



Gateway Load Balancers

Elastic Load Balancing



Elastic Load Balancing: Gateway Load Balancers

Copyright © 2024 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 qu'un équilibreur de charge Gateway Load Balancer ?	1
Présentation du Gateway Load Balancer	1
Fournisseurs d'appareils	2
Premiers pas	2
Tarification	2
Premiers pas	3
Présentation	3
Routage	5
Prérequis	6
Étape 1 : Créer un Gateway Load Balancer	6
Étape 2 : Création d'un service de point de terminaison Gateway Load Balancer	8
Étape 3 : Création d'un point de terminaison Gateway Load Balancer	9
Étape 4 : Configuration du routage	10
Prise en main à l'aide de l'CLI	12
Présentation	12
Routage	5
Prérequis	15
Étape 1 : Création d'un Gateway Load Balancer et enregistrement des cibles	16
Étape 2 : Création d'un point de terminaison Gateway Load Balancer	17
Étape 3 : Configuration du routage	18
Gateway Load Balancers	20
États d'un équilibreur de charge	20
Type d'adresse IP	21
Zones de disponibilité	22
Délai d'inactivité	22
Attributs de l'équilibreur de charge	22
Réseau ACLs	23
Flux asymétriques	23
Unité de transmission maximale du réseau (MTU)	23
Créer un équilibreur de charge	24
Prérequis	24
Créer l'équilibreur de charge	24
Étapes suivantes importantes	25
Mettre à jour le type d'adresse IP	26

Modifier les attributs de l'équilibreur de charge	26
Deletion protection (Protection contre la suppression)	27
Équilibrage de charge entre zones	27
Marquer un équilibreur de charge	28
Supprimer un équilibreur de charge	29
Écouteurs	31
Attributs de l'écouteur	31
Mettre à jour le groupe cible des auditeurs	31
Mettre à jour le délai d'inactivité	32
Groupes cibles	33
Configuration du routage	33
Type de cible	34
Cibles enregistrées	34
Attributs de groupe cible	35
Créer un groupe cible	36
Configurer la surveillance de l'état	37
Paramètres de surveillance de l'état	38
État de santé d'une cible	40
Codes de motif de vérification de l'état	41
Motifs d'échec de la cible	42
Vérifier l'état de santé de vos cibles	43
Paramètres de surveillance de l'état	43
Modifier les attributs du groupe cible	44
Basculement cible	44
Délai d'annulation d'enregistrement	46
Permanence du flux	47
Enregistrer des cibles	48
Considérations	48
Groupes de sécurité cibles	49
Réseau ACLs	49
Enregistrer les cibles par ID d'instance	49
Enregistrer les cibles par adresse IP	50
Désenregistrer les cibles	50
Marquer un groupe cible	51
Supprimer un groupe cible	52
Surveiller vos équilibreurs de charge	53

CloudWatch métriques	54
Métriques de Gateway Load Balancer	55
Dimensions de métriques pour les Gateway Load Balancers	58
Afficher CloudWatch les statistiques de votre Gateway Load Balancer	58
CloudTrail journaux	60
Informations sur Elastic Load Balancing dans CloudTrail	60
Présentation des entrées du fichier journal Elastic Load Balancing	61
Quotas	65
Historique de la documentation	67
.....	Ixix

Qu'est-ce qu'un équilibreur de charge Gateway Load Balancer ?

Elastic Load Balancing distribue automatiquement votre trafic entrant sur plusieurs cibles dans une ou plusieurs zones de disponibilité. Il contrôle l'état des cibles enregistrées et achemine le trafic uniquement vers les cibles saines. Elastic Load Balancing met à l'échelle votre équilibreur de charge à mesure que votre trafic entrant change au fil du temps. Il est capable de s'adapter automatiquement à la plupart des applications.

Elastic Load Balancing prend en charge les équilibreurs de charge suivants : Application Load Balancers, dispositifs d'équilibrage de charge de réseau, dispositifs d'équilibrage de charge de passerelle et Classic Load Balancers. Vous pouvez sélectionner le type d'équilibreur de charge qui correspond le mieux à vos besoins. Ce guide traite des Gateway Load Balancers. Pour plus d'informations sur les autres équilibreurs de charge, consultez le [Guide de l'utilisateur des Application Load Balancers](#), le [Guide de l'utilisateur des dispositifs d'équilibrage de charge de réseau](#) et le [Guide de l'utilisateur pour les Gateway Load Balancers](#).

Présentation du Gateway Load Balancer

Les équilibreurs de charge Gateway Load Balancer vous permettent de déployer, de mettre à l'échelle et de gérer des appliances virtuelles, telles que des pare-feu, des systèmes de détection et de prévention des intrusions et des systèmes d'inspection approfondie des paquets. Ils combinent une passerelle réseau transparente (c'est-à-dire un point d'entrée et de sortie unique pour tout le trafic) et distribuent le trafic tout en adaptant vos appliances virtuelles à la demande.

Un Gateway Load Balancer fonctionne au niveau de la troisième couche du modèle Open Systems Interconnection (OSI), la couche réseau. Ils écoutent tous les paquets IP sur tous les ports et transfèrent le trafic vers le groupe cible spécifié dans la règle d'écoute. Il maintient la [fidélité du flux](#) à une appliance cible spécifique en utilisant 5 tuples (par défaut), 3 tuples ou 2 tuples. Le Gateway Load Balancer et ses instances d'appliance virtuelle enregistrées échangent du trafic applicatif à l'aide du [GENEVE](#) protocole sur le port 6081.

Les Gateway Load Balancers utilisent les points de terminaison Gateway Load Balancer pour échanger du trafic en toute sécurité au-delà des frontières. VPC Un point de terminaison Gateway Load Balancer est un VPC point de terminaison qui fournit une connectivité privée entre les appliances virtuelles du fournisseur de services VPC et les serveurs d'applications du consommateur

de services. VPC Vous déployez le Gateway Load Balancer de la même manière VPC que les appliances virtuelles. Vous enregistrez les appliances virtuelles auprès d'un groupe cible pour l'équilibreur de charge Gateway Load Balancer.

Le trafic en provenance et à destination d'un point de terminaison Gateway Load Balancer est configuré à l'aide de tables de routage. Le trafic circule du consommateur de services VPC via le point de terminaison Gateway Load Balancer vers le Gateway Load Balancer du VPC fournisseur de services, puis revient au consommateur de services. VPC Vous devez créer le point de terminaison Gateway Load Balancer et les serveurs d'applications dans différents sous-réseaux. Cela vous permet de configurer le point de terminaison Gateway Load Balancer en tant que prochain saut dans la table de routage pour le sous-réseau d'une application.

Pour plus d'informations, consultez [Accès aux appareils virtuels via AWS PrivateLink](#) dans le Guide AWS PrivateLink .

Fournisseurs d'appareils

Vous êtes responsable du choix et de la qualification des logiciels proposés par les fournisseurs d'appareils. Vous devez faire confiance au logiciel d'un appareil pour inspecter ou modifier le trafic en provenance de l'équilibreur de charge. Les fournisseurs d'appliances répertoriés dans la liste des [partenaires Elastic Load Balancing](#) ont intégré et qualifié leur logiciel d'appliance avec AWS. Vous pouvez accorder une plus grande confiance aux logiciels d'appareils fournis par les prestataires figurant dans cette liste. Toutefois, AWS ne garantit pas la sécurité ou la fiabilité des logiciels de ces fournisseurs.

Premiers pas

Pour créer un Gateway Load Balancer à l'aide du AWS Management Console, voir. [Premiers pas](#)
Pour créer un Gateway Load Balancer à l'aide du AWS Command Line Interface, voir. [Prise en main à l'aide de l'CLI](#)

Tarifification

Avec votre équilibreur de charge, vous payez uniquement en fonction de votre utilisation. Pour plus d'informations, veuillez consulter [Tarification Elastic Load Balancing](#).

Premiers pas avec les équilibreurs de charge Gateway Load Balancers

Gateway Load Balancers facilite le déploiement, la mise à l'échelle et la gestion des appareils virtuels tiers, tels que les appareils de sécurité.

Dans le cadre de ce tutoriel, nous allons implémenter un système d'inspection à l'aide d'un Gateway Load Balancer et d'un point de terminaison Gateway Load Balancer.

Table des matières

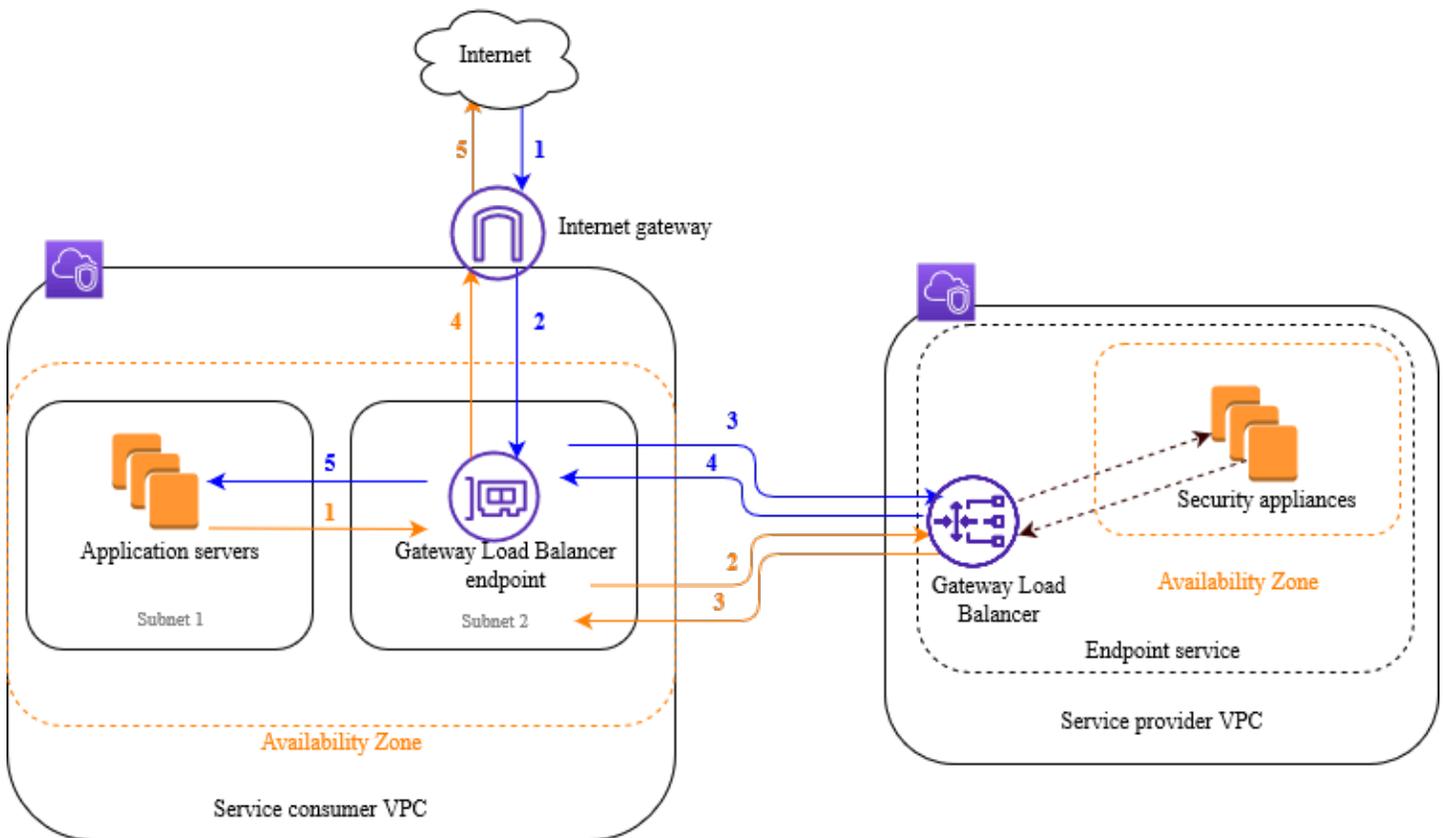
- [Présentation](#)
- [Prérequis](#)
- [Étape 1 : Créer un Gateway Load Balancer](#)
- [Étape 2 : Création d'un service de point de terminaison Gateway Load Balancer](#)
- [Étape 3 : Création d'un point de terminaison Gateway Load Balancer](#)
- [Étape 4 : Configuration du routage](#)

Présentation

Un point de terminaison Gateway Load Balancer est un VPC point de terminaison qui fournit une connectivité privée entre les appliances virtuelles du fournisseur VPC de services et les serveurs d'applications du consommateur de services. VPC Le Gateway Load Balancer est déployé de la même manière VPC que celui des dispositifs virtuels. Ces appareils sont enregistrés en tant que groupe cible de l'équilibreur de charge Gateway Load Balancer.

Les serveurs d'applications s'exécutent dans un sous-réseau (sous-réseau de destination) du consommateur de services VPC, tandis que le point de terminaison Gateway Load Balancer se trouve dans un autre sous-réseau du même sous-réseau. VPC Tout le trafic entrant dans le consommateur de services VPC via la passerelle Internet est d'abord acheminé vers le point de terminaison Gateway Load Balancer, puis vers le sous-réseau de destination.

De même, tout le trafic quittant les serveurs d'applications (sous-réseau de destination) est acheminé vers le point de terminaison Gateway Load Balancer avant d'être réacheminé vers Internet. Le schéma de réseau suivant est une représentation visuelle de la manière dont un point de terminaison Gateway Load Balancer est utilisé pour accéder à un service de point de terminaison.



Les éléments numérotés qui suivent, mettent en évidence et expliquent ceux affichés sur l'image précédente.

Trafic depuis Internet vers l'application (flèches bleues) :

1. Le trafic entre dans le consommateur de services VPC par le biais de la passerelle Internet.
2. Le trafic est envoyé au point de terminaison Gateway Load Balancer à la suite du routage d'entrée.
3. Le trafic est envoyé au Gateway Load Balancer qui distribue le trafic vers un des appareils de sécurité.
4. Le trafic est renvoyé au point de terminaison Gateway Load Balancer après avoir été inspecté par l'appareil de sécurité.
5. Le trafic est envoyé aux serveurs d'applications (sous-réseau de destination).

Trafic de l'application vers Internet (flèches oranges) :

1. Le trafic est envoyé au point de terminaison Gateway Load Balancer à la suite du routage par défaut configuré sur le sous-réseau du serveur d'application.

2. Le trafic est envoyé au Gateway Load Balancer qui distribue le trafic vers un des appareils de sécurité.
3. Le trafic est renvoyé au point de terminaison Gateway Load Balancer après avoir été inspecté par l'appareil de sécurité.
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.

Routage

La table de routage de la passerelle Internet doit comporter une entrée qui achemine le trafic destiné aux serveurs d'applications vers le point de terminaison Gateway Load Balancer. Pour spécifier le point de terminaison Gateway Load Balancer, utilisez l'ID du point de terminaison. VPC L'exemple suivant montre les routages pour une configuration dualstack.

Destination	Target
<i>VPC IPv4 CIDR</i>	Local
<i>VPC IPv6 CIDR</i>	Local
<i>Subnet 1 IPv4 CIDR</i>	<i>vpc-endpoint-id</i>
<i>Subnet 1 IPv6 CIDR</i>	<i>vpc-endpoint-id</i>

La table de routage du sous-réseau avec les serveurs d'application doit comporter des entrées qui acheminent tout le trafic des serveurs d'applications vers le point de terminaison Gateway Load Balancer.

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

La table de routage du sous-réseau avec le point de terminaison Gateway Load Balancer doit acheminer le trafic qui revient de l'inspection à sa destination finale. Pour le trafic provenant d'Internet, l'acheminement local s'assure qu'il atteigne les serveurs d'applications. Pour le trafic provenant des serveurs d'applications, ajoutez des entrées qui acheminent tout le trafic à la passerelle Internet.

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

Prérequis

- Assurez-vous que le client du service VPC dispose d'au moins deux sous-réseaux pour chaque zone de disponibilité contenant des serveurs d'applications. Un sous-réseau est destiné au point de terminaison Gateway Load Balancer et l'autre aux serveurs d'applications.
- Le Gateway Load Balancer et les cibles peuvent se trouver dans le même sous-réseau.
- Vous ne pouvez pas utiliser un sous-réseau partagé depuis un autre compte pour déployer le Gateway Load Balancer.
- Lancez au moins une instance d'appliance de sécurité dans chaque sous-réseau d'appliance de sécurité du fournisseur VPC de services. Les groupes de sécurité de ces instances doivent autoriser le UDP trafic sur le port 6081.

Étape 1 : Créer un Gateway Load Balancer

Utilisez la procédure suivante pour créer votre équilibreur de charge, votre écouteur et votre groupe cible.

Pour créer l'équilibreur de charge, l'écouteur et le groupe cible à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le volet de navigation, sous Équilibrage de charge, choisissez Équilibreurs de charge.
3. Choisissez Créer un équilibreur de charge.
4. Sous Gateway Load Balancer, choisissez Créer.
5. Configuration de base
 - a. Pour Load balancer name (Nom de l'équilibreur de charge), saisissez un nom pour l'équilibreur de charge.
 - b. Pour le type d'adresse IP, choisissez de prendre IPv4 en charge les IPv4 adresses uniquement ou Dualstack pour prendre en charge à la fois les adresses IPv4 et IPv6 les adresses.
6. Mappage du réseau
 - a. Pour VPC, sélectionnez le fournisseur de services VPC.
 - b. Pour Mappages, sélectionnez toutes les zones de disponibilité dans lesquelles vous avez lancé les instances d'appareils de sécurité, et un sous-réseau par zone de disponibilité.
7. Routage d'écouteur d'IP
 - a. Pour Action par défaut, sélectionnez un groupe cible existant pour recevoir le trafic. Ce groupe cible doit utiliser le GENEVE protocole.

Si vous n'avez pas de groupe cible, choisissez Créer un groupe cible, qui ouvre un nouvel onglet dans votre navigateur. Choisissez un type de cible, entrez un nom pour le groupe cible et conservez le GENEVE protocole. Sélectionnez les instances VPC avec vos dispositifs de sécurité. Modifiez les paramètres de surveillance de l'état selon vos besoins et ajoutez les balises dont vous avez besoin. Choisissez Suivant. Vous pouvez enregistrer vos instances de dispositif de sécurité auprès du groupe cible dès à présent ou après avoir terminé cette procédure. Choisissez Créer un groupe cible, puis revenez à l'onglet précédent du navigateur.
 - b. (Facultatif) Développez Balises d'écouteur et ajoutez les balises dont vous avez besoin.
8. (Facultatif) Développez Balises d'équilibreur de charge et ajoutez les balises dont vous avez besoin.
9. Choisissez Créer un équilibreur de charge.

Étape 2 : Création d'un service de point de terminaison Gateway Load Balancer

Utilisez la procédure suivante pour créer un service de point de terminaison à l'aide de votre Gateway Load Balancer.

Pour créer un service de point de terminaison Gateway Load Balancer

1. Ouvrez la VPC console Amazon à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
3. Choisissez Créer un service de point de terminaison, puis effectuez les opérations suivantes :
 - a. Pour Load balancer type (Type d'équilibreur de charge), choisissez Gateway (Passerelle).
 - b. Pour Available load balancers (Équilibreurs de charge disponibles), sélectionnez l'équilibreur de charge de passerelle.
 - c. Dans la section Require acceptance for endpoint (Acceptation requise pour le point de terminaison), sélectionnez Acceptance required (Acceptation requise) pour accepter les demandes de connexion à votre service manuellement. Sinon, elles sont acceptées automatiquement.
 - d. Pour Supported IP address types (Types d'adresse IP pris en charge), effectuez l'une des opérations suivantes :
 - Sélectionner IPv4— Activez le service de point de terminaison pour qu'il accepte les IPv4 demandes.
 - Sélectionner IPv6— Activez le service de point de terminaison pour qu'il accepte les IPv6 demandes.
 - Sélectionnez IPv4et IPv6— Activez le service de point de terminaison pour qu'il accepte à la fois les IPv6 demandes IPv4 et.
 - e. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
 - f. Sélectionnez Create (Créer). Notez le nom du service ; vous en aurez besoin lors de la création du point de terminaison.
4. Sélectionnez le nouveau service de point de terminaison et choisissez Actions (Actions), Allow principals (Autoriser les mandataires). Entrez le ARNs nombre de consommateurs de services autorisés à créer un point de terminaison pour votre service. Un consommateur de services

peut être un utilisateur, un IAM rôle ou Compte AWS. Choisissez Allow principaux (Autoriser les mandataires).

Étape 3 : Création d'un point de terminaison Gateway Load Balancer

Utilisez la procédure suivante pour créer un point de terminaison Gateway Load Balancer qui se connecte à votre service de point de terminaison Gateway Load Balancer. Les points de terminaison Gateway Load Balancer sont répartis par zone. Nous vous recommandons de créer un point de terminaison Gateway Load Balancer par zone. Pour plus d'informations, consultez les [Accès aux appareils virtuels via AWS PrivateLink](#) dans le Guide AWS PrivateLink .

Pour créer un point de terminaison Gateway Load Balancer

1. Ouvrez la VPC console Amazon à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison, puis effectuez les opérations suivantes :
 - a. Pour Service category (Catégorie de service), choisissez Other endpoint services (Autres services de point de terminaison).
 - b. Pour Service Name (Nom du service), saisissez le nom du service que vous avez noté précédemment, puis choisissez Verify service (Vérifier le service).
 - c. Pour VPC, sélectionnez le consommateur de servicesVPC.
 - d. Pour Subnets (Sous-réseaux), sélectionnez un sous-réseau pour le point de terminaison Gateway Load Balancer.
 - e. Pour IP address type (Type d'adresse IP), choisissez l'une des options suivantes :
 - IPv4— Attribuez IPv4 des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent des plages d'IPv4adresses.
 - IPv6— Attribuez IPv6 des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés IPv6 ne sont que des sous-réseaux.
 - Dualstack — Attribuez à la fois des IPv6 adresses IPv4 et des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-

réseaux sélectionnés possèdent à la fois des plages d'IPv6adresses IPv4 et des plages d'adresses.

- f. (Facultatif) Pour ajouter une identification, choisissez Add new tag (Ajouter une identification) et saisissez la clé et la valeur de l'identification.
- g. Choisissez Créer un point de terminaison. L'état initial est pending acceptance.

Utilisez la procédure suivante pour accepter la demande de connexion au point de terminaison.

1. Dans le volet de navigation, choisissez Endpoint Services (Services de point de terminaison).
2. Sélectionnez le service de point de terminaison.
3. Dans l'onglet Endpoint connections (Connexions de point de terminaison), sélectionnez la connexion de point de terminaison.
4. 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).

Étape 4 : Configuration du routage

Configurez les tables de routage pour le consommateur de services VPC comme suit. Cela permet aux dispositifs de sécurité d'effectuer une inspection de sécurité du trafic entrant destiné aux serveurs d'applications.

Pour configurer le routage

1. Ouvrez la VPC console Amazon à l'adresse <https://console.aws.amazon.com/vpc/>.
2. Dans le volet de navigation, choisissez Route tables (Tables de routage).
3. Sélectionnez la table de routage pour la passerelle Internet et procédez comme suit :
 - a. Choisissez Actions, Modifier les routes.
 - b. Choisissez Ajouter une route. Pour Destination, entrez le IPv4 CIDR bloc du sous-réseau pour les serveurs d'applications. Pour Target, sélectionnez le VPC point de terminaison.
 - c. Si vous êtes d'IPv6accord, choisissez Ajouter un itinéraire. Pour Destination, entrez le IPv6 CIDR bloc du sous-réseau pour les serveurs d'applications. Pour Target, sélectionnez le VPC point de terminaison.
 - d. Sélectionnez Enregistrer les modifications.

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

Commencer à utiliser les équilibreur de charge Gateway à l'aide du AWS CLI

Gateway Load Balancers facilite le déploiement, la mise à l'échelle et la gestion des appareils virtuels tiers, tels que les appareils de sécurité.

Dans le cadre de ce tutoriel, nous allons implémenter un système d'inspection à l'aide d'un Gateway Load Balancer et d'un point de terminaison Gateway Load Balancer.

Table des matières

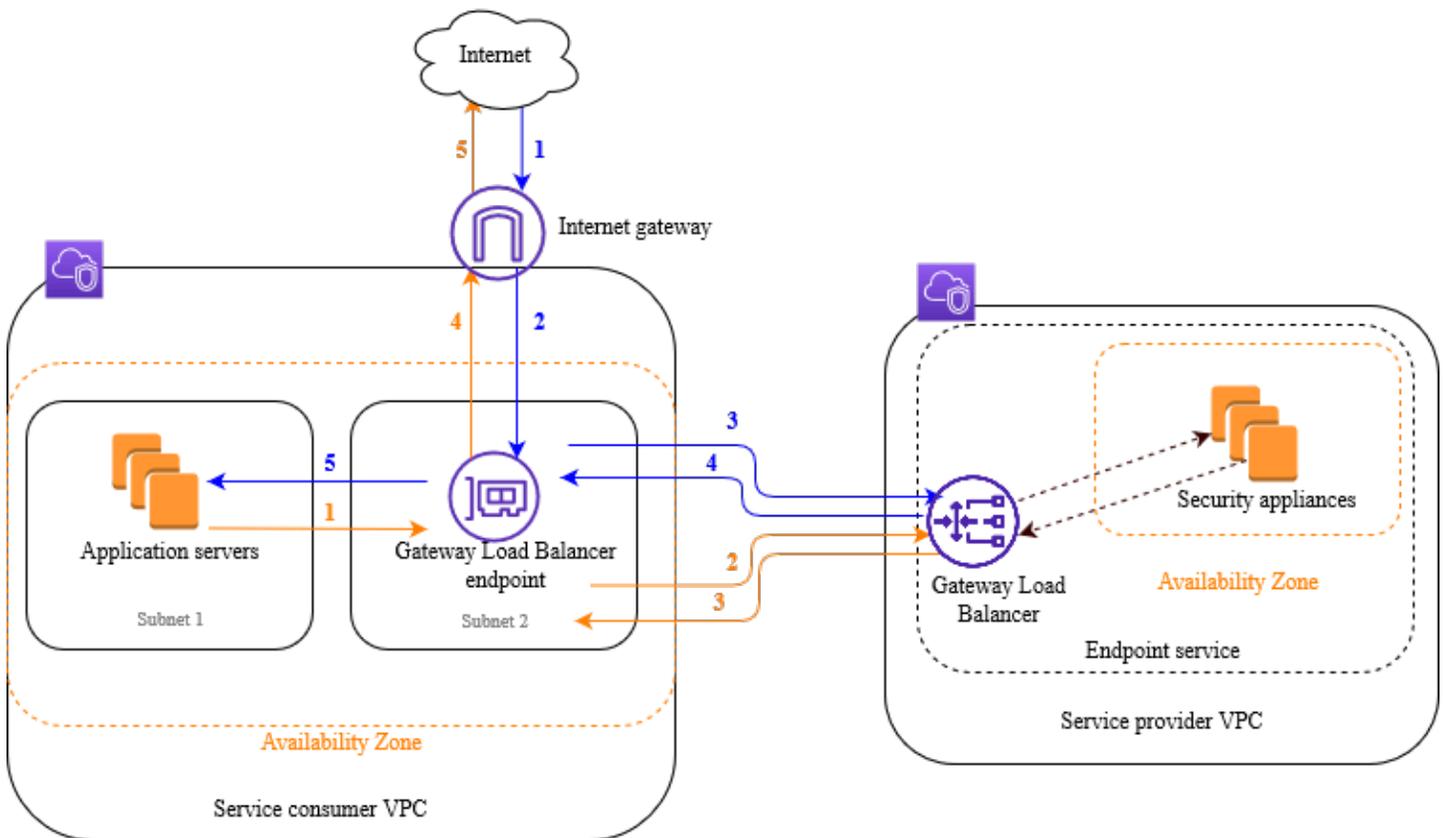
- [Présentation](#)
- [Prérequis](#)
- [Étape 1 : Création d'un Gateway Load Balancer et enregistrement des cibles](#)
- [Étape 2 : Création d'un point de terminaison Gateway Load Balancer](#)
- [Étape 3 : Configuration du routage](#)

Présentation

Un point de terminaison Gateway Load Balancer est un VPC point de terminaison qui fournit une connectivité privée entre les appliances virtuelles du fournisseur VPC de services et les serveurs d'applications du consommateur de services. VPC Le Gateway Load Balancer est déployé de la même manière VPC que celui des dispositifs virtuels. Ces appareils sont enregistrés en tant que groupe cible de l'équilibreur de charge Gateway Load Balancer.

Les serveurs d'applications s'exécutent dans un sous-réseau (sous-réseau de destination) du consommateur de services VPC, tandis que le point de terminaison Gateway Load Balancer se trouve dans un autre sous-réseau du même sous-réseau. VPC Tout le trafic entrant dans le consommateur de services VPC via la passerelle Internet est d'abord acheminé vers le point de terminaison Gateway Load Balancer, puis vers le sous-réseau de destination.

De même, tout le trafic quittant les serveurs d'applications (sous-réseau de destination) est acheminé vers le point de terminaison Gateway Load Balancer avant d'être réacheminé vers Internet. Le schéma de réseau suivant est une représentation visuelle de la manière dont un point de terminaison Gateway Load Balancer est utilisé pour accéder à un service de point de terminaison.



Les éléments numérotés qui suivent, mettent en évidence et expliquent ceux affichés sur l'image précédente.

Trafic depuis Internet vers l'application (flèches bleues) :

1. Le trafic entre dans le consommateur de services VPC via la passerelle Internet.
2. Le trafic est envoyé au point de terminaison Gateway Load Balancer à la suite du routage d'entrée.
3. Le trafic est envoyé au Gateway Load Balancer qui distribue le trafic vers un des appareils de sécurité.
4. Le trafic est renvoyé au point de terminaison Gateway Load Balancer après avoir été inspecté par l'appareil de sécurité.
5. Le trafic est envoyé aux serveurs d'applications (sous-réseau de destination).

Trafic de l'application vers Internet (flèches oranges) :

1. Le trafic est envoyé au point de terminaison Gateway Load Balancer à la suite du routage par défaut configuré sur le sous-réseau du serveur d'application.

2. Le trafic est envoyé au Gateway Load Balancer qui distribue le trafic vers un des appareils de sécurité.
3. Le trafic est renvoyé au point de terminaison Gateway Load Balancer après avoir été inspecté par l'appareil de sécurité.
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.

Routage

La table de routage de la passerelle Internet doit comporter une entrée qui achemine le trafic destiné aux serveurs d'applications vers le point de terminaison Gateway Load Balancer. Pour spécifier le point de terminaison Gateway Load Balancer, utilisez l'ID du point de terminaison. VPC L'exemple suivant montre les routages pour une configuration dualstack.

Destination	Target
<i>VPC IPv4 CIDR</i>	Local
<i>VPC IPv6 CIDR</i>	Local
<i>Subnet 1 IPv4 CIDR</i>	<i>vpc-endpoint-id</i>
<i>Subnet 1 IPv6 CIDR</i>	<i>vpc-endpoint-id</i>

La table de routage du sous-réseau avec les serveurs d'application doit comporter des entrées qui acheminent tout le trafic des serveurs d'applications vers le point de terminaison Gateway Load Balancer.

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

La table de routage du sous-réseau avec le point de terminaison Gateway Load Balancer doit acheminer le trafic qui revient de l'inspection à sa destination finale. Pour le trafic provenant d'Internet, l'acheminement local s'assure qu'il atteigne les serveurs d'applications. Pour le trafic provenant des serveurs d'applications, ajoutez des entrées qui acheminent tout le trafic à la passerelle Internet.

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

Prérequis

- Installez AWS CLI ou mettez à jour la version actuelle du AWS CLI si vous utilisez une version qui ne prend pas en charge les Gateway Load Balancers. Pour plus d'informations, consultez [Installation d' AWS Command Line Interface](#) dans le Guide de l'utilisateur AWS Command Line Interface .
- Assurez-vous que le client du service VPC dispose d'au moins deux sous-réseaux pour chaque zone de disponibilité contenant des serveurs d'applications. Un sous-réseau est destiné au point de terminaison Gateway Load Balancer et l'autre aux serveurs d'applications.
- Assurez-vous que le fournisseur de services VPC dispose d'au moins deux sous-réseaux pour chaque zone de disponibilité contenant des instances de dispositifs de sécurité. Un sous-réseau est destiné au Gateway Load Balancer et l'autre aux instances.
- Lancez au moins une instance d'appliance de sécurité dans chaque sous-réseau d'appliance de sécurité du fournisseur VPC de services. Les groupes de sécurité de ces instances doivent autoriser le UDP trafic sur le port 6081.

Étape 1 : Création d'un Gateway Load Balancer et enregistrement des cibles

Utilisez la procédure suivante pour créer votre équilibreur de charge, votre écouteur et vos groupes cibles, et pour enregistrer vos instances de dispositif de sécurité en tant que cibles.

Pour créer un Gateway Load Balancer et enregistrer les cibles

1. Utilisez la [create-load-balancer](#) commande pour créer un équilibreur de charge de type gateway. Vous pouvez spécifier un sous-réseau pour chaque zone de disponibilité dans laquelle vous avez lancé les instances d'appareil de sécurité.

```
aws elbv2 create-load-balancer --name my-load-balancer --type gateway --  
subnets provider-subnet-id
```

Par défaut, seules les IPv4 adresses sont prises en charge. Pour prendre en charge à la fois IPv6 les adresses IPv4 et les adresses, ajoutez l'`--ip-address-type dualstack` option.

La sortie inclut le nom de ressource Amazon (ARN) de l'équilibreur de charge, au format illustré dans l'exemple suivant.

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:loadbalancer/gwy/my-load-  
balancer/1234567890123456
```

2. Utilisez la [create-target-group](#) commande pour créer un groupe cible, en spécifiant le fournisseur VPC de services auprès duquel vous avez lancé vos instances.

```
aws elbv2 create-target-group --name my-targets --protocol GENEVE --port 6081 --  
vpc-id provider-vpc-id
```

La sortie inclut ARN le groupe cible, au format suivant.

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-  
targets/0123456789012345
```

3. Utilisez la commande [register-targets](#) pour enregistrer vos instances auprès de votre groupe cible.

```
aws elbv2 register-targets --target-group-arn targetgroup-arn --targets  
Id=i-1234567890abcdef0 Id=i-0abcdef1234567890
```

- Utilisez la commande [create-listener](#) pour créer un écouteur pour votre équilibreur de charge avec une règle par défaut qui transfère les demandes à votre groupe cible.

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --default-actions  
Type=forward,TargetGroupArn=targetgroup-arn
```

La sortie contient le fichier ARN de l'écouteur, au format suivant.

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:listener/gwy/my-load-  
balancer/1234567890123456/abc1234567890123
```

- (Facultatif) Vous pouvez vérifier l'état des cibles enregistrées pour votre groupe cible à l'aide de la [describe-target-health](#) commande suivante.

```
aws elbv2 describe-target-health --target-group-arn targetgroup-arn
```

Étape 2 : Création d'un point de terminaison Gateway Load Balancer

Utilisez la procédure suivante pour créer un service de point de terminaison Gateway Load Balancer. Les points de terminaison Gateway Load Balancer sont répartis par zone. Nous vous recommandons de créer un point de terminaison Gateway Load Balancer par zone. Pour plus d'informations, veuillez consulter [Accès aux appareils virtuels via AWS PrivateLink](#).

Pour créer un point de terminaison Gateway Load Balancer

- Utilisez la commande [create-vpc-endpoint-service-configuration](#) pour créer une configuration de service de point de terminaison à l'aide de votre Gateway Load Balancer.

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

Pour prendre en charge à la fois IPv6 les adresses IPv4 et les adresses, ajoutez l'option `--supported-ip-address-types ipv4 ipv6option`.

La sortie contient l'ID du service (par exemple, `vpce-svc-12345678901234567`) et le nom du service (par exemple, `com.amazonaws.vpce.us-east-2.vpce-svc-12345678901234567`).

2. Utilisez la commande [modify-vpc-endpoint-service-permissions](#) pour permettre aux consommateurs de services de créer un point de terminaison pour votre service. Un consommateur de services peut être un utilisateur, un IAM rôle ou Compte AWS. L'exemple suivant ajoute une autorisation pour ce qui est spécifié Compte AWS.

```
aws ec2 modify-vpc-endpoint-service-permissions --service-id vpce-svc-12345678901234567 --add-allowed-principals arn:aws:iam::123456789012:root
```

3. Utilisez la [create-vpc-endpoint](#) commande pour créer le point de terminaison Gateway Load Balancer pour votre service.

```
aws ec2 create-vpc-endpoint --vpc-endpoint-type GatewayLoadBalancer --service-name com.amazonaws.vpce.us-east-2.vpce-svc-12345678901234567 --vpc-id consumer-vpc-id --subnet-ids consumer-subnet-id
```

Pour prendre en charge à la fois IPv6 les adresses IPv4 et les adresses, ajoutez l'`--ip-address-type dualstack` option.

La sortie contient l'ID du point de terminaison Gateway Load Balancer (par exemple, `vpce-01234567890abcdef`).

Étape 3 : Configuration du routage

Configurez les tables de routage pour le consommateur de services VPC comme suit. Cela permet aux dispositifs de sécurité d'effectuer une inspection de sécurité du trafic entrant destiné aux serveurs d'applications.

Pour configurer le routage

1. Utilisez la commande [create-route](#) pour ajouter des entrées à la table de routage de la passerelle Internet qui achemine le trafic destiné aux serveurs d'applications vers le point de terminaison Gateway Load Balancer.

```
aws ec2 create-route --route-table-id gateway-rtb --destination-cidr-block Subnet 1 IPv4 CIDR --vpc-endpoint-id vpce-01234567890abcdef
```

Si vous êtes d'IPv6 accord, ajoutez l'itinéraire suivant.

```
aws ec2 create-route --route-table-id gateway-rtb --destination-cidr-block Subnet 1 IPv6 CIDR --vpc-endpoint-id vpce-01234567890abcdef
```

- Utilisez la commande [create-route](#) pour ajouter une entrée à la table de routage du sous-réseau avec les serveurs d'applications qui achemine le trafic des serveurs d'applications vers le point de terminaison Gateway Load Balancer.

```
aws ec2 create-route --route-table-id application-rtb --destination-cidr-block 0.0.0.0/0 --vpc-endpoint-id vpce-01234567890abcdef
```

Si vous êtes d'IPv6 accord, ajoutez l'itinéraire suivant.

```
aws ec2 create-route --route-table-id application-rtb --destination-cidr-block ::/0 --vpc-endpoint-id vpce-01234567890abcdef
```

- Utilisez la commande [create-route](#) pour ajouter une entrée à la table de routage du sous-réseau avec le point de terminaison Gateway Load Balancer qui achemine tout le trafic provenant des serveurs d'applications vers la passerelle Internet.

```
aws ec2 create-route --route-table-id endpoint-rtb --destination-cidr-block 0.0.0.0/0 --gateway-id igw-01234567890abcdef
```

Si vous êtes d'IPv6 accord, ajoutez l'itinéraire suivant.

```
aws ec2 create-route --route-table-id endpoint-rtb --destination-cidr-block ::/0 --gateway-id igw-01234567890abcdef
```

- Répétez l'opération pour la table de routage du sous-réseau de chaque application dans chaque zone.

Gateway Load Balancers

Utilisez un Gateway Load Balancer pour déployer et gérer un parc d'appareils virtuels compatibles avec le GENEVE protocole.

Un Gateway Load Balancer fonctionne au niveau de la troisième couche du modèle Open Systems Interconnection (OSI). Il écoute tous les paquets IP sur tous les ports et transmet le trafic au groupe cible spécifié dans la règle d'écoute, en utilisant le GENEVE protocole du port 6081.

Vous pouvez ajouter ou supprimer des cibles de votre équilibreur de charge au fur et à mesure que vos besoins évoluent, sans interrompre le flux global de demandes. Elastic Load Balancing fait évoluer votre équilibreur de charge au fur et à mesure que le trafic vers votre application change. Elastic Load Balancing peut s'adapter automatiquement à la plupart des applications.

Table des matières

- [États d'un équilibreur de charge](#)
- [Type d'adresse IP](#)
- [Zones de disponibilité](#)
- [Délai d'inactivité](#)
- [Attributs de l'équilibreur de charge](#)
- [Réseau ACLs](#)
- [Flux asymétriques](#)
- [Unité de transmission maximale du réseau \(MTU\)](#)
- [Création d'un Gateway Load Balancer](#)
- [Mettez à jour les types d'adresses IP de votre Gateway Load Balancer](#)
- [Modifier les attributs de votre Gateway Load Balancer](#)
- [Marquer un Gateway Load Balancer](#)
- [Supprimer un Gateway Load Balancer](#)

États d'un équilibreur de charge

Un Gateway Load Balancer peut avoir l'un des états suivants :

provisioning

Le Gateway Load Balancer est en cours de mise en place.

active

Le Gateway Load Balancer est entièrement mis en place et prêt à acheminer le trafic.

failed

Le Gateway Load Balancer n'a pas pu être configuré.

Type d'adresse IP

Vous pouvez définir les types d'adresses IP que les serveurs d'applications peuvent utiliser pour accéder à vos Gateway Load Balancers.

Les équilibreurs de charge de passerelle prennent en charge les types d'adresses IP suivants :

ipv4

Seule la clause IPv4 est prise en charge.

dualstack

Les deux IPv4 IPv6 sont pris en charge.

Considérations

- Le cloud privé virtuel (VPC) et les sous-réseaux que vous spécifiez pour l'équilibreur de charge doivent être associés à IPv6 CIDR des blocs.
- Les tables de routage des sous-réseaux du consommateur de services VPC doivent acheminer le IPv6 trafic, et le réseau ACLs de ces sous-réseaux doit autoriser IPv6 le trafic.
- Un Gateway Load Balancer encapsule à la fois le trafic IPv6 client IPv4 et le trafic client avec un IPv4 GENEVE en-tête et l'envoi à l'appliance. L'appliance encapsule à la fois IPv6 le trafic client IPv4 et le trafic client avec un IPv4 GENEVE en-tête et le renvoie au Gateway Load Balancer.

Pour plus d'informations sur les types d'adresses IP, consultez [Mettez à jour les types d'adresses IP de votre Gateway Load Balancer](#).

Zones de disponibilité

Lorsque vous créez un Gateway Load Balancer, vous activez une ou plusieurs zones de disponibilité et vous spécifiez le sous-réseau correspondant à chaque zone. Lorsque vous activez plusieurs zones de disponibilité, cela garantit que l'équilibreur de charge puisse continuer à acheminer le trafic même si une zone de disponibilité devient indisponible. Les sous-réseaux que vous spécifiez doivent disposer d'au moins 8 adresses IP disponibles. Les sous-réseaux ne peuvent pas être supprimés une fois l'équilibreur de charge créé. Pour supprimer un sous-réseau, vous devez créer un nouvel équilibreur de charge.

Délai d'inactivité

Pour chaque TCP demande effectuée via un Gateway Load Balancer, l'état de cette connexion est suivi. Si aucune donnée n'est envoyée via la connexion par le client ou la cible au cours d'une période plus longue que le délai d'inactivité, la connexion est fermée. Une fois le délai d'inactivité écoulé, l'équilibreur de charge considère le flux suivant TCP SYN comme un nouveau flux et l'achemine vers une nouvelle cible. Cependant, les paquets de données envoyés après l'expiration du délai d'inactivité sont supprimés.

La valeur du délai d'inactivité par défaut pour les TCP flux est de 350 secondes, mais elle peut être mise à jour à n'importe quelle valeur comprise entre 60 et 6 000 secondes. Les clients ou les cibles peuvent utiliser des paquets TCP keepalive pour réinitialiser le délai d'inactivité.

Lorsqu'UDPil n'est pas connecté, l'équilibreur de charge maintient l'état UDP du flux en fonction des adresses IP et des ports source et de destination. Cela garantit que les paquets appartenant au même flux sont systématiquement envoyés à la même cible. Une fois le délai d'inactivité écoulé, l'équilibreur de charge considère le UDP paquet entrant comme un nouveau flux et l'achemine vers une nouvelle cible. Elastic Load Balancing définit la valeur du délai d'inactivité pour les UDP flux à 120 secondes. Elles ne peuvent pas être modifiées.

EC2les instances doivent répondre à une nouvelle demande dans les 30 secondes afin d'établir un chemin de retour.

Pour de plus amples informations, veuillez consulter [Mettre à jour le délai d'inactivité](#).

Attributs de l'équilibreur de charge

Ce qui suit constitue les attributs de l'équilibreur de charge pour les Gateway Load Balancers :

`deletion_protection.enabled`

Indique si la protection contre la suppression est activée. L'argument par défaut est `false`.

`load_balancing.cross_zone.enabled`

Indique si l'équilibrage de charge entre zones est activé. L'argument par défaut est `false`.

Pour de plus amples informations, veuillez consulter [Modifier les attributs de l'équilibreur de charge](#).

Réseau ACLs

Si les serveurs d'applications et le point de terminaison Gateway Load Balancer se trouvent dans le même sous-réseau, les NACL règles sont évaluées pour le trafic entre les serveurs d'applications et le point de terminaison Gateway Load Balancer.

Flux asymétriques

Les Gateway Load Balancers prennent en charge les flux asymétriques lorsque l'équilibreur de charge traite le paquet de flux initial et que le paquet de flux de réponse n'est pas acheminé via l'équilibreur de charge. Le routage asymétrique n'est pas recommandé car il peut réduire les performances du réseau. Les Gateway Load Balancers ne prennent pas en charge les flux asymétriques lorsque l'équilibreur de charge ne traite pas le paquet de flux initial et que le paquet de flux de réponse n'est pas acheminé via l'équilibreur de charge.

Unité de transmission maximale du réseau (MTU)

L'unité de transmission maximale (MTU) est la taille du plus gros paquet de données pouvant être transmis via le réseau. L'interface Gateway Load Balancer prend en charge MTU les paquets d'une taille maximale de 8 500 octets. Les paquets d'une taille supérieure à 8 500 octets qui arrivent à l'interface Gateway Load Balancer sont supprimés.

Un Gateway Load Balancer encapsule le trafic IP avec un GENEVE en-tête et le transmet à l'appliance. Le processus GENEVE d'encapsulation ajoute 64 octets au paquet d'origine. Par conséquent, pour prendre en charge des paquets allant jusqu'à 8 500 octets, assurez-vous que le MTU paramètre de votre appliance prend en charge les paquets d'au moins 8 564 octets.

Les Gateway Load Balancers ne prennent pas en charge la fragmentation IP. De plus, les équilibreurs de charge de passerelle ne génèrent pas le ICMP message « Destination inaccessible » :

fragmentation nécessaire et DF défini ». Pour cette raison, Path MTU Discovery (PMTUD) n'est pas pris en charge.

Création d'un Gateway Load Balancer

Un Gateway Load Balancer prend les demandes des clients et les distribue entre les cibles d'un groupe cible, telles que EC2 les instances.

Pour créer un Gateway Load Balancer à l'aide du AWS Management Console, effectuez les tâches suivantes. Vous pouvez également créer un Gateway Load Balancer à l'aide du AWS CLI, voir. [Prise en main à l'aide de l'CLI](#)

Tâches

- [Prérequis](#)
- [Créer l'équilibreur de charge](#)
- [Étapes suivantes importantes](#)

Prérequis

Avant de commencer, assurez-vous que le cloud privé virtuel (VPC) de votre Gateway Load Balancer possède au moins un sous-réseau dans chaque zone de disponibilité où vous avez des cibles.

Créer l'équilibreur de charge

Utilisez la procédure suivante pour créer votre Gateway Load Balancer. Fournissez des informations de configuration de base pour votre équilibreur de charge, comme un nom et un type d'adresse IP. Fournissez ensuite des informations sur votre réseau et sur l'écouteur qui achemine le trafic vers vos groupes cibles. Les Gateway Load Balancers nécessitent des groupes cibles qui utilisent le GENEVE protocole.

Pour créer l'équilibreur de charge et l'écouteur à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sous Équilibrage de charge, choisissez Équilibreurs de charge.
3. Choisissez Créer un équilibreur de charge.
4. Sous Gateway Load Balancer, choisissez Créer.

5. Configuration de base

- a. Pour Load balancer name (Nom de l'équilibreur de charge), saisissez un nom pour l'équilibreur de charge. Par exemple, **my-g1b**. Le nom de votre Gateway Load Balancer doit être unique au sein de votre ensemble d'équilibreurs de charge pour la région. Il doit comporter un maximum de 32 caractères et ne peut contenir que des caractères alphanumériques et des traits d'union.
- b. Pour le type d'adresse IP, choisissez de prendre IPv4 en charge les IPv4 adresses uniquement ou Dualstack pour prendre en charge à la fois les adresses IPv4 et IPv6 les adresses.

6. Mappage du réseau

- a. Pour VPC, sélectionnez le fournisseur de services VPC.
- b. Pour Mappages, sélectionnez toutes les zones de disponibilité dans lesquelles vous avez lancé les instances d'appareils de sécurité et les sous-réseaux publics correspondants.

7. Routage d'écouteur d'IP

- a. Pour Action par défaut, sélectionnez le groupe cible pour recevoir le trafic. Si vous n'avez pas de groupe cible, choisissez Créer un groupe cible. Pour de plus amples informations, veuillez consulter [Créer un groupe cible](#).
- b. (Facultatif) Développez Balises d'écouteur et ajoutez les balises dont vous avez besoin.

8. (Facultatif) Développez Balises d'équilibreur de charge et ajoutez les balises dont vous avez besoin.

9. Vérifiez votre configuration, puis choisissez Create load balancer (Créer l'équilibreur de charge).

Étapes suivantes importantes

Après avoir créé votre équilibreur de charge, vérifiez que vos EC2 instances ont passé avec succès le test de santé initial. Pour tester votre équilibreur de charge, vous devez créer un point de terminaison Gateway Load Balancer et mettre à jour votre table de routage pour faire du point de terminaison Gateway Load Balancer le prochain saut. Ces configurations sont définies dans la VPC console Amazon. Pour plus d'informations, consultez le didacticiel [Premiers pas](#).

Mettez à jour les types d'adresses IP de votre Gateway Load Balancer

Vous pouvez configurer votre Gateway Load Balancer de manière à ce que les serveurs d'applications puissent accéder à votre équilibreur de charge en utilisant uniquement des IPv4 adresses, ou en utilisant à la fois des adresses IPv4 et des IPv6 adresses (dualstack). L'équilibreur de charge communique avec les cibles en fonction du type d'adresse IP du groupe cible. Pour de plus amples informations, veuillez consulter [Type d'adresse IP](#).

Pour mettre à jour le type d'adresse IP à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Load Balancing (Équilibrage de charge), choisissez Load Balancers (Équilibreurs de charge).
3. Sélectionnez l'équilibreur de charge.
4. Choisissez Actions, Edit IP address type.
5. Pour le type d'adresse IP, choisissez ipv4 pour prendre en charge IPv4 les adresses uniquement ou dualstack pour prendre en charge les deux IPv4 adresses. IPv6
6. Choisissez Save (Enregistrer).

Pour mettre à jour le type d'adresse IP à l'aide du AWS CLI

Utilisez la [set-ip-address-type](#) commande.

Modifier les attributs de votre Gateway Load Balancer

Après avoir créé un Gateway Load Balancer, vous pouvez modifier ses attributs d'équilibreur de charge.

Attributs de l'équilibreur de charge

- [Deletion protection \(Protection contre la suppression\)](#)
- [Équilibrage de charge entre zones](#)

Deletion protection (Protection contre la suppression)

Pour éviter la suppression accidentelle de votre Gateway Load Balancer, vous pouvez activer la protection contre la suppression. Par défaut, la protection contre la suppression est désactivée.

Si vous activez la protection contre la suppression de votre Gateway Load Balancer, vous devez la désactiver pour pouvoir supprimer le Gateway Load Balancer.

Pour activer la protection contre la suppression à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sous Équilibrage de charge, choisissez Équilibreurs de charge.
3. Sélectionnez le Gateway Load Balancer.
4. Choisissez Actions, Edit Attributes (Modifier les attributs).
5. Sur la page Modifier les attributs de l'équilibreur de charge, sélectionnez Activer pour Protection contre la suppression, puis choisissez Enregistrer.

Pour désactiver la protection contre la suppression à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sous Équilibrage de charge, choisissez Équilibreurs de charge.
3. Sélectionnez le Gateway Load Balancer.
4. Choisissez Actions, Edit Attributes (Modifier les attributs).
5. Sur la page Modifier les attributs de l'équilibreur de charge, désélectionnez Activer pour Protection contre la suppression, puis choisissez Enregistrer.

Pour activer ou désactiver la protection contre la suppression à l'aide du AWS CLI

Utilisez la [modify-load-balancer-attributes](#) commande avec l'attribut `deletion_protection.enabled`.

Équilibrage de charge entre zones

Par défaut, chaque nœud d'équilibreur de charge répartit le trafic parmi les cibles enregistrées dans sa zone de disponibilité uniquement. Si vous activez l'équilibrage de charge entre zones, chaque nœud de Gateway Load Balancer répartit le trafic entre les cibles enregistrées dans toutes les zones

de disponibilité activées. Pour de plus amples informations, consultez [Répartition de charge entre zones](#) dans le Guide de l'utilisateur Elastic Load Balancing.

Pour activer l'équilibrage de charge entre zones à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sous Équilibrage de charge, choisissez Équilibreurs de charge.
3. Sélectionnez le Gateway Load Balancer.
4. Choisissez Actions, Edit Attributes (Modifier les attributs).
5. Sur la page Modifier les attributs de l'équilibreur de charge, sélectionnez Activer pour Équilibrage de charge entre zones, puis choisissez Enregistrer.

Pour activer l'équilibrage de charge entre zones à l'aide du AWS CLI

Utilisez la [modify-load-balancer-attributes](#) commande avec l'`load_balancing.cross_zone.enabled` attribut.

Marquer un Gateway Load Balancer

Les balises vous aident à classer vos équilibreurs de charge de différentes manières, par exemple, par objectif, par propriétaire ou par environnement.

Vous pouvez ajouter plusieurs balises à chaque équilibreur de charge. Les clés de balise doivent être uniques pour chaque Gateway Load Balancer. Si vous ajoutez une balise avec une clé qui est déjà associée à l'équilibreur de charge, cela met à jour la valeur de cette balise.

Lorsque vous avez fini avec une balise, vous pouvez la supprimer de votre Gateway Load Balancer.

Restrictions

- Nombre maximal de balises par ressource : 50
- Longueur de clé maximale : 127 caractères Unicode
- Longueur de valeur maximale : 255 caractères Unicode
- Les clés et valeurs d'étiquette sont sensibles à la casse. Les caractères autorisés sont les lettres, les espaces et les chiffres représentables en UTF -8, ainsi que les caractères spéciaux suivants : + - = . _ : / @. N'utilisez pas d'espaces de début ou de fin.

- N'utilisez pas le aws : préfixe dans les noms ou les valeurs de vos balises, car il est réservé à AWS l'usage. Vous ne pouvez pas modifier ou supprimer des noms ou valeurs de balise ayant ce préfixe. Les balises avec ce préfixe ne sont pas comptabilisées comme vos balises pour la limite de ressources.

Pour mettre à jour les balises d'un Gateway Load Balancer à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sous Équilibrage de charge, choisissez Équilibreurs de charge.
3. Sélectionnez le Gateway Load Balancer.
4. Choisissez Balises, Ajouter/modifier des balises, puis exécutez une ou plusieurs des actions suivantes :
 - a. Pour mettre à jour une balise, modifiez les valeurs de Clé et Valeur.
 - b. Pour ajouter une nouvelle balise, choisissez Create Tag. (Créer une identification). Pour Clé et Valeur, saisissez les valeurs.
 - c. Pour supprimer une balise, choisissez l'icône de suppression (X) à côté de la balise.
5. Lorsque vous avez terminé de mettre à jour les balises, choisissez Enregistrer.

Pour mettre à jour les balises d'un Gateway Load Balancer à l'aide du AWS CLI

Utilisez la commande [add-tags](#) et [remove-tags](#).

Supprimer un Gateway Load Balancer

Dès que votre Gateway Load Balancer est disponible, vous êtes facturé pour chaque heure ou heure partielle pendant laquelle vous le laissez tourner. Lorsque vous n'avez plus besoin du Gateway Load Balancer, vous pouvez le supprimer. Dès que le Gateway Load Balancer est supprimé, vous cessez d'être facturé pour celui-ci.

Vous ne pouvez pas supprimer un Gateway Load Balancer s'il est utilisé par un autre service. Par exemple, si le Gateway Load Balancer est associé à un service de point de VPC terminaison, vous devez supprimer la configuration du service de point de terminaison avant de pouvoir supprimer le Gateway Load Balancer associé.

La suppression d'un Gateway Load Balancer supprime également ses écouteurs. La suppression d'un Gateway Load Balancer n'affecte pas ses cibles enregistrées. Par exemple, vos EC2 instances

continuent de s'exécuter et sont toujours enregistrées auprès de leurs groupes cibles. Pour supprimer vos groupes cible, consultez la page [Supprimer un groupe cible pour votre Gateway Load Balancer](#).

Pour supprimer un Gateway Load Balancer à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sous Équilibrage de charge, choisissez Équilibreurs de charge.
3. Sélectionnez le Gateway Load Balancer.
4. Choisissez Actions, Delete (Supprimer).
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

Pour supprimer un Gateway Load Balancer à l'aide du AWS CLI

Utilisez la [delete-load-balancer](#) commande.

Écouteurs pour vos Gateway Load Balancers

Lorsque vous créez votre Gateway Load Balancer, vous ajoutez un écouteur. Un écouteur est un processus qui vérifie les demandes de connexion.

Les écouteurs pour les Gateway Load Balancers écoutent tous les paquets IP sur tous les ports. Vous ne pouvez pas spécifier de protocole ou de port lorsque vous créez un écouteur pour un Gateway Load Balancer.

Lorsque vous créez un écouteur, vous spécifiez une règle pour l'acheminement des requêtes. Cette règle achemine les demandes vers le groupe cible spécifié. Vous pouvez mettre à jour la règle d'écouteur pour transférer les demandes à un autre groupe cible.

Attributs de l'écouteur

Les attributs de l'écouteur pour les équilibreurs de charge Gateway sont les suivants :

`tcp.idle_timeout.seconds`

La valeur du délai d'inactivité du protocole TCP, en secondes. La plage valide est comprise entre 60 et 6 000 secondes. La valeur par défaut est de 350 secondes.

Pour de plus amples informations, veuillez consulter [Mettre à jour le délai d'inactivité](#).

Mettez à jour le groupe cible de votre écouteur Gateway Load Balancer

Lorsque vous créez un écouteur, vous spécifiez une règle pour l'acheminement des requêtes. Cette règle achemine les demandes vers le groupe cible spécifié. Vous pouvez mettre à jour la règle d'écouteur pour transférer les demandes à un autre groupe cible.

Pour mettre à jour votre écouteur à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sous Équilibrage de charge, choisissez Équilibreurs de charge.
3. Sélectionnez l'équilibreur de charge, puis choisissez l'onglet Ecouteurs.

4. Choisissez Modifier l'écouteur.
5. Pour Transférer vers un groupe cible, choisissez un groupe cible.
6. Choisissez Save (Enregistrer).

Pour mettre à jour votre écouteur à l'aide du AWS CLI

Utilisez la commande [modify-listener](#).

Mettez à jour le TCP délai d'inactivité de votre écouteur Gateway Load Balancer

Pour chaque TCP demande effectuée via un Gateway Load Balancer, l'état de cette connexion est suivi. Si aucune donnée n'est envoyée via la connexion par le client ou la cible au cours d'une période plus longue que le délai d'inactivité, la connexion est fermée. La valeur du délai d'inactivité par défaut pour les TCP flux est de 350 secondes, mais elle peut être mise à jour à n'importe quelle valeur comprise entre 60 et 6 000 secondes.

Pour mettre à jour le délai TCP d'inactivité à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sous Équilibrage de charge, choisissez Équilibreurs de charge.
3. Sélectionnez le Gateway Load Balancer.
4. Dans l'onglet écouteurs, choisissez Actions, Afficher les détails de l'écouteur.
5. Sur la page de détails de l'écouteur, dans l'onglet Attributs, sélectionnez Modifier.
6. Sur la page Modifier les attributs du récepteur, dans la section Attributs du récepteur, entrez une valeur pour le délai d'TCPinactivité.
7. Choisissez Enregistrer les modifications

Pour mettre à jour le délai TCP d'inactivité à l'aide du AWS CLI

Utilisez la [modify-listener-attributes](#) commande avec l'`tcp.idle_timeout.seconds`attribut.

Groupes cibles pour vos Gateway Load Balancers

Chaque groupe cible est utilisé pour acheminer les demandes vers une ou plusieurs cibles enregistrées. Lorsque vous créez un écouteur, vous spécifiez un groupe cible pour son action par défaut. Le trafic est transféré vers le groupe cible spécifié dans la règle de l'écouteur. Vous pouvez créer différents groupes cibles pour les différents types de demandes.

Vous définissez des paramètres de vérification de l'état de votre Gateway Load Balancer pour chaque groupe cible. Chaque groupe cible utilise les paramètres de vérification de l'état par défaut, sauf si vous les remplacez lors de la création du groupe cible ou que vous les modifiez ultérieurement. Une fois que vous avez spécifié un groupe cible dans une règle destinée à un écouteur, le Gateway Load Balancer surveille continuellement l'état de santé de toutes les cibles enregistrées auprès du groupe cible qui résident dans une zone de disponibilité activée pour le Gateway Load Balancer. Le Gateway Load Balancer achemine les demandes vers les cibles enregistrées qui sont saines. Pour de plus amples informations, veuillez consulter [Contrôles de santé pour les groupes cibles de Gateway Load Balancer](#).

Table des matières

- [Configuration du routage](#)
- [Type de cible](#)
- [Cibles enregistrées](#)
- [Attributs de groupe cible](#)
- [Création d'un groupe cible pour votre Gateway Load Balancer](#)
- [Contrôles de santé pour les groupes cibles de Gateway Load Balancer](#)
- [Modifier les attributs du groupe cible pour votre Gateway Load Balancer](#)
- [Enregistrez des cibles pour votre Gateway Load Balancer](#)
- [Identifiez un groupe cible pour votre Gateway Load Balancer](#)
- [Supprimer un groupe cible pour votre Gateway Load Balancer](#)

Configuration du routage

Les groupes cibles pour les Gateway Load Balancers prennent en charge le protocole et port suivants :

- Protocole : GENEVE

- Port : 6#081

Type de cible

Lorsque vous créez un groupe cible, vous spécifiez son type de cible, qui détermine la façon dont vous spécifiez ses cibles. Après avoir créé un groupe cible, vous ne pouvez pas changer son type.

Les éléments suivants constituent les types de cibles possibles :

instance

Les cibles sont spécifiées par ID d'instance.

ip

Les cibles sont spécifiées par adresse IP.

Lorsque le type de cible est `ip`, vous pouvez spécifier des adresses IP à partir de l'un des CIDR blocs suivants :

- Les sous-réseaux du VPC pour le groupe cible
- [10,0.0.0/8 \(1918\) RFC](#)
- [100,64,0,0/10 \(6598\) RFC](#)
- 172,16,0,0/12 (1918) RFC
- 192,168.0.0/16 (1918) RFC

Important

Vous ne pouvez pas spécifier d'adresses IP publiquement routables.

Cibles enregistrées

Votre Gateway Load Balancer sert de point de contact unique pour les clients et répartit le trafic entrant sur ses cibles enregistrées saines. Chaque groupe cible doit avoir au moins une cible enregistrée dans chaque zone de disponibilité qui est activée pour le Gateway Load Balancer. Vous pouvez enregistrer chaque cible auprès d'un ou plusieurs groupes cibles.

Si la demande augmente, vous pouvez enregistrer des cibles supplémentaires auprès d'un ou plusieurs groupes cible afin de pouvoir gérer la demande. Le Gateway Load Balancer commence à acheminer le trafic vers la cible nouvellement enregistrée dès que le processus d'enregistrement est terminé.

Si la demande diminue ou que vous avez besoin de répondre aux demandes de vos cibles, vous pouvez annuler l'enregistrement des cibles dans vos groupes cible. L'annulation de l'enregistrement d'une cible supprime la cible de votre groupe cible, mais n'affecte pas autrement la cible. Le Gateway Load Balancer arrête d'acheminer le trafic vers une cible dès que l'enregistrement de celle-ci a été annulé. La cible passe à l'état `draining` jusqu'à ce que les demandes en cours soient terminées. Vous pouvez enregistrer à nouveau la cible auprès du groupe cible lorsque vous êtes prêt à reprendre la réception du trafic.

Attributs de groupe cible

Vous pouvez utiliser les attributs suivants avec les groupes cibles :

`deregistration_delay.timeout_seconds`

Durée d'attente pour Elastic Load Balancing avant de changer l'état de la cible dont l'enregistrement est annulé de `draining` à `unused`. La plage est comprise entre 0 et 3 600 secondes. La valeur par défaut est de 300 secondes.

`stickiness.enabled`

Indique si la permanence du flux configurable est activée pour le groupe cible. Les valeurs possibles sont `true` ou `false`. La valeur par défaut est `false`. Lorsque l'attribut est défini sur `false`, `5_tuple` est utilisé.

`stickiness.type`

Indique le type de permanence. Les valeurs possibles pour les groupes cibles associés aux Gateway Load Balancers sont les suivantes :

- `source_ip_dest_ip`
- `source_ip_dest_ip_proto`

`target_failover.on_deregistration`

Indique comment le Gateway Load Balancer gère les flux existants lorsqu'une cible est désenregistrée. Les valeurs possibles sont `rebalance` et `no_rebalance`. La valeur par

défaut est `no_rebalance`. Les deux attributs (`target_failover.on_deregistration` et `target_failover.on_unhealthy`) ne peuvent pas être définis indépendamment. La valeur que vous définissez pour les deux attributs doit être identique.

`target_failover.on_unhealthy`

Indique comment le Gateway Load Balancer gère les flux existants lorsqu'une cible n'est pas saine. Les valeurs possibles sont `rebalance` et `no_rebalance`. La valeur par défaut est `no_rebalance`. Les deux attributs (`target_failover.on_deregistration` et `target_failover.on_unhealthy`) ne peuvent pas être définis indépendamment. La valeur que vous définissez pour les deux attributs doit être identique.

Pour de plus amples informations, veuillez consulter [Modifier les attributs du groupe cible](#).

Création d'un groupe cible pour votre Gateway Load Balancer

Vous enregistrez les cibles pour votre Gateway Load Balancer avec un groupe cible.

Pour acheminer le trafic vers les cibles d'un groupe cible, créez un écouteur et spécifiez le groupe cible dans une action par défaut pour l'écouteur. Pour de plus amples informations, veuillez consulter [Écouteurs](#).

Vous pouvez ajouter ou supprimer des cibles dans votre groupe cible à tout moment. Pour de plus amples informations, veuillez consulter [Enregistrer des cibles](#). Vous pouvez aussi modifier les paramètres de vérification de l'état de votre groupe cible. Pour de plus amples informations, veuillez consulter [Paramètres de surveillance de l'état](#).

Pour créer un groupe cible à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Répartition de charge, choisissez Groupes cibles.
3. Sélectionnez Créer un groupe cible.
4. Configuration de base
 - a. Pour Choisir un type de cible, sélectionnez Instances pour spécifier les cibles par ID d'instance, ou sélectionnez Adresses IP pour spécifier les cibles par adresse IP.
 - b. Pour Nom du groupe cible, saisissez un nom pour le groupe cible. Ce nom doit être unique par région et par compte, peut comporter un maximum de 32 caractères, doit contenir

- uniquement des caractères alphanumériques ou des traits d'union et ne doit pas commencer ou se terminer par un trait d'union.
- c. Vérifiez que le protocole est GENEVE et que le port est 6081. Aucun autre protocole ou port n'est pris en charge.
 - d. Pour VPC, sélectionnez le cloud privé virtuel (VPC) contenant les instances de dispositif de sécurité à inclure dans votre groupe cible.
5. (Facultatif) Pour Health checks (Surveillances de l'état), modifiez les paramètres par défaut en fonction des besoins. Si les surveillances de l'état dépassent consécutivement le Seuil de défectuosité, l'équilibreur de charge met la cible hors service. Lorsque les surveillances de l'état dépassent consécutivement le Seuil de défectuosité, l'équilibreur de charge remet la cible en service. Pour de plus amples informations, veuillez consulter [Contrôles de santé pour les groupes cibles de Gateway Load Balancer](#).
 6. (Facultatif) Développez Balises et ajoutez les balises dont vous avez besoin.
 7. Choisissez Suivant.
 8. Sur la page Enregistrer les cibles, ajoutez une ou plusieurs cibles comme suit :
 - Si le type de cible est Instances, sélectionnez une ou plusieurs instances, saisissez un ou plusieurs ports, puis choisissez Inclure comme étant en attente ci-dessous.
 - Si le type de cible est Adresses IP, sélectionnez le réseau, saisissez l'adresse IP et les ports, puis choisissez Inclure comme étant en attente ci-dessous.
 9. Sélectionnez Créer un groupe cible.

Pour créer un groupe cible à l'aide du AWS CLI

Utilisez la [create-target-group](#) commande pour créer le groupe cible, la commande [add tags](#) pour étiqueter votre groupe cible et la commande [register-targets pour ajouter des cibles](#).

Contrôles de santé pour les groupes cibles de Gateway Load Balancer

Vous pouvez enregistrer vos cibles auprès d'un ou de plusieurs groupes cibles. Votre Gateway Load Balancer commence à acheminer les demandes vers la cible nouvellement enregistrée dès que le processus d'enregistrement est terminé. Quelques minutes peuvent être nécessaires pour que le processus d'inscription soit effectué et que les surveillances de l'état commencent.

Le Gateway Load Balancer envoie périodiquement une demande à chaque cible enregistrée pour vérifier son état. Lorsque toutes les vérifications de l'état sont terminées, le Gateway Load Balancer ferme la connexion qui a été établie pour la surveillance de l'état.

Paramètres de surveillance de l'état

Vous configurez les surveillances de l'état actives pour les cibles d'un groupe cible en utilisant les paramètres suivants. Si les contrôles de santé dépassent le nombre spécifié de défaillances `UnhealthyThresholdCount` consécutives, le Gateway Load Balancer met la cible hors service. Lorsque les bilans de santé dépassent le nombre spécifié de réussites `HealthyThresholdCount` consécutives, le Gateway Load Balancer remet la cible en service.

Paramètre	Description
<code>HealthCheckProtocol</code>	Protocole utilisé par l'équilibreur de charge lors des vérifications de l'état sur les cibles. Les protocoles possibles sont HTTPHTTPS, etTCP. La valeur par défaut estTCP.
<code>HealthCheckPort</code>	Le port utilisé par Gateway Load Balancer lors de la surveillance de l'état des cibles. La plage est comprise entre 1 et 65 535. La valeur par défaut est 80.
<code>HealthCheckPath</code>	[HTTP/HTTPSbilans de santé] Le chemin du bilan de santé qui est la destination des cibles pour les bilans de santé. La valeur par défaut est /.
<code>HealthCheckTimeoutSeconds</code>	Durée, en secondes, pendant laquelle l'absence de réponse d'une cible indique l'échec de la vérification de l'état. La plage est comprise entre 2 et 120. La valeur par défaut est 5.
<code>HealthCheckIntervalSeconds</code>	Durée approximative, en secondes, entre les vérifications de l'état d'une cible. La plage est comprise entre 5 et 300. Le durée par

Paramètre	Description
	<p>défaut est 10 secondes. Cette valeur doit être supérieure ou égale à HealthCheckTimeout Seconds.</p> <div data-bbox="829 384 1507 888" style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><p>Les surveillances de l'état des Gateway Load Balancers sont distribuées et utilisent un mécanisme de consensus pour déterminer l'état des cibles. Par conséquent, vous devez vous attendre à ce que les dispositifs cibles reçoivent plusieurs surveillances de l'état dans l'intervalle de temps configuré.</p></div>
HealthyThresholdCount	Le nombre de réussites consécutives de la vérification de l'état à partir duquel une cible défectueuse est considérée comme saine. La plage est comprise entre 2 et 10. La valeur par défaut est 5.
UnhealthyThresholdCount	Le nombre d'échecs consécutifs de la vérification de l'état à partir duquel une cible est considérée comme défectueuse. La plage est comprise entre 2 et 10. La valeur par défaut est 2.
Matcher	[HTTP/HTTPSbilans de santé] HTTP Codes à utiliser lors de la vérification de l'efficacité de la réponse d'une cible. La valeur doit être comprise entre 200 et 399.

État de santé d'une cible

Avant que le Gateway Load Balancer n'envoie une demande de vérification de l'état à une cible, vous devez enregistrer cette cible auprès d'un groupe cible, spécifier son groupe cible dans une règle d'écouteur et vous assurer que la zone de disponibilité de la cible est activée pour le Gateway Load Balancer.

Le tableau suivant décrit les valeurs possibles de l'état de santé d'une cible enregistrée.

Valeur	Description
<code>initial</code>	<p>Le Gateway Load Balancer est en train d'enregistrer la cible ou d'exécuter les vérifications de l'état initiales sur la cible.</p> <p>Codes de motif connexes : <code>Elb.RegistrationInProgress</code> <code>Elb.InitialHealthChecking</code></p>
<code>healthy</code>	<p>La cible est saine.</p> <p>Codes de motif connexes : aucun</p>
<code>unhealthy</code>	<p>La cible n'a pas répondu à une vérification de l'état ou a échoué à la vérification de l'état.</p> <p>Code motif connexe : <code>Target.FailedHealthChecks</code></p>
<code>unused</code>	<p>La cible n'est pas enregistrée auprès d'un groupe cible, le groupe cible n'est pas utilisé dans une règle d'écouteur, la cible est dans une zone de disponibilité qui n'est pas activée pour l'équilibreur de charge, ou l'état de la cible indique qu'elle a été arrêtée ou résiliée.</p> <p>Codes de motif connexes : <code>Target.NotRegistered</code> <code>Target.NotInUse</code> <code>Target.InvalidState</code> <code>Target.IpUnusable</code></p>
<code>draining</code>	<p>L'enregistrement de la cible est en cours d'annulation et le drainage de la connexion est en cours.</p>

Valeur	Description
	Code motif connexe : <code>Target.DeregistrationInProgress</code>
<code>unavailable</code>	L'état cible n'est pas disponible. Code motif connexe : <code>Elb.InternalError</code>

Codes de motif de vérification de l'état

Si le statut d'une cible est une valeur autre que `Healthy`, elle API renvoie un code de raison et une description du problème, et la console affiche la même description. Les codes de motif qui commencent par `Elb` proviennent du côté Gateway Load Balancer et ceux qui commencent par `Target` proviennent du côté cible.

Code de motif	Description
<code>Elb.InitialHealthChecking</code>	Vérifications de l'état initiales en cours
<code>Elb.InternalError</code>	Échec des vérifications de l'état initiales en raison d'une erreur interne
<code>Elb.RegistrationInProgress</code>	Enregistrement de la cible en cours
<code>Target.DeregistrationInProgress</code>	Annulation de l'enregistrement de la cible en cours
<code>Target.FailedHealthChecks</code>	Échec des vérifications de l'état
<code>Target.InvalidState</code>	La cible est à l'état arrêté. La cible est à l'état résilié. La cible est à l'état résilié ou arrêté. La cible est à un état non valide.

Code de motif	Description
Target.IpUnusable	L'adresse IP ne peut pas être utilisée en tant que cible, car elle est utilisée par un équilibreur de charge
Target.NotInUse	Le groupe cible n'est pas configuré de façon à recevoir le trafic du Gateway Load Balancer La cible est dans une zone de disponibilité qui n'est pas activée pour le Gateway Load Balancer
Target.NotRegistered	La cible n'est pas enregistrée auprès du groupe cible

Scénarios de défaillance de la cible du Gateway Load Balancer

Flux existants : Par défaut, les flux existants sont dirigés vers la même cible à moins que le flux n'expire ou ne soit réinitialisé, quels que soient l'état de santé et l'état d'enregistrement de la cible. Cette approche facilite l'épuisement des connexions et s'adapte aux pare-feux tiers qui sont parfois incapables de répondre aux contrôles de santé en raison d'une utilisation intensive. CPU Pour plus d'informations, consultez la section [Target Failover](#).

New flows (Nouveaux flux) : les nouveaux flux sont envoyés vers une cible saine. Lorsqu'une décision d'équilibrage de charge a été prise pour un flux, le Gateway Load Balancer envoie le flux vers la même cible même si cette cible n'est plus saine ou si d'autres cibles le deviennent.

Lorsque toutes les cibles ne sont pas saines, le Gateway Load Balancer choisit une cible au hasard et lui transmet le trafic pendant toute la durée du flux, jusqu'à ce qu'elle soit réinitialisée ou qu'elle ait expiré. Comme le trafic est transféré vers une cible défectueuse, le trafic est supprimé jusqu'à ce que cette cible redevienne saine.

TLS1.3 : Si un groupe cible est configuré avec des contrôles de HTTPS santé, ses cibles enregistrées échouent aux tests de santé s'ils ne prennent en charge que la TLS version 1.3. Ces cibles doivent prendre en charge une version antérieure de TLS, telle que TLS 1.2.

Cross-zone load balancing (Équilibrage de charge entre zones) : par défaut, l'équilibrage de charge entre les zones de disponibilité est désactivé. Si l'équilibrage de charge entre les zones est activé, chaque Gateway Load Balancer peut voir toutes les cibles dans toutes les zones de disponibilité, et elles sont toutes traitées de la même manière, quelle que soit leur zone.

Les décisions relatives à l'équilibrage de charge et à la surveillance de l'état sont toujours indépendantes d'une zone à l'autre. Même lorsque l'équilibrage de charge entre les zones est activé, le comportement des flux existants et des nouveaux flux est le même que celui décrit ci-dessus. Pour de plus amples informations, consultez [Répartition de charge entre zones](#) dans le Guide de l'utilisateur Elastic Load Balancing.

Vérifier l'état de santé de vos cibles

Vous pouvez vérifier l'état de santé des cibles enregistrées auprès de vos groupes cible.

Pour vérifier l'état de santé de vos cibles à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Répartition de charge, choisissez Groupes cibles.
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Targets, la colonne Status indique l'état de chaque cible.
5. Si le statut d'une cible est une valeur autre que `Healthy`, la colonne Détails de l'état contient des informations supplémentaires.

Pour vérifier l'état de santé de vos cibles à l'aide du AWS CLI

Utilisez la [describe-target-health](#) commande. La sortie de cette commande contient l'état de santé de la cible. Elle inclut un code de motif si le statut a une valeur différente de `Healthy`.

Pour recevoir des notifications par e-mail concernant des cibles non saines

Utilisez des CloudWatch alarmes pour déclencher une fonction Lambda afin d'envoyer des informations sur les cibles défectueuses. Pour step-by-step obtenir des instructions, consultez le billet de blog suivant : [Identifier les cibles défectueuses de votre équilibreur de charge](#).

Paramètres de surveillance de l'état

Vous pouvez modifier certains paramètres de vérification de l'état de votre groupe cible.

Pour modifier les paramètres de vérification de l'état pour un groupe cible à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Répartition de charge, choisissez Groupes cibles.

3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Détails du groupe, dans la section Paramètres de surveillance de l'état, choisissez Modifier.
5. Sur la page Modifier les paramètres de surveillance de l'état, modifiez les paramètres selon vos besoins, puis choisissez Enregistrer les modifications.

Pour modifier les paramètres de contrôle de santé d'un groupe cible à l'aide du AWS CLI

Utilisez la [modify-target-group](#) commande.

Modifier les attributs du groupe cible pour votre Gateway Load Balancer

Après avoir créé un groupe cible pour votre Gateway Load Balancer, vous pouvez modifier ses attributs.

Attributs de groupe cible

- [Basculement cible](#)
- [Délai d'annulation d'enregistrement](#)
- [Permanence du flux](#)

Basculement cible

Avec le basculement cible, vous définissez comment le Gateway Load Balancer gère les flux de trafic existants lorsqu'une cible devient défectueuse ou qu'elle est désenregistrée. Par défaut, le Gateway Load Balancer continue d'envoyer les flux existants vers la même cible, même si la cible est défectueuse ou est désenregistrée. Vous pouvez gérer ces flux en les remaniant (`rebalance`) ou en les laissant à l'état par défaut (`no_rebalance`).

Aucun rééquilibrage :

Le Gateway Load Balancer continue d'envoyer les flux existants vers des cibles défailtantes ou drainées. Si le Gateway Load Balancer ne parvient pas à atteindre la cible, le trafic est supprimé.

Cependant, les nouveaux flux sont envoyés vers des cibles saines. Il s'agit du comportement de par défaut.

Rééquilibrage :

Le Gateway Load Balancer réorganise les flux existants et les envoie vers des cibles saines après l'expiration du délai de désenregistrement.

Pour les cibles désenregistrées, le délai minimum de basculement dépend du délai de désenregistrement. La cible n'est pas marquée comme désenregistrée tant que le délai de désinscription n'est pas terminé.

Pour les cibles défectueuses, le délai minimum de basculement dépend de la configuration du contrôle de santé du groupe cible (intervalle multiplié par le seuil). Il s'agit de la durée minimale avant laquelle une cible est signalée comme non saine. Passé ce délai, le Gateway Load Balancer peut prendre plusieurs minutes en raison du temps de propagation supplémentaire et du retard de TCP retransmission avant de rediriger les nouveaux flux vers des cibles saines.

Pour mettre à jour l'attribut de basculement cible à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Load Balancing (Répartition de charge), choisissez Target Groups (Groupes cibles).
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Sur la page Détails du groupe, dans la section Attributs, choisissez Modifier.
5. Sur la page Modifier les attributs, modifiez la valeur de Basculement cible selon vos besoins.
6. Sélectionnez Enregistrer les modifications.

Pour mettre à jour l'attribut de basculement cible à l'aide du AWS CLI

Utilisez la [modify-target-group-attributes](#) commande, avec les paires clé-valeur suivantes :

- Clé = `target_failover.on_deregistration` et Valeur = `no_rebalance` (par défaut) ou `rebalance`
- Clé = `target_failover.on_unhealthy` et Valeur = `no_rebalance` (par défaut) ou `rebalance`

Note

Les deux attributs (`target_failover.on_deregistration` et `target_failover.on_unhealthy`) doivent avoir la même valeur.

Délai d'annulation d'enregistrement

Lorsque vous annulez l'enregistrement d'une cible, le Gateway Load Balancer gère les flux vers cette cible comme suit :

Nouveaux flux

Le Gateway Load Balancer arrête d'envoyer de nouveaux flux.

Flux existants

Le Gateway Load Balancer gère les flux existants en fonction du protocole :

- TCP: les flux existants sont fermés s'ils sont inactifs pendant plus de 350 secondes.
- Autres protocoles : les flux existants sont fermés s'ils sont inactifs pendant plus de 120 secondes.

Pour aider à drainer les flux existants, vous pouvez activer le rééquilibrage des flux pour votre groupe cible. Pour de plus amples informations, veuillez consulter [the section called "Basculement cible"](#).

Une cible désenregistrée indique `draining` jusqu'à ce que le délai imparti soit expiré. Une fois le délai de désenregistrement expiré, la cible passe à un état `unused`.

Pour mettre à jour l'attribut de délai de désenregistrement à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Load Balancing (Répartition de charge), choisissez Target Groups (Groupes cibles).
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Sur la page Détails du groupe, dans la section Attributs, choisissez Modifier.
5. Dans la page Edit attributes, remplacez la valeur de Deregistration delay en fonction des besoins.

6. Sélectionnez Enregistrer les modifications.

Pour mettre à jour l'attribut de délai de désenregistrement à l'aide du AWS CLI

Utilisez la [modify-target-group-attributes](#) commande.

Permanence du flux

Par défaut, le Gateway Load Balancer maintient l'adhérence des flux à un dispositif cible spécifique à l'aide de 5 tuples (pour TCP/UDP flows). Les 5 tuples incluent l'adresse IP source, le port source, l'adresse IP de destination, le port de destination et le protocole de transport. Vous pouvez utiliser l'attribut de type de permanence pour modifier la valeur par défaut (5-tuple) et choisir entre 3-tuple (IP source, IP de destination et protocole de transport) ou 2-tuple (IP source et IP de destination).

Considérations relatives à la permanence du flux

- La permanence du flux est configurée et appliquée au niveau du groupe cible et elle s'applique à tout le trafic destiné au groupe cible.
- La permanence du flux à 2-tuple et 3-tuple n'est pas prise en charge lorsque le mode appareil AWS Transit Gateway est activé. Pour utiliser le mode appliance sur votre AWS Transit Gateway, utilisez le mode Flow Stickiness à 5 tuples sur votre Gateway Load Balancer
- La permanence du flux peut entraîner une distribution inégale des connexions et des flux, ce qui peut avoir un impact sur la disponibilité de la cible. Il est recommandé de mettre fin à tous les flux existants ou de les vider avant de modifier le type de permanence du groupe cible.

Pour mettre à jour l'attribut flow stickiness à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Load Balancing (Répartition de charge), choisissez Target Groups (Groupes cibles).
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Sur la page Détails du groupe, dans la section Attributs, choisissez Modifier.
5. Sur la page Modifier les attributs, modifiez la valeur de Permanence cible selon vos besoins.
6. Sélectionnez Enregistrer les modifications.

Pour mettre à jour l'attribut flow stickiness à l'aide du AWS CLI

Utilisez la [modify-target-group-attributes](#) commande avec les attributs `stickiness.enabled` et le groupe `stickiness.type` cible.

Enregistrez des cibles pour votre Gateway Load Balancer

Lorsque votre cible est prête à traiter les demandes, vous l'inscrivez auprès d'un ou plusieurs groupes cibles. Vous pouvez enregistrer des cibles par ID d'instance ou par adresse IP. Le Gateway Load Balancer commence à acheminer les demandes vers la cible dès que le processus d'enregistrement est terminé et que la cible a passé avec succès les vérifications de l'état initiales. Quelques minutes peuvent être nécessaires pour que le processus d'inscription soit effectué et que les surveillances de l'état commencent. Pour de plus amples informations, veuillez consulter [Contrôles de santé pour les groupes cibles de Gateway Load Balancer](#).

Si la demande augmente sur les cibles actuellement enregistrées, vous pouvez enregistrer des cibles supplémentaires afin de pouvoir gérer la demande. Si la demande sur vos cibles enregistrées diminue, vous pouvez désinscrire des cibles de votre groupe cible. Quelques minutes peuvent être nécessaires pour que le processus de désinscription soit effectué et que le réacheminement des demandes vers la cible par le Gateway Load Balancer s'arrête. Si la demande augmente par la suite, vous pouvez réinscrire les cibles que vous avez désinscrites auprès du groupe cible. Si vous devez procéder à la maintenance d'une cible, vous pouvez la désinscrire puis l'inscrire à nouveau lorsque la maintenance est terminée.

Table des matières

- [Considérations](#)
- [Groupes de sécurité cibles](#)
- [Réseau ACLs](#)
- [Enregistrer les cibles par ID d'instance](#)
- [Enregistrer les cibles par adresse IP](#)
- [Désenregistrer les cibles](#)

Considérations

- Chaque groupe cible doit avoir au moins une cible enregistrée dans chaque zone de disponibilité qui est activée pour le Gateway Load Balancer.
- Le type de cible de votre groupe cible détermine la façon dont vous enregistrez les cibles auprès du groupe cible. Pour de plus amples informations, veuillez consulter [Type de cible](#).

- Vous ne pouvez pas enregistrer de cibles sur un VPC peering interrégional.
- Vous ne pouvez pas enregistrer des instances par ID d'instance dans le cadre d'un VPC peering intra-régional, mais vous pouvez les enregistrer par adresse IP.

Groupes de sécurité cibles

Lorsque vous enregistrez des EC2 instances en tant que cibles, vous devez vous assurer que les groupes de sécurité associés à ces instances autorisent le trafic entrant et sortant sur le port 6081.

Les Gateway Load Balancers ne sont pas associés à des groupes de sécurité. Par conséquent, les groupes de sécurité pour vos cibles doivent utiliser des adresses IP pour autoriser le trafic depuis l'équilibreur de charge.

Réseau ACLs

Lorsque vous enregistrez des EC2 instances en tant que cibles, vous devez vous assurer que les listes de contrôle d'accès réseau (ACL) pour les sous-réseaux de vos instances autorisent le trafic sur le port 6081. Le réseau par défaut ACL pour a VPC autorise tout le trafic entrant et sortant. Si vous créez un réseau personnalisé ACLs, vérifiez qu'il autorise le trafic approprié.

Enregistrer les cibles par ID d'instance

Une instance doit être à l'état `running` lorsque vous l'inscrivez.

Pour enregistrer les cibles par ID d'instance à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Load Balancing (Répartition de charge), choisissez Target Groups (Groupes cibles).
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Cibles, choisissez Enregistrer les cibles.
5. Sélectionnez les instances, puis choisissez Inclure comme instance en attente ci-dessous.
6. Lorsque vous avez terminé d'ajouter des instances, choisissez Enregistrer les cibles en attente.

Pour enregistrer les cibles par ID d'instance à l'aide du AWS CLI

Utilisez la commande [register-targets](#) avec les IDs instances.

Enregistrer les cibles par adresse IP

L'adresse IP que vous enregistrez doit provenir de l'un des CIDR blocs suivants :

- Les sous-réseaux du VPC pour le groupe cible
- 10,0.0.0/8 (1918) RFC
- 100,64,0,0/10 (6598) RFC
- 172,16,0,0/12 (1918) RFC
- 192,168.0.0/16 (1918) RFC

Pour enregistrer les cibles par adresse IP à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Load Balancing (Répartition de charge), choisissez Target Groups (Groupes cibles).
3. Sélectionnez le nom du groupe cible pour ouvrir sa page de détails.
4. Dans l'onglet Cibles, choisissez Enregistrer les cibles.
5. Choisissez le réseau, les adresses IP et les ports, puis choisissez Inclure comme en attente ci-dessous.
6. Lorsque vous avez terminé de spécifier les adresses, choisissez Enregistrer les cibles en attente.

Pour enregistrer des cibles par adresse IP à l'aide du AWS CLI

Utilisez la commande [register-targets](#) avec les adresses IP des cibles.

Désenregistrer les cibles

Lorsque vous annulez l'enregistrement d'une cible, Elastic Load Balancing attend que les demandes en cours soient terminées. Cela s'appelle le drainage de la connexion. L'état d'une cible est `draining` lorsque le drainage de la connexion est en cours. Une fois l'enregistrement annulé, l'état de la cible passe à `unused`. Pour de plus amples informations, veuillez consulter [Délai d'annulation d'enregistrement](#).

Pour désenregistrer des cibles à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le panneau de navigation, sous Load Balancing (Répartition de charge), choisissez Target Groups (Groupes cibles).
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Choisissez l'onglet Cibles.
5. Sélectionnez les cibles, puis choisissez Désenregistrer.

Pour désenregistrer des cibles à l'aide du AWS CLI

Utilisez la commande [deregister-targets pour supprimer des cibles](#).

Identifiez un groupe cible pour votre Gateway Load Balancer

Les balises vous aident à classer vos groupes cibles de différentes manières, par exemple, par objectif, par propriétaire ou par environnement.

Vous pouvez ajouter plusieurs balises à chaque groupe cible. Les clés de balise doivent être uniques pour chaque groupe cible. Si vous ajoutez une balise avec une clé qui est déjà associée au groupe cible, cela met à jour la valeur de cette balise.

Lorsque vous avez terminé avec une balise, vous pouvez la supprimer.

Restrictions

- Nombre maximal de balises par ressource : 50
- Longueur de clé maximale : 127 caractères Unicode
- Longueur de valeur maximale – 255 caractères Unicode
- Les clés et valeurs de balise sont sensibles à la casse. Les caractères autorisés sont les lettres, les espaces et les chiffres représentables en UTF -8, ainsi que les caractères spéciaux suivants : + - =. _ : / @. N'utilisez pas d'espaces de début ou de fin.
- N'utilisez pas le aws : préfixe dans les noms ou les valeurs de vos balises, car il est réservé à AWS l'usage. Vous ne pouvez pas modifier ou supprimer des noms ou valeurs de balise ayant ce préfixe. Les balises avec ce préfixe ne sont pas comptabilisées comme vos balises pour la limite de ressources.

Pour mettre à jour les balises d'un groupe cible à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.

2. Dans le panneau de navigation, sous Load Balancing (Répartition de charge), choisissez Target Groups (Groupes cibles).
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Balises, choisissez Gérer les balises, puis effectuez une ou plusieurs des actions suivantes :
 - a. Pour mettre à jour une balise, saisissez de nouvelles valeurs pour Clé et Valeur.
 - b. Pour ajouter une balise, sélectionnez Ajouter une balise et saisissez des valeurs pour Clé et Valeur.
 - c. Pour supprimer une balise, choisissez Retirer en regard de la balise.
5. Lorsque vous avez terminé de mettre à jour les balises, choisissez Enregistrer les modifications.

Pour mettre à jour les balises d'un groupe cible à l'aide du AWS CLI

Utilisez la commande [add-tags](#) et [remove-tags](#).

Supprimer un groupe cible pour votre Gateway Load Balancer

Vous pouvez supprimer un groupe cible s'il n'est pas référencé par les actions de transfert des règles d'écoute. La suppression d'un groupe cible n'affecte pas les cibles enregistrées auprès de ce groupe cible. Si vous n'avez plus besoin d'une EC2 instance enregistrée, vous pouvez l'arrêter ou y mettre fin.

Pour supprimer un groupe cible à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Répartition de charge, choisissez Groupes cibles.
3. Sélectionnez le groupe cible et choisissez Actions, Supprimer.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Oui, supprimer.

Pour supprimer un groupe cible à l'aide du AWS CLI

Utilisez la [delete-target-group](#) commande.

Surveiller vos Gateway Load Balancers

Vous pouvez utiliser les fonctions suivantes pour surveiller vos Gateway Load Balancers, analyser les modèles de trafic et résoudre les problèmes. Toutefois, le Gateway Load Balancer ne génère pas de journaux d'accès car il s'agit d'un équilibreur de charge transparent de couche 3 qui ne met pas fin aux flux. Pour recevoir les journaux d'accès, vous devez activer la journalisation des accès sur les dispositifs cibles de Gateway Load Balancer tels que les pare-feux IPS, IDS/et les dispositifs de sécurité. En outre, vous pouvez également choisir d'activer les journaux de VPC flux sur les Gateway Load Balancers.

CloudWatch métriques

Vous pouvez utiliser Amazon CloudWatch pour récupérer des statistiques sur les points de données de vos Gateway Load Balancers et de vos cibles sous la forme d'un ensemble ordonné de séries chronologiques, appelées métriques. Vous pouvez utiliser ces métriques pour vérifier que le système fonctionne comme prévu. Pour de plus amples informations, veuillez consulter [CloudWatch métriques pour votre Gateway Load Balancer](#).

Journaux de flux VPC

Vous pouvez utiliser VPC Flow Logs pour recueillir des informations détaillées sur le trafic entrant et sortant de votre Gateway Load Balancer. Pour plus d'informations, consultez les [journaux de VPC flux](#) dans le guide de VPC l'utilisateur Amazon.

Créez un journal de flux pour chaque interface réseau pour votre Gateway Load Balancer. Il existe une interface réseau par sous-réseau. Pour identifier les interfaces réseau pour un Gateway Load Balancer, recherchez le nom du Gateway Load Balancer dans le champ de description de l'interface réseau.

Il existe deux entrées pour chaque connexion via votre Gateway Load Balancer : une pour la connexion frontend entre le client et Gateway Load Balancer et l'autre pour la connexion backend entre le Gateway Load Balancer et la cible. Si la cible est enregistrée par ID d'instance, la connexion semble être une connexion à partir du client pour l'instance. Si le groupe de sécurité de l'instance n'autorise pas les connexions depuis le client mais que le réseau ACLs du sous-réseau les autorise, les journaux de l'interface réseau du Gateway Load Balancer indiquent ACCEPT « OK » pour les connexions frontales et dorsales, tandis que les journaux de l'interface réseau de l'instance indiquent REJECT « OK » pour la connexion.

CloudTrail journaux

Vous pouvez l'utiliser AWS CloudTrail pour capturer des informations détaillées sur les appels passés à Elastic Load Balancing API et les stocker sous forme de fichiers journaux dans Amazon S3. Vous pouvez utiliser ces CloudTrail journaux pour déterminer quels appels ont été passés, l'adresse IP source d'où provient l'appel, qui a effectué l'appel, quand l'appel a été passé, etc. Pour de plus amples informations, veuillez consulter [Enregistrement API des appels pour votre Gateway Load Balancer à l'aide de AWS CloudTrail](#).

CloudWatch métriques pour votre Gateway Load Balancer

Elastic Load Balancing publie des points de données sur Amazon CloudWatch pour vos Gateway Load Balancers et vos cibles. 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. Par exemple, vous pouvez surveiller le nombre total de cibles saines pour un Gateway Load Balancer sur une période spécifiée. 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.

Elastic Load Balancing communique des métriques CloudWatch uniquement lorsque les demandes transitent par le Gateway Load Balancer. Si des demandes passent par l'équilibreur de charge, Elastic Load Balancing mesure et envoie ses métriques au cours d'intervalles de 60 secondes. Si aucune demande ne passe ou s'il n'existe pas de données pour une métrique, cette dernière n'est pas présentée.

Pour plus d'informations, consultez le [guide de CloudWatch l'utilisateur Amazon](#).

Table des matières

- [Métriques de Gateway Load Balancer](#)
- [Dimensions de métriques pour les Gateway Load Balancers](#)
- [Afficher CloudWatch les statistiques de votre Gateway Load Balancer](#)

Métriques de Gateway Load Balancer

L'espace de noms AWS/GatewayELB inclut les métriques suivantes.

Métrique	Description
ActiveFlowCount	<p>Nombre total de flux (ou connexions) simultanés provenant des clients vers des cibles.</p> <p>Critères de notification : il existe une valeur différente de zéro</p> <p>Statistics : les statistiques les plus utiles sont Average, Maximum et Minimum.</p> <p>Dimensions</p> <ul style="list-style-type: none"> LoadBalancer AvailabilityZone , LoadBalancer
ConsumedLCUs	<p>Le nombre d'unités de capacité de l'équilibreur de charge (LCU) utilisées par votre équilibreur de charge. Vous payez le montant LCUs que vous utilisez par heure. Pour plus d'informations, consultez Tarification Elastic Load Balancing.</p> <p>Critères de notification : toujours signalé</p> <p>Statistics : All</p> <p>Dimensions</p> <ul style="list-style-type: none"> LoadBalancer
HealthyHostCount	<p>Nombre de cibles considérées saines.</p> <p>Critères de notification : Signalé si les vérifications de l'état sont activées</p> <p>Statistiques : les statistiques les plus utiles sont Maximum et Minimum.</p>

Métrique	Description
	<p>Dimensions</p> <ul style="list-style-type: none"> • <code>LoadBalancer</code> , <code>TargetGroup</code> • <code>AvailabilityZone</code> , <code>LoadBalancer</code> , <code>TargetGroup</code>
NewFlowCount	<p>Nombre total de nouveaux flux (ou connexions) établis entre les clients et les cibles pendant la période.</p> <p>Critères de notification : il existe une valeur différente de zéro</p> <p>Statistics : la statistique la plus utile est Sum.</p> <p>Dimensions</p> <ul style="list-style-type: none"> • <code>LoadBalancer</code> • <code>AvailabilityZone</code> , <code>LoadBalancer</code>
ProcessedBytes	<p>Nombre total d'octets traités par l'équilibreur de charge. Ce nombre inclut le trafic vers et depuis les cibles, mais pas le trafic lié à la vérification de l'état.</p> <p>Critères de notification : il existe une valeur différente de zéro</p> <p>Statistics : la statistique la plus utile est Sum.</p> <p>Dimensions</p> <ul style="list-style-type: none"> • <code>LoadBalancer</code> • <code>AvailabilityZone</code> , <code>LoadBalancer</code>

Métrique	Description
RejectedFlowCount	<p>Nombre total de flux (ou de connexions) rejetés par l'équilibreur de charge.</p> <p>Critères de notification : toujours signalé.</p> <p>Statistics : les statistiques les plus utiles sont Average, Maximum et Minimum.</p> <p>Dimensions</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer
RejectedFlowCount_TCP	<p>Le nombre de TCP flux (ou de connexions) rejetés par l'équilibreur de charge.</p> <p>Critères de notification : il existe une valeur différente de zéro.</p> <p>Statistics : la statistique la plus utile est Sum.</p> <p>Dimensions</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer
UnHealthyHostCount	<p>Nombre de cibles considérées non saines.</p> <p>Critères de notification : Signalé si les vérifications de l'état sont activées</p> <p>Statistiques : les statistiques les plus utiles sont Maximum et Minimum.</p> <p>Dimensions</p> <ul style="list-style-type: none"> • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup

Dimensions de métriques pour les Gateway Load Balancers

Pour filtrer les métriques pour votre Gateway Load Balancer, utilisez les dimensions ci-dessous.

Dimension	Description
AvailabilityZone	Filtrer les données métriques par Zone de disponibilité.
LoadBalancer	Filtre les données métriques en fonction du Gateway Load Balancer. Spécifiez le Gateway Load Balancer comme suit : gateway/ load-balancer-name/1234567890123456 (la dernière partie du). ARN
TargetGroup	Filtre les données métriques en fonction du groupe cible. Spécifiez le groupe cible comme suit : targetgroup/ target-group-name/1234567890123456 (dernière partie du groupe cible). ARN

Afficher CloudWatch les statistiques de votre Gateway Load Balancer

Vous pouvez consulter les CloudWatch métriques de vos équilibreurs de charge Gateway à l'aide de la EC2 console Amazon. Ces métriques s'affichent sous forme de graphiques de surveillance. Les graphiques de surveillance affichent des points de données si le Gateway Load Balancer est actif et reçoit des demandes.

Vous pouvez également consulter les métriques de votre Gateway Load Balancer à l'aide de la CloudWatch console.

Pour afficher des métriques à l'aide de la console

1. Ouvrez la EC2 console Amazon à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Pour afficher les métriques filtrées par groupe cible, procédez comme suit :
 - a. Dans le volet de navigation, sélectionnez Groupes cibles.
 - b. Sélectionnez votre groupe cible et choisissez Surveillance.
 - c. (Facultatif) Pour filtrer les résultats par période, sélectionnez un intervalle de temps dans Affichage des données pour.
 - d. Pour obtenir une vue plus grande d'une métrique individuelle, sélectionnez son graphique.

3. Pour afficher les métriques filtrées par Gateway Load Balancer, procédez comme suit :
 - a. Dans le volet de navigation, choisissez Load Balancers.
 - b. Sélectionnez votre Gateway Load Balancer, puis choisissez Surveillance.
 - c. (Facultatif) Pour filtrer les résultats par période, sélectionnez un intervalle de temps dans Affichage des données pour.
 - d. Pour obtenir une vue plus grande d'une métrique individuelle, sélectionnez son graphique.

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 ELB noms Gateway.
4. (Facultatif) Pour afficher une métrique pour toutes les dimensions, entrez son nom dans le champ de recherche.

Pour consulter les statistiques à l'aide du AWS CLI

Utilisez la commande [list-metrics](#) suivante pour répertorier les métriques disponibles :

```
aws cloudwatch list-metrics --namespace AWS/GatewayELB
```

Pour obtenir les statistiques d'une métrique à l'aide du AWS CLI

Utilisez la [get-metric-statistics](#) commande suivante pour obtenir des statistiques pour la métrique et la dimension spécifiées. Notez que CloudWatch chaque combinaison unique de dimensions est traitée comme une métrique distincte. Vous ne pouvez pas récupérer les statistiques à l'aide de combinaisons de dimensions qui n'ont pas été spécialement publiées. Vous devez spécifier les mêmes dimensions que celles utilisées lorsque les mesures ont été créées.

```
aws cloudwatch get-metric-statistics --namespace AWS/GatewayELB \  
--metric-name UnHealthyHostCount --statistics Average --period 3600 \  
--dimensions Name=LoadBalancer,Value=net/my-load-balancer/50dc6c495c0c9188 \  
Name=TargetGroup,Value=targetgroup/my-targets/73e2d6bc24d8a067 \  
--start-time 2017-04-18T00:00:00Z --end-time 2017-04-21T00:00:00Z
```

Voici un exemple de sortie.

```
{
  "Datapoints": [
    {
      "Timestamp": "2020-12-18T22:00:00Z",
      "Average": 0.0,
      "Unit": "Count"
    },
    {
      "Timestamp": "2020-12-18T04:00:00Z",
      "Average": 0.0,
      "Unit": "Count"
    },
    ...
  ],
  "Label": "UnHealthyHostCount"
}
```

Enregistrement API des appels pour votre Gateway Load Balancer à l'aide de AWS CloudTrail

Elastic Load Balancing est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Elastic Load Balancing. CloudTrail capture tous les API appels à Elastic Load Balancing sous forme d'événements. Les appels capturés incluent des appels provenant des appels de code AWS Management Console et destinés aux API opérations Elastic Load Balancing. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris des événements pour Elastic Load Balancing. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à Elastic Load Balancing, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite, ainsi que des informations supplémentaires.

Pour en savoir plus CloudTrail, consultez le [guide de AWS CloudTrail l'utilisateur](#).

Informations sur Elastic Load Balancing dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans Elastic Load Balancing, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter,

rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section [Affichage des événements avec l'historique des CloudTrail événements](#).

Pour un enregistrement continu des événements de votre AWS compte, y compris ceux relatifs à Elastic Load Balancing, créez un historique. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à toutes les AWS régions. Le journal de suivi consigne les événements de toutes les régions dans la partition AWS, et il livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- [Présentation de la création d'un journal de suivi](#)
- [CloudTrail services et intégrations pris en charge](#)
- [Configuration des SNS notifications Amazon pour CloudTrail](#)
- [Réception de fichiers CloudTrail journaux de plusieurs régions](#) et [réception de fichiers CloudTrail journaux de plusieurs comptes](#)

Toutes les actions Elastic Load Balancing pour les Gateway Load Balancers sont enregistrées CloudTrail et documentées dans la [version 2015-12-01 d'Elastic Load Balancing API Reference](#). Par exemple, les appels aux `DeleteLoadBalancer` actions `CreateLoadBalancer` et génèrent des entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer les éléments suivants :

- Si la demande a été effectuée avec les informations d'identification utilisateur racine ou .
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'[CloudTrail userIdentity élément](#).

Présentation des entrées du fichier journal Elastic Load Balancing

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux

contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des API appels publics, ils n'apparaissent donc pas dans un ordre spécifique.

Les fichiers journaux incluent les événements relatifs à tous les AWS API appels relatifs à votre AWS compte, et pas uniquement API aux appels Elastic Load Balancing. Vous pouvez localiser les appels à Elastic Load Balancing API en recherchant les eventSource éléments contenant la valeur `elasticloadbalancing.amazonaws.com`. Pour afficher l'enregistrement d'une action spécifique, par exemple `CreateLoadBalancer`, recherchez des éléments eventName avec le nom de l'action.

Voici des exemples d'enregistrements de CloudTrail journal pour Elastic Load Balancing destinés à un utilisateur qui a créé un Gateway Load Balancer puis l'a supprimé à l'aide du AWS CLI. Vous pouvez identifier l'utilisation des userAgent éléments. Vous pouvez identifier les API appels demandés à l'aide des eventName éléments. Il est possible de trouver des informations sur l'utilisateur (Alice) dans l'élément userIdentity.

Exemple Exemple : CreateLoadBalancer

```
{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2020-12-11T15:31:48Z",
  "eventSource": "elasticloadbalancing.amazonaws.com",
  "eventName": "CreateLoadBalancer",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "198.51.100.1",
  "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 boto3/1.4.1",
  "requestParameters": {
    "subnets": ["subnet-8360a9e7", "subnet-b7d581c0"],
    "name": "my-load-balancer",
    "type": "gateway"
  }
}
```

```

    },
    "responseElements": {
      "loadBalancers": [{
        "type": "gateway",
        "loadBalancerName": "my-load-balancer",
        "vpcId": "vpc-3ac0fb5f",
        "state": {"code": "provisioning"},
        "availabilityZones": [
          {"subnetId": "subnet-8360a9e7", "zoneName": "us-west-2a"},
          {"subnetId": "subnet-b7d581c0", "zoneName": "us-west-2b"}
        ],
        "createdTime": "Dec 11, 2020 5:23:50 PM",
        "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/gateway/my-load-balancer/ffcddace1759e1d0",
      }]
    },
    "requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
    "eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
  }
}

```

Example Exemple : DeleteLoadBalancer

```

{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2020-12-12T15:31:48Z",
  "eventSource": "elasticloadbalancing.amazonaws.com",
  "eventName": "DeleteLoadBalancer",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "198.51.100.1",
  "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 boto3/1.4.1",
  "requestParameters": {

```

```
    "loadBalancerArn": "arn:aws:elasticloadbalancing:us-  
west-2:123456789012:loadbalancer/gateway/my-load-balancer/ffcddace1759e1d0"  
  },  
  "responseElements": null,  
  "requestID": "349598b3-000e-11e6-a82b-298133eEXAMPLE",  
  "eventID": "75e81c95-4012-421f-a0cf-babdaEXAMPLE",  
  "eventType": "AwsApiCall",  
  "apiVersion": "2015-12-01",  
  "recipientAccountId": "123456789012"  
}
```

Quotas de vos Gateway Load Balancers

Votre AWS compte dispose de quotas par défaut, anciennement appelés limites, pour chaque AWS service. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés.

Pour demander une augmentation de quota, utilisez le [formulaire de demande d'augmentation de limite](#).

Équilibreur de charge

Votre AWS compte possède les quotas suivants relatifs aux Gateway Load Balancers.

Nom	Par défaut	Ajustable
Gateway Load Balancers par région	100	Oui
Équilibreurs de charge Gateway pour VPC	100	Oui
Gateway Load Balancer ENIs pour VPC	300 *	Oui
Écouteurs par Gateway Load Balancer	1	Non

* Chaque Gateway Load Balancer utilise une interface réseau par zone.

Groupes cibles

Les quotas suivants sont destinés aux groupes cibles.

Nom	Par défaut	Ajustable
GENEVEgroupes cibles par région	100	Oui
Cibles par groupe cible	1 000	Oui
Cibles par zone de disponibilité et par groupe GENEVE cible	300	Non

Nom	Par défaut	Ajustable
Cibles par Gateway Load Balancer par zone de disponibilité	300	Non
Cibles par Gateway Load Balancer	300	Non

Bande passante

Par défaut, chaque VPC point de terminaison peut prendre en charge une bande passante allant jusqu'à 10 Gbit/s par zone de disponibilité et évolue automatiquement jusqu'à 100 Gbit/s. Si votre application a besoin d'un débit plus élevé, contactez le AWS support.

Histoire du document pour les Gateway Load Balancers

Le tableau suivant décrit les versions des Gateway Load Balancers.

Modification	Description	Date
IPv6soutien	Vous pouvez configurer votre Gateway Load Balancer pour qu'il prenne en charge à la fois les adresses IPv4 et IPv6 les adresses.	12 décembre 2022
Rééquilibrage du débit	Cette version ajoute la prise en charge de la définition du comportement de gestion des flux pour les équilibreur de charge de passerelle lorsque les cibles échouent ou se désenregistrent.	13 octobre 2022
Permanence du flux configurable	Vous pouvez configurer le hachage qui préserve la permanence des flux sur un dispositif cible spécifique.	25 août 2022
Disponible dans de nouvelles régions	Cette version ajoute la prise en charge des équilibreurs de charge Gateway dans les AWS GovCloud (US) régions.	17 juin 2021
Disponible dans de nouvelles régions	Cette version ajoute la prise en charge des équilibreurs de charge Gateway dans les régions du Canada (centre), de l'Asie-Pacifique (Séoul) et de l'Asie-Pacifique (Osaka).	31 mars 2021

[Disponible dans de nouvelles régions](#)

Cette version ajoute la prise en charge des équilibreur de charge Gateway dans l'ouest des États-Unis (Californie du Nord), en Europe (Londres), en Europe (Paris), en Europe (Milan), en Afrique (Le Cap), au Moyen-Orient (Bahreïn), en Asie-Pacifique (Hong Kong), en Asie-Pacifique (Singapour) et dans la région Asie-Pacifique (Mumbai).

19 mars 2021

[Première version](#)

Cette version d'Elastic Load Balancing présente les Gateway Load Balancers.

10 novembre 2020

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.