identifiant rgw-0bba03f3d56060135 \
  --domain-verification-identifiant dv-aaaa000000011111
```

La [commande](#) `create-resource-configuration` suivante crée une configuration de ressource enfant et l'associe au nom de domaine personnalisé. `child.example.com`

```
aws vpc-lattice-custom-dns create-resource-configuration \
  --name my-custom-dns-resource-config-child \
```

```
--type CHILD \  
--resource-configuration-definition 'dnsResource={domainName=my-alb-123456789.us-west-2.elb.amazonaws.com,ipAddressType=IPV4}' \  
--resource-configuration-group-identifier rcfg-07129f3acded87626 \  
--custom-domain-name child.example.com
```

Gestion des associations pour une configuration de ressources VPC Lattice

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

Gérer les associations de ressources du réseau de services

Créez ou supprimez une association de réseau de service.

Note

Si vous recevez un message d'accès refusé lors de la création de l'association entre le réseau de service et la configuration des ressources, vérifiez la version de votre AWS RAM politique et assurez-vous qu'il s'agit de la version 2. Pour plus d'informations, consultez le guide de [AWS RAM l'utilisateur](#).

Pour gérer une association de services à un réseau 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, sous PrivateLink Lattice, choisissez Resource Configurations.
3. Sélectionnez le nom de la configuration des ressources pour ouvrir sa page de détails.
4. Sélectionnez l'onglet Associations de réseaux de services.
5. Choisissez Créer des associations.
6. Sélectionnez un réseau de service parmi les réseaux de service VPC Lattice. Pour créer un réseau de service, choisissez Créer un réseau VPC Lattice.

7. (Facultatif) Pour ajouter une étiquette, développez Tags d'association de services, choisissez Ajouter une nouvelle étiquette, puis entrez une clé de balise et une valeur de balise.
8. (Facultatif) Pour activer les noms DNS privés pour cette association de ressources réseau de service, choisissez Activer les noms DNS privés. Pour plus d'informations, consultez [the section called "Noms de domaine personnalisés pour les propriétaires de réseaux de service"](#).
9. Sélectionnez Save Changes (Enregistrer les modifications).
10. Pour supprimer une association, cochez la case correspondante, puis choisissez Actions, Supprimer. Lorsque vous êtes invité à confirmer, entrez **confirm**, puis choisissez Delete (Supprimer).

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

Utilisez la commande [create-service-network-resource-association](#).

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

Utilisez la commande [delete-service-network-resource-association](#).

Gérer les associations de points de terminaison VPC de ressources

Les comptes consommateurs ayant accès à la configuration de vos ressources ou les clients de votre compte peuvent accéder à la configuration des ressources à l'aide d'un point de terminaison VPC de ressources. Si votre configuration de ressources possède un nom de domaine personnalisé, vous pouvez utiliser Activer le DNS privé pour permettre à VPC Lattice de provisionner des zones hébergées privées pour votre point de terminaison de ressources ou votre point de terminaison de réseau de services. Les clients peuvent ainsi directement courber le nom de domaine pour accéder à la configuration des ressources. Pour plus d'informations, consultez [the section called "Noms de domaine personnalisés pour les consommateurs de ressources"](#).

Console de gestion AWS

1. Pour créer une nouvelle association de points de terminaison, accédez à PrivateLink Lattice dans le volet de navigation de gauche et choisissez Endpoints.
2. Choisissez Créer des points de terminaison.
3. Sélectionnez la configuration de ressources que vous souhaitez connecter à votre VPC.
4. Sélectionnez le VPC, les sous-réseaux et les groupes de sécurité.

5. (Facultatif) Pour activer le DNS privé et configurer les options DNS, sélectionnez **Activer le nom DNS**.
6. (Facultatif) Pour baliser votre point de terminaison VPC, choisissez **Ajouter une nouvelle étiquette**, puis entrez une clé de balise et une valeur de balise.
7. Choisissez **Créer un point de terminaison**.

AWS CLI

La [commande](#) `create-vpc-endpoint` suivante crée un point de terminaison VPC qui utilise un DNS privé. Les préférences DNS privées sont définies sur `VERIFIED_AND_SELECTED` et les domaines sélectionnés sont `example.com` et `example.org`. VPC Lattice fournit uniquement des zones hébergées privées pour tous les domaines vérifiés ou `example.com`, `example.org`

```
aws ec2 create-vpc-endpoint \  
  --vpc-endpoint-type Resource \  
  --vpc-id vpc-111122223333aabbcc \  
  --subnet-ids subnet-0011aabbcc2233445 \  
  --resource-configuration-arn arn:aws:vpc-lattice:us-  
west-2:111122223333:resourceconfiguration/rcfg-07129f3acded87625 \  
  --private-dns-enabled \  
  --private-dns-preferences VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS \  
  --private-domains-set example.com, example.org
```

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

Utilisez la commande [create-vpc-endpoint](#).

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

Utilisez la commande [delete-vpc-endpoint](#).

Passerelle de ressources dans VPC Lattice

Une passerelle de ressources est un point de trafic entrant vers le VPC où réside une ressource. Il couvre plusieurs zones de disponibilité.

Un VPC doit disposer d'une passerelle de ressources si vous envisagez de rendre les ressources du VPC accessibles depuis d'autres VPC ou comptes. Chaque ressource que vous partagez est associée à une passerelle de ressources. Lorsque les clients d'autres VPC ou comptes accèdent à une ressource de votre VPC, le trafic provient localement de la passerelle de ressources de ce VPC. L'adresse IP source du trafic est l'adresse IP de la passerelle de ressources. Vous pouvez attribuer plusieurs adresses IP à une passerelle de ressources pour permettre davantage de connexions réseau avec la ressource. Plusieurs ressources d'un VPC peuvent être associées à la même passerelle de ressources.

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

Table des matières

- [Considérations](#)
- [Groupes de sécurité](#)
- [Types d'adresses IP](#)
- [Adresses IPv4 par ENI](#)
- [Configuration des ressources et résolution DNS](#)
- [Création d'une passerelle de ressources dans VPC Lattice](#)
- [Suppression d'une passerelle de ressources dans VPC Lattice](#)

Considérations

Les considérations suivantes s'appliquent aux passerelles de ressources :

- Pour que votre ressource soit accessible depuis toutes les zones de [disponibilité](#), vous devez créer vos passerelles de ressources de manière à couvrir autant de zones de disponibilité que possible.
- Au moins une zone de disponibilité du terminal VPC et de la passerelle de ressources doit se chevaucher.

- Un VPC peut disposer d'un maximum de 100 passerelles de ressources. Pour plus d'informations, consultez la section [Quotas pour VPC](#) Lattice.
- Vous ne pouvez pas créer de passerelle de ressources dans un sous-réseau partagé.

Groupes de sécurité

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

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

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

Destination	Protocole	Plage de ports	Comment
<i>CIDR range for resource</i>	TCP	3306	Autorise le trafic depuis la passerelle de ressources vers les bases de données.

Types d'adresses IP

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

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

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

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

Adresses IPv4 par ENI

Si votre passerelle de ressources possède un type d'adresse IP IPv4 ou à double pile, vous pouvez configurer le nombre d'adresses IPv4 attribuées à chaque ENI de votre passerelle de ressources. Lorsque vous créez une passerelle de ressources, vous choisissez entre 1 et 62 adresses IPv4. Une fois que vous avez défini le nombre d'adresses IPv4, la valeur ne peut pas être modifiée.

Les adresses IPv4 sont utilisées pour la traduction des adresses réseau et déterminent le nombre maximum de connexions IPv4 simultanées à une ressource. Par défaut, 16 adresses IPv4 sont attribuées à toutes les passerelles de ressources par ENI. Il s'agit d'un nombre approprié d'adresses IP pour établir des connexions avec les ressources de votre backend.

Si votre passerelle de ressources utilise le type d'adresse IPv6, elle reçoit automatiquement un CIDR /80 par ENI. Cette valeur ne peut pas être modifiée.

Configuration des ressources et résolution DNS

Vous pouvez spécifier la manière dont une passerelle de ressources exécute la résolution DNS pour les configurations de ressources qui sont des cibles de nom de domaine. Cette propriété est immuable. Vous pouvez choisir :

- **PUBLIC** (par défaut) - Les noms de domaine sont résolus à l'aide de résolveurs DNS publics.
- **IN_VPC** - Les noms de domaine sont résolus à l'aide du serveur DNS configuré dans le jeu d'options DHCP du VPC dans lequel se trouve la passerelle de ressources. Vous devez l'utiliser si vous utilisez un serveur DNS privé ou si les cibles de votre nom de domaine se trouvent dans une zone hébergée privée Route 53.

Si la résolution DNS est **IN_VPC**, vous ne pouvez pas associer les configurations de ressources définies par l'ARN à la passerelle de ressources. Vous ne pouvez pas définir la résolution DNS sur

IN_VPC si la passerelle de ressources utilise des sous-réseaux. IPv6-only La résolution DNS doit être IN_VPC pour associer les configurations de ressources CIDR à la passerelle de ressources.

Création d'une passerelle de ressources dans VPC Lattice

Utilisez la console pour créer une passerelle de ressources.

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

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, sous PrivateLink Lattice, sélectionnez Resource gateways.
3. Choisissez Créer une passerelle de ressources.
4. Entrez un nom unique dans votre AWS compte.
5. Choisissez le type d'adresse IP pour la passerelle de ressources.
6. Pour le type d'adresse IP, choisissez le type d'adresse IP pour la passerelle de ressources.
 - Si vous avez sélectionné IPv4 ou Dualstack pour le type d'adresse IP, vous pouvez entrer le nombre d'adresses IPv4 par ENI pour votre passerelle de ressources.

La valeur par défaut est de 16 adresses IPv4 par ENI. Il s'agit d'un nombre approprié d'adresses IP pour établir des connexions avec les ressources de votre backend.
7. Choisissez le VPC dans lequel se trouve la ressource.
8. Pour les groupes de sécurité, choisissez jusqu'à cinq groupes de sécurité pour contrôler le trafic entrant du VPC vers le réseau de service.
9. Pour Resource Config DNS Resolution, choisissez la manière dont vous souhaitez que le DNS soit résolu pour les cibles de noms de domaine.
 - Si vous utilisez un serveur DNS privé ou si les cibles de votre nom de domaine se trouvent dans une zone hébergée privée Route 53, définissez la résolution DNS sur IN_VPC.
10. (Facultatif) Pour ajouter une balise, choisissez Ajouter une nouvelle balise et entrez la clé et la valeur de la balise.
11. Choisissez Créer une passerelle de ressources.

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

Utilisez la commande [create-resource-gateway](#).

Suppression d'une passerelle de ressources dans VPC Lattice

Utilisez la console pour supprimer une passerelle de ressources.

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

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

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

Utilisez la commande [delete-resource-gateway](#).

Gestion des identités et des accès pour AWS PrivateLink

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

Table des matières

- [Public ciblé](#)
- [Authentification par des identités](#)
- [Gestion de l'accès à l'aide de politiques](#)
- [Comment AWS PrivateLink fonctionne avec IAM](#)
- [Identity-based exemples de politiques pour AWS PrivateLink](#)
- [Utilisation des stratégies de point de terminaison pour contrôler l'accès à des points de terminaison d'un VPC](#)
- [AWS politiques gérées pour AWS PrivateLink](#)

Public ciblé

La façon dont vous utilisez Gestion des identités et des accès AWS (IAM) varie en fonction du travail que vous effectuez. AWS PrivateLink

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

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

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaitez peut-être en savoir plus sur la façon d'écrire des politiques pour gérer l'accès à AWS PrivateLink.

Authentification par des identités

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

Vous pouvez vous connecter en tant qu'identité fédérée à l'aide d'informations d'identification provenant d'une source d'identité telle que AWS IAM Identity Center (IAM Identity Center), d'une authentification unique ou d'informations d'identification. Google/Facebook Pour plus d'informations sur la connexion, consultez [Connexion à votre Compte AWS](#) dans le Guide de l'utilisateur Connexion à AWS .

Pour l'accès par programmation, AWS fournit un SDK et une CLI pour signer les demandes de manière cryptographique. Pour plus d'informations, consultez [Signature AWS Version 4 pour les demandes d'API](#) dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une seule identité de connexion appelée utilisateur Compte AWS root qui dispose d'un accès complet à toutes Services AWS les ressources. Il est vivement déconseillé d'utiliser l'utilisateur racine pour vos tâches quotidiennes. Pour les tâches qui requièrent des informations d'identification de l'utilisateur racine, consultez [Tâches qui requièrent les informations d'identification de l'utilisateur racine](#) dans le Guide de l'utilisateur IAM.

Identité fédérée

Il est recommandé d'obliger les utilisateurs humains à utiliser la fédération avec un fournisseur d'identité pour accéder à Services AWS l'aide d'informations d'identification temporaires.

Une identité fédérée est un utilisateur provenant de l'annuaire de votre entreprise, de votre fournisseur d'identité Web ou Directory Service qui y accède à Services AWS l'aide d'informations d'identification provenant d'une source d'identité. Les identités fédérées assument des rôles qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Pour plus d'informations, consultez [Qu'est-ce que IAM Identity Center ?](#) dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un [utilisateur IAM](#) est une identité qui dispose d'autorisations spécifiques pour une seule personne ou application. Nous vous recommandons d'utiliser ces informations d'identification temporaires au lieu des utilisateurs IAM avec des informations d'identification à long terme. Pour plus d'informations, voir [Exiger des utilisateurs humains qu'ils utilisent la fédération avec un fournisseur d'identité pour accéder à AWS l'aide d'informations d'identification temporaires](#) dans le guide de l'utilisateur IAM.

[Les groupes IAM](#) spécifient une collection d'utilisateurs IAM et permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Pour plus d'informations, consultez [Cas d'utilisation pour les utilisateurs IAM](#) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un [rôle IAM](#) est une identité dotée d'autorisations spécifiques qui fournit des informations d'identification temporaires. Vous pouvez assumer un rôle en [passant d'un rôle d'utilisateur à un rôle IAM \(console\)](#) ou en appelant une opération d' AWS API AWS CLI ou d'API. Pour plus d'informations, consultez [Méthodes pour endosser un rôle](#) dans le Guide de l'utilisateur IAM.

Les rôles IAM sont utiles pour l'accès des utilisateurs fédérés, les autorisations temporaires des utilisateurs IAM, les accès intercompte, les accès entre services et les applications exécutées sur Amazon EC2. Pour plus d'informations, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

Gestion de l'accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique définit les autorisations lorsqu'elles sont associées à une identité ou à une ressource. AWS évalue ces politiques lorsqu'un directeur fait une demande. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations les documents de politique JSON, consultez [Vue d'ensemble des politiques JSON](#) dans le Guide de l'utilisateur IAM.

À l'aide de politiques, les administrateurs précisent qui a accès à quoi en définissant quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Un administrateur IAM crée des politiques IAM et les ajoute aux rôles, que les utilisateurs peuvent ensuite assumer. Les

politiques IAM définissent les autorisations quelle que soit la méthode que vous utilisez pour exécuter l'opération.

Identity-based politiques

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous attachez à une identité (utilisateur, groupe ou rôle). Ces politiques contrôlent les actions que peuvent exécuter ces identités, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez [Définition d'autorisations IAM personnalisées avec des politiques gérées par le client](#) dans le Guide de l'utilisateur IAM.

Identity-based les politiques peuvent être des politiques intégrées (intégrées directement dans une seule identité) ou des politiques gérées (politiques autonomes associées à plusieurs identités). Pour découvrir comment choisir entre des politiques gérées et en ligne, consultez [Choix entre les politiques gérées et les politiques en ligne](#) dans le Guide de l'utilisateur IAM.

Resource-based politiques

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource. Les exemples incluent les politiques de confiance de rôle IAM et les stratégies de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources.

Resource-based les politiques sont des politiques intégrées qui se trouvent dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Autres types de politique

AWS prend en charge des types de politiques supplémentaires qui peuvent définir les autorisations maximales accordées par les types de politiques les plus courants :

- Limites d'autorisations : une limite des autorisations définit le nombre maximum d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM. Pour plus d'informations, consultez [Limites d'autorisations pour des entités IAM](#) dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) : spécifient les autorisations maximales pour une organisation ou une unité organisationnelle dans AWS Organizations. Pour plus d'informations, consultez [Politiques de contrôle de service](#) dans le Guide de l'utilisateur AWS Organizations .

- Politiques de contrôle des ressources (RCP) : définissent les autorisations maximales disponibles pour les ressources de votre organisation. Pour plus d'informations, consultez [Politiques de contrôle des ressources \(RCP\)](#) dans le Guide de l'utilisateur AWS Organizations .
- Politiques de session : politiques avancées que vous passez en tant que paramètre lorsque vous créez par programmation une session temporaire pour un rôle ou un utilisateur fédéré. Pour plus d'informations, consultez [Politiques de session](#) dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

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

Comment AWS PrivateLink fonctionne avec IAM

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

Fonctionnalité IAM	AWS PrivateLink soutien
Identity-based politiques	Oui
Resource-based politiques	Oui
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui

Fonctionnalité IAM	AWS PrivateLink soutien
Autorisations de principal	Oui
Rôles du service	Non
Service-linked rôles	Non

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

Identity-based politiques pour AWS PrivateLink

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

Identity-based les politiques sont des documents de politique d'autorisation JSON que vous pouvez associer à une identité, telle qu'un utilisateur IAM, un groupe d'utilisateurs ou un rôle. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez [Définition d'autorisations IAM personnalisées avec des politiques gérées par le client](#) dans le Guide de l'utilisateur IAM.

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

Identity-based exemples de politiques pour AWS PrivateLink

Pour consulter des exemples de politiques AWS PrivateLink basées sur l'identité, consultez. [Identity-based exemples de politiques pour AWS PrivateLink](#)

Resource-based politiques au sein de AWS PrivateLink

Prend en charge les politiques basées sur les ressources : oui

Resource-based les politiques sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment

Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez [spécifier un principal](#) dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. Pour plus d'informations, consultez [Accès intercompte aux ressources dans IAM](#) dans le Guide de l'utilisateur IAM.

AWS PrivateLink le service prend en charge un type de politique basée sur les ressources, connue sous le nom de stratégie de point de terminaison. Une politique de contrôle de point de terminaison que les principaux AWS peuvent utiliser le point de terminaison pour accéder au service de point de terminaison. Pour de plus amples informations, veuillez consulter [the section called "Politiques de point de terminaison"](#).

Actions politiques pour AWS PrivateLink

Prend en charge les actions de politique : oui

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

L'élément Action d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Actions dans l'espace de noms ec2

Certaines actions pour AWS PrivateLink font partie de l'API Amazon EC2. Ces actions de politique utilisent le ec2 préfixe. Pour plus d'informations, consultez les [AWS PrivateLink actions](#) dans la Référence API d'Amazon EC2.

Actions dans l'espace de noms vpce

AWS PrivateLink fournit également l'action basée AllowMultiRegion uniquement sur les autorisations. Cette action de politique utilise le vpce préfixe.

Ressources politiques pour AWS PrivateLink

Prend en charge les ressources de politique : oui

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

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Il est recommandé de définir une ressource à l'aide de son [Amazon Resource Name \(ARN\)](#). Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*" 
```

Clés de conditions de politique pour AWS PrivateLink

Prend en charge les clés de condition de politique spécifiques au service : oui

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

L'élément `Condition` indique à quel moment les instructions s'exécutent en fonction de critères définis. Vous pouvez créer des expressions conditionnelles qui utilisent des [opérateurs de condition](#), tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande. Pour voir toutes les clés de condition AWS globales, voir les clés de [contexte de condition AWS globales](#) dans le guide de l'utilisateur IAM.

Les clés de condition suivantes sont spécifiques à AWS PrivateLink :

- `ec2:VpceMultiRegion`
- `ec2:VpceServiceName`
- `ec2:VpceServiceOwner`
- `ec2:VpceServicePrivateDnsName`
- `ec2:VpceServiceRegion`
- `ec2:VpceSupportedRegion`

Pour plus d'informations, consultez [Clés de condition pour Amazon EC2](#).

ACL dans AWS PrivateLink

Prend en charge les ACL : non

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

ABAC avec AWS PrivateLink

Prise en charge d'ABAC (balises dans les politiques) : Oui

Attribute-based le contrôle d'accès (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction d'attributs appelés balises. Vous pouvez associer des balises aux entités et aux AWS ressources IAM, puis concevoir des politiques ABAC pour autoriser les opérations lorsque la balise du principal correspond à la balise de la ressource.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans [l'élément de condition](#) d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez [Définition d'autorisations avec l'autorisation ABAC](#) dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez [Utilisation du contrôle d'accès par attributs \(ABAC\)](#) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec AWS PrivateLink

Prend en charge les informations d'identification temporaires : oui

Les informations d'identification temporaires fournissent un accès à court terme aux AWS ressources et sont automatiquement créées lorsque vous utilisez la fédération ou que vous changez de rôle. AWS recommande de générer dynamiquement des informations d'identification temporaires au

lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez [Informations d'identification de sécurité temporaires dans IAM](#) et [Services AWS compatibles avec IAM](#) dans le Guide de l'utilisateur IAM.

Cross-service autorisations principales pour AWS PrivateLink

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

Les sessions d'accès direct (FAS) utilisent les autorisations du principal appelant et Service AWS, combinées Service AWS à la demande d'envoi de demandes aux services en aval. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez la section [Sessions de transmission d'accès](#).

Rôles de service pour AWS PrivateLink

Prend en charge les rôles de service : Non

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

Service-linked rôles pour AWS PrivateLink

Prend en charge les rôles liés à un service : non

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut assumer le rôle d'effectuer une action en votre nom. Service-linked les rôles apparaissent dans votre fichier Compte AWS et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Identity-based exemples de politiques pour AWS PrivateLink

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier les ressources AWS PrivateLink . Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez [Création de politiques IAM \(console\)](#) dans le Guide de l'utilisateur IAM.

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

Exemples

- [Contrôler l'utilisation de points de terminaison d'un VPC](#)
- [Contrôler la création de points de terminaison d'un VPC en fonction du propriétaire du service](#)
- [Contrôle des noms DNS privés pouvant être spécifiés pour les services de point de terminaison d'un VPC](#)
- [Contrôle des noms de services pouvant être spécifiés pour les services de point de terminaison d'un VPC](#)

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

Par défaut, les utilisateurs ne sont pas autorisés à utiliser des points de terminaison. Vous pouvez créer une stratégie basée sur l'identité qui autorise les utilisateurs à créer, modifier, décrire et supprimer des points de terminaison. Voici un exemple.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:*VpcEndpoint*",
      "Resource": "*"
    }
  ]
}
```

Pour plus d'informations sur le contrôle de l'accès aux services avec des points de terminaison de VPC, consultez [the section called "Politiques de point de terminaison"](#).

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

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

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcEndpoint",
      "Resource": [
        "arn:aws:ec2:us-east-1:111111111111:vpc/*",
        "arn:aws:ec2:us-east-1:111111111111:security-group/*",
        "arn:aws:ec2:us-east-1:111111111111:subnet/*",
        "arn:aws:ec2:us-east-1:111111111111:route-table/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcEndpoint",
      "Resource": [
        "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint/*"
      ],
      "Condition": {
        "StringEquals": {
          "ec2:VpceServiceOwner": [
            "amazon"
          ]
        }
      }
    }
  ]
}
```

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

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

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:ModifyVpcEndpointServiceConfiguration",
        "ec2:CreateVpcEndpointServiceConfiguration"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint-service/*"
      ],
      "Condition": {
        "StringEquals": {
          "ec2:VpceServicePrivateDnsName": [
            "example.com"
          ]
        }
      }
    }
  ]
}
```

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

Vous pouvez utiliser la clé de condition `ec2:VpceServiceName` pour contrôler quel point de terminaison d'un VPC peut être créé en fonction du nom du service de point de terminaison d'un

VPC. L'exemple suivant accorde l'autorisation de créer un point de terminaison d'un VPC avec le nom de service spécifié. Pour utiliser cet exemple, remplacez la région, l'ID de compte et le nom de service.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcEndpoint",
      "Resource": [
        "arn:aws:ec2:us-east-1:111111111111:vpc/*",
        "arn:aws:ec2:us-east-1:111111111111:security-group/*",
        "arn:aws:ec2:us-east-1:111111111111:subnet/*",
        "arn:aws:ec2:us-east-1:111111111111:route-table/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:CreateVpcEndpoint",
      "Resource": [
        "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint/*"
      ],
      "Condition": {
        "StringEquals": {
          "ec2:VpceServiceName": [
            "com.amazonaws.111111111111.s3"
          ]
        }
      }
    }
  ]
}
```

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

Une politique de point de terminaison est une politique basée sur les ressources que vous attachez à un point de terminaison VPC pour contrôler quels AWS principaux peuvent utiliser le point de terminaison pour accéder à un Service AWS.

Une stratégie de point de terminaison n'annule ni ne remplace les politiques basées sur l'identité ni sur les ressources. Par exemple, si vous utilisez un point de terminaison d'interface pour vous connecter à Amazon S3, vous pouvez également utiliser les politiques de compartiment Amazon S3 pour contrôler l'accès aux compartiments depuis des points de terminaison ou des VPC spécifiques.

Table des matières

- [Considérations](#)
- [Politique de point de terminaison par défaut](#)
- [Politiques relatives aux points de terminaison d'interface](#)
- [Principaux pour les points de terminaison de passerelle](#)
- [Mise à jour d'une politique de point de terminaison d'un VPC](#)

Considérations

- Une politique de point de terminaison est un document de politique JSON qui utilise le langage de politique IAM. Elle doit contenir un élément [Principal](#). La taille d'une politique de point de terminaison ne peut excéder 20 480 caractères, espaces blancs compris.
- Lorsque vous créez une interface ou un point de terminaison de passerelle pour un Service AWS, vous pouvez associer une politique de point de terminaison unique au point de terminaison. Vous pouvez [mettre à jour la politique de point de terminaison](#) à tout moment. Si vous n'associez pas une politique de point de terminaison, nous associons la [politique de point de terminaison par défaut](#).
- Toutes ne sont pas Services AWS compatibles avec les politiques relatives aux terminaux. Si un Service AWS ne prend pas en charge les politiques relatives aux terminaux, nous autorisons l'accès complet à n'importe quel point de terminaison pour le service. Pour de plus amples informations, veuillez consulter [the section called “Afficher la prise en charge de stratégie de point de terminaison”](#).

- Lorsque vous créez un point de terminaison d'un VPC pour un service de point de terminaison autre qu'un Service AWS, nous autorisons un accès complet au point de terminaison.
- Vous ne pouvez pas utiliser de caractères génériques (* ou ?) ou des [opérateurs de condition numériques](#) avec des clés de contexte globales qui font référence à des identifiants générés par le système (par exemple, ou). `aws:PrincipalAccount` `aws:SourceVpc`
- Lorsque vous utilisez un [opérateur de condition de chaîne](#), vous devez utiliser au moins six caractères consécutifs avant ou après chaque caractère générique.
- Lorsque vous spécifiez un ARN dans une ressource ou un élément de condition, la partie compte de l'ARN peut inclure un identifiant de compte ou un caractère générique, mais pas les deux.
- Après avoir mis à jour une politique de point de terminaison, il faut parfois quelques minutes pour que les changements prennent effet.

Politique de point de terminaison par défaut

La politique de point de terminaison par défaut accorde un accès total au point de terminaison.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*"
    }
  ]
}
```

Politiques relatives aux points de terminaison d'interface

Par exemple, les politiques relatives aux terminaux pour Services AWS, voir [the section called “Services qui s'intègrent”](#). La première colonne du tableau contient des liens vers la AWS PrivateLink documentation de chacun d'entre eux Service AWS. Si un Service AWS prend en charge les politiques relatives aux terminaux, sa documentation inclut des exemples de politiques relatives aux points de terminaison.

Principaux pour les points de terminaison de passerelle

Pour * les points de terminaison de passerelle, l'Principalélément doit être défini sur. Pour spécifier un principal, utilisez la clé de `aws:PrincipalArn` condition.

```
"Condition": {
  "StringEquals": {
    "aws:PrincipalArn": "arn:aws:iam::123456789012:user/endpointuser"
  }
}
```

Si vous spécifiez le principal dans le format suivant, l'accès n'est accordé Utilisateur racine d'un compte AWS qu'aux seuls utilisateurs et rôles du compte, et non à tous.

```
"AWS": "account_id"
```

Pour obtenir des exemples de politiques de point de terminaison relatives aux points de terminaison de la passerelle, veuillez consulter ce qui suit :

- [Points de terminaison pour Amazon S3](#)
- [Points de terminaison pour DynamoDB](#)

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

Utilisez la procédure suivante pour mettre à jour une politique de point de terminaison relative à un Service AWS. Après avoir mis à jour une politique de point de terminaison, il faut parfois quelques minutes pour que les changements prennent effet.

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

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

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

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

AWS politiques gérées pour AWS PrivateLink

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des [politiques gérées par le client](#) qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez [Politiques gérées par AWS](#) dans le Guide de l'utilisateur IAM.

AWS PrivateLink mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS PrivateLink depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page Historique du AWS PrivateLink document.

Modifier	Description	Date
AWS PrivateLink a commencé à suivre les modifications	AWS PrivateLink a commencé à suivre les modifications	1er mars 2021

Modifier	Description	Date
	apportées AWS à ses politique s gérées.	

CloudWatch métriques pour AWS PrivateLink

AWS PrivateLink publie des points de données sur Amazon CloudWatch pour vos points de terminaison d'interface, vos points de terminaison Gateway Load Balancer et vos services de point de terminaison. CloudWatch vous permet de récupérer des statistiques sur ces points de données sous la forme d'un ensemble ordonné de séries chronologiques, appelées métriques. Considérez une métrique comme une variable à surveiller, et les points de données comme les valeurs de cette variable au fil du temps. Un horodatage et une unité de mesure facultative sont associés à chaque point de données.

Vous pouvez utiliser les métriques pour vérifier que le système fonctionne comme prévu. Par exemple, vous pouvez créer une CloudWatch alarme pour surveiller une métrique spécifiée et lancer une action (telle que l'envoi d'une notification à une adresse e-mail) si la métrique dépasse ce que vous considérez comme une plage acceptable.

Les métriques sont publiées pour tous les points de terminaison d'interface, les points de terminaison Gateway Load Balancer et les services de point de terminaison. Ils ne sont pas publiés pour les points de terminaison de passerelle ou pour les consommateurs de services de point de terminaison qui utilisent un accès interrégional. Par défaut, AWS PrivateLink envoie les métriques CloudWatch à des intervalles d'une minute, sans frais supplémentaires.

Pour plus d'informations, consultez le [guide de CloudWatch l'utilisateur Amazon](#).

Table des matières

- [Métriques et dimensions des points de terminaison](#)
- [Métriques et dimensions de point de terminaison de service](#)
- [Afficher les CloudWatch indicateurs](#)
- [Utilisation des règles intégrées de Contributor Insights](#)

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	<p>Le nombre de connexions actives simultanées. Cela inclut les connexions dont l'état est SYN_SENT et ESTABLISHED.</p> <p>Critères de rapport : le point de terminaison a reçu du trafic pendant la période d'une minute.</p> <p>Statistics : les statistiques les plus utiles sont Average, Maximum et Minimum.</p> <p>Dimensions</p> <ul style="list-style-type: none"> • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id
BytesProcessed	<p>Le nombre d'octets échangés entre les points de terminaison et les services de terminaison, agrégés dans les deux sens. Il s'agit du nombre d'octets facturés au propriétaire du point de terminaison. La facture affiche cette valeur en Go.</p> <p>Critères de rapport : le point de terminaison a reçu du trafic pendant la période d'une minute.</p> <p>Statistiques : les statistiques les plus utiles sont Average, Sum, Maximum, et Minimum.</p> <p>Dimensions</p> <ul style="list-style-type: none"> • Endpoint Type, Service Name, VPC Endpoint Id, VPC Id • Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id
NewConnections	<p>Le nombre de nouvelles connexions établies par le point de terminaison.</p> <p>Critères de rapport : le point de terminaison a reçu du trafic pendant la période d'une minute.</p>

Métrique	Description
	<p>Statistiques : les statistiques les plus utiles sont Average, Sum, Maximum, et Minimum.</p> <p>Dimensions</p> <ul style="list-style-type: none">• Endpoint Type, Service Name, VPC Endpoint Id, VPC Id• Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id
PacketsDropped	<p>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.</p> <p>Critères de rapport : le point de terminaison a reçu du trafic pendant la période d'une minute.</p> <p>Statistics : les statistiques les plus utiles sont Average, Sum et Maximum.</p> <p>Dimensions</p> <ul style="list-style-type: none">• Endpoint Type, Service Name, VPC Endpoint Id, VPC Id• Endpoint Type, Service Name, Subnet Id, VPC Endpoint Id, VPC Id

Métrique	Description
RstPacketsReceived	<p>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.</p> <p>Critères de rapport : le point de terminaison a reçu du trafic pendant la période d'une minute.</p> <p>Statistics : les statistiques les plus utiles sont Average, Sum et Maximum.</p> <p>Dimensions</p> <ul style="list-style-type: none">Endpoint Type, Service Name, VPC Endpoint Id, VPC IdEndpoint 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	<p>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.</p> <p>Critères de rapport : un point de terminaison connecté au service de point de terminaison a envoyé du trafic pendant la période d'une minute.</p> <p>Statistiques : les statistiques les plus utiles sont Average et Maximum.</p> <p>Dimensions</p> <ul style="list-style-type: none"> • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id
BytesProcessed	<p>Le nombre d'octets échangés entre les services de point de terminaison et les points de terminaison, dans les deux sens.</p> <p>Critères de rapport : un point de terminaison connecté au service de point de terminaison a envoyé du trafic pendant la période d'une minute.</p> <p>Statistics : les statistiques les plus utiles sont Average, Sum et Maximum.</p> <p>Dimensions</p> <ul style="list-style-type: none"> • Service Id • Az, Service Id • Load Balancer Arn, Service Id • Az, Load Balancer Arn, Service Id • Service Id, VPC Endpoint Id
EndpointsCount	<p>Le nombre de points de terminaison connectés au service de point de terminaison.</p>

Métrique	Description
	<p>Critères de rapport : il y a une valeur non nulle pendant la période de cinq minutes.</p> <p>Statistiques : les statistiques les plus utiles sont Average et Maximum.</p> <p>Dimensions</p> <ul style="list-style-type: none">• Service Id
NewConnections	<p>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.</p> <p>Critères de rapport : un point de terminaison connecté au service de point de terminaison a envoyé du trafic pendant la période d'une minute.</p> <p>Statistics : les statistiques les plus utiles sont Average, Sum et Maximum.</p> <p>Dimensions</p> <ul style="list-style-type: none">• Service Id• Az, Service Id• Load Balancer Arn, Service Id• Az, Load Balancer Arn, Service Id• Service Id, VPC Endpoint Id

Métrique	Description
RstPacketsSent	<p>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.</p> <p>Critères de rapport : un point de terminaison connecté au service de point de terminaison a envoyé du trafic pendant la période d'une minute.</p> <p>Statistics : les statistiques les plus utiles sont Average, Sum et Maximum.</p> <p>Dimensions</p> <ul style="list-style-type: none">• 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.

Afficher les CloudWatch indicateurs

Vous pouvez consulter ces CloudWatch métriques à l'aide de la console Amazon VPC, de la CloudWatch console ou de la manière AWS CLI suivante.

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

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Points de terminaison. Sélectionnez le point de terminaison, puis choisissez l'onglet Monitoring (Surveillance).
3. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison). Sélectionnez le service de votre point de terminaison, puis choisissez l'onglet Monitoring (Surveillance).

Pour afficher les métriques à l'aide de la CloudWatch console

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

Pour consulter les statistiques à l'aide du AWS CLI

Utilisez la commande [list-metrics](#) suivante pour répertorier les métriques disponibles pour les points de terminaison d'interface et les points de terminaison de Gateway Load Balancer :

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkEndpoints
```

Utilisez la commande [list-metrics](#) suivante pour répertorier les métriques disponibles pour les services de points de terminaison :

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkServices
```

Utilisation des règles intégrées de Contributor Insights

AWS PrivateLink fournit des règles intégrées d'analyse des contributeurs pour vos services de point de terminaison afin de vous aider à déterminer quels points de terminaison contribuent le plus à chaque métrique prise en charge. Pour plus d'informations, consultez [Contributor Insights](#) dans le guide de CloudWatch l'utilisateur Amazon.

AWS PrivateLink fournit les règles suivantes :

- `VpcEndpointService-ActiveConnectionsByEndpointId-v1` : classe les points de terminaison en fonction du nombre de connexions actives.
- `VpcEndpointService-BytesByEndpointId-v1` : classe les points de terminaison en fonction du nombre d'octets traités.
- `VpcEndpointService-NewConnectionsByEndpointId-v1` : classe les points de terminaison en fonction du nombre de nouvelles connexions.
- `VpcEndpointService-RstPacketsByEndpointId-v1` : classe les points de terminaison en fonction du nombre de paquets RST envoyés aux points de terminaison.

Avant de pouvoir utiliser une règle intégrée, vous devez l'activer. Une fois que vous avez activé une règle, elle commence à collecter les données des contributeurs. Pour plus d'informations sur les frais associés à Contributor Insights, consultez [Amazon CloudWatch Pricing](#).

Vous devez disposer des autorisations suivantes pour utiliser Contributor Insights :

- `cloudwatch:DeleteInsightRules` – Pour supprimer les règles Contributor Insights.
- `cloudwatch:DisableInsightRules` – Pour désactiver les règles Contributor Insights.
- `cloudwatch:GetInsightRuleReport` – Pour obtenir les données.
- `cloudwatch:ListManagedInsightRules` – Pour répertorier les règles Contributor Insights disponibles.
- `cloudwatch:PutManagedInsightRules` – Pour activer les règles Contributor Insights.

Tâches

- [Activez les règles Contributor Insights](#)
- [Désactivez les règles Contributor Insights](#)
- [Supprimer les règles Contributor Insights](#)

Activez les règles Contributor Insights

Utilisez les procédures suivantes pour activer les règles intégrées permettant AWS PrivateLink d'utiliser le Console de gestion AWS ou le AWS CLI.

Pour activer les règles de Contributor Insights relatives à AWS PrivateLink l'utilisation de la console

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

2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez votre service de point de terminaison.
4. Sur l'onglet Contributor Insights, choisissez Enable (Activer).
5. (Facultatif) Par défaut, toutes les règles sont activées. Pour activer uniquement des règles spécifiques, sélectionnez les règles qui ne doivent pas être activées, puis choisissez Actions (Actions), Désactiver la règle. Lorsque vous êtes invité à confirmer l'opération, choisissez Désactiver .

Pour activer les règles de Contributor Insights relatives à AWS PrivateLink l'utilisation du AWS CLI

1. Utilisez la commande [list-managed-insight-rules](#) comme suit pour énumérer les règles disponibles. Pour l'option `--resource-arn`, spécifiez l'ARN de votre service de point de terminaison.

```
aws cloudwatch list-managed-insight-rules --resource-arn
arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-svc-0123456789EXAMPLE
```

2. Dans la sortie de la commande `list-managed-insight-rules`, copiez le nom du modèle depuis le champ `TemplateName`. Voici un exemple de ce champ.

```
"TemplateName": "VpcEndpointService-NewConnectionsByEndpointId-v1"
```

3. Utilisez la commande [put-managed-insight-rules](#) comme suit pour activer la règle. Vous devez spécifier le nom du modèle et l'ARN de votre service de point de terminaison.

```
aws cloudwatch put-managed-insight-rules --managed-rules
TemplateName=VpcEndpointService-NewConnectionsByEndpointId-
v1,ResourceARN=arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-
svc-0123456789EXAMPLE
```

Désactivez les règles Contributor Insights

Vous pouvez désactiver les règles intégrées AWS PrivateLink à tout moment. Une fois que vous avez désactivé une règle, elle arrête de collecter les données des contributeurs, mais les données de contributeurs existantes sont conservées jusqu'à ce qu'elles aient 15 jours. Après avoir désactivé une règle, vous pouvez l'activer à nouveau pour reprendre la collecte de données des contributeurs.

Pour désactiver les règles de Contributor Insights relatives à AWS PrivateLink l'utilisation de la console

1. Ouvrez la console Amazon VPC à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Sélectionnez votre service de point de terminaison.
4. Sur l'onglet Contributor Insights, choisissez Désactiver tout pour désactiver toutes les règles. Sinon, développez le panneau Règles, sélectionnez les règles à désactiver, puis choisissez Actions, Désactiver la règle
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Désactiver .

Pour désactiver les règles de Contributor Insights relatives à AWS PrivateLink l'utilisation du AWS CLI

Utilisez la commande [disable-insight-rules](#) pour désactiver une règle.

Supprimer les règles Contributor Insights

Utilisez les procédures suivantes pour supprimer les règles intégrées relatives AWS PrivateLink à l'utilisation du Console de gestion AWS ou du AWS CLI. Une fois que vous supprimez une règle, elle cesse de collecter les données des contributeurs et nous supprimons les données de contributeurs existantes.

Pour supprimer les règles de Contributor Insights relatives à AWS PrivateLink l'utilisation de la console

1. Ouvrez la CloudWatch console à l'adresse <https://console.aws.amazon.com/cloudwatch/>.
2. Dans le panneau de navigation, choisissez Insights, puis choisissez Contributor Insights.
3. Développez le panneau Règles et sélectionnez les règles.
4. Choisissez Actions, puis Supprimer la règle.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Pour supprimer les règles de Contributor Insights relatives à AWS PrivateLink l'utilisation du AWS CLI

Utilisez la commande [delete-insight-rules](#) pour supprimer une règle.

AWS PrivateLink quotas

Votre AWS compte dispose de quotas par défaut, anciennement appelés limites, pour chaque AWS service. Sauf indication contraire, chaque quota est Region-specific. Vous pouvez demander des augmentations de certains quotas, tandis que d'autres quotas ne peuvent pas être augmentés. Si vous demandez d'augmenter un quota s'appliquant par ressource, nous l'augmentons pour toutes les ressources de la région.

Pour demander une augmentation de quota, consultez [Demande d'augmentation de quota](#) dans le Guide de l'utilisateur Service Quotas.

Limitation des demandes

Les actions d'API pour AWS PrivateLink font partie de l'API Amazon EC2. Amazon EC2 limite ses demandes d'API au niveau. Compte AWS Pour plus d'informations, consultez la section [Régulation des demandes dans le manuel](#) Amazon EC2 Developer Guide. En outre, les demandes d'API sont également limitées au niveau de l'organisation pour améliorer les performances de. AWS PrivateLink Si vous utilisez un code d'erreur AWS Organizations et que vous recevez un code RequestLimitExceeded d'erreur alors que vous respectez les limites d'API au niveau de votre compte, consultez [Comment identifier les AWS comptes qui effectuent un grand nombre d'appels d'API](#). Si vous avez besoin d'aide, contactez l'équipe chargée de votre compte ou ouvrez un dossier de support technique en utilisant le service VPC et la catégorie VPC Endpoints. Assurez-vous de joindre une image du code RequestLimitExceeded d'erreur.

Quotas de points de terminaison VPC

Votre AWS compte possède les quotas suivants relatifs aux points de terminaison VPC.

Nom	Par défaut	Ajustable	Commentaires
Points de terminaison d'équilibreur de charge d'interface et de passerelle par VPC	50	Oui	Il s'agit d'un quota combiné pour les points de terminaison d'interface et les points de terminaison d'équilibreur de charge de passerelle

Nom	Par défaut	Ajustable	Commentaires
Points de terminaison d'un VPC de passerelle par région	20	Oui	Vous pouvez créer jusqu'à 255 points de terminaison de passerelle par VPC
Points de terminaison VPC de ressource par VPC	200	Oui	
Points de terminaison VPC du réseau de services par VPC	50	Oui	
Caractères par politique de point de terminaison d'un VPC	20 480	Non	La taille maximale d'une politique de point de terminaison d'un VPC inclut des espaces blancs

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

- Par défaut, chaque point de terminaison d'un VPC peut prendre en charge une bande passante allant jusqu'à 10 Gbit/s par zone de disponibilité et augmente automatiquement jusqu'à 100 Gb/s. La bande passante maximale pour un point de terminaison VPC, lors de la répartition de la charge entre toutes les zones de disponibilité, correspond au nombre de zones de disponibilité multiplié par 100 Gb/s. Si votre application nécessite un débit plus élevé, contactez le support AWS .
- L'unité de transmission maximale (MTU) d'une connexion réseau est la taille, en octets, du plus gros paquet autorisé qui peut passer par un point de terminaison d'un VPC. Plus la MTU est grande, plus la quantité de données pouvant être transmises dans un seul paquet est importante. Un point de terminaison d'un VPC prend en charge une MTU de 8 500 octets. Les paquets d'une taille supérieure à 8 500 octets arrivant au point de terminaison d'un VPC sont supprimés.
- La détection de la MTU du chemin (PMTUD) n'est pas prise en charge. Les points de terminaison d'un VPC ne génèrent pas le message ICMP suivant : `Destination Unreachable: Fragmentation needed and Don't Fragment was Set (Type 3, Code 4)`.
- Les points de terminaison d'un VPC appliquent la taille maximale du segment (MSS) pour tous les paquets. Pour de plus amples informations, veuillez consulter [RFC879](#).

Historique du document pour AWS PrivateLink

Le tableau suivant décrit les versions de AWS PrivateLink.

Modification	Description	Date
Ressources d'accès et réseaux de services	AWS PrivateLink prend en charge l'accès aux ressources et aux réseaux de services au-delà des limites des VPC et des comptes.	1er décembre 2024
Cross-Region accès	Un fournisseur de services peut héberger un service dans une région et le rendre disponible dans un ensemble de AWS régions. Un consommateur de services sélectionne une région de service lors de la création d'un point de terminaison.	26 novembre 2024
Adresses IP désignées	Vous pouvez spécifier les adresses IP pour les interfaces réseau de vos points de terminaison lorsque vous créez ou modifiez votre point de terminaison d'un VPC.	17 août 2023
Prise en charge d'IPv6	Vous pouvez configurer vos services de point de terminaison Équilibreur de charge de Passerelle et vos points de terminaison Équilibreur de charge de Passerelle pour qu'ils prennent en charge à la fois les adresses IPv4 et IPv6	le 12 décembre 2022

ou uniquement les adresses IPv6.

[Contributor Insights](#)

Vous pouvez utiliser les règles intégrées de Contributor Insights pour identifier les points de terminaison spécifiques qui contribuent le plus aux CloudWatch statistiques pour AWS PrivateLink.

18 août 2022

[Prise en charge d'IPv6](#)

Les fournisseurs du service peuvent permettre à leur service de point de terminaison d'accepter les requêtes IPv6, même si leurs services backend ne prennent en charge que l'IPv4. Si un service de point de terminaison accepte les requêtes IPv6, les consommateurs du service peuvent activer la prise en charge d'IPv6 pour leurs points de terminaison d'interface afin de pouvoir accéder au service de point de terminaison via IPv6.

11 mai 2022

[CloudWatch métriques](#)

AWS PrivateLink publie des CloudWatch métriques pour les points de terminaison de votre interface, les points de terminaison Gateway Load Balancer et les services de point de terminaison.

27 janvier 2022

[Points de terminaison de l'équilibreur de charge de passerelle](#)

Vous pouvez créer un point de terminaison 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 AWS service afin de contrôler l'accès au service.

23 mars 2020

[Clés de condition pour les points de terminaison d'un VPC et les services de point de terminaison](#)

Vous pouvez utiliser des clés de condition EC2 pour contrôler l'accès aux points de terminaison d'un VPC et aux services de point de terminaison.

6 mars 2020

[Identification des points de terminaison d'un VPC et des services de point de terminaison lors de la création](#)

Vous pouvez ajouter des identifications lorsque vous créez des points de terminaison d'un VPC et des services de points de terminaison.

5 février 2020

[Noms DNS privés](#)

Vous pouvez accéder aux services AWS PrivateLink basés depuis votre VPC à l'aide de noms DNS privés.

6 janvier 2020

[Services de points de terminaison d'un VPC](#)

Vous pouvez créer vos propres services de points de terminaison et permettre à d'autres comptes Comptes AWS et utilisateurs de se connecter à votre service via un point de terminaison d'un VPC d'interface. Vous pouvez proposer vos services de point de terminaison à l'abonnement sur AWS Marketplace.

28 novembre 2017

[Points de terminaison VPC d'interface pour Services AWS](#)

Vous pouvez créer un point de terminaison d'interface auquel vous connecter à Services AWS cette intégration AWS PrivateLink sans utiliser de passerelle Internet ou de périphérique NAT.

8 novembre 2017

[Points de terminaison d'un VPC pour DynamoDB](#)

Vous pouvez créer un point de terminaison d'un VPC de passerelle pour accéder à Amazon DynamoDB depuis votre VPC sans utiliser de passerelle Internet ou de dispositif NAT.

le 16 août 2017

[Points de terminaison d'un VPC pour Amazon S3](#)

Vous pouvez créer un point de terminaison d'un VPC de passerelle pour accéder à Amazon S3 depuis votre VPC sans utiliser de passerelle Internet ou de dispositif NAT.

le 11 mai 2015

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.