



Network Load Balancers

Elastic Load Balancing



Elastic Load Balancing: Network 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 Network Load Balancer ?	1
Composants du Network Load Balancer	1
Présentation du Network Load Balancer	2
Avantages de la migration depuis un Classic Load Balancer	3
Comment démarrer	4
Tarification	4
Premiers pas	5
Avant de commencer	5
Étape 1 : configurer votre groupe cible	5
Étape 2 : Choisir un type d'équilibreur de charge	6
Étape 3 : configurer votre équilibreur de charge et votre écouteur	7
Étape 4 : tester votre équilibreur de charge	8
Étape 5 : (facultatif) supprimer votre équilibreur de charge	8
Prise en main à l'aide de l'AWS CLI	10
Avant de commencer	10
Création de votre équilibreur de charge IPv4	10
Création de votre équilibreur de charge à double pile	12
Spécifier une adresse IP Elastic pour votre équilibreur de charge	14
Supprimer votre équilibreur de charge	14
Équilibreurs de charge	15
États d'un équilibreur de charge	16
Attributs de l'équilibreur de charge	16
Type d'adresse IP	17
Carte des ressources de l'équilibreur de charge	18
Composants de la carte des ressources	18
Zones de disponibilité	20
Équilibrage de charge entre zones	21
Suppression de la protection (Protection contre la suppression)	22
Délai d'inactivité des connexions	23
Nom du DNS	23
Affinité DNS de zone de disponibilité	25
Surveillance	27
Activation de l'affinité de zone de disponibilité	27
Désactivation de l'affinité de zone de disponibilité	28

Créer un équilibreur de charge	28
Étape 1 : Configurer un groupe cible	29
Étape 2 : enregistrer les cibles	30
Étape 3 : configurer un équilibreur de charge et un écouteur	31
Étape 4 : tester l'équilibreur de charge	8
Mise à jour du type d'adresse	34
Groupes de sécurité	35
Considérations	36
Exemple : filtrer le trafic client	36
Exemple : accepter le trafic uniquement depuis l'équilibreur de charge	37
Mise à jour des groupes de sécurité associés	38
Mise à jour des paramètres de sécurité	39
Surveillance des groupes de sécurité d'équilibreur de charge	39
Mettre à jour des balises	39
Supprimer un équilibreur de charge	41
Changement de zone	42
Lancement d'un changement de zone	43
Mise à jour d'un changement de zone	44
Annulation d'un changement de zone	45
Écouteurs	46
Configuration des écouteurs	46
Règles d'un écouteur	47
Créer un écouteur	47
Prérequis	47
Ajouter un écouteur	48
Configurer des écouteurs TLS	49
Certificats de serveur	49
Stratégies de sécurité	52
Stratégies ALPN	76
Mette à jour un écouteur	77
Mettre à jour un écouteur TLS	78
Remplacer le certificat par défaut	78
Ajouter des certificats à la liste des certificats	79
Supprimer des certificats de la liste des certificats	79
Mettre à jour la stratégie de sécurité	80
Mettre à jour la stratégie ALPN	81

Supprimer un écouteur	81
Groupes cibles	83
Configuration du routage	84
Type de cible	85
Demande de routage et adresses IP	86
Ressources sur site en tant que cibles	87
Type d'adresse IP	88
Cibles enregistrées	88
Attributs de groupe cible	89
Préservation des adresses IP client	91
Délai d'annulation d'enregistrement	94
Protocole proxy	95
Connexions de vérification de l'état	96
Services de points de terminaison d'un VPC	96
Activer le protocole proxy	97
Sessions permanentes	98
Créer un groupe cible	99
Configurer la surveillance de l'état	101
Paramètres de surveillance de l'état	102
État de santé d'une cible	105
Codes de motif de vérification de l'état	106
Vérifier l'état de santé de vos cibles	107
Modifier les paramètres de vérification de l'état d'un groupe cible	108
Équilibrage de charge entre zones	109
Modification de l'équilibrage de charge entre zones d'un équilibreur de charge	110
Modification de l'équilibrage de charge entre zones pour un groupe cible	110
État du groupe cible	111
Actions d'état défectueux	111
Exigences et considérations	111
Exemple	112
Modification des paramètres d'état du groupe cible	113
Interruption de connexion pour des cibles défectueuses	114
Utiliser le basculement DNS Route 53 pour votre équilibreur de charge	116
Enregistrer des cibles	117
Groupes de sécurité cibles	118
Listes ACL réseau	119

Sous-réseaux partagés	122
Enregistrer ou annuler l'enregistrement de cibles	122
Application Load Balancers en tant que cibles	125
Étape 1 : créer l'Application Load Balancer	126
Étape 2 : créer le groupe cible	127
Étape 3 : créer le Network Load Balancer	129
Étape 4 : (Facultatif) Activer AWS PrivateLink	130
Mettre à jour des balises	131
Supprimer un groupe cible	132
Surveiller vos équilibres de charge	133
CloudWatch métriques	134
Métriques des Network Load Balancers	135
Dimensions de métriques des Network Load Balancers	147
Statistiques des métriques Network Load Balancer	147
Afficher CloudWatch les statistiques de votre équilibreur de charge	148
Journaux d'accès	150
Fichiers journaux d'accès	151
Entrées des journaux d'accès	152
Conditions requises pour le compartiment	155
Activer la journalisation des accès	158
Désactiver la journalisation des accès	158
Traitement des fichiers journaux d'accès	159
CloudTrail journaux	160
Informations sur Elastic Load Balancing dans CloudTrail	160
Présentation des entrées du fichier journal Elastic Load Balancing	161
Résolution des problèmes	164
Une cible enregistrée n'est pas en service	164
Les demandes ne sont pas acheminées vers les cibles	164
Les cibles reçoivent plus de demandes de vérification de l'état que prévu	165
Les cibles reçoivent moins de demandes de vérification de l'état que prévu	165
Des cibles non saines reçoivent des demandes de l'équilibreur de charge.	165
La cible échoue aux vérifications d'intégrité HTTP ou HTTPS en raison d'une incompatibilité d'en-tête d'hôte	166
Impossible d'associer un groupe de sécurité à un équilibreur de charge	166
Impossible de supprimer tous les groupes de sécurité	166
Augmentation de la métrique TCP_ELB_Reset_Count	166

Connexions expirées pour les demandes d'une cible vers son équilibreur de charge	167
Diminution des performances lorsque des cibles sont déplacées vers un Network Load Balancer	167
Erreurs d'allocation de port lors de la connexion AWS PrivateLink	168
Échec de connexion intermittent lorsque la préservation des adresses IP client est activée	168
Retards de connexion TCP	169
Défaillance potentielle lors du provisionnement de l'équilibreur de charge	169
La résolution de noms DNS contient moins d'adresses IP que les zones de disponibilité activées	169
Résoudre les problèmes liés aux cibles défectueuses à l'aide de la carte des ressources	170
Quotas	172
Historique de la documentation	174
.....	clxxx

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

Elastic Load Balancing distribue automatiquement votre trafic entrant sur plusieurs cibles (par exemple, des instances EC2, des conteneurs et des adresses IP) 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 Network Load Balancers. Pour plus d'informations sur les autres équilibreurs de charge, veuillez consulter le [Guide de l'utilisateur des Application Load Balancers](#), le [Guide de l'utilisateur des Gateway Load Balancers](#) et le [Guide de l'utilisateur des Classic Load Balancers](#).

Composants du Network Load Balancer

Un équilibreur de charge constitue le point de contact unique pour les clients. L'équilibreur de charge répartit le trafic entrant sur plusieurs cibles, comme des instances Amazon EC2. La disponibilité de votre application s'en trouve accrue. Vous ajoutez un ou plusieurs écouteurs à l'équilibreur de charge.

Un écouteur vérifie des demandes de connexion des clients, à l'aide du protocole et du port que vous configurez et transmet des requêtes à un groupe cible.

Un groupe cible achemine les demandes vers une ou plusieurs cibles enregistrées, telles que des instances EC2, à l'aide du protocole et du numéro de port que vous spécifiez. Les groupes cibles Network Load Balancer prennent en charge les protocoles TCP, UDP, TCP_UDP et TLS. Vous pouvez enregistrer une cible auprès de plusieurs groupes cible. Vous pouvez configurer les vérifications de l'état pour chaque groupe cible. Les vérifications de l'état sont effectuées sur toutes les cibles enregistrées dans un groupe cible spécifié dans une règle de l'écouteur de votre équilibreur de charge.

Pour plus d'informations, consultez la documentation de suivante :

- [Équilibreur de charge](#)
- [Écouteurs](#)
- [Groupes cibles](#)

Présentation du Network Load Balancer

Un Network Load Balancer fonctionne à la quatrième couche du modèle Open Systems Interconnection (OSI). Il est capable de traiter des millions de requêtes par seconde. Lorsque l'équilibreur de charge reçoit une demande de connexion, il sélectionne une cible depuis le groupe cible pour la règle par défaut. Il tente d'ouvrir une connexion TCP à la cible sélectionnée sur le port spécifié dans la configuration de l'écouteur.

Lorsque vous activez une zone de disponibilité pour l'équilibreur de charge, Elastic Load Balancing crée un nœud d'équilibreur de charge dans la zone de disponibilité. 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 permet, chaque nœud d'équilibreur de charge répartit le trafic entre les cibles enregistrées dans toutes les zones de disponibilité activées. Pour plus d'informations, consultez [Zones de disponibilité](#).

Pour renforcer la tolérance aux pannes de vos applications, vous pouvez activer plusieurs zones de disponibilité pour votre équilibreur de charge et veiller à ce que chaque groupe cible possède au moins une cible dans chaque zone de disponibilité activée. Par exemple, si un ou plusieurs groupes cibles n'ont pas une cible saine dans une zone de disponibilité, nous supprimons l'adresse IP pour le sous-réseau correspondant à partir de DNS, mais les nœuds de l'équilibreur de charge des autres zones de disponibilité sont toujours disponibles pour acheminer le trafic. Si un client n'honore pas le time-to-live (TTL) et envoie des demandes à l'adresse IP après sa suppression du DNS, les demandes échouent.

Pour un trafic TCP, l'équilibreur de charge sélectionne une cible à l'aide d'un algorithme de hachage de flux, selon le protocole, l'adresse IP source, le port source, l'adresse IP de destination, le port de destination et le numéro de séquence TCP. Les connexions TCP d'un client ont des ports source et des numéros de séquence différents, et peuvent être acheminées vers des cibles différentes. Chaque connexion TCP est acheminée vers une seule cible pendant la durée de vie de la connexion.

Pour un trafic UDP, l'équilibreur de charge sélectionne une cible à l'aide d'un algorithme de hachage de flux, selon le protocole, l'adresse IP source, le port source, l'adresse IP de destination et le port de destination dans le paquet. Un flux UDP a les mêmes source et destination, il est donc toujours

acheminé vers une seule cible tout au long de son cycle de vie. Les différents flux UDP ont différents ports et adresses IP source, de telle sorte qu'ils puissent être acheminés vers des cibles différentes.

Elastic Load Balancing crée une interface réseau pour chaque zone de disponibilité que vous activez. Chaque nœud d'équilibreur de charge dans la zone de disponibilité utilise cette interface réseau pour obtenir une adresse IP statique. Lorsque vous créez un équilibreur de charge accessible sur Internet, vous pouvez associer une adresse IP Elastic à chaque sous-réseau.

Lorsque vous créez un groupe cible, vous spécifiez son type de cible, qui détermine la façon dont vous enregistrez les cibles. Par exemple, vous pouvez enregistrer des ID d'instance, des adresses IP ou un Application Load Balancer. Le type de cible détermine également si les adresses IP client sont préservées. Pour plus d'informations, consultez [the section called "Préservation des adresses IP client"](#).

Vous pouvez ajouter et supprimer des cibles de votre équilibreur de charge au fur et à mesure que vos besoins évoluent, sans interrompre le flux de demandes global vers votre application. 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.

Vous pouvez configurer des vérifications de l'état qui sont utilisées pour surveiller l'état de santé des cibles enregistrées afin que l'équilibreur de charge envoie les demandes uniquement aux cibles saines.

Pour de plus amples informations, consultez la section [Fonctionnement d'Elastic Load Balancing](#), dans le Guide de l'utilisateur Elastic Load Balancing.

Avantages de la migration depuis un Classic Load Balancer

L'utilisation d'un Network Load Balancer au lieu d'un Classic Load Balancer présente les avantages suivants :

- Possibilité de traiter des charges de travail volatiles et de passer à des millions de requêtes par seconde.
- Prise en charge des adresses IP statiques pour l'équilibreur de charge. Vous pouvez également attribuer une adresse IP Elastic pour chaque sous-réseau activé pour l'équilibreur de charge.
- Prise en charge de l'enregistrement des cibles par adresse IP, y compris les cibles en dehors du VPC pour l'équilibreur de charge.

- Prise en charge de l'acheminement des demandes vers plusieurs applications sur une seule instance EC2. Vous pouvez enregistrer chaque instance ou adresse IP avec le même groupe cible à l'aide de plusieurs ports.
- Prise en charge des applications conteneurisées. Amazon Elastic Container Service (Amazon ECS) peut sélectionner un port inutilisé lors de la planification d'une tâche et enregistrer la tâche auprès d'un groupe cible en utilisant ce port. Cela vous permet d'utiliser vos clusters plus efficacement.
- Support pour surveiller l'état de santé de chaque service de manière indépendante, car les bilans de santé sont définis au niveau du groupe cible et de nombreux CloudWatch indicateurs Amazon sont signalés au niveau du groupe cible. Attacher un groupe cible à un groupe Auto Scaling vous permet de mettre à l'échelle chaque service dynamiquement en fonction de la demande.

Pour de plus amples informations sur les fonctions prises en charge par chaque type d'équilibreur de charge, consultez [Comparaison des produits](#) pour Elastic Load Balancing.

Comment démarrer

Pour créer un Network Load Balancer, utilisez l'un des didacticiels suivants :

- [Mise en route avec les Network Load Balancers](#)
- [Didacticiel : création d'un Network Load Balancer à l'aide de l'AWS CLI](#)

Des démonstrations de configurations courantes d'équilibreur de charge sont disponibles sur la page [Démonstrations Elastic Load Balancing](#) (langue française non garantie).

Tarifification

Pour plus d'informations, veuillez consulter la [tarification Network Load Balancer](#) (langue française non garantie).

Mise en route avec les Network Load Balancers

Ce didacticiel fournit une introduction pratique aux équilibreurs de charge réseau via une interface Web. AWS Management Console Pour créer votre premier Network Load Balancer, procédez comme suit.

Tâches

- [Avant de commencer](#)
- [Étape 1 : configurer votre groupe cible](#)
- [Étape 2 : Choisir un type d'équilibreur de charge](#)
- [Étape 3 : configurer votre équilibreur de charge et votre écouteur](#)
- [Étape 4 : tester votre équilibreur de charge](#)
- [Étape 5 : \(facultatif\) supprimer votre équilibreur de charge](#)

Des démonstrations de configurations courantes d'équilibreur de charge sont disponibles sur la page [Démonstrations Elastic Load Balancing](#) (langue française non garantie).

Avant de commencer

- Choisissez les zones de disponibilité que vous utiliserez pour vos instances EC2. Configurez votre réseau Virtual Private Cloud (VPC) avec au moins un sous-réseau public dans chacune de ces zones de disponibilité. Ces sous-réseaux publics sont utilisés pour configurer l'équilibreur de charge. Vous pouvez plutôt lancer vos instances EC2 dans d'autres sous-réseaux de ces zones de disponibilité.
- Lancez au moins une instance EC2 dans chaque zone de disponibilité. Assurez-vous que les groupes de sécurité de ces instances autorisent l'accès TCP des clients sur le port d'écoute et les requêtes de vérification de l'état de votre VPC. Pour plus d'informations, consultez [Groupes de sécurité cibles](#).

Étape 1 : configurer votre groupe cible

Créez un groupe cible, qui sert à acheminer les demandes. La règle de votre écouteur achemine les demandes vers les cibles enregistrées dans ce groupe cible. L'équilibreur de charge vérifie l'état de

santé des cibles dans ce groupe cible en utilisant les paramètres de vérification de l'état définis pour ce groupe cible.

Pour configurer votre groupe cible à l'aide de la console

1. Ouvrez la console Amazon EC2 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. Conservez instances comme type de cible.
5. Pour Nom du groupe cible, saisissez un nom pour le nouveau groupe cible.
6. Pour Protocole, choisissez TCP, et pour Port, choisissez 80.
7. Pour VPC, sélectionnez le VPC qui contient vos instances.
8. Pour Vérifications de la santé, conservez les paramètres par défaut.
9. Choisissez Suivant.
10. Sur la page Enregistrer les cibles, procédez comme suit. Il s'agit d'une étape facultative pour créer un groupe cible. Toutefois, vous devez enregistrer vos cibles si vous souhaitez tester votre équilibreur de charge et vous assurer qu'il achemine le trafic vers vos cibles.
 - a. Pour Instances disponibles, sélectionnez une ou plusieurs instances.
 - b. Conservez le port 80 par défaut et choisissez Inclure comme étant en attente ci-dessous.
11. Sélectionnez Créer un groupe cible.

Étape 2 : Choisir un type d'équilibreur de charge

Elastic Load Balancing prend en charge différents types d'équilibreurs de charge. Dans le cadre de ce didacticiel, vous créez un Network Load Balancer.

Pour créer un Network Load Balancer à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans la barre de navigation, choisissez une Région pour votre équilibreur de charge. Veillez à choisir la même région que celle que vous avez utilisée pour vos instances EC2.
3. Dans le volet de navigation, sous Équilibrage de charge, choisissez Équilibreurs de charge.
4. Choisissez Créer un équilibreur de charge.
5. Pour Network Load Balancer, choisissez Créer.

Étape 3 : configurer votre équilibreur de charge et votre écouteur

Pour créer un Network Load Balancer, vous devez d'abord fournir des informations de configuration de base pour votre équilibreur de charge, comme un nom, un schéma et un type d'adresse IP.

Fournissez ensuite des informations sur votre réseau et sur un ou plusieurs écouteurs. Un écouteur est un processus qui vérifie les demandes de connexion. Il est configuré avec un protocole et un port pour les connexions des clients vers l'équilibreur de charge. Pour plus d'informations sur les protocoles et les ports pris en charge, consultez [Configuration des écouteurs](#).

Pour configurer votre équilibreur de charge et votre écouteur

1. Pour Load balancer name (Nom de l'équilibreur de charge), saisissez un nom pour l'équilibreur de charge. Par exemple, my-nlb.
2. Pour Méthode et Type d'adresse IP, conservez les valeurs par défaut.
3. Dans Mappage réseau, sélectionnez le VPC que vous avez utilisé pour vos instances EC2. Pour chacune des zones de disponibilité que vous utilisez pour lancer vos instances EC2, sélectionnez la zone de disponibilité, puis sélectionnez le sous-réseau public de cette zone de disponibilité.

Par défaut, AWS attribue une adresse IPv4 à chaque nœud d'équilibreur de charge à partir du sous-réseau correspondant à sa zone de disponibilité. Sinon, lorsque vous créez un équilibreur de charge accessible sur Internet, vous pouvez sélectionner une adresse IP Elastic pour chaque zone de disponibilité. Ceci fournit des adresses IP statiques à votre équilibreur de charge.

4. Pour Groupes de sécurité, nous présélectionnons le groupe de sécurité par défaut pour votre VPC. Vous pouvez sélectionner d'autres groupes de sécurité si nécessaire. Si vous ne disposez pas d'un groupe de sécurité adapté, choisissez Créer un groupe de sécurité et créez-en un qui répond à vos besoins en matière de sécurité. Pour plus d'informations, veuillez consulter [Création d'un groupe de sécurité](#) dans le Guide de l'utilisateur Amazon VPC.

Warning

Si vous n'associez aucun groupe de sécurité à votre équilibreur de charge pour le moment, vous ne pourrez pas les associer ultérieurement.

5. Pour Écouteurs et routage, conservez le protocole et le port par défaut et sélectionnez le groupe cible dans la liste. Cela permet de configurer un écouteur qui accepte le trafic TCP sur le port 80 et transmet le trafic au groupe cible sélectionné par défaut.

6. (Facultatif) Ajoutez des balises pour catégoriser votre équilibreur de charge. Les clés de balise doivent être uniques pour chaque équilibreur de charge. Les caractères autorisés sont les lettres, les espaces et les chiffres (en UTF-8), ainsi que les caractères spéciaux suivants : + - =. _ : / @. N'utilisez pas d'espaces de début ou de fin. Les valeurs de balises sont sensibles à la casse.
7. Examinez votre configuration, puis choisissez Create load balancer (Créer l'équilibreur de charge). Quelques attributs par défaut sont appliqués à votre équilibreur de charge lors de sa création. Vous pouvez les consulter et les modifier après avoir créé l'équilibreur de charge. Pour plus d'informations, consultez [Attributs de l'équilibreur de charge](#).

Étape 4 : tester votre équilibreur de charge

Une fois que l'équilibreur de charge a été créé, vérifiez qu'il envoie le trafic vers vos instances EC2.

Pour tester l'équilibreur de charge

1. Une fois que vous êtes informé que votre équilibreur de charge a été créé, choisissez Close.
2. Dans le panneau de navigation, sous Répartition de charge, choisissez Groupes cibles.
3. Sélectionnez le groupe cible nouvellement créé.
4. Choisissez Cibles et vérifiez que vos instances sont prêtes. Si l'état d'une instance est `initial`, c'est probablement dû au fait que cette instance est encore en cours d'enregistrement ou qu'elle n'est pas considérée comme saine, car elle n'a pas passé le nombre minimal de vérifications de l'état. Une fois que l'état d'au moins une instance est `healthy`, vous pouvez tester votre équilibreur de charge.
5. Dans le volet de navigation, sous Équilibrage de charge, choisissez Équilibreurs de charge.
6. Sélectionnez le nom de votre nouvel équilibreur de charge afin d'ouvrir sa page de détails.
7. Copiez le nom DNS de l'équilibreur de charge (par exemple, `my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com`). Collez le nom DNS dans le champ d'adresse d'un navigateur Web connecté à Internet. Si tout fonctionne, le navigateur affiche la page par défaut de votre serveur.

Étape 5 : (facultatif) supprimer votre équilibreur de charge

Dès que votre équilibreur de charge est disponible, vous êtes facturé pour chaque heure ou heure partielle pendant laquelle vous le laissez tourner. Lorsque vous n'avez plus besoin d'un équilibreur de charge, vous pouvez le supprimer. Dès que l'équilibreur de charge est supprimé, vous cessez d'être

facturé pour celui-ci. Notez que la suppression d'un équilibreur de charge n'affecte pas les cibles enregistrées auprès de celui-ci. Par exemple, vos instances EC2 continuent à s'exécuter.

Pour supprimer votre équilibreur de charge à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sous Équilibrage de charge, choisissez Équilibreurs de charge.
3. Cochez la case correspondant à l'équilibreur de charge, puis choisissez Actions, Supprimer.
4. Lorsque vous êtes invité à confirmer, saisissez **confirm**, puis choisissez Supprimer.

Didacticiel : création d'un Network Load Balancer à l'aide de l'AWS CLI

Ce didacticiel fournit une présentation pratique des Network Load Balancers via l'AWS CLI.

Avant de commencer

- Installez l'AWS CLI ou passez à la version actuelle de l'AWS CLI si vous utilisez une version qui ne prend pas en charge les Network Load Balancers. Pour plus d'informations, consultez [Installation d'AWS Command Line Interface](#) dans le Guide de l'utilisateur AWS Command Line Interface.
- Choisissez les zones de disponibilité que vous utiliserez pour vos instances EC2. Configurez votre réseau Virtual Private Cloud (VPC) avec au moins un sous-réseau public dans chacune de ces zones de disponibilité.
- Décidez si vous allez créer un équilibreur de charge IPv4 ou à double pile. Utilisez IPv4 si vous voulez que vos clients communiquent avec l'équilibreur de charge à l'aide d'adresses IPv4 uniquement. Choisissez le mode double pile si vous voulez que vos clients communiquent avec l'équilibreur de charge à l'aide d'adresses IPv4 et IPv6. Vous pouvez également utiliser le mode double pile pour communiquer avec des cibles backend, telles que les applications IPv6 ou les sous-réseaux à double pile, en utilisant IPv6.
- Lancez au moins une instance EC2 dans chaque zone de disponibilité. Assurez-vous que les groupes de sécurité de ces instances autorisent l'accès TCP des clients sur le port d'écoute et les requêtes de vérification de l'état de votre VPC. Pour plus d'informations, consultez [Groupes de sécurité cibles](#).

Création de votre équilibreur de charge IPv4

Pour créer votre premier équilibreur de charge, procédez comme il est indiqué ci-après.

Pour créer un équilibreur de charge IPv4

1. Utilisez la [create-load-balancer](#) commande pour créer un équilibreur de charge IPv4, en spécifiant un sous-réseau public pour chaque zone de disponibilité dans laquelle vous avez lancé des instances. Vous pouvez spécifier un seul sous-réseau par zone de disponibilité.

Par défaut, lorsque les Network Load Balancers sont créés à l'aide de l'AWS CLI, ils n'utilisent pas automatiquement le groupe de sécurité par défaut pour le VPC. Si vous n'associez aucun groupe de sécurité à votre équilibreur de charge lors de sa création, vous ne pourrez pas les ajouter ultérieurement. Nous vous recommandons de spécifier des groupes de sécurité pour votre équilibreur de charge lors de sa création à l'aide de l'option `--security-groups`.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets
subnet-0e3f5cac72EXAMPLE --security-groups sg-0123456789EXAMPLE
```

Les données de sortie contiennent l'Amazon Resource Name (ARN) de l'équilibreur de charge, au format suivant :

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

- Utilisez la [create-target-group](#) commande pour créer un groupe cible IPv4, en spécifiant le même VPC que celui que vous avez utilisé pour vos instances EC2. Les groupes cibles IPv4 prennent en charge les cibles de type IP et instance.

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 --vpc-id
vpc-0598c7d356EXAMPLE
```

Les données de sortie contiennent l'ARN du groupe cible, au format suivant :

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-
targets/1234567890123456
```

- 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 --protocol TCP --
port 80 \
```

```
--default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

Les données de sortie contiennent l'ARN de l'auditeur, au format suivant :

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

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

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

Création de votre équilibreur de charge à double pile

Pour créer votre premier équilibreur de charge, procédez comme il est indiqué ci-après.

Pour créer un équilibreur de charge à double pile

1. Utilisez la [create-load-balancer](#) commande pour créer un équilibreur de charge à double pile, en spécifiant un sous-réseau public pour chaque zone de disponibilité dans laquelle vous avez lancé des instances. Vous pouvez spécifier un seul sous-réseau par zone de disponibilité.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network --subnets subnet-0e3f5cac72EXAMPLE --ip-address-type dualstack
```

Les données de sortie contiennent l'Amazon Resource Name (ARN) de l'équilibreur de charge, au format suivant :

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

2. Utilisez la [create-target-group](#) commande pour créer un groupe cible, en spécifiant le même VPC que celui que vous avez utilisé pour vos instances EC2.

Vous devez utiliser un groupe cible TCP ou TLS avec votre équilibreur de charge à double pile.

Vous pouvez créer des groupes cibles IPv4 et IPv6 à associer aux équilibreurs de charge à double pile. Le type d'adresse IP du groupe cible détermine la version IP que l'équilibreur de charge utilisera à la fois pour communiquer avec vos cibles backend et pour surveiller leur état.

Les groupes cibles IPv4 prennent en charge les cibles de type IP et instance. Les cibles IPv6 ne prennent en charge que les cibles IP.

```
aws elbv2 create-target-group --name my-targets --protocol TCP --port 80 --vpc-id vpc-0598c7d356EXAMPLE --ip-address-type [ipv4 or ipv6]
```

Les données de sortie contiennent l'ARN du groupe cible, au format suivant :

```
arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/my-targets/1234567890123456
```

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
```

4. 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. Les équilibreurs de charge à double pile doivent être équipés d'écouteurs TCP ou TLS.

```
aws elbv2 create-listener --load-balancer-arn loadbalancer-arn --protocol TCP --port 80 \ --default-actions Type=forward,TargetGroupArn=targetgroup-arn
```

Les données de sortie contiennent l'ARN de l'auditeur, au format suivant :

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

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

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

Spécifier une adresse IP Elastic pour votre équilibreur de charge

Lorsque vous créez un Network Load Balancer, vous pouvez spécifier une adresse IP Elastic par sous-réseau à l'aide d'un mappage de sous-réseaux.

```
aws elbv2 create-load-balancer --name my-load-balancer --type network \  
--subnet-mappings SubnetId=subnet-0e3f5cac72EXAMPLE,AllocationId=eipalloc-12345678
```

Supprimer votre équilibreur de charge

Lorsque vous n'avez plus besoin de votre équilibreur de charge et de votre groupe cible, vous pouvez les supprimer en procédant comme suit :

```
aws elbv2 delete-load-balancer --load-balancer-arn loadbalancer-arn  
aws elbv2 delete-target-group --target-group-arn targetgroup-arn
```

Network Load Balancers

Un équilibreur de charge constitue le point de contact unique pour les clients. Les clients envoient des demandes à l'équilibreur de charge, et l'équilibreur de charge les envoie aux cibles, par exemple aux instances EC2, dans une zone de disponibilité ou plus.

Pour configurer votre équilibreur de charge, vous créez des [groupes cible](#) et vous enregistrez ensuite les cibles auprès de vos groupes cible. Votre équilibreur de charge est plus efficace si vous vous assurez que chaque zone de disponibilité activée a au moins une cible enregistrée. Vous créez également des [écouteurs](#) pour rechercher les demandes de connexion des clients et pour acheminer les demandes des clients vers les cibles dans vos groupes cibles.

Les équilibreurs de charge réseau prennent en charge les connexions des clients via le peering VPC AWS , le VPN géré et les AWS Direct Connect solutions VPN tierces.

Table des matières

- [États d'un équilibreur de charge](#)
- [Attributs de l'équilibreur de charge](#)
- [Type d'adresse IP](#)
- [Carte des ressources du Network Load Balancer](#)
- [Zones de disponibilité](#)
- [Équilibrage de charge entre zones](#)
- [Suppression protection \(Protection contre la suppression\)](#)
- [Délai d'inactivité des connexions](#)
- [Nom du DNS](#)
- [Affinité DNS de zone de disponibilité](#)
- [Création d'un Network Load Balancer](#)
- [Types d'adresses IP de votre Network Load Balancer](#)
- [Groupes de sécurité de votre Network Load Balancer](#)
- [Balises de votre Network Load Balancer](#)
- [Suppression d'un Network Load Balancer](#)
- [Changement de zone](#)

États d'un équilibreur de charge

Un équilibreur de charge a l'un des états suivants :

`provisioning`

L'équilibreur de charge est en cours de mise en place.

`active`

L'équilibreur de charge est entièrement mis en place et prêt à acheminer le trafic.

`failed`

L'équilibreur de charge n'a pas pu être configuré.

Attributs de l'équilibreur de charge

Un équilibreur de charge a les attributs suivants :

`access_logs.s3.enabled`

Indique si les journaux d'accès stockés dans Amazon S3 sont activés. L'argument par défaut est `false`.

`access_logs.s3.bucket`

Le nom du compartiment Amazon S3 pour les journaux d'accès. Cet attribut est obligatoire si les journaux d'accès sont activés. Pour plus d'informations, consultez [Conditions requises pour le compartiment](#).

`access_logs.s3.prefix`

Le préfixe pour l'emplacement dans le compartiment Amazon S3.

`deletion_protection.enabled`

Indique si la [protection contre la suppression](#) est activée. L'argument par défaut est `false`.

`ipv6.deny_all_igw_traffic`

Bloque l'accès de la passerelle Internet (IGW) à l'équilibreur de charge, empêchant les accès non prévus à votre équilibreur de charge interne via une passerelle Internet. Il est défini sur `false` pour les équilibreurs de charge accessibles sur Internet et sur `true` pour les équilibreurs de

charge internes. Cet attribut n'empêche pas l'accès à Internet hors IGW (par exemple, via le peering, AWS Direct Connect Transit Gateway ou). AWS VPN

`load_balancing.cross_zone.enabled`

Indique si l'[équilibrage de charge entre zones](#) est activé. L'argument par défaut est `false`.

`dns_record.client_routing_policy`

Indique comment le trafic est réparti entre les zones de disponibilité de l'équilibreur de charge. Les valeurs possibles sont `availability_zone_affinity` avec 100 % d'affinité zonale, `partial_availability_zone_affinity` avec 85 % d'affinité zonale et `any_availability_zone` avec 0 % d'affinité zonale.

Type d'adresse IP

Vous pouvez définir les types d'adresses IP que les clients peuvent utiliser avec votre équilibreur de charge.

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

ipv4

Les clients doivent se connecter à l'équilibreur de charge à l'aide d'adresses IPv4 (par exemple, 192.0.2.1). Les équilibreurs de charge compatibles IPv4 (internes et accessibles sur Internet) prennent en charge les écouteurs TCP, UDP, TCP_UDP et TLS.

dualstack

Les clients peuvent se connecter à l'équilibreur de charge à l'aide d'adresses IPv4 (par exemple, 192.0.2.1) et d'adresses Pv6 (par exemple, 2001:0db8:85a3:0:0:8a2e:0370:7334). Les équilibreurs de charge compatibles double pile (internes et accessibles sur Internet) prennent en charge les écouteurs TCP et TLS.

Considérations

- L'équilibreur de charge communique avec les cibles en fonction du type d'adresse IP du groupe cible.
- Lorsque vous activez le mode double pile pour l'équilibreur de charge, Elastic Load Balancing fournit un enregistrement DNS AAAA pour l'équilibreur de charge. Les clients qui communiquent avec l'équilibreur de charge à l'aide d'adresses IPv4 résolvent l'enregistrement

DNS A. Les clients qui communiquent avec l'équilibreur de charge à l'aide d'adresses IPv6 résolvent l'enregistrement DNS AAAA.

- L'accès à vos équilibreurs de charge internes à double pile via la passerelle Internet est bloqué pour empêcher tout accès Internet non prévu. Toutefois, cela n'empêche pas d'autres accès à Internet (par exemple, via le peering, Transit Gateway ou AWS VPN). AWS Direct Connect

Pour plus d'informations sur les types d'adresses IP, consultez [Types d'adresses IP de votre Network Load Balancer](#).

Carte des ressources du Network Load Balancer

La carte des ressources Network Load Balancer fournit un affichage interactif de l'architecture de votre équilibreur de charge, y compris ses auditeurs, groupes cibles et cibles associés. La carte des ressources met également en évidence les relations et les chemins de routage entre toutes les ressources, produisant ainsi une représentation visuelle de la configuration de votre équilibreur de charge.

Pour afficher la carte des ressources de votre Network Load Balancer à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers (Équilibreurs de charge).
3. Sélectionnez l'équilibreur de charge.
4. Choisissez l'onglet Carte des ressources pour afficher la carte des ressources de l'équilibreur de charge.

Composants de la carte des ressources

Vues cartographiques

Deux vues sont disponibles dans la carte des ressources de Network Load Balancer : Overview et Unhealthy Target Map. L'option Vue d'ensemble est sélectionnée par défaut et affiche toutes les ressources de votre équilibreur de charge. La sélection de la vue Carte des cibles malsaines n'affichera que les cibles malsaines et les ressources qui leur sont associées.

La vue Malhealthy Target Map peut être utilisée pour dépanner les cibles dont les tests de santé échouent. Pour plus d'informations, consultez [Résoudre les problèmes liés aux cibles défectueuses à l'aide de la carte des ressources](#).

Colonnes de ressources

La carte des ressources Network Load Balancer contient trois colonnes de ressources, une pour chaque type de ressource. Les groupes de ressources sont les auditeurs, les groupes cibles et les cibles.

Tuiles de ressources

Chaque ressource d'une colonne possède sa propre vignette, qui affiche les détails relatifs à cette ressource spécifique.

- Le survol d'une vignette de ressources permet de mettre en évidence les relations entre celle-ci et les autres ressources.
- La sélection d'une vignette de ressources met en évidence les relations entre celle-ci et les autres ressources et affiche des informations supplémentaires sur cette ressource.
 - résumé de l'état de santé du groupe cible : nombre de cibles enregistrées pour chaque état de santé.
 - état de santé de la cible : état de santé actuel et description de la cible.

Note

Vous pouvez désactiver l'option Afficher les détails des ressources pour masquer des détails supplémentaires dans la carte des ressources.

- Chaque vignette de ressource contient un lien qui, lorsqu'il est sélectionné, permet d'accéder à la page de détails de cette ressource.
 - Écouteurs - Sélectionnez le protocole des écouteurs : port. Par exemple, TCP : 80
 - Groupes cibles - Sélectionnez le nom du groupe cible. Par exemple, my-target-group
 - Cibles - Sélectionnez l'ID des cibles. Par exemple, i-1234567890abcdef0

Exporter la carte des ressources

La sélection d'Exporter vous donne la possibilité d'exporter la vue actuelle de la carte des ressources de votre Network Load Balancer au format PDF.

Zones de disponibilité

Vous activez une ou plusieurs zones de disponibilité pour votre équilibreur de charge lors de sa création. En activant plusieurs zones de disponibilité pour votre équilibreur de charge, vous augmentez la tolérance aux pannes de vos applications. Vous ne pouvez pas désactiver des zones de disponibilité pour un Network Load Balancer après l'avoir créé, mais vous pouvez activer des zones de disponibilité supplémentaires.

Lorsque vous activez une zone de disponibilité, vous spécifiez un sous-réseau depuis cette zone de disponibilité. Elastic Load Balancing crée un nœud d'équilibreur de charge dans la zone de disponibilité et une interface réseau pour le sous-réseau (la description commence par « ELB net » et comprend le nom de l'équilibreur de charge). Chaque nœud d'équilibreur de charge de la zone de disponibilité utilise cette interface réseau pour obtenir une adresse IPv4. Veuillez noter que vous pouvez consulter cette interface réseau, mais vous ne pouvez pas la modifier.

Lorsque vous créez un équilibreur de charge accessible sur Internet, vous pouvez associer une adresse IP Elastic à chaque sous-réseau. Si vous ne choisissez pas l'une de vos propres adresses IP Elastic, Elastic Load Balancing vous fournit une adresse IP Elastic par sous-réseau. Ces adresses IP Elastic fournissent à votre équilibreur de charge des adresses IP statiques qui ne changeront pas pendant la durée de vie de l'équilibreur de charge. Vous ne pouvez pas modifier ces adresses IP Elastic après avoir créé l'équilibreur de charge.

Lorsque vous créez un équilibreur de charge interne, vous pouvez, si vous le souhaitez, spécifier une adresse IP privée pour chaque sous-réseau. Si vous ne spécifiez pas d'adresse IP à partir du sous-réseau, Elastic Load Balancing en choisit une pour vous. Ces adresses IP privées fournissent à votre équilibreur de charge des adresses IP statiques qui ne changeront pas pendant la durée de vie de l'équilibreur de charge. Vous ne pouvez pas modifier ces adresses IP privées après avoir créé l'équilibreur de charge.

Considérations

- Pour les équilibreurs de charge accessibles sur Internet, les sous-réseaux que vous spécifiez doivent avoir au moins 8 adresses IP disponibles. Pour les équilibreurs de charge internes, cela n'est nécessaire que si vous autorisez la AWS sélection d'une adresse IPv4 privée dans le sous-réseau.
- Vous ne pouvez pas spécifier un sous-réseau dans une zone de disponibilité limitée. Le message d'erreur indique que les équilibreurs de charge du type « réseau » ne sont pas pris en charge dans `az_name`. Vous pouvez spécifier un sous-réseau dans une autre zone de disponibilité qui n'est pas

limitée et utiliser l'équilibrage de charge entre zones pour distribuer le trafic vers les cibles dans la zone de disponibilité limitée.

- Vous ne pouvez pas spécifier un sous-réseau qui a été partagé avec vous.
- Vous ne pouvez pas spécifier de sous-réseau dans une zone locale.

Une fois que vous avez activé une zone de disponibilité, l'équilibreur de charge commence à acheminer les demandes vers les cibles enregistrées dans cette zone de disponibilité. Votre équilibreur de charge est plus efficace si vous vous assurez que chaque zone de disponibilité activée a au moins une cible enregistrée.

Pour ajouter des zones de disponibilité à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Sélectionnez le nom de l'équilibreur de charge afin d'ouvrir sa page de détails.
4. Sous l'onglet Network mapping, choisissez Edit subnets.
5. Pour activer une zone de disponibilité, sélectionnez la case à cocher correspondante. S'il existe un sous-réseau pour cette zone de disponibilité, elle est sélectionnée. S'il y a plusieurs sous-réseaux dans cette zone de disponibilité, sélectionnez l'un d'eux. Notez que vous ne pouvez sélectionner qu'un seul sous-réseau par zone de disponibilité.

Pour un équilibreur de charge accessible sur Internet, vous pouvez sélectionner une adresse IP Elastic pour chaque zone de disponibilité. Pour un équilibreur de charge interne, vous pouvez attribuer une adresse IP privée à partir de la plage IPv4 de chaque sous-réseau plutôt que de laisser Elastic Load Balancing en attribuer une.

6. Sélectionnez Enregistrer les modifications.

Pour ajouter des zones de disponibilité à l'aide du AWS CLI

Utilisez la commande [set-subnets](#).

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 d'équilibreur de charge répartit le trafic entre les cibles enregistrées dans toutes les zones de disponibilité activées. Vous pouvez également activer l'équilibrage de charge entre zones au niveau du groupe cible. Pour plus d'informations, veuillez consulter [the section called “Équilibrage de charge entre zones”](#) et [Équilibrage de charge entre zones](#) (langue française non garantie) dans le Guide de l'utilisateur Elastic Load Balancing.

Deletion protection (Protection contre la suppression)

Pour éviter la suppression accidentelle de votre équilibreur de charge, vous pouvez activer la protection contre la suppression. Par défaut, la protection contre la suppression est désactivée pour votre équilibreur de charge.

Si vous activez la protection contre la suppression de votre équilibreur de charge, vous devez la désactiver pour pouvoir supprimer l'équilibreur de charge.

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

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Sélectionnez le nom de l'équilibreur de charge afin d'ouvrir sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sous Configuration, activez la Protection contre la suppression.
6. Sélectionnez Enregistrer les modifications.

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

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Sélectionnez le nom de l'équilibreur de charge afin d'ouvrir sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sous Configuration, activez la Protection contre la suppression.
6. Sélectionnez Enregistrer les modifications.

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

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

Délai d'inactivité des connexions

Pour chaque demande TCP effectuée par un client via un Network 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. Si un client ou une cible envoie des données après que le délai d'inactivité est écoulé, il reçoit un paquet TCP RST pour indiquer que la connexion n'est plus valide.

Nous définissons la valeur du délai d'inactivité à 350 secondes pour les flux TCP. Vous ne pouvez pas modifier cette valeur. Les clients ou les cibles peuvent utiliser des paquets TCP keepalive pour réinitialiser le délai d'inactivité. Les paquets keepalive envoyés pour maintenir les connexions TLS ne peuvent pas contenir de données ou de charge utile.

Lorsqu'un écouteur TLS reçoit un paquet TCP keepalive d'un client ou d'une cible, l'équilibreur de charge génère des paquets TCP keepalive et les envoie aux connexions frontend et backend toutes les 20 secondes. Vous ne pouvez pas modifier ce comportement.

Même si UDP est sans connexion, l'équilibreur de charge conserve l'état de flux UDP en fonction des ports et des adresses IP source et cible. Cela garantit que les paquets appartenant au même flux sont systématiquement envoyés à la même cible. Après la fin du délai d'inactivité, l'équilibreur de charge considère les paquets UDP entrants en tant que nouveaux flux et les achemine vers une nouvelle cible. Elastic Load Balancing définit la valeur du délai d'inactivité pour les flux UDP à 120 secondes.

Les instances EC2 doivent répondre à une nouvelle demande dans les 30 secondes afin d'établir un chemin de retour.

Nom du DNS

Chaque Network Load Balancer reçoit un nom de système de nom de domaine (DNS) par défaut avec la syntaxe suivante : `nom-id.elb.région.amazonaws.com`. Par exemple, `my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com`.

Si vous préférez utiliser un nom de DNS plus facile à mémoriser, vous pouvez créer un nom de domaine personnalisé et l'associer au nom de DNS de votre équilibreur de charge. Lorsqu'un client

effectue une demande à l'aide de ce nom de domaine personnalisé, le serveur DNS résout le nom DNS pour votre équilibreur de charge.

Tout d'abord, enregistrez un nom de domaine auprès d'un bureau d'enregistrement de noms de domaine accrédité. Utilisez ensuite votre service DNS, par exemple, votre serveur d'inscriptions de domaine, pour créer un enregistrement DNS afin d'acheminer les demandes vers votre équilibreur de charge. Pour plus d'informations, consultez la documentation de votre service DNS. Par exemple, si vous utilisez Amazon Route 53 comme service DNS, vous créez un enregistrement d'alias qui pointe vers votre équilibreur de charge. Pour plus d'informations, veuillez consulter [Routage du trafic vers un équilibreur de charge ELB](#) dans le Guide du développeur Amazon Route 53.

L'équilibreur de charge possède une adresse IP par zone de disponibilité activée. Il s'agit des adresses IP des nœuds d'équilibreur de charge. Le nom de DNS de l'équilibreur de charge est résolu en ces adresses. Par exemple, supposons que le nom de domaine personnalisé de votre équilibreur de charge soit `example.networkloadbalancer.com`. Utilisez la commande `dig` ou `nslookup` suivante pour déterminer les adresses IP des nœuds d'équilibreur de charge.

Linux ou Mac

```
$ dig +short example.networkloadbalancer.com
```

Windows

```
C:\> nslookup example.networkloadbalancer.com
```

L'équilibreur de charge comporte des enregistrements DNS pour ses nœuds d'équilibreur de charge. Vous pouvez utiliser des noms de DNS avec la syntaxe suivante pour déterminer les adresses IP des nœuds d'équilibreur de charge : `az.nom-id.elb.région.amazonaws.com`.

Linux ou Mac

```
$ dig +short us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

Windows

```
C:\> nslookup us-east-2b.my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com
```

Affinité DNS de zone de disponibilité

Lorsque vous utilisez la stratégie de routage client par défaut, les demandes envoyées au nom DNS de vos Network Load Balancers recevront toutes les adresses IP d'équilibreur de charge saines. Cela conduit à la distribution des connexions client entre les zones de disponibilité des équilibreurs de charge. Avec les stratégies de routage par affinité de zone de disponibilité, les requêtes DNS des clients privilégient les adresses IP des équilibreurs de charge dans leur propre zone de disponibilité. Cela permet d'améliorer à la fois la latence et la résilience, car les clients n'ont pas besoin de franchir les limites de la zone de disponibilité lorsqu'ils se connectent à des cibles.

Stratégies de routage client disponibles pour les Network Load Balancers utilisant Route 53 Resolver :

- Affinité de zone de disponibilité : 100 % d'affinité zonale

Les requêtes DNS des clients privilégieront l'adresse IP de l'équilibreur de charge dans leur propre zone de disponibilité. Les requêtes peuvent être résolues vers d'autres zones s'il n'existe aucune adresse IP d'équilibreur de charge saine dans leur propre zone.

- Affinité de zone de disponibilité partielle : 85 % d'affinité zonale

85 % des requêtes DNS des clients privilégieront les adresses IP des équilibreurs de charge dans leur propre zone de disponibilité, tandis que les requêtes restantes seront résolues vers n'importe quelle zone saine. Les requêtes peuvent être résolues vers d'autres zones saines s'il n'existe aucune adresse IP saine dans leur zone. Lorsqu'il n'existe aucune adresse IP saine dans une zone, les requêtes sont résolues vers n'importe quelle zone.

- N'importe quelle zone de disponibilité (par défaut) : 0 % d'affinité zonale

Les requêtes DNS des clients sont résolues vers les adresses IP d'équilibreurs de charge saines de toutes les zones de disponibilité de l'équilibreur de charge.

Note

Les stratégies de routage par affinité de zone de disponibilité s'appliquent uniquement aux clients résolvant le nom DNS des Network Load Balancers à l'aide de Route 53 Resolver. Pour plus d'informations, veuillez consulter [Qu'est-ce qu'Amazon Route 53 Resolver ?](#) dans le Guide du développeur Amazon Route 53.

L'affinité de zone de disponibilité permet d'acheminer les requêtes du client vers l'équilibreur de charge, tandis que l'équilibrage de charge entre zones est utilisé pour aider à acheminer les requêtes de l'équilibreur de charge vers les cibles. Lorsque vous utilisez l'affinité de zone de disponibilité, l'équilibrage de charge entre zones doit être désactivé, afin de garantir que le trafic de l'équilibreur de charge entre les clients et les cibles reste dans la même zone de disponibilité. Avec cette configuration, le trafic client est envoyé vers la même zone de disponibilité du Network Load Balancer. Il est donc recommandé de configurer votre application pour qu'elle évolue indépendamment dans chaque zone de disponibilité. Il s'agit d'une considération importante lorsque le nombre de clients par zone de disponibilité ou le trafic par zone de disponibilité ne sont pas les mêmes. Pour plus d'informations, consultez [Équilibrage de charge entre zones pour groupes cibles](#).

Lorsqu'une zone de disponibilité est considérée comme défectueuse ou lorsqu'un changement de zone est entamé, l'adresse IP zonale est considérée comme défectueuse et ne sera pas renvoyée aux clients, sauf si le mode fail-open est activé. L'affinité de zone de disponibilité est maintenue lorsque l'enregistrement DNS est en mode fail-open. Cela permet de préserver l'indépendance des zones de disponibilité et d'éviter les défaillances potentielles entre zones.

Lorsque vous utilisez l'affinité de zone de disponibilité, des périodes de déséquilibre entre les zones de disponibilité sont attendues. Il est recommandé de s'assurer que vos cibles se mettent à l'échelle au niveau zonal, afin de prendre en charge la charge de travail de chaque zone de disponibilité. Dans les cas où ces déséquilibres sont importants, il est recommandé de désactiver l'affinité de zone de disponibilité. Cela permet une distribution uniforme des connexions client entre toutes les zones de disponibilité d'équilibreurs de charge en 60 secondes, ou durant la TTL du DNS.

Avant d'utiliser l'affinité de zone de disponibilité, tenez compte des éléments suivants :

- L'affinité de zone de disponibilité entraîne des modifications sur tous les clients Network Load Balancers qui utilisent Route 53 Resolver.
 - Les clients ne sont pas en mesure de choisir entre les résolutions DNS zonales-locales et multizones. L'affinité de zone de disponibilité décide pour eux.
 - Les clients ne disposent pas d'une méthode fiable pour déterminer à quel moment ils sont concernés par l'affinité de zone de disponibilité ou comment savoir quelle adresse IP se trouve dans quelle zone de disponibilité.
- Les clients resteront affectés à leur adresse IP locale de zone jusqu'à ce qu'elle soit jugée totalement défectueuse selon les surveillances de l'état du DNS et qu'elle soit supprimée du DNS.
- L'utilisation de l'affinité de zone de disponibilité avec l'équilibrage de charge entre zones activé peut entraîner une répartition déséquilibrée des connexions client entre les zones de disponibilité.

Il est recommandé de configurer votre pile d'applications pour qu'elle se mette à l'échelle indépendamment dans chaque zone de disponibilité, afin de garantir qu'elle puisse prendre en charge le trafic des clients zonaux.

- Si l'équilibrage de charge entre zones est activé, le Network Load Balancer est soumis à un impact entre zones.
- La charge sur chacune des zones de disponibilité des Network Load Balancers sera proportionnelle aux emplacements zonaux des demandes des clients. Si vous ne configurez pas le nombre de clients exécutés dans chaque zone de disponibilité, vous devrez mettre à l'échelle chaque zone de disponibilité de manière réactive et indépendante.

Surveillance

Il est recommandé de suivre la distribution des connexions entre les zones de disponibilité à l'aide des métriques zonales de l'équilibreur de charge. Vous pouvez utiliser des métriques pour afficher le nombre de connexions nouvelles et actives par zone.

Nous vous recommandons d'effectuer le suivi des éléments suivants :

- **ActiveFlowCount** : nombre total de flux (ou connexions) simultanés provenant des clients vers des cibles.
- **NewFlowCount** : nombre total de nouveaux flux (ou connexions) établis entre les clients et les cibles pendant la période.
- **HealthyHostCount** : nombre de cibles considérées saines.
- **UnHealthyHostCount** : nombre de cibles considérées défectueuses.

Pour plus d'informations, consultez [CloudWatch métriques pour votre Network Load Balancer](#).

Activation de l'affinité de zone de disponibilité

Les étapes de cette procédure expliquent comment activer l'affinité de zone de disponibilité à l'aide de la console Amazon EC2.

Pour activer l'affinité de zone de disponibilité à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.

3. Sélectionnez le nom de l'équilibreur de charge afin d'ouvrir sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sous Configuration de l'acheminement de la zone de disponibilité, Politique de routage du client (enregistrement DNS), sélectionnez Affinité de zone de disponibilité ou Affinité partielle de zone de disponibilité.
6. Sélectionnez Enregistrer les modifications.

Pour activer l'affinité de zone de disponibilité à l'aide du AWS CLI

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

Désactivation de l'affinité de zone de disponibilité

Les étapes de cette procédure expliquent comment désactiver l'affinité de zone de disponibilité à l'aide de la console Amazon EC2.

Pour désactiver l'affinité de zone de disponibilité à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Sélectionnez le nom de l'équilibreur de charge afin d'ouvrir sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sous Configuration de l'acheminement de la zone de disponibilité, Politique de routage du client (enregistrement DNS), sélectionnez Toute zone de disponibilité.
6. Sélectionnez Enregistrer les modifications.

Pour désactiver l'affinité de zone de disponibilité à l'aide du AWS CLI

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

Création d'un Network Load Balancer

Un équilibreur de charge prend les demandes des clients et les répartit sur les cibles d'un groupe de cibles, par exemple des instances EC2.

Avant de commencer, assurez-vous que le réseau Virtual Private Cloud (VPC) de votre équilibreur de charge comporte au moins un sous-réseau public dans chaque zone de disponibilité dans laquelle vous avez des cibles. Vous devez également configurer un groupe cible et enregistrer au moins une cible à définir comme valeur par défaut afin d'acheminer votre trafic vers le groupe cible.

Pour créer un équilibreur de charge à l'aide du AWS CLI, voir [Didacticiel : création d'un Network Load Balancer à l'aide de l'AWS CLI](#).

Pour créer un équilibreur de charge à l'aide du AWS Management Console, effectuez les tâches suivantes.

Tâches

- [Étape 1 : Configurer un groupe cible](#)
- [Étape 2 : enregistrer les cibles](#)
- [Étape 3 : configurer un équilibreur de charge et un écouteur](#)
- [Étape 4 : tester l'équilibreur de charge](#)

Étape 1 : Configurer un groupe cible

La configuration d'un groupe cible vous permet d'enregistrer des cibles telles que des instances EC2. Le groupe cible que vous configurez à cette étape est utilisé comme groupe cible dans la règle d'écouteur lorsque vous configurez votre équilibreur de charge. Pour plus d'informations, consultez [Groupes cibles de vos Network Load Balancers](#).

Pour configurer votre groupe cible à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sélectionnez Groupes cibles.
3. Sélectionnez Créer un groupe cible.
4. Sous le panneau Configuration de base, procédez comme suit :
 - a. Pour Choisir un type de cible, sélectionnez Instances pour enregistrer les cibles par ID d'instance, Adresses IP pour enregistrer les cibles par adresse IP ou Application Load Balancer pour enregistrer un Application Load Balancer en tant que cible.
 - b. Pour Nom du groupe cible, saisissez un nom pour le groupe cible.
 - c. Pour Protocole, choisissez un protocole comme suit :

- Si l'écouteur est un protocole TCP, choisissez TCP ou TCP_UDP.
 - Si l'écouteur est un protocole TLS, choisissez TCP ou TLS.
 - Si l'écouteur est un protocole UDP, choisissez UDP ou TCP_UDP.
 - Si l'écouteur protocole est TCP_UDP, choisissez TCP_UDP.
- d. (Facultatif) Pour Port, modifiez la valeur par défaut en fonction des besoins.
- e. Pour Type d'adresse IP, choisissez IPv4 ou IPv6. Cette option n'est disponible que si le type de cible est Instances ou Adresses IP et si le protocole est TCP ou TLS.
- Vous devez associer un groupe cible IPv6 à un équilibreur de charge à double pile. Toutes les cibles du groupe cible doivent avoir le même type d'adresse IP. Vous ne pouvez pas modifier le type d'adresse IP d'un groupe cible après l'avoir créé.
- f. Pour un VPC, sélectionnez le cloud privé virtuel (VPC) avec les cibles à enregistrer.
5. Pour le panneau Surveillances de l'état, modifiez les paramètres par défaut selon vos besoins. Pour les Paramètres avancés de surveillance de l'état, choisissez le port de surveillance de l'état, le nombre, le délai d'expiration, l'intervalle et les codes de réussite. Si les surveillances de l'état dépassent consécutivement le Seuil de défektivité, l'équilibreur de charge met la cible hors service. Lorsque les surveillances de l'état dépassent consécutivement le Seuil de défektivité, l'équilibreur de charge remet la cible en service. Pour plus d'informations, consultez [Surveillance de l'état de vos groupes cibles](#).
6. (Facultatif) Pour ajouter une balise, choisissez Balises, puis Ajouter une balise et saisissez la clé et la valeur de la balise.
7. Choisissez Suivant.

Étape 2 : enregistrer les cibles

Vous pouvez enregistrer des instances EC2, des adresses IP ou un Application Load Balancer auprès de votre groupe cible. Il s'agit d'une étape facultative pour créer un équilibreur de charge. Cependant, vous devez enregistrer vos cibles pour vous assurer que votre équilibreur de charge peut acheminer le trafic vers ces dernières.

1. Sur la page Enregistrer les cibles, ajoutez une ou plusieurs cibles comme suit :
 - Si le type de cible est Instances, sélectionnez les instances, saisissez les ports, puis choisissez Inclure comme étant en attente ci-dessous.

- Si le type de cible est Adresses IP, sélectionnez le réseau, saisissez les adresses IP et les ports, puis choisissez Inclure comme étant en attente ci-dessous.
- Si le type de cible est Application Load Balancer, sélectionnez un Application Load Balancer.

2. Sélectionnez Créer un groupe cible.

Étape 3 : configurer un équilibreur de charge et un écouteur

Pour créer un Network Load Balancer, vous devez d'abord fournir des informations de configuration de base pour votre équilibreur de charge, comme un nom, un schéma et un type d'adresse IP.

Fournissez ensuite des informations sur votre réseau et sur un ou plusieurs écouteurs. Un écouteur est un processus qui vérifie les demandes de connexion. Il est configuré avec un protocole et un port pour les connexions des clients vers l'équilibreur de charge. Pour plus d'informations sur les protocoles et les ports pris en charge, consultez [Configuration des écouteurs](#).

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

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Choisissez Créer un équilibreur de charge.
4. Sous Network 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-nlb**. Le nom de votre Network Load Balancer doit être unique dans votre ensemble d'Application Load Balancers et de Network Load Balancers pour la région. Le nom doit avoir un maximum de 32 caractères et ne peut contenir que des caractères alphanumériques et des traits d'union. Il ne peut pas commencer ou se terminer par un trait d'union, ou par `internal-`.
 - b. Pour Scheme (Méthode), choisissez Internet-facing (Accessible sur Internet) ou Internal (Interne). Un équilibreur de charge accessible sur Internet achemine les demandes des clients vers les cibles via Internet. Un équilibreur de charge interne achemine les demandes vers les cibles à l'aide d'adresses IP privées.
 - c. Pour Type d'adresse IP, choisissez IPv4 si vos clients utilisent des adresses IPv4 pour communiquer avec l'équilibreur de charge ou Dualstack s'ils utilisent des adresses IPv4 et IPv6.

6. Mappage du réseau

- a. Dans VPC, sélectionnez le VPC que vous avez utilisé pour vos instances EC2.

Si vous avez sélectionné Accessible via Internet pour Schéma, seuls les VPC dotés d'une passerelle Internet pourront être sélectionnés.

- b. Pour les Mappages, sélectionnez une ou plusieurs zones de disponibilité et les sous-réseaux correspondants. L'activation de plusieurs zones de disponibilité renforce la tolérance aux pannes de vos applications. Vous ne pouvez pas spécifier un sous-réseau qui a été partagé avec vous.

Pour des équilibreurs de charge accessibles sur Internet, vous pouvez sélectionner une adresse IP Elastic pour chaque zone de disponibilité. Ceci fournit des adresses IP statiques à votre équilibreur de charge. Sinon, pour un équilibreur de charge interne, vous pouvez attribuer une adresse IP privée à partir de la plage IPv4 de chaque sous-réseau au lieu de vous en AWS attribuer une pour vous.

7. Pour Groupes de sécurité, nous présélectionnons le groupe de sécurité par défaut pour votre VPC. Vous pouvez sélectionner d'autres groupes de sécurité si nécessaire. Si vous ne disposez pas d'un groupe de sécurité adapté, choisissez Créer un groupe de sécurité et créez-en un qui répond à vos besoins en matière de sécurité. Pour plus d'informations, veuillez consulter [Création d'un groupe de sécurité](#) dans le Guide de l'utilisateur Amazon VPC.

Warning

Si vous n'associez aucun groupe de sécurité à votre équilibreur de charge pour le moment, vous ne pourrez pas les associer ultérieurement.

8. Écouteurs et routage

- a. La valeur par défaut est un écouteur qui accepte le trafic TCP sur le port 80. Vous pouvez conserver les paramètres de l'écouteur par défaut ou modifier Protocole et Port selon vos besoins.
- b. Pour Action par défaut, sélectionnez un groupe cible pour transférer le trafic. Si vous n'avez pas créé de groupe cible auparavant, vous devez en créer un maintenant. Vous pouvez éventuellement choisir Ajouter un écouteur pour ajouter un autre écouteur (par exemple, un écouteur TLS).
- c. (Facultatif) Attribuez des balises pour catégoriser votre écouteur.

- d. Pour Paramètres d'écouteur sécurisé (disponibles uniquement pour les écouteurs TLS), procédez comme suit :
 - i. Pour Stratégie de sécurité, choisissez une stratégie de sécurité qui répond à vos exigences.
 - ii. Pour la stratégie ALPN, choisissez une stratégie pour activer ALPN ou choisissez Aucun pour désactiver ALPN.
 - iii. Pour Certificat SSL par défaut, choisissez Depuis ACM (recommandé) et sélectionnez un certificat. Si vous n'avez pas de certificat disponible, vous pouvez en importer un dans ACM ou utiliser ACM pour vous en faire approvisionner un. Pour plus d'informations, veuillez consulter [Émission et gestion de certificats](#) dans le Guide de l'utilisateur AWS Certificate Manager .
9. (Facultatif) Vous pouvez utiliser des services complémentaires avec votre équilibreur de charge. Par exemple, vous pouvez choisir de AWS Global Accelerator créer un accélérateur pour vous et d'associer votre équilibreur de charge à l'accélérateur. Le nom de l'accélérateur peut comporter les caractères suivants (64 caractères maximum) : a-z, A-Z, 0-9, . (point) et - (tiret). Une fois l'accélérateur créé, accédez à la AWS Global Accelerator console pour terminer sa configuration. Pour plus d'informations, voir [Ajouter un accélérateur lors de la création d'un équilibreur de charge](#)
10. Balises

(Facultatif) Ajoutez des balises pour catégoriser votre équilibreur de charge. Pour plus d'informations, veuillez consulter [Balises](#).
11. Récapitulatif

Examinez votre configuration, puis choisissez Create load balancer (Créer l'équilibreur de charge). Quelques attributs par défaut sont appliqués à votre équilibreur de charge lors de sa création. Vous pouvez les consulter et les modifier après avoir créé l'équilibreur de charge. Pour plus d'informations, consultez [Attributs de l'équilibreur de charge](#).

Étape 4 : tester l'équilibreur de charge

Une fois que vous avez créé votre équilibreur de charge, vous pouvez vérifier que la surveillance de l'état initiale de vos instances EC2 a été réussie, puis vous assurer que l'équilibreur de charge envoie le trafic à vos instances EC2. Pour supprimer l'équilibreur de charge, veuillez consulter [Suppression d'un Network Load Balancer](#).

Pour tester l'équilibreur de charge

1. Une fois que l'équilibreur de charge est créé, cliquez sur Close.
2. Dans le panneau de navigation de gauche, choisissez Groupes cibles.
3. Sélectionnez le nouveau groupe cible.
4. Choisissez Cibles et vérifiez que vos instances sont prêtes. Si le statut d'une instance est `initial`, c'est probablement dû au fait que cette instance est encore en cours d'enregistrement ou qu'elle n'est pas considérée comme saine, car elle n'a pas passé le nombre minimal de surveillances de l'état. Une fois que l'état d'au moins une instance est saine, vous pouvez tester votre équilibreur de charge. Pour plus d'informations, consultez [État de santé d'une cible](#).
5. Dans le volet de navigation, choisissez Load Balancers.
6. Sélectionnez le nouvel équilibreur de charge.
7. Copiez le nom DNS de l'équilibreur de charge (par exemple, my-load-balancer-1234567890abcdef.elb.us-east-2.amazonaws.com). Collez le nom DNS dans le champ d'adresse d'un navigateur Web connecté à Internet. Si tout fonctionne, le navigateur affiche la page par défaut de votre serveur.

Types d'adresses IP de votre Network Load Balancer

Vous pouvez configurer votre Network Load Balancer pour que les clients puissent communiquer avec l'équilibreur de charge en utilisant uniquement des adresses IPv4 ou à la fois des adresses IPv4 et IPv6 (double pile). L'équilibreur de charge communique avec les cibles en fonction du type d'adresse IP du groupe cible. Pour plus d'informations, consultez [Type d'adresse IP](#).

Exigences en matière de double pile

- Vous pouvez définir le type d'adresse IP lorsque vous créez l'équilibreur de charge et pouvez la mettre à jour à tout moment.
- Le Virtual Private Cloud (VPC) et les sous-réseaux que vous spécifiez pour l'équilibreur de charge doivent avoir des blocs CIDR IPv6 associés. Pour plus d'informations, veuillez consulter [Adresses IPv6](#) dans le Guide de l'utilisateur Amazon EC2.
- L'équilibreur de charge ne doit comporter que des écouteurs TCP et TLS.
- Les tables de routage des sous-réseaux d'équilibrage de charge doivent acheminer le trafic IPv6.
- Les listes ACL réseau des sous-réseaux d'équilibrage de charge doivent autoriser le trafic IPv6.

Pour définir le type d'adresse IP lors de la création

Configurez les paramètres comme décrit dans [Créer un équilibreur de charge](#).

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

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Cochez la case correspondant à l'équilibreur de charge.
4. Choisissez Actions, Edit IP address type.
5. Pour Type d'adresse IP, choisissez IPv4 afin de prendre en charge uniquement les adresses IPv4 ou Dualstack pour prendre en charge à la fois les adresses IPv4 et IPv6.
6. Sélectionnez Enregistrer les modifications.

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

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

Groupes de sécurité de votre Network Load Balancer

Vous pouvez associer un groupe de sécurité à votre Network Load Balancer afin de contrôler le trafic autorisé à atteindre et à quitter l'équilibreur de charge. Vous spécifiez les ports, protocoles et sources à autoriser pour le trafic entrant, ainsi que les ports, protocoles et destinations à autoriser pour le trafic sortant. Si vous n'attribuez aucun groupe de sécurité à votre équilibreur de charge, tout le trafic client peut atteindre les écouteurs de l'équilibreur de charge et tout le trafic peut quitter l'équilibreur de charge.

Vous pouvez ajouter une règle aux groupes de sécurité associés à vos cibles qui fait référence au groupe de sécurité associé à votre Network Load Balancer. Cela permet aux clients d'envoyer du trafic vers vos cibles via votre équilibreur de charge, mais les empêche d'envoyer du trafic directement vers vos cibles. Le fait de référencer le groupe de sécurité associé à votre Network Load Balancer dans les groupes de sécurité associés à vos cibles garantit que celles-ci acceptent le trafic provenant de votre équilibreur de charge, même si vous activez la [préservation des adresses IP client](#) pour votre équilibreur de charge.

Le trafic bloqué par les règles entrantes des groupes de sécurité ne vous est pas facturé.

Table des matières

- [Considérations](#)
- [Exemple : filtrer le trafic client](#)
- [Exemple : accepter le trafic uniquement depuis l'équilibreur de charge](#)
- [Mise à jour des groupes de sécurité associés](#)
- [Mise à jour des paramètres de sécurité](#)
- [Surveillance des groupes de sécurité d'équilibreur de charge](#)

Considérations

- Vous pouvez associer des groupes de sécurité à un Network Load Balancer lorsque vous le créez. Si vous créez un Network Load Balancer sans associer de groupes de sécurité, vous ne pourrez pas les associer ultérieurement à l'équilibreur de charge. Nous vous recommandons d'associer un groupe de sécurité à votre équilibreur de charge lorsque vous le créez.
- Après avoir créé un Network Load Balancer avec des groupes de sécurité associés, vous pouvez modifier ces derniers à tout moment.
- Les surveillances de l'état sont soumises aux règles sortantes, mais pas aux règles entrantes. Vous devez vous assurer que les règles sortantes ne bloquent pas le trafic lié aux surveillances de l'état. Dans le cas contraire, l'équilibreur de charge considère que les cibles sont défectueuses.
- Vous pouvez contrôler si le PrivateLink trafic est soumis à des règles entrantes. Si vous activez les règles de PrivateLink trafic entrant, la source du trafic est l'adresse IP privée du client, et non l'interface du point de terminaison.

Exemple : filtrer le trafic client

Les règles entrantes suivantes dans le groupe de sécurité associé à votre Network Load Balancer autorisent uniquement le trafic provenant de la plage d'adresses spécifiée. S'il s'agit d'un équilibreur de charge interne, vous pouvez spécifier une plage d'adresses CIDR VPC comme source pour autoriser uniquement le trafic provenant d'un VPC spécifique. S'il s'agit d'un équilibreur de charge accessible sur Internet qui doit accepter le trafic depuis n'importe où sur Internet, vous pouvez spécifier 0.0.0.0/0 comme source.

Entrant

Protocole	Source	Plage de ports	Comment
<i>protocole</i>	<i>plage d'adresses IP client</i>	<i>port de l'écouteur</i>	Autorise le trafic entrant depuis la plage d'adresses CIDR source sur le port d'écoute.
ICMP	0.0.0.0/0	Tous	Permet au trafic ICMP entrant de prendre en charge la MTU ou la détection de la MTU du chemin †.

† Pour plus d'informations, consultez [Path MTU Discovery](#) dans le guide de l'utilisateur Amazon EC2.

Sortant

Protocole	Destination	Plage de ports	Comment
Tous	N'importe où	Tous	Autorise tout le trafic sortant

Exemple : accepter le trafic uniquement depuis l'équilibreur de charge

Supposons que votre Network Load Balancer possède un groupe de sécurité sg-1111222233333. Utilisez les règles suivantes dans les groupes de sécurité associés à vos instances cibles pour vous assurer qu'elles n'acceptent que le trafic provenant du Network Load Balancer. Vous devez vous assurer que les cibles acceptent le trafic depuis l'équilibreur de charge à la fois sur le port cible et le port de surveillance de l'état. Pour plus d'informations, consultez [the section called "Groupes de sécurité cibles"](#).

Entrant

Protocole	Source	Plage de ports	Comment
<i>protocole</i>	sg-111112 222233333	<i>port cible</i>	Autorise le trafic entrant depuis l'équilibreur de charge sur le port cible.

Protocole	Source	Plage de ports	Comment
<i>protocole</i>	sg-111112 222233333	<i>vérification_état</i>	Autorise le trafic entrant depuis l'équilibreur de charge sur le port de surveillance de l'état.

Sortant

Protocole	Destination	Plage de ports	Comment
Tous	N'importe où	N'importe quel compte	Autorise tout le trafic sortant

Mise à jour des groupes de sécurité associés

Si vous avez associé au moins un groupe de sécurité à un équilibreur de charge lors de sa création, vous pouvez mettre à jour les groupes de sécurité de cet équilibreur de charge à tout moment.

Pour mettre à jour les groupes de sécurité à l'aide de la console

1. Ouvrez la console Amazon EC2 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. Dans l'onglet Security, choisissez Edit.
5. Pour associer un groupe de sécurité à votre équilibreur de charge, sélectionnez-le. Pour supprimer un groupe de sécurité de votre équilibreur de charge, décochez-le.
6. Sélectionnez Enregistrer les modifications.

Pour mettre à jour les groupes de sécurité à l'aide du AWS CLI

Utilisez la commande [set-security-groups](#).

Mise à jour des paramètres de sécurité

Par défaut, nous appliquons les règles entrantes du groupe de sécurité à l'ensemble du trafic envoyé à l'équilibreur de charge. Toutefois, il se peut que vous ne souhaitiez pas appliquer ces règles au trafic envoyé vers l'équilibreur de charge AWS PrivateLink, qui peut provenir d'adresses IP qui se chevauchent. Dans ce cas, vous pouvez configurer l'équilibreur de charge afin que nous n'appliquions pas les règles entrantes pour le trafic envoyé via l'équilibreur de charge. AWS PrivateLink

Pour mettre à jour les paramètres de sécurité à l'aide de la console

1. Ouvrez la console Amazon EC2 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. Dans l'onglet Security, choisissez Edit.
5. Sous Paramètre de sécurité, décochez Appliquer les règles de trafic entrant au PrivateLink trafic.
6. Sélectionnez Enregistrer les modifications.

Pour mettre à jour les paramètres de sécurité à l'aide du AWS CLI

Utilisez la commande [set-security-groups](#).

Surveillance des groupes de sécurité d'équilibreur de charge

Utilisez les `SecurityGroupBlockedFlowCount_Outbound` CloudWatch métriques `SecurityGroupBlockedFlowCount_Inbound` et pour surveiller le nombre de flux bloqués par les groupes de sécurité de l'équilibreur de charge. Le trafic bloqué n'est pas reflété dans les autres métriques. Pour plus d'informations, consultez [the section called "CloudWatch métriques"](#).

Utilisez les journaux de flux VPC pour surveiller le trafic accepté ou rejeté par les groupes de sécurité de l'équilibreur de charge. Pour plus d'informations, veuillez consulter [Journaux de flux VPC](#) dans le Guide de l'utilisateur Amazon VPC.

Balises de votre Network Load Balancer

Les balises vous permettent de catégoriser vos équilibreurs de charge de différentes manières. Par exemple, vous pouvez baliser une ressource par objectif, propriétaire ou environnement.

Vous pouvez ajouter plusieurs balises à chaque équilibreur de charge. 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 équilibreur de charge.

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 équilibreur de charge à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Sélectionnez le nom de l'équilibreur de charge afin d'ouvrir sa page de détails.
4. Dans l'onglet Balises, choisissez Gérer les balises.
5. Pour ajouter une balise, choisissez Ajouter une balise, puis saisissez la clé et la valeur de la balise. Les caractères autorisés sont les lettres, les espaces et les chiffres (en UTF-8), ainsi que les caractères spéciaux suivants : + - = . _ : / @. N'utilisez pas d'espaces de début ou de fin. Les valeurs de balises sont sensibles à la casse.
6. Pour mettre à jour une balise, saisissez de nouvelles valeurs dans Clé et Valeur.
7. Pour supprimer une étiquette, choisissez le bouton Remove (Retirer) à côté de l'étiquette.
8. Lorsque vous avez terminé, choisissez Enregistrer les modifications.

Pour mettre à jour les balises d'un équilibreur de charge à l'aide du AWS CLI

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

Suppression d'un Network Load Balancer

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

Vous ne pouvez pas supprimer un équilibreur de charge si la protection contre la suppression est activée. Pour plus d'informations, consultez [Deletion protection \(Protection contre la suppression\)](#).

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

La suppression d'un équilibreur de charge supprime également ses écouteurs. La suppression d'un équilibreur de charge n'affecte pas ses cibles enregistrées. Par exemple, vos instances EC2 continuent à s'exécuter et sont toujours enregistrées pour leurs groupes cible. Pour supprimer vos groupes cible, consultez la page [Supprimer un groupe cible](#).

Pour supprimer un équilibreur de charge à l'aide de la console

1. Si vous avez un enregistrement DNS pour votre domaine qui pointe sur votre équilibreur de charge, faites-le pointer sur un nouvel emplacement et attendez que le changement DNS prenne effet avant de supprimer votre équilibreur de charge.

Exemple :

- S'il s'agit d'un enregistrement CNAME avec une durée de vie (TTL) de 300 secondes, attendez au moins 300 secondes avant de passer à l'étape suivante.
 - Si l'enregistrement est un enregistrement Route 53 Alias(A), attendez au moins 60 secondes.
 - Si vous utilisez Route 53, la modification d'enregistrement prend 60 secondes pour se propager à tous les serveurs de noms Route 53 mondiaux. Ajoutez ce temps à la valeur TTL de l'enregistrement en cours de mise à jour.
2. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
 3. Dans le volet de navigation, choisissez Load Balancers.
 4. Cochez la case correspondant à l'équilibreur de charge.
 5. Sélectionnez Actions, Delete load balancer.

6. Lorsque vous êtes invité à confirmer, saisissez **confirm**, puis choisissez Supprimer.

Pour supprimer un équilibreur de charge à l'aide du AWS CLI

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

Changement de zone

Le changement de zone est une fonctionnalité du Contrôleur de récupération d'application Amazon Route 53 (Route 53 ARC). Avec le changement de zone, vous pouvez déplacer une ressource d'équilibreur de charge hors d'une zone de disponibilité altérée en une seule action. De cette façon, vous pouvez continuer à opérer depuis d'autres zones de disponibilité saines dans une Région AWS.

Lorsque vous lancez un changement de zone, votre équilibreur de charge arrête d'envoyer le trafic pour la ressource vers la zone de disponibilité concernée. Route 53 ARC crée le changement de zone immédiatement. Cependant, l'établissement des connexions existantes en cours dans la zone de disponibilité concernée peut prendre un certain temps, généralement quelques minutes. Pour plus d'informations, veuillez consulter [Comment fonctionne un changement de zone : surveillances de l'état et adresses IP zonales](#) (langue française non garantie) dans Guide du développeur du Contrôleur de récupération d'application Amazon Route 53.

Les changements de zone ne sont pris en charge que sur les Application Load Balancers et les Network Load Balancers lorsque la répartition de charge entre zones est désactivée. Si vous activez la répartition de charge entre zones, vous ne pouvez pas démarrer de changement de zone. Pour plus d'informations, veuillez consulter [Ressources prises en charge pour les changements de zone](#) dans le Guide du développeur du Contrôleur de récupération d'application Amazon Route 53.

Avant d'utiliser un changement de zone, passez en revue les points suivants :

- La répartition de charge entre zones n'est pas prise en charge avec les changements de zone. Vous devez désactiver la répartition de charge entre zones pour utiliser cette fonctionnalité.
- Le changement de zone n'est pas pris en charge lorsque vous utilisez un Application Load Balancer comme point de terminaison d'accélérateur dans AWS Global Accelerator.
- Vous pouvez démarrer un changement de zone pour un équilibreur de charge spécifique uniquement pour une zone de disponibilité unique. Vous ne pouvez pas commencer un changement de zone pour plusieurs zones de disponibilité.

- AWS supprime de manière proactive les adresses IP des équilibreurs de charge zonaux du DNS lorsque plusieurs problèmes d'infrastructure ont un impact sur les services. Vérifiez toujours la capacité actuelle de la zone de disponibilité avant de commencer un changement de zone. Si la répartition de charge entre zones de vos équilibreurs de charge est désactivée et que vous utilisez un changement de zone pour supprimer une adresse IP d'équilibreur de charge zonal, la zone de disponibilité affectée par le changement de zone perd également sa capacité cible.
- Lorsqu'un Application Load Balancer est la cible d'un Network Load Balancer, commencez toujours le changement de zone à partir du Network Load Balancer. Si vous commencez un changement de zone à partir de l'Application Load Balancer, le Network Load Balancer ne reconnaît pas le changement et continue à envoyer du trafic vers l'Application Load Balancer.

Pour plus de conseils et d'informations, veuillez consulter les [Bonnes pratiques relatives aux changements de zone Route 53 ARC](#) (langue française non garantie) dans le Guide du développeur du Contrôleur de récupération d'application Amazon Route 53.

Lancement d'un changement de zone

Les étapes de cette procédure expliquent comment démarrer un changement de zone à l'aide de la console Amazon EC2. Pour connaître les étapes à suivre pour démarrer un changement de zone à l'aide de la console Route 53 ARC, veuillez consulter [Lancement d'un changement de zone](#) (langue française non garantie) dans le Guide du développeur du Contrôleur de récupération d'application Amazon Route 53.

Pour démarrer un changement de zone à l'aide de la console

1. Ouvrez la console Amazon EC2 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 le nom de l'équilibreur de charge.
4. Dans l'onglet Intégrations, sous Contrôleur de récupération d'application Route 53, choisissez Démarrer le changement de zone.
5. Sélectionnez la zone de disponibilité depuis laquelle vous voulez déplacer le trafic.
6. Choisissez ou saisissez une date d'expiration pour le changement de zone. Au départ, un changement de zone peut être défini entre 1 minute et 3 jours (72 heures).

Tous les changements de zone sont temporaires. Vous devez définir une date d'expiration, mais vous pouvez mettre à jour les changements actifs ultérieurement pour définir une nouvelle date d'expiration.

7. Saisissez un commentaire. Vous pouvez mettre à jour le changement de zone ultérieurement pour modifier le commentaire, si vous le souhaitez.
8. Cochez la case pour confirmer que le lancement d'un changement de zone réduira la capacité de votre application en déplaçant le trafic hors de la zone de disponibilité.
9. Sélectionnez Démarrer.

Pour démarrer un changement de zone à l'aide du AWS CLI

Pour utiliser le changement de zone par programmation, veuillez consulter le [Guide des références d'API relatif au changement de zone](#) (langue française non garantie).

Mise à jour d'un changement de zone

Les étapes de cette procédure expliquent comment mettre à jour un changement de zone à l'aide de la console Amazon EC2. Pour connaître les étapes à suivre pour mettre à jour un changement de zone à l'aide de la console du Contrôleur de récupération d'application Amazon Route 53, veuillez consulter [Mise à jour d'un changement de zone](#) (langue française non garantie) dans le Guide du développeur du Contrôleur de récupération d'application Amazon Route 53.

Pour mettre à jour un changement de zone à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Load Balancing (Équilibrage de charge), choisissez Load Balancers (Équilibreur de charge).
3. Sélectionnez le nom d'un équilibreur de charge dont le changement de zone est actif.
4. Dans l'onglet Intégrations, sous Contrôleur de récupération d'application Route 53, choisissez Mettre à jour le changement de zone.

Cela ouvre la console Route 53 ARC pour poursuivre la mise à jour.

5. Pour Définir l'expiration du changement de zone, sélectionnez ou saisissez éventuellement une date d'expiration.
6. Pour Commentaire, modifiez éventuellement le commentaire existant ou saisissez-en un nouveau.

7. Choisissez Mettre à jour.

Pour mettre à jour un décalage de zone à l'aide du AWS CLI

Pour utiliser le changement de zone par programmation, veuillez consulter le [Guide des références d'API relatif au changement de zone](#) (langue française non garantie).

Annulation d'un changement de zone

Les étapes de cette procédure expliquent comment annuler un changement de zone à l'aide de la console Amazon EC2. Pour connaître les étapes à suivre pour annuler un changement de zone à l'aide de la console du Contrôleur de récupération d'application Amazon Route 53, veuillez consulter [Annulation d'un changement de zone](#) (langue française non garantie) dans le Guide du développeur du Contrôleur de récupération d'application Amazon Route 53.

Pour annuler un changement de zone à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Load Balancing (Équilibrage de charge), choisissez Load Balancers (Équilibreur de charge).
3. Sélectionnez le nom d'un équilibreur de charge dont le changement de zone est actif.
4. Dans l'onglet Intégrations, sous Contrôleur de récupération d'application Route 53, choisissez Annuler le changement de zone.

Cela ouvre la console Route 53 ARC pour poursuivre l'annulation.

5. Choisissez Annuler le changement de zone.
6. Dans la boîte de dialogue de confirmation, choisissez Confirmer.

Pour annuler un changement de zone à l'aide du AWS CLI

Pour utiliser le changement de zone par programmation, veuillez consulter le [Guide des références d'API relatif au changement de zone](#) (langue française non garantie).

Écouteurs pour vos Network Load Balancers

Un écouteur est un processus qui recherche les demandes de connexion à l'aide du protocole et du port que vous avez configurés. Avant de commencer à utiliser votre Network Load Balancer, vous devez ajouter au moins un écouteur. Si votre équilibreur de charge ne possède aucun écouteur, il ne peut pas recevoir le trafic des clients. La règle que vous définissez pour un écouteur détermine la manière dont l'équilibreur de charge achemine les demandes vers les cibles que vous enregistrez, comme les instances EC2.

Table des matières

- [Configuration des écouteurs](#)
- [Règles d'un écouteur](#)
- [Création d'un écouteur pour votre Network Load Balancer](#)
- [Écouteurs TLS pour votre Network Load Balancer](#)
- [Mise à jour d'un écouteur pour votre Network Load Balancer](#)
- [Mise à jour d'un écouteur TLS pour votre Network Load Balancer](#)
- [Suppression d'un écouteur pour votre Network Load Balancer](#)

Configuration des écouteurs

Les écouteurs prennent en charge les protocoles et ports suivants :

- Protocoles: TCP, TLS, UDP TCP_UDP
- Ports : 1 à 65535

Vous pouvez utiliser un écouteur TLS pour confier le travail de chiffrement et de déchiffrement à votre équilibreur de charge afin que vos applications puissent se concentrer sur leur logique métier. Si le protocole d'écoute est TLS, vous devez déployer un seul certificat de serveur SSL sur l'écouteur. Pour plus d'informations, consultez [Écouteurs TLS pour votre Network Load Balancer](#).

Si vous devez vous assurer que les cibles déchiffrent le trafic TLS plutôt que l'équilibreur de charge, vous pouvez créer un écouteur TCP sur le port 443 au lieu de créer un écouteur TLS. Avec un écouteur TCP, l'équilibreur de charge transmet le trafic chiffré aux cibles sans le déchiffrer.

Pour prendre en charge les protocoles TCP et UDP sur le même port, créez un écouteur TCP_UDP. Les groupes cibles pour un écouteur TCP_UDP doivent utiliser le protocole TCP_UDP.

Pour les Network Load Balancers à double pile, les seuls protocoles pris en charge sont TCP et TLS.

Vous pouvez l'utiliser WebSockets avec vos auditeurs.

Tout le trafic réseau envoyé vers un écouteur configuré est classé comme trafic prévu. Le trafic réseau qui ne correspond pas à un écouteur configuré est classé comme trafic imprévu. Les demandes ICMP autres que celles de type 3 sont également considérées comme du trafic non prévu. Les Network Load Balancers éliminent le trafic non prévu sans le transférer vers aucune cible. Les paquets de données TCP envoyés au port de l'écouteur pour un écouteur configuré qui ne sont pas de nouvelles connexions ou ne font pas partie d'une connexion TCP active sont rejetés avec une réinitialisation TCP (RST).

Pour plus d'informations, veuillez consulter [Demande de routage](#) (langue française non garantie) dans le Guide de l'utilisateur Elastic Load Balancing.

Règles d'un écouteur

Lorsque vous créez un écouteur, vous spécifiez une règle pour l'acheminement des requêtes. Cette règle achemine les demandes vers le groupe cible spécifié. Pour mettre à jour cette règle, consultez [Mise à jour d'un écouteur pour votre Network Load Balancer](#).

Création d'un écouteur pour votre Network Load Balancer

Un écouteur est un processus qui vérifie les demandes de connexion. Vous définissez un écouteur lorsque vous créez votre équilibreur de charge et vous pouvez ajouter des écouteurs à votre équilibreur de charge à tout moment.

Prérequis

- Vous devez spécifier un groupe cible pour la règle d'écouteur. Pour plus d'informations, consultez [Création d'un groupe cible pour votre Network Load Balancer](#).
- Vous devez spécifier un certificat SSL pour un écouteur TLS. L'équilibreur de charge utilise le certificat pour mettre fin à la connexion et déchiffrer les demandes des clients avant de les acheminer vers les cibles. Pour plus d'informations, consultez [Certificats de serveur](#).

Ajouter un écouteur

Vous configurez un écouteur avec un protocole et un port pour les connexions des clients vers l'équilibreur de charge, et un groupe cible pour la règle d'écouteur par défaut. Pour plus d'informations, consultez [Configuration des écouteurs](#).

Pour ajouter un écouteur à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Sélectionnez le nom de l'équilibreur de charge afin d'ouvrir sa page de détails.
4. Sous l'onglet Écouteurs, choisissez Ajouter un écouteur.
5. Pour Protocole, choisissez TCP, UDP, TCP_UDP ou TLS. Conservez le port par défaut ou entrez un autre port. Pour les Network Load Balancers à double pile, les seuls protocoles pris en charge sont TCP et TLS.
6. Pour Action par défaut, choisissez un groupe cible disponible.
7. [Écouteurs TLS] Pour Stratégie de sécurité, nous vous recommandons de conserver la stratégie de sécurité par défaut.
8. [Écouteurs TLS] Pour Certificat SSL par défaut, effectuez l'une des opérations suivantes :
 - Si vous avez créé ou importé un certificat à l'aide de AWS Certificate Manager, choisissez From ACM et choisissez le certificat.
 - Si vous avez chargé un certificat à l'aide d'IAM, choisissez Depuis IAM, puis sélectionnez le certificat.
9. [Écouteurs TLS] Pour la stratégie ALPN, choisissez une stratégie pour activer ALPN ou choisissez Aucun pour désactiver ALPN. Pour plus d'informations, consultez [Stratégies ALPN](#).
10. Choisissez Ajouter.
11. [Écouteurs TLS] Pour ajouter une liste de certificats facultatifs à utiliser avec le protocole SNI, consultez [Ajouter des certificats à la liste des certificats](#).

Pour ajouter un écouteur à l'aide du AWS CLI

Utilisez la commande [create-listener](#) pour créer l'écouteur.

Écouteurs TLS pour votre Network Load Balancer

Pour utiliser un écouteur TLS, vous devez déployer au moins un certificat de serveur sur votre équilibreur de charge. L'équilibreur de charge utilise un certificat de serveur pour mettre fin à la connexion frontale, puis déchiffrer les demandes des clients avant de les envoyer aux cibles. Veuillez noter que si vous devez transmettre du trafic chiffré aux cibles sans que l'équilibreur de charge le déchiffre, créez un écouteur TCP sur le port 443 au lieu de créer un écouteur TLS. L'équilibreur de charge transmet la demande à la cible telle quelle, sans la déchiffrer.

Elastic Load Balancing utilise une configuration de négociation TLS (ou stratégie de sécurité) pour négocier des connexions TLS entre un client et l'équilibreur de charge. Une stratégie de sécurité est une combinaison de protocoles et de chiffrements. Le protocole établit une connexion sécurisée entre un client et un serveur, et s'assure que toutes les données transmises entre le client et votre équilibreur de charge sont privées. Un chiffrement est un algorithme de chiffrement qui utilise des clés de chiffrement pour créer un message codé. Les protocoles utilisent plusieurs chiffrements pour chiffrer les données sur Internet. Pendant le processus de négociation de connexion, le client et l'équilibreur de charge présentent une liste de chiffrements et de protocoles pris en charge par chacun d'entre eux dans l'ordre de préférence. Le premier chiffrement sur la liste du serveur qui correspond à l'un des chiffrements du client est sélectionné pour la connexion sécurisée.

Les Network Load Balancers ne prennent pas en charge la renégociation TLS ni l'authentification TLS mutuelle (mTLS). Pour la prise en charge de mTLS, créez un écouteur TCP au lieu d'un écouteur TLS. L'équilibreur de charge transmet la demande en l'état pour que vous puissiez implémenter mTLS sur la cible.

Pour créer un écouteur TLS, consultez [Ajouter un écouteur](#). Pour les démonstrations associées, veuillez consulter [Prise en charge de TLS sur Network Load Balancer](#) et [Prise en charge de SNI sur Network Load Balancer](#) (langue française non garantie).

Certificats de serveur

L'équilibreur de charge exige des certificats X.509 (certificats de serveur). Les certificats constituent une forme numérique d'identification émise par une autorité de certification (AC). Un certificat contient les informations d'identification, une période de validité, une clé publique, un numéro de série et la signature numérique de l'émetteur.

Lorsque vous créez un certificat à utiliser avec votre équilibreur de charge, vous devez spécifier un nom de domaine. Le nom de domaine figurant sur le certificat doit correspondre à l'enregistrement

du nom de domaine personnalisé, afin que nous puissions vérifier la connexion TLS. S'ils ne correspondent pas, le trafic n'est pas chiffré.

Vous devez spécifier un nom de domaine complet (FQDN) pour votre certificat, tel que `www.example.com` ou un nom de domaine apex tel que `example.com`. Vous pouvez également utiliser un astérisque (*) comme caractère générique pour protéger plusieurs noms de sites dans le même domaine. Lorsque vous demandez un certificat générique, l'astérisque (*) doit se trouver tout à gauche du nom de domaine et ne peut protéger qu'un seul niveau de sous-domaine. Par exemple, `*.example.com` protège `corp.example.com` et `images.example.com`, mais ne peut pas protéger `test.login.example.com`. Notez également que `*.example.com` ne protège que les sous-domaines de `example.com`, il ne protège pas le domaine strict ou apex (`example.com`). Le nom générique apparaît dans le champ Objet et dans l'extension Autre nom de l'objet du certificat. Pour plus d'informations sur les certificats publics, consultez [Demande de certificat public](#) du Guide de l'utilisateur AWS Certificate Manager .

Nous vous recommandons de créer des certificats pour vos équilibreurs de charge à l'aide d'[AWS Certificate Manager \(ACM\)](#). ACM s'intègre à Elastic Load Balancing afin que vous puissiez déployer le certificat sur votre équilibreur de charge. Pour plus d'informations, consultez le [Guide de l'utilisateur AWS Certificate Manager](#).

Vous pouvez également utiliser les outils TLS pour créer une demande de signature de certificat (CSR), puis faire signer la CSR par une autorité de certification pour produire un certificat, puis importer le certificat dans ACM ou télécharger le certificat vers AWS Identity and Access Management (IAM). Pour plus d'informations, veuillez consulter [Importation de certificats](#) dans le Guide de l'utilisateur AWS Certificate Manager ou [Gestion des certificats de serveur](#) dans le Guide de l'utilisateur IAM.

Table des matières

- [Algorithmes clés supportés](#)
- [Certificat par défaut](#)
- [Liste de certificats](#)
- [Renouvellement des certificats](#)

Algorithmes clés supportés

- RSA 1024 bits
- RSA 2048 bits

- RSA 3072 bits
- ECDSA 256 bits
- ECDSA 384 bits
- ECDSA 512 bits

Certificat par défaut

Lorsque vous créez un écouteur TLS, vous devez spécifier précisément un certificat par défaut. Ce certificat est connu comme le certificat par défaut. Vous pouvez remplacer le certificat par défaut après avoir créé l'écouteur TLS. Pour plus d'informations, consultez [Remplacer le certificat par défaut](#).

Si vous spécifiez des certificats supplémentaires dans une [liste de certificats](#), le certificat par défaut est uniquement utilisé si un client se connecte sans utiliser le protocole SNI (Server Name Indication) pour spécifier un nom d'hôte ou si la liste de certificats ne contient aucun certificat correspondant.

Si vous ne spécifiez aucun certificat supplémentaire, mais que vous devez héberger plusieurs applications sécurisées via un seul équilibreur de charge, vous pouvez utiliser un certificat générique ou ajouter un Subject Alternative Name (SAN) pour chaque domaine supplémentaire à votre certificat.

Liste de certificats

Après avoir créé un écouteur TLS, il comprend un certificat par défaut et une liste de certificats vide. Vous pouvez éventuellement ajouter des certificats à la liste de certificats pour l'écouteur. Grâce à une liste de certificats, l'équilibreur de charge peut ainsi prendre en charge plusieurs domaines sur le même port et fournir un certificat différent pour chaque domaine. Pour plus d'informations, consultez [Ajouter des certificats à la liste des certificats](#).

L'équilibreur de charge prend également en charge un algorithme de sélection de certificat intelligent avec prise en charge de SNI. Si le nom d'hôte fourni par un client correspond à un seul certificat de la liste de certificats, l'équilibreur de charge sélectionne ce certificat. Si un nom d'hôte fourni par un client correspond à plusieurs certificats de la liste de certificats, l'équilibreur de charge sélectionne celui qui est le mieux adapté par rapport aux capacités du client. La sélection des certificats dépend des critères suivants, dans l'ordre indiqué :

- Algorithme de hachage (préférer SHA plutôt que MD5)

- Longueur de clé (préférer la plus longue)
- Période de validité

Les entrées de journaux d'accès de l'équilibreur de charge indiquent le nom d'hôte spécifié par le client et le certificat présenté à ce dernier. Pour plus d'informations, consultez [Entrées des journaux d'accès](#).

Renouvellement des certificats

Chaque certificat est associé à une durée de validité. Vous devez veiller à renouveler ou remplacer chaque certificat pour votre équilibreur de charge avant la fin de la période de validité. Cela inclut le certificat par défaut les certificats dans une liste de certificats. Le renouvellement ou le remplacement d'un certificat n'affecte pas les demandes en cours reçues par le nœud d'équilibreur de charge et qui sont en attente d'acheminement vers une cible saine. Après le renouvellement d'un certificat, les nouvelles demandes utilisent le certificat renouvelé. Après le remplacement d'un certificat, les nouvelles demandes utilisent le nouveau certificat.

La gestion des renouvellements et des remplacements s'effectue comme suit :

- Les certificats fournis AWS Certificate Manager et déployés sur votre équilibreur de charge peuvent être renouvelés automatiquement. ACM essaie de renouveler les certificats avant leur expiration. Pour plus d'informations, consultez [Renouvellement géré](#) dans le Guide de l'utilisateur AWS Certificate Manager .
- Si vous avez importé un certificat dans ACM, vous devez surveiller sa date d'expiration et le renouveler avant qu'il n'arrive à expiration. Pour plus d'informations, consultez la section [Importation de certificats](#) dans le AWS Certificate Manager Guide de l'utilisateur.
- Si vous avez importé un certificat dans IAM, vous devez en créer un nouveau, l'importer dans ACM ou IAM, l'ajouter dans votre équilibreur de charge et supprimer de votre équilibreur de charge le certificat arrivé à expiration.

Stratégies de sécurité

Lorsque vous créez un écouteur TLS, vous devez sélectionner une stratégie de sécurité. Vous pouvez mettre à jour la stratégie de sécurité si nécessaire. Pour plus d'informations, consultez [Mettre à jour la stratégie de sécurité](#).

Considérations :

- Il s'agit `ELBSecurityPolicy-TLS13-1-2-2021-06` de la politique de sécurité par défaut pour les écouteurs TLS créés à l'aide du AWS Management Console
 - Nous recommandons la politique `ELBSecurityPolicy-TLS13-1-2-2021-06` de sécurité, qui inclut le protocole TLS 1.3 et qui est rétrocompatible avec le protocole TLS 1.2.
- Il s'agit `ELBSecurityPolicy-2016-08` de la politique de sécurité par défaut pour les écouteurs TLS créés à l'aide du AWS CLI
- Vous pouvez choisir la politique de sécurité qui est utilisée pour les connexions frontales, mais pas pour les connexions dorsales.
 - Pour les connexions backend, si votre écouteur TLS utilise une stratégie de sécurité TLS 1.3, c'est la stratégie de sécurité `ELBSecurityPolicy-TLS13-1-0-2021-06` qui est utilisée. Dans le cas contraire, la stratégie de sécurité `ELBSecurityPolicy-2016-08` est utilisée pour les connexions backend.
- Pour respecter les normes de conformité et de sécurité qui nécessitent la désactivation de certaines versions du protocole TLS, ou pour prendre en charge les anciens clients nécessitant des chiffrements obsolètes, vous pouvez utiliser l'une des politiques de sécurité. `ELBSecurityPolicy-TLS-` Vous pouvez activer les journaux d'accès pour obtenir des informations sur les requêtes TLS envoyées à votre Network Load Balancer, analyser les modèles de trafic TLS, gérer les mises à niveau des politiques de sécurité et résoudre les problèmes. Activez la journalisation des accès pour votre équilibreur de charge et examinez les entrées du journal d'accès correspondantes. Pour plus d'informations, veuillez consulter [Accès aux journaux](#) (langue française non garantie) et [Exemples de requêtes du Network Load Balancer](#).
- Vous pouvez restreindre les politiques de sécurité accessibles aux utilisateurs de votre pays Comptes AWS et en AWS Organizations utilisant les [clés de condition Elastic Load Balancing](#) dans vos politiques IAM et de contrôle des services (SCP), respectivement. Pour plus d'informations, voir [Politiques de contrôle des services \(SCP\)](#) dans le guide de l'AWS Organizations utilisateur

Stratégies de sécurité TLS 1.3

Elastic Load Balancing fournit les politiques de sécurité TLS 1.3 suivantes pour les Network Load Balancers :

- `ELBSecurityPolicy-TLS13-1-2-2021-06`(Recommandé)
- `ELBSecurityPolicy-TLS13-1-2-Res-2021-06`

- ELBSecurityPolicy-TLS13-1-2-Ext1-2021-06
- ELBSecurityPolicy-TLS13-1-2-Ext2-2021-06
- ELBSecurityPolicy-TLS13-1-1-2021-06
- ELBSecurityPolicy-TLS13-1-0-2021-06
- ELBSecurityPolicy-TLS13-1-3-2021-06

Politiques de sécurité FIPS

La norme fédérale de traitement de l'information (FIPS) est une norme gouvernementale américaine et canadienne qui spécifie les exigences de sécurité pour les modules cryptographiques qui protègent les informations sensibles. Pour en savoir plus, consultez la [norme fédérale de traitement de l'information \(FIPS\) 140](#) sur la page Conformité à la sécurité du AWS cloud.

Toutes les politiques FIPS tirent parti du module cryptographique AWS-LC validé FIPS. Pour en savoir plus, consultez la page du module [cryptographique AWS-LC sur le site du programme de validation du module](#) cryptographique du NIST.

Elastic Load Balancing fournit les politiques de sécurité FIPS suivantes pour Network Load Balancer :

- ELBSecurityPolicy-TLS13-1-3-FIPS-2023-04
- ELBSecurityPolicy-TLS13-1-2-Res-FIPS-2023-04
- ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04(Recommandé)
- ELBSecurityPolicy-TLS13-1-2-Ext0-FIPS-2023-04
- ELBSecurityPolicy-TLS13-1-2-Ext1-FIPS-2023-04
- ELBSecurityPolicy-TLS13-1-2-Ext2-FIPS-2023-04
- ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04
- ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04

Politiques FS prises en charge

Elastic Load Balancing fournit les politiques de sécurité compatibles FS (Forward Secrecy) suivantes pour les Network Load Balancers :

- ELBSecurityPolicy-FS-1-2-Res-2020-10
- ELBSecurityPolicy-FS-1-2-Res-2019-08

- ELBSecurityPolicy-FS-1-2-2019-08
- ELBSecurityPolicy-FS-1-1-2019-08
- ELBSecurityPolicy-FS-2018-06

Politiques de sécurité TLS 1.0 - 1.2

Elastic Load Balancing fournit les politiques de sécurité TLS 1.0 à 1.2 suivantes pour les Network Load Balancers :

- ELBSecurityPolicy-TLS-1-2-Ext-2018-06
- ELBSecurityPolicy-TLS-1-2-2017-01
- ELBSecurityPolicy-TLS-1-1-2017-01
- ELBSecurityPolicy-2016-08
- ELBSecurityPolicy-TLS-1-0-2015-04
- ELBSecurityPolicy-2015-05(identique à **ELBSecurityPolicy-2016-08**)

Protocoles et chiffrements TLS

TLS 1.3

Le tableau suivant décrit les protocoles et chiffrements TLS pris en charge pour les politiques de sécurité TLS 1.3 disponibles.

Remarque : Le ELBSecurityPolicy- préfixe a été supprimé des noms des politiques dans la ligne des politiques de sécurité.

Exemple : La politique de sécurité ELBSecurityPolicy-TLS13-1-2-2021-06 s'affiche sous la forme TLS13-1-2-2021-06.

Stratégies de sécurité	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
Protocoles TLS							
Protocol-TLSv1							✓
Protocol-TLSv1.1						✓	✓
Protocol-TLSv1.2	✓		✓	✓	✓	✓	✓
Protocole-TLSv1.3	✓	✓	✓	✓	✓	✓	✓
Chiffrements TLS							
TLS_AES_128_GCM_SHA256	✓	✓	✓	✓	✓	✓	✓
TLS_AES_256_GCM_SHA384	✓	✓	✓	✓	✓	✓	✓
TLS_CHACHA20_POLY1305_SHA256	✓	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128	✓		✓	✓	✓	✓	✓

Stratégies de sécurité	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
-GCM- SHA256							
ECDHE- RSA- AES128- GCM- SHA256	✓		✓	✓	✓	✓	✓
ECDHE- ECDSA- AES128- SHA256	✓			✓	✓	✓	✓
ECDHE- RSA- AES128- SHA256	✓			✓	✓	✓	✓
ECDHE- ECDSA- AES128- SHA				✓		✓	✓
ECDHE- RSA- AES128- SHA				✓		✓	✓

Stratégies de sécurité	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
ECDHE- ECDSA- AES256- -GCM- SHA384	✓		✓	✓	✓	✓	✓
ECDHE- RSA- AES256- GCM- SHA384	✓		✓	✓	✓	✓	✓
ECDHE- ECDSA- AES256- SHA384	✓			✓	✓	✓	✓
ECDHE- RSA- AES256- SHA384	✓			✓	✓	✓	✓
ECDHE- RSA- AES256- SHA				✓		✓	✓
ECDHE- ECDSA- AES256- SHA				✓		✓	✓

Stratégies de sécurité	TLS13-1-2-2021-06	TLS13-1-3-2021-06	TLS13-1-2-Res-2021-06	TLS13-1-2-Ext2-2021-06	TLS13-1-2-Ext1-2021-06	TLS13-1-1-2021-06	TLS13-1-0-2021-06
AES128-GCM-SHA256				✓	✓	✓	✓
AES128-SHA256				✓	✓	✓	✓
AES128-SHA				✓		✓	✓
AES256-GCM-SHA384				✓	✓	✓	✓
AES256-SHA256				✓	✓	✓	✓
AES256-SHA				✓		✓	✓

Pour créer un écouteur TLS utilisant une politique TLS 1.3 à l'aide de la CLI

Utilisez la commande [create-listener](#) avec n'importe quelle politique de sécurité [TLS 1.3](#).

L'exemple utilise la politique `ELBSecurityPolicy-TLS13-1-2-2021-06` de sécurité.

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-2021-06
```

Pour modifier un écouteur TLS afin d'utiliser une politique TLS 1.3 à l'aide de la CLI

Utilisez la commande [modify-listener](#) avec n'importe quelle politique de sécurité [TLS 1.3](#).

L'exemple utilise la politique `ELBSecurityPolicy-TLS13-1-2-2021-06` de sécurité.

```
aws elbv2 modify-listener \  
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-  
Load-balancer/abcdef01234567890/1234567890abcdef0 \  
--ssl-policy ELBSecurityPolicy-TLS13-1-2-2021-06
```

Pour afficher les politiques de sécurité utilisées par un écouteur à l'aide de la CLI

Utilisez la commande [describe-listener](#) avec le arn de votre écouteur.

```
aws elbv2 describe-listener \  
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-  
Load-balancer/abcdef01234567890/1234567890abcdef0
```

Pour afficher la configuration d'une politique de sécurité TLS 1.3 à l'aide de la CLI

Utilisez la [describe-ssl-policies](#) commande avec n'importe quelle [politique de sécurité TLS 1.3](#).

L'exemple utilise la politique `ELBSecurityPolicy-TLS13-1-2-2021-06` de sécurité.

```
aws elbv2 describe-ssl-policies \  
--names ELBSecurityPolicy-TLS13-1-2-2021-06
```

FIPS

Important

Les politiques `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04` `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04` sont fournies uniquement à des fins de compatibilité avec les anciennes versions. Bien qu'ils utilisent la cryptographie FIPS à l'aide du module FIPS140, ils peuvent ne pas être conformes aux dernières directives du NIST pour la configuration TLS.

Le tableau suivant décrit les protocoles et chiffrements TLS pris en charge pour les politiques de sécurité FIPS disponibles.

Remarque : Le ELBSecurityPolicy- préfixe a été supprimé des noms des politiques dans la ligne des politiques de sécurité.

Exemple : La politique de sécurité ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04 s'affiche sous la forme TLS13-1-2-FIPS-2023-04.

Stratégies de sécurité	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
Protocoles TLS								
Protocol-TLSv1								✓
Protocol-TLSv1.1							✓	✓
Protocol-TLSv1.2		✓	✓	✓	✓	✓	✓	✓
Protocole - TLSv1.3	✓	✓	✓	✓	✓	✓	✓	✓
Chiffrements TLS								
TLS_AES_128_GCM_SHA256		✓	✓	✓	✓	✓	✓	✓
TLS_AES_256_GCM_SHA384		✓	✓	✓	✓	✓	✓	✓

Stratégies de sécurité	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-ECD SA-AES128 -GCM-SHA256		✓	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓		✓	✓	✓	✓	✓	✓
ECDHE-ECD SA-AES128 -SHA256			✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256			✓	✓	✓	✓	✓	✓

Stratégies de sécurité	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-ECD SA-AES128 -SHA				✓		✓	✓	✓
ECDHE-RSA-AES128-SHA				✓		✓	✓	✓
ECDHE-ECD SA-AES256 -GCM-SHA3 84	✓	✓	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓	✓	✓

Stratégies de sécurité	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
ECDHE-ECD SA-AES256 - SHA384			✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-S HA384		✓	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA				✓		✓	✓	✓
ECDHE-ECD SA-AES256 -SHA				✓		✓	✓	✓
AES128-GCM-SHA256					✓	✓	✓	✓

Stratégies de sécurité	TLS13-1-3-FIPS-2023-04	TLS13-1-2-Res-FIPS-2023-04	TLS13-1-2-FIPS-2023-04	TLS13-1-2-Ext0-FIPS-2023-04	TLS13-1-2-Ext1-FIPS-2023-04	TLS13-1-2-Ext2-FIPS-2023-04	TLS13-1-1-FIPS-2023-04	TLS13-1-0-FIPS-2023-04
AES128-SHA256					✓	✓	✓	✓
AES128-SHA						✓	✓	✓
AES256-GCM-SHA384					✓	✓	✓	✓
AES256-SHA256					✓	✓	✓	✓
AES256-SHA						✓	✓	✓

Pour créer un écouteur TLS utilisant une politique FIPS à l'aide de la CLI

Utilisez la commande [create-listener](#) avec n'importe quelle politique de sécurité [FIPS](#).

L'exemple utilise la politique `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` de sécurité.

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

Pour modifier un écouteur TLS afin d'utiliser une politique FIPS à l'aide de la CLI

[Utilisez la commande modify-listener](#) avec n'importe quelle politique de sécurité [FIPS](#).

L'exemple utilise la politique `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` de sécurité.

```
aws elbv2 modify-listener \  
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-  
Load-balancer/abcdef01234567890/1234567890abcdef0 \  
--ssl-policy ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

Pour afficher les politiques de sécurité utilisées par un écouteur à l'aide de la CLI

Utilisez la commande [describe-listener](#) avec le arn de votre écouteur.

```
aws elbv2 describe-listener \  
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-  
Load-balancer/abcdef01234567890/1234567890abcdef0
```

Pour afficher la configuration d'une politique de sécurité FIPS à l'aide de la CLI

Utilisez la [describe-ssl-policies](#) commande avec n'importe quelle [politique de sécurité FIPS](#).

L'exemple utilise la politique `ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04` de sécurité.

```
aws elbv2 describe-ssl-policies \  
--names ELBSecurityPolicy-TLS13-1-2-FIPS-2023-04
```

FS

Le tableau suivant décrit les protocoles et chiffrements TLS pris en charge pour les politiques de sécurité prises en charge par FS disponibles.

Remarque : Le `ELBSecurityPolicy-` préfixe a été supprimé des noms des politiques dans la ligne des politiques de sécurité.

Exemple : La politique de sécurité `ELBSecurityPolicy-FS-2018-06` s'affiche sous la forme `FS-2018-06`.

Stratégies de sécurité	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
Protocoles TLS						
Protocol-TLSv1	✓					✓
Protocol-TLSv1.1	✓				✓	✓
Protocol-TLSv1.2	✓	✓	✓	✓	✓	✓
Chiffrements TLS						
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓		✓	✓	✓	✓

Stratégies de sécurité	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
ECDHE-RSA-AES128-SHA256	✓		✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA	✓			✓	✓	✓
ECDHE-RSA-AES128-SHA	✓			✓	✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓

Stratégies de sécurité	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
ECDHE- ECDSA- AES256- SHA384	✓		✓	✓	✓	✓
ECDHE- RSA- AES256-S HA384	✓		✓	✓	✓	✓
ECDHE- RSA- AES256-S HA	✓			✓	✓	✓
ECDHE- ECDSA- AES256- SHA	✓			✓	✓	✓
AES128- GCM- SHA256	✓					
AES128- SHA256	✓					
AES128- SHA	✓					

Stratégies de sécurité	Default	FS-1-2-Res-2020-10	FS-1-2-Res-2019-08	FS-1-2-2019-08	FS-1-1-2019-08	FS-2018-06
AES256-GCM-SHA384	✓					
AES256-SHA256	✓					
AES256-SHA	✓					

Pour créer un écouteur TLS utilisant une politique prise en charge par FS à l'aide de la CLI

Utilisez la commande [create-listener](#) avec n'importe quelle politique de sécurité [prise en charge par FS](#).

L'exemple utilise la politique `ELBSecurityPolicy-FS-2018-06` de sécurité.

```
aws elbv2 create-listener --name my-listener \
--protocol TLS --port 443 \
--ssl-policy ELBSecurityPolicy-FS-2018-06
```

Pour modifier un écouteur TLS afin d'utiliser une politique prise en charge par FS à l'aide de la CLI

Utilisez la commande [modify-listener](#) avec n'importe quelle politique de sécurité prise en charge par [FS](#).

L'exemple utilise la politique `ELBSecurityPolicy-FS-2018-06` de sécurité.

```
aws elbv2 modify-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \
```

```
--ssl-policy ELBSecurityPolicy-FS-2018-06
```

Pour afficher les politiques de sécurité utilisées par un écouteur à l'aide de la CLI

Utilisez la commande [describe-listener](#) avec le arn de votre écouteur.

```
aws elbv2 describe-listener \
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Pour afficher la configuration d'une politique de sécurité prise en charge par FS à l'aide de la CLI

Utilisez la [describe-ssl-policies](#) commande avec n'importe quelle [politique de sécurité prise en charge par FS](#).

L'exemple utilise la politique *ELBSecurityPolicy-FS-2018-06* de sécurité.

```
aws elbv2 describe-ssl-policies \
--names ELBSecurityPolicy-FS-2018-06
```

TLS 1.0 - 1.2

Le tableau suivant décrit les protocoles et chiffrements TLS pris en charge pour les politiques de sécurité TLS 1.0-1.2 disponibles.

Remarque : Le *ELBSecurityPolicy-* préfixe a été supprimé des noms des politiques dans la ligne des politiques de sécurité.

Exemple : La politique de sécurité *ELBSecurityPolicy-TLS-1-2-Ext-2018-06* s'affiche sous la forme *TLS-1-2-Ext-2018-06*.

Stratégies de sécurité	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
Protocoles TLS					

Stratégies de sécurité	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
Protocol-TLSv1	✓				✓
Protocol-TLSv1.1	✓			✓	✓
Protocol-TLSv1.2	✓	✓	✓	✓	✓
Chiffrements TLS					
ECDHE-ECD SA-AES128 -GCM-SHA2 56	✓	✓	✓	✓	✓
ECDHE-RSA -AES128-G CM-SHA256	✓	✓	✓	✓	✓
ECDHE-ECD SA-AES128- SHA256	✓	✓	✓	✓	✓
ECDHE-RSA -AES128-S HA256	✓	✓	✓	✓	✓

Stratégies de sécurité	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
ECDHE-ECD SA-AES128- SHA	✓	✓		✓	✓
ECDHE-RSA -AES128-S HA	✓	✓		✓	✓
ECDHE-ECD SA-AES256 -GCM-SHA3 84	✓	✓	✓	✓	✓
ECDHE-RSA -AES256-G CM-SHA384	✓	✓	✓	✓	✓
ECDHE-ECD SA-AES256- SHA384	✓	✓	✓	✓	✓
ECDHE-RSA -AES256-S HA384	✓	✓	✓	✓	✓
ECDHE-RSA -AES256-S HA	✓	✓		✓	✓

Stratégies de sécurité	Default	TLS-1-2-Ext-2018-06	TLS-1-2-2017-01	TLS-1-1-2017-01	TLS-1-0-2015-04*
ECDHE-ECD SA-AES256- SHA	✓	✓		✓	✓
AES128-GC M-SHA256	✓	✓	✓	✓	✓
AES128-SH A256	✓	✓	✓	✓	✓
AES128-SH A	✓	✓		✓	✓
AES256-GC M-SHA384	✓	✓	✓	✓	✓
AES256-SH A256	✓	✓	✓	✓	✓
AES256-SH A	✓	✓		✓	✓
DES-CBC3- SHA					✓

* N'utilisez pas cette stratégie, sauf si vous devez prendre en charge un client hérité nécessitant le chiffrement DES-CBC3-SHA, qui est un chiffrement faible.

Pour créer un écouteur TLS utilisant une politique TLS 1.0-1.2 à l'aide de la CLI

Utilisez la commande [create-listener](#) avec n'importe quelle politique de sécurité compatible avec le [protocole TLS 1.0-1.2](#).

L'exemple utilise la politique `ELBSecurityPolicy-2016-08` de sécurité.

```
aws elbv2 create-listener --name my-listener \  
--protocol TLS --port 443 \  
--ssl-policy ELBSecurityPolicy-2016-08
```

Pour modifier un écouteur TLS afin d'utiliser une politique TLS 1.0-1.2 à l'aide de la CLI

Utilisez la commande [modify-listener avec n'importe quelle politique de sécurité](#) compatible avec le [protocole TLS 1.0-1.2](#).

L'exemple utilise la politique `ELBSecurityPolicy-2016-08` de sécurité.

```
aws elbv2 modify-listener \  
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0 \  
--ssl-policy ELBSecurityPolicy-2016-08
```

Pour afficher les politiques de sécurité utilisées par un écouteur à l'aide de la CLI

Utilisez la commande [describe-listener](#) avec le arn de votre écouteur.

```
aws elbv2 describe-listener \  
--listener-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:listener/app/my-load-balancer/abcdef01234567890/1234567890abcdef0
```

Pour afficher la configuration d'une politique de sécurité TLS 1.0-1.2 à l'aide de la CLI

Utilisez la [describe-ssl-policies](#) commande avec n'importe quelle politique de sécurité [compatible avec le protocole TLS 1.0-1.2](#).

L'exemple utilise la politique `ELBSecurityPolicy-2016-08` de sécurité.

```
aws elbv2 describe-ssl-policies \  
--names ELBSecurityPolicy-2016-08
```

Stratégies ALPN

Application-Layer Protocol Negotiation (ALPN) est une extension TLS qui est envoyée sur les messages de liaison Hello TLS initiaux. ALPN permet à la couche d'application de négocier les protocoles à utiliser sur une connexion sécurisée, telle que HTTP/1 et HTTP/2.

Lorsque le client lance une connexion ALPN, l'équilibreur de charge compare la liste des préférences ALPN client à sa stratégie ALPN. Si le client prend en charge un protocole de la stratégie ALPN, l'équilibreur de charge établit la connexion en fonction de la liste des préférences de la stratégie ALPN. Sinon, l'équilibreur de charge n'utilise pas ALPN.

Stratégies ALPN prises en charge

Les stratégies ALPN prises en charge sont les suivantes :

HTTP1only

Négocier uniquement HTTP/1.*. La liste des préférences ALPN est http/1.1, http/1.0.

HTTP2only

Négocier uniquement HTTP/2. La liste des préférences ALPN est h2.

HTTP2optional

Privilégiez HTTP/1.* par rapport à HTTP/2 (ce qui peut être utile pour les tests HTTP/2). La liste des préférences ALPN est http/1.1, http/1.0, h2.

HTTP2Preferred

Privilégiez HTTP/2 par rapport à HTTP/1.*. La liste des préférences ALPN est h2, http/1.1, http/1.0.

None

Ne négociez pas ALPN. Il s'agit de l'option par défaut.

Activer les connexions ALPN

Vous pouvez activer les connexions ALPN lorsque vous créez ou modifiez un écouteur TLS. Pour plus d'informations, consultez [Ajouter un écouteur](#) et [Mettre à jour la stratégie ALPN](#).

Mise à jour d'un écouteur pour votre Network Load Balancer

Vous pouvez mettre à jour le protocole d'écouteur, le port d'écouteur ou le groupe cible qui reçoit le trafic provenant de l'action de transfert. L'action par défaut, également connue sous le nom de règle par défaut, transmet les demandes au groupe cible sélectionné.

Si vous modifiez le protocole de TCP ou UDP en TLS, vous devez spécifier une stratégie de sécurité et un certificat de serveur. Si vous modifiez le protocole de TLS en TCP ou UDP, la stratégie de sécurité et le certificat de serveur sont supprimés.

Lorsque le groupe cible de l'action par défaut de l'écouteur est mis à jour, les nouvelles connexions sont acheminées vers le groupe cible nouvellement configuré. Toutefois, cela n'a aucun effet sur les connexions actives créées avant cette modification. Ces connexions actives restent associées à la cible dans le groupe cible d'origine pendant une heure au maximum si du trafic est envoyé, ou jusqu'à l'expiration du délai d'inactivité si aucun trafic n'est envoyé, selon la première éventualité. Le paramètre `Connection termination on deregistration` n'est pas appliqué lors de la mise à jour de l'écouteur, comme il l'est lors de l'annulation d'enregistrement des cibles.

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

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Choisissez le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Dans l'onglet Écouteurs, choisissez le texte dans la colonne Protocole : port pour ouvrir la page détaillée de l'écouteur.
5. Choisissez Modifier.
6. (Facultatif) Modifiez les valeurs spécifiées pour Protocole et Port selon vos besoins.
7. (Facultatif) Choisissez un autre groupe cible pour l'Action par défaut.
8. (Facultatif) Ajoutez, mettez à jour ou supprimez des balises en fonction des besoins.
9. Sélectionnez Enregistrer les modifications.

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

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

Mise à jour d'un écouteur TLS pour votre Network Load Balancer

Après avoir créé un écouteur TLS, vous pouvez remplacer le certificat par défaut, ajouter ou supprimer des certificats de la liste des certificats, mettre à jour la stratégie de sécurité ou mettre à jour la stratégie ALPN.

Tâches

- [Remplacer le certificat par défaut](#)
- [Ajouter des certificats à la liste des certificats](#)
- [Supprimer des certificats de la liste des certificats](#)
- [Mettre à jour la stratégie de sécurité](#)
- [Mettre à jour la stratégie ALPN](#)

Remplacer le certificat par défaut

Vous pouvez remplacer le certificat par défaut de votre écouteur TLS à l'aide de la procédure qui suit. Pour plus d'informations, consultez [Certificat par défaut](#).

Pour remplacer le certificat par défaut à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers (Équilibreurs de charge).
3. Choisissez le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Dans l'onglet Écouteurs, choisissez le texte dans la colonne Protocole : port pour ouvrir la page détaillée de l'écouteur.
5. Pour Default SSL certificate (Certificat SSL par défaut), effectuez l'une des opérations suivantes :
 - Si vous avez créé ou importé un certificat à l'aide de AWS Certificate Manager, choisissez From ACM et choisissez le certificat.
 - Si vous avez chargé un certificat à l'aide d'IAM, choisissez Depuis IAM, puis sélectionnez le certificat.
6. Sélectionnez Enregistrer les modifications.

Pour remplacer le certificat par défaut à l'aide du AWS CLI

Utilisez la commande [modify-listener](#) avec l'option `--certificates`.

Ajouter des certificats à la liste des certificats

Vous pouvez ajouter des certificats à la liste destinée à votre écouteur à l'aide de la procédure qui suit. Lorsque vous créez un écouteur TLS pour la première fois, la liste des certificats est vide. Vous pouvez ajouter un ou plusieurs certificats. Vous pouvez éventuellement ajouter le certificat par défaut pour vous assurer qu'il est utilisé avec le protocole SNI, même s'il est remplacé en tant que certificat par défaut. Pour plus d'informations, consultez [Liste de certificats](#).

Ajout de certificats à la liste des certificats à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Choisissez le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Dans l'onglet Écouteurs, choisissez le texte dans la colonne Protocole : port pour ouvrir la page détaillée de l'écouteur.
5. Cochez la case correspondant à l'écouteur et choisissez Actions, Ajouter des certificats SSL pour SNI.
6. Pour ajouter des certificats déjà gérés par ACM ou IAM, sélectionnez les cases à cocher pour les certificats et choisissez Inclure comme étant en attente ci-dessous.
7. Si vous avez un certificat qui n'est pas géré par ACM ou IAM, choisissez Importer un certificat, complétez le formulaire, puis choisissez Importer.
8. Choisissez Ajouter des certificats en attente.

Pour ajouter un certificat à la liste des certificats à l'aide du AWS CLI

Utilisez la commande [add-listener-certificates](#).

Supprimer des certificats de la liste des certificats

Vous pouvez supprimer des certificats de la liste destinée à un écouteur TLS à l'aide de la procédure suivante. Pour supprimer le certificat par défaut d'un écouteur TLS, consultez [Remplacer le certificat par défaut](#).

Suppression de certificats de la liste des certificats à l'aide de la console

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

2. Dans le volet de navigation, choisissez Load Balancers.
3. Choisissez le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Dans l'onglet Écouteurs, choisissez le texte dans la colonne Protocole : port pour ouvrir la page détaillée de l'écouteur.
5. Cochez la case correspondant à l'écouteur et choisissez Actions, Ajouter des certificats SSL pour SNI.
6. Cochez les cases en regard des certificats et choisissez Remove (Supprimer).
7. À l'invite de confirmation, saisissez **confirm**, puis choisissez Supprimer.

Pour supprimer un certificat de la liste des certificats à l'aide du AWS CLI

Utilisez la commande [remove-listener-certificates](#).

Mettre à jour la stratégie de sécurité

Lorsque vous créez un écouteur TLS, vous pouvez sélectionner la stratégie de sécurité qui correspond à vos besoins. Lorsqu'une nouvelle stratégie de sécurité est ajoutée, vous pouvez mettre à jour votre écouteur TLS afin de pouvoir l'utiliser. Les Network Load Balancers ne prennent pas en charge les stratégies de sécurité personnalisées. Pour plus d'informations, consultez [Stratégies de sécurité](#).

Pour mettre à jour la stratégie de sécurité à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Choisissez le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Dans l'onglet Écouteurs, choisissez le texte dans la colonne Protocole : port pour ouvrir la page détaillée de l'écouteur.
5. Choisissez Modifier.
6. Pour Security Policy (Stratégie de sécurité), choisissez une stratégie de sécurité.
7. Sélectionnez Enregistrer les modifications.

Pour mettre à jour la politique de sécurité à l'aide du AWS CLI

Utilisez la commande [modify-listener](#) avec l'option `--ssl-policy`.

Mettre à jour la stratégie ALPN

Vous pouvez mettre à jour la stratégie ALPN pour votre écouteur TLS à l'aide de la procédure suivante. Pour plus d'informations, consultez [Stratégies ALPN](#).

Pour mettre à jour la stratégie ALPN à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Choisissez le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Dans l'onglet Écouteurs, choisissez le texte dans la colonne Protocole : port pour ouvrir la page détaillée de l'écouteur.
5. Choisissez Modifier.
6. Pour la stratégie ALPN, choisissez une stratégie pour activer ALPN ou choisissez Aucun pour désactiver ALPN.
7. Sélectionnez Enregistrer les modifications.

Pour mettre à jour la politique ALPN à l'aide du AWS CLI

Utilisez la commande [modify-listener](#) avec l'option `--alpn-policy`.

Suppression d'un écouteur pour votre Network Load Balancer

Vous pouvez supprimer un écouteur à tout moment.

Pour supprimer un écouteur à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Cochez la case correspondant à l'équilibreur de charge.
4. Dans l'onglet Écouteurs, sélectionnez la case à cocher pour l'écouteur, puis choisissez Actions, Supprimer l'écouteur.
5. Lorsque vous êtes invité à confirmer, saisissez **confirm**, puis choisissez Supprimer.

Pour supprimer un écouteur à l'aide du AWS CLI

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

Groupes cibles de vos Network 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. Par exemple, créez un groupe cible pour les demandes générales et d'autres groupes cibles pour les demandes adressées aux microservices pour votre application. Pour plus d'informations, consultez [Composants du Network Load Balancer](#).

Vous définissez des paramètres de vérification de l'état de votre équilibreur de charge 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, l'équilibreur de charge surveille continuellement l'état de santé de toutes les cibles enregistrées auprès du groupe cible qui résident dans une zone de disponibilité activée pour l'équilibreur de charge. L'équilibreur de charge achemine les demandes vers les cibles enregistrées qui sont saines. Pour plus d'informations, consultez [Surveillance de l'état de vos groupes cibles](#).

Table des matières

- [Configuration du routage](#)
- [Type de cible](#)
- [Type d'adresse IP](#)
- [Cibles enregistrées](#)
- [Attributs de groupe cible](#)
- [Préservation des adresses IP client](#)
- [Délai d'annulation d'enregistrement](#)
- [Protocole proxy](#)
- [Sessions permanentes](#)
- [Création d'un groupe cible pour votre Network Load Balancer](#)
- [Surveillance de l'état de vos groupes cibles](#)
- [Équilibrage de charge entre zones pour groupes cibles](#)
- [État du groupe cible](#)
- [Enregistrer des cibles auprès de votre groupe cible](#)

- [Application Load Balancers en tant que cibles](#)
- [Balises pour votre groupe cible](#)
- [Supprimer un groupe cible](#)

Configuration du routage

Par défaut, un équilibreur de charge achemine les demandes vers ses cibles à l'aide du protocole et du numéro de port que vous avez spécifiés lorsque vous avez créé le groupe cible. Vous pouvez également remplacer le port utilisé pour l'acheminement du trafic vers une cible lorsque vous l'enregistrez auprès du groupe cible.

Les groupes cibles des Network Load Balancers prennent en charge les protocoles et ports suivants :

- Protocoles: TCP, TLS, UDP TCP_UDP
- Ports : 1 à 65535

Si un groupe cible est configuré avec le protocole TLS, l'équilibreur de charge établit des connexions TLS avec les cibles à l'aide des certificats que vous installez sur les cibles. L'équilibreur de charge ne valide pas ces certificats. Par conséquent, vous pouvez utiliser des certificats auto-signés ou des certificats qui ont expiré. Comme l'équilibreur de charge se trouve dans un cloud privé virtuel (VPC), le trafic entre l'équilibreur de charge et les cibles est authentifié au niveau du paquet, de sorte qu'il n'est pas exposé au risque man-in-the-middle d'attaques ou d'usurpation, même si les certificats des cibles ne sont pas valides.

Le tableau suivant récapitule la prise en charge des combinaisons de paramètres de groupe cible et le protocole d'écoute.

Protocole de l'écouteur	Protocole du groupe cible	Type de groupe cible	Health check protocol (Protocole de vérification de l'état)
TCP	TCP TCP_UDP	instance ip	HTTP HTTPS TCP
TCP	TCP	alb	HTTP HTTPS
TLS	TCP TLS	instance ip	HTTP HTTPS TCP

Protocole de l'écouteur	Protocole du groupe cible	Type de groupe cible	Health check protocol (Protocole de vérification de l'état)
UDP	UDP TCP_UDP	instance ip	HTTP HTTPS TCP
TCP_UDP	TCP_UDP	instance ip	HTTP HTTPS TCP

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.

alb

La cible est un Application Load Balancer.

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

- Les sous-réseaux du VPC pour le groupe cible
- 10.0.0.0/8 ([RFC 1918](#))
- 100.64.0.0/10 ([RFC 6598](#))
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

⚠ Important

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

Tous les blocs CIDR pris en charge vous permettent d'enregistrer les cibles suivantes auprès d'un groupe cible :

- AWS ressources adressables par adresse IP et port (par exemple, bases de données).
- Ressources locales reliées à une connexion VPN Site-to-Site AWS Direct Connect ou AWS via une connexion VPN.

Lorsque la préservation des adresses IP client est désactivée pour vos groupes cibles, l'équilibreur de charge peut prendre en charge environ 55 000 connexions par minute pour chaque combinaison d'adresse IP Network Load Balancer et de cible unique (adresse IP et port). Si vous dépassez ce nombre de connexions, il y a plus de risque d'erreurs d'attribution de port. Si vous obtenez des erreurs d'attribution de port, ajoutez davantage de cibles au groupe cible.

Lorsque vous lancez un Network Load Balancer dans un Amazon VPC partagé (en tant que participant), vous ne pouvez enregistrer des cibles que dans des sous-réseaux partagés avec vous.

Lorsque le type de cible est a1b, vous pouvez enregistrer un Application Load Balancer unique en tant que cible. Pour plus d'informations, consultez [Application Load Balancers en tant que cibles](#).

Les Network Load Balancers ne prennent pas en charge le type de cible lambda. Les Application Load Balancers sont les seuls équilibreurs de charge prenant en charge le type de cible lambda. Pour plus d'informations, veuillez consulter [Fonctions Lambda en tant que cibles](#) (langue française non garantie) dans le Guide de l'utilisateur pour les Application Load Balancers.

Si vous avez des microservices sur des instances enregistrées auprès d'un Network Load Balancer, vous ne pouvez pas utiliser l'équilibreur de charge pour assurer la communication entre les microservices, sauf si l'équilibreur de charge est accessible sur Internet ou si les instances sont enregistrées par adresse IP. Pour plus d'informations, consultez [Connexions expirées pour les demandes d'une cible vers son équilibreur de charge](#).

Demande de routage et adresses IP

Si vous spécifiez des cibles à l'aide de l'ID d'une instance, le trafic est acheminé vers des instances à l'aide de l'adresse IP privée principale spécifiée dans l'interface réseau principale de l'instance.

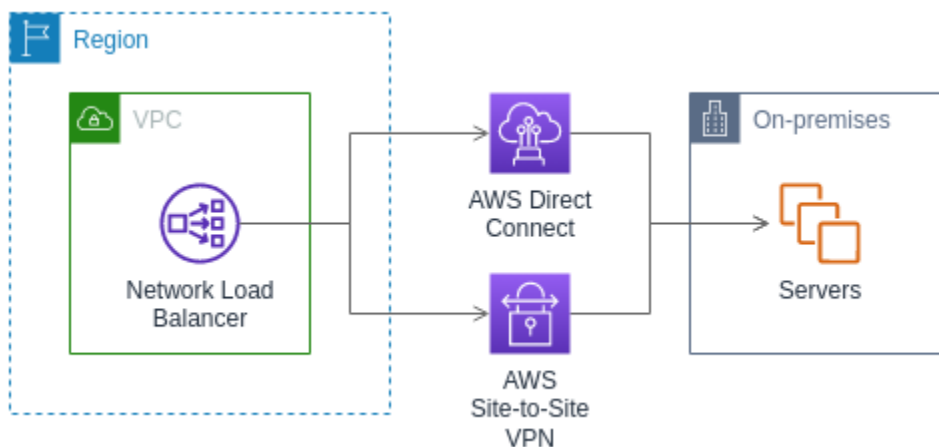
L'équilibreur de charge réécrit l'adresse IP de destination à partir du paquet de données avant de la transmettre à l'instance cible.

Si vous spécifiez des objectifs à l'aide d'adresses IP, vous pouvez acheminer le trafic vers une instance à l'aide de n'importe quelle adresse IP privée à partir d'une ou plusieurs interfaces réseau. Ceci permet à plusieurs applications d'une même instance d'utiliser le même port. Notez que chaque interface réseau peut avoir son propre groupe de sécurité. L'équilibreur de charge réécrit l'adresse IP de destination avant de la transmettre à la cible.

Pour plus d'informations sur l'autorisation du trafic vers vos instances, veuillez consulter [Groupes de sécurité cibles](#).

Ressources sur site en tant que cibles

Les ressources locales reliées par le biais AWS Direct Connect d'une connexion VPN Site-to-Site peuvent servir de cible, lorsque le type de cible est. `ip`



Lorsque vous utilisez des ressources sur site, les adresses IP de ces cibles doivent toujours provenir de l'un des blocs CIDR suivants :

- 10.0.0.0/8 ([RFC 1918](#))
- 100.64.0.0/10 ([RFC 6598](#))
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

Pour plus d'informations AWS Direct Connect, voir [Qu'est-ce que c'est AWS Direct Connect ?](#)

Pour plus d'informations AWS Site-to-Site VPN, voir [Qu'est-ce que c'est AWS Site-to-Site VPN ?](#)

Type d'adresse IP

Lorsque vous créez un nouveau groupe cible, vous pouvez sélectionner le type d'adresse IP de votre groupe cible. Cela contrôle la version IP utilisée pour communiquer avec les cibles et vérifier leur état de santé.

Les Network Load Balancers prennent en charge à la fois les groupes cibles IPv4 et IPv6. La sélection par défaut est IPv4. Les groupes cibles IPv6 ne peuvent être associés qu'aux Network Load Balancers à double pile.

Considérations

- Toutes les adresses IP d'un groupe cible doivent avoir le même type d'adresse IP. Par exemple, vous ne pouvez pas enregistrer une cible IPv4 auprès d'un groupe cible IPv6.
- Les groupes cibles IPv6 ne peuvent être utilisés qu'avec des équilibreurs de charge `duallstack` dotés d'écouteurs TCP ou TLS.
- Les groupes cibles IPv6 prennent en charge les cibles de type IP et instance.

Cibles enregistrées

Votre équilibreur de charge 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 l'équilibreur de charge. Vous pouvez enregistrer chaque cible auprès d'un ou plusieurs groupes cibles.

Si la demande augmente sur votre application, vous pouvez enregistrer des cibles supplémentaires auprès d'un ou plusieurs groupes cible afin de pouvoir gérer la demande. L'équilibreur de charge commence à acheminer le trafic vers une cible nouvellement enregistrée dès que le processus d'enregistrement est terminé et que la cible passe le premier contrôle de santé initial, quel que soit le seuil configuré.

Si la demande diminue sur votre application ou que vous avez besoin de répondre aux demandes de vos cibles, vous pouvez annuler l'enregistrement des cibles dans vos groupes cibles. L'annulation de l'enregistrement d'une cible supprime la cible de votre groupe cible, mais n'affecte pas autrement la cible. L'équilibreur de charge 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.

Si vous enregistrez des objectifs par ID d'instance, vous pouvez utiliser votre équilibreur de charge avec un groupe Auto Scaling. Une fois que vous avez attaché un groupe cible à un groupe Auto Scaling, Auto Scaling enregistre vos cibles auprès du groupe cible pour vous lorsqu'il les lance. Pour plus d'informations, veuillez consulter [Attacher un équilibreur de charge à votre groupe Auto Scaling](#) (langue française non garantie) dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.

Exigences et considérations

- Vous ne pouvez pas enregistrer des instances par ID d'instance si elles utilisent l'un des types d'instance suivants : C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 ou T1.
- Lorsque vous enregistrez des cibles par ID d'instance pour un groupe cible IPv6, une adresse IPv6 principale doit être attribuée aux cibles. Pour en savoir plus, consultez les [adresses IPv6](#) dans le guide de l'utilisateur Amazon EC2
- Lorsque vous enregistrez des cibles par ID d'instance, les instances doivent se trouver dans le même Amazon VPC que le Network Load Balancer. Vous ne pouvez pas enregistrer des instances par ID d'instance si elles se trouvent dans un VPC apparié au VPC de l'équilibreur de charge (même région ou région différente). Vous pouvez enregistrer ces instances par adresse IP.
- Si vous enregistrez une cible par adresse IP et que l'adresse IP se trouve dans le même VPC que l'équilibreur de charge, ce dernier vérifie qu'elle provient d'un sous-réseau qu'elle peut atteindre.
- L'équilibreur de charge achemine le trafic vers les cibles uniquement dans les zones de disponibilité activées. Les cibles situées dans des zones non activées ne sont pas utilisées.
- Pour les groupes cibles UDP et TCP_UDP, n'enregistrez pas les instances par adresse IP si elles se trouvent en dehors du VPC de l'équilibreur de charge ou si elles utilisent l'un des types d'instance suivants : C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 ou T1. Les cibles situées en dehors du VPC de l'équilibreur de charge ou utilisant un type d'instance non pris en charge peuvent être en mesure de recevoir du trafic en provenance de l'équilibreur de charge, mais ne pas être en mesure de répondre.

Attributs de groupe cible

Les attributs de groupe cible suivants sont pris en charge. Vous ne pouvez modifier ces attributs que si le type de groupe cible est `instance` ou `ip`. Si le type de groupe cible est `alb`, ces attributs utilisent toujours leurs valeurs par défaut.

`deregistration_delay.timeout_seconds`

Durée d'attente d'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.

`deregistration_delay.connection_termination.enabled`

Indique si l'équilibreur de charge interrompt les connexions à la fin du délai d'expiration de l'annulation d'enregistrement. La valeur est `true` ou `false`. Pour les nouveaux groupes cibles `UDP/TCP_UDP`, la valeur par défaut est `true`. Sinon, la valeur par défaut est `false`.

`load_balancing.cross_zone.enabled`

Indique si l'équilibrage de charge entre zones est activé. La valeur est `true`, `false` ou `use_load_balancer_configuration`. L'argument par défaut est `use_load_balancer_configuration`.

`preserve_client_ip.enabled`

Indique si la préservation des adresses IP client est activée. La valeur est `true` ou `false`. La valeur par défaut est désactivée si le type de groupe cible est adresse IP et que le protocole de groupe cible est `TCP` ou `TLS`. Sinon, la valeur par défaut est activée. La préservation des adresses IP client ne peut pas être désactivée pour les groupes cibles `UDP` et `TCP_UDP`.

`proxy_protocol_v2.enabled`

Indique si le protocole proxy version 2 est activé. Par défaut, le protocole proxy est désactivé.

`stickiness.enabled`

Indique si les sessions permanentes sont activées.

`stickiness.type`

Type de permanence. La valeur admise est `source_ip`.

`target_group_health.dns_failover.minimum_healthy_targets.count`

Nombre minimal de cibles qui doivent être saines. Si le nombre de cibles saines est inférieur à cette valeur, marquez la zone comme non saine dans le DNS, afin que le trafic soit acheminé uniquement vers des zones saines. Les valeurs possibles sont `off`, ou un entier compris entre 1 et le nombre maximal de cibles. Lorsque la valeur est `off`, l'échec du DNS est désactivé, ce qui signifie que chaque groupe cible contribue de manière indépendante au basculement du DNS. La valeur par défaut est 1.

`target_group_health.dns_failover.minimum_healthy_targets.percentage`

Pourcentage minimal de cibles qui doivent être saines. Si le pourcentage de cibles saines est inférieur à cette valeur, marquez la zone comme non saine dans le DNS, afin que le trafic soit acheminé uniquement vers des zones saines. Les valeurs possibles sont `off` ou un entier compris entre 1 et 100. Lorsque la valeur est `off`, l'échec du DNS est désactivé, ce qui signifie que chaque groupe cible contribue de manière indépendante au basculement du DNS. La valeur par défaut est 1.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.count`

Le nombre minimal de cibles qui doivent être saines. Si le nombre de cibles saines est inférieur à cette valeur, acheminez le trafic vers toutes les cibles, y compris les cibles non saines. La plage est comprise entre 1 et le nombre maximal de cibles. La valeur par défaut est 1.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage`

Le pourcentage minimal de cibles qui doivent être saines. Si le pourcentage de cibles saines est inférieur à cette valeur, acheminez le trafic vers toutes les cibles, y compris les cibles non saines. Les valeurs possibles sont `off` ou un entier compris entre 1 et 100. L'argument par défaut est `off`.

`target_health_state.unhealthy.connection_termination.enabled`

Indique si l'équilibreur de charge interrompt les connexions aux cibles défectueuses. La valeur est `true` ou `false`. L'argument par défaut est `true`.

`target_health_state.unhealthy.draining_interval_seconds`

Durée pendant laquelle Elastic Load Balancing doit attendre avant de faire passer l'état d'une cible défectueuse de `unhealthy.draining` à `unhealthy`. La plage est comprise entre 0 et 360 000 secondes. La valeur par défaut est de 0 seconde.

Remarque : Cet attribut ne peut être configuré que lorsqu'il
l'`target_health_state.unhealthy.connection_termination.enabled` est `false`.

Préservation des adresses IP client

Les Network Load Balancers peuvent préserver l'adresse IP source des clients lors du routage des demandes vers des cibles backend. Lorsque vous désactivez la préservation des adresses IP client, l'adresse IP privée du Network Load Balancer devient l'adresse IP client pour tout le trafic entrant.

Par défaut, la préservation des adresses IP client est activée (et ne peut pas être désactivée) pour les groupes cibles de type IP et instance utilisant les protocoles UDP et TCP_UDP. Toutefois, vous pouvez activer ou désactiver la préservation des adresses IP client pour les groupes cibles TCP et TLS à l'aide de l'attribut de groupe cible `preserve_client_ip.enabled`.

Paramètres par défaut

- Groupes cibles de type instance : activé
- Groupes cibles de type IP (UDP, TCP_UDP) : activé
- Groupes cibles de type IP (TCP, TLS) : désactivé

Exigences et considérations

- Lorsque la préservation des adresses IP client est activée, les cibles doivent se trouver dans le même VPC que le Network Load Balancer, et le trafic doit circuler directement du Network Load Balancer vers la cible.
- La préservation des adresses IP client n'est pas prise en charge lors de l'utilisation d'un point de terminaison Gateway Load Balancer pour inspecter le trafic entre le Network Load Balancer et la cible (instance ou IP), même si la cible se trouve dans le même Amazon VPC que le Network Load Balancer.
- Les types d'instance suivants ne prennent pas en charge la préservation de l'IP du client : C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 et T1. Nous vous recommandons d'enregistrer ces types d'instances en tant qu'adresses IP en désactivant la préservation des adresses IP client.
- La préservation de l'adresse IP du client n'a aucun effet sur le trafic entrant en provenance de AWS PrivateLink. L'adresse IP source du AWS PrivateLink trafic est toujours l'adresse IP privée du Network Load Balancer.
- La préservation des adresses IP client n'est pas prise en charge lorsqu'un groupe cible contient des ENI AWS PrivateLink ou l'ENI d'un autre Network Load Balancer. Cela entraînera une perte de communication avec ces cibles.
- La préservation des adresses IP client n'a aucun effet sur le trafic converti d'IPv6 en IPv4. L'adresse IP source de ce type de trafic est toujours l'adresse IP privée du Network Load Balancer.
- Lorsque vous spécifiez des cibles par type d'Application Load Balancer, l'adresse IP client de tout le trafic entrant est préservée par le Network Load Balancer et envoyée à l'Application Load Balancer. L'Application Load Balancer ajoute ensuite l'adresse IP client à l'en-tête de la demande `X-Forwarded-For` avant de l'envoyer à la cible.

- Les modifications de préservation des adresses IP client ne prennent effet que pour les nouvelles connexions TCP.
- La boucle NAT, également appelée hairpinning, n'est pas prise en charge lorsque la préservation des adresses IP client est activée. Lorsque cette option est activée, vous pouvez rencontrer des limitations de connexion TCP/IP liées à la réutilisation observée des sockets sur les cibles. Ces limitations de connexion peuvent survenir lorsqu'un client, ou un périphérique NAT situé devant le client, utilise la même adresse IP source et le même port source pour se connecter simultanément à plusieurs nœuds d'équilibreur de charge. Si l'équilibreur de charge achemine ces connexions vers la même cible, celles-ci apparaissent à la cible comme si elles provenaient du même socket source, ce qui entraîne des erreurs de connexion. Dans ce cas, les clients peuvent réessayer (si la connexion échoue) ou se reconnecter (si la connexion est interrompue). Vous pouvez réduire ce type d'erreur de connexion en augmentant le nombre de ports éphémères sources ou en augmentant le nombre de cibles pour l'équilibreur de charge. Vous pouvez éviter ce type d'erreur de connexion en désactivant la préservation des adresses IP client ou en désactivant l'équilibrage de charge entre zones.
- Lorsque la préservation des adresses IP client est désactivée, un Network Load Balancer prend en charge 55 000 connexions simultanées ou environ 55 000 connexions par minute sur chaque cible unique (adresse IP et port). Si vous dépassez ce nombre de connexions, il y a plus de risque d'erreurs d'attribution de port, ce qui entraîne l'échec d'établissement de nouvelles connexions. Les erreurs d'attribution de ports peuvent être suivies à l'aide de la métrique `PortAllocationErrorCount`. Pour résoudre les erreurs d'attribution de port, ajoutez davantage de cibles au groupe cible. Pour plus d'informations, consultez [CloudWatch métriques pour votre Network Load Balancer](#).

Pour configurer la conservation de l'adresse IP du client à l'aide de la console

1. Ouvrez la console Amazon EC2 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 Attributes, choisissez Edit.
5. Pour activer la préservation des adresses IP client, activez l'option Préserver les adresses IP client. Pour désactiver la préservation des adresses IP client, désactivez l'option Préserver les adresses IP client.
6. Sélectionnez Enregistrer les modifications.

Pour activer ou désactiver la préservation de l'adresse IP du client à l'aide du AWS CLI

Utilisez la commande [modify-target-group-attributes](#) avec l'attribut `preserve_client_ip.enabled`.

Par exemple, utilisez la commande suivante pour désactiver la préservation des adresses IP client.

```
aws elbv2 modify-target-group-attributes --attributes
  Key=preserve_client_ip.enabled,Value=false --target-group-arn ARN
```

Votre sortie doit ressembler à l'exemple suivant.

```
{
  "Attributes": [
    {
      "Key": "proxy_protocol_v2.enabled",
      "Value": "false"
    },
    {
      "Key": "preserve_client_ip.enabled",
      "Value": "false"
    },
    {
      "Key": "deregistration_delay.timeout_seconds",
      "Value": "300"
    }
  ]
}
```

Délai d'annulation d'enregistrement

Lorsque vous annulez l'enregistrement d'une cible, l'équilibreur de charge cesse de créer de nouvelles connexions vers la cible. L'équilibreur de charge utilise le drainage de la connexion pour s'assurer que le trafic en vol se termine sur les connexions existantes. Si la cible dont l'enregistrement a été annulé reste saine et qu'une connexion existante n'est pas inactive, l'équilibreur de charge peut continuer à envoyer du trafic vers la cible. Pour vous assurer que les connexions existantes sont fermées, vous pouvez procéder de l'une des manières suivantes : activer l'attribut du groupe cible pour l'interruption de la connexion, vérifier que l'instance est défectueuse avant d'annuler son enregistrement, ou fermer périodiquement les connexions client.

L'état initial d'une cible dont l'enregistrement est en cours d'annulation est `draining`. Par défaut, l'équilibreur de charge change l'état d'une cible dont l'enregistrement est en cours d'annulation en `unused` au bout de 300 secondes. Pour modifier la durée pendant laquelle l'équilibreur de charge attend avant de modifier l'état d'une cible dont l'enregistrement est en cours d'annulation en `unused`, mettez à jour la valeur du délai d'annulation de l'enregistrement. Nous vous recommandons de spécifier une valeur d'au moins 120 secondes pour vous assurer que les demandes sont terminées.

Si vous activez l'attribut de groupe cible pour l'interruption de la connexion, les connexions aux cibles dont l'enregistrement a été annulé sont fermées peu après la fin du délai d'annulation d'enregistrement.

Pour mettre à jour les attributs de désinscription à l'aide de la console

1. Ouvrez la console Amazon EC2 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 Attributs, choisissez Modifier.
5. Pour modifier le délai d'annulation de l'enregistrement, saisissez une nouvelle valeur pour Délai d'annulation de l'enregistrement. Pour vous assurer que les connexions existantes sont fermées après l'annulation d'enregistrement des cibles, sélectionnez Arrêter les connexions lors de l'annulation de l'enregistrement.
6. Sélectionnez Enregistrer les modifications.

Pour mettre à jour les attributs de désinscription à l'aide du AWS CLI

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

Protocole proxy

Les Network Load Balancers utilisent le protocole proxy version 2 pour envoyer des informations de connexion supplémentaires comme la source et la destination. Le protocole proxy version 2 fournit un codage binaire de l'en-tête de protocole proxy. Avec les écouteurs TCP, l'équilibreur de charge ajoute un en-tête de protocole proxy aux données TCP. Il ne supprime ou ne remplace pas les données existantes, y compris les en-têtes de protocole proxy entrants envoyés par le client ou tous les autres proxys, les équilibreurs de charge ou les serveurs dans le chemin d'accès réseau. Par

conséquent, il est possible de recevoir plusieurs en-têtes de protocole proxy. En outre, s'il existe un autre chemin d'accès réseau à vos cibles en dehors de votre Network Load Balancer, le premier en-tête de protocole proxy risque de ne pas être celui provenant de votre Network Load Balancer.

Si vous spécifiez les cibles par adresse IP, les adresses IP source fournies à vos applications dépendent du protocole du groupe cible comme suit :

- TCP et TLS : les adresses IP source sont les adresses IP privées des nœuds d'équilibreur de charge. Si vous avez besoin des adresses IP des clients, activez le protocole proxy et obtenez les adresses IP du client à partir de l'en-tête de protocole proxy.
- UDP et TCP_UDP : les adresses IP source sont les adresses IP des clients.

Si vous spécifiez des cibles par ID d'instance, les adresses IP source fournies à vos applications sont les adresses IP client. Toutefois, si vous préférez, vous pouvez activer le protocole proxy et obtenir les adresses IP client à partir de l'en-tête de protocole proxy.

Note

Les écouteurs TLS ne prennent pas en charge les connexions entrantes avec des en-têtes de protocole proxy envoyés par le client ou tout autre proxy.

Connexions de vérification de l'état

Une fois que vous avez activé le protocole proxy, l'en-tête de protocole proxy est également inclus dans les connexions de vérification de l'état à partir de l'équilibreur de charge. Toutefois, avec les connexions de vérification de l'état, les informations de connexion client ne sont pas envoyées dans l'en-tête de protocole proxy.

Services de points de terminaison d'un VPC

Pour le trafic provenant d'utilisateurs du service via un [service de point de terminaison d'un VPC](#), les adresses IP source fournies à vos applications sont les adresses IP privées des nœuds d'équilibreur de charge. Si vos applications ont besoin des adresses IP des utilisateurs du service, activez le protocole proxy et obtenez-les à partir de l'en-tête de protocole proxy.

L'en-tête de protocole proxy inclut également l'ID du point de terminaison. Cette information est codée à l'aide d'un vecteur TLV (Type-Length-Value) personnalisé de la manière suivante.

Champ	Longueur (en octets)	Description
Type	1	PP2_TYPE_AWS (0xEA)
Longueur	2	Longueur de la valeur
Value	1	PP2_SUBTYPE_AWS_VPCE_ID (0x01)
	variable (longueur de la valeur moins 1)	ID du point de terminaison

Pour obtenir un exemple qui analyse type de TLV 0xEA, consultez <https://github.com/aws/elastic-load-balancing-tools/tree/master/proprot>.

Activer le protocole proxy

Avant d'activer le protocole proxy sur un groupe cible, vérifiez que vos applications attendent et peuvent analyser l'en-tête du protocole proxy v2. Sinon, vos applications risquent d'échouer. Pour plus d'informations, consultez [Protocole proxy versions 1 et 2](#).

Pour activer le protocole proxy v2 avec la console

1. Ouvrez la console Amazon EC2 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 Attributes, choisissez Edit.
5. Sur la page Modifier les attributs, sélectionnez Protocole proxy v2.
6. Sélectionnez Enregistrer les modifications.

Pour activer le protocole proxy v2 à l'aide du AWS CLI

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

Sessions permanentes

Les sessions permanentes constituent un mécanisme qui permet d'acheminer le trafic client vers la même cible d'un groupe cible. Elles sont très utiles aux serveurs qui tiennent à jour les informations d'état afin de fournir une expérience continue aux clients.

Considérations

- L'utilisation de sessions permanentes peut entraîner une distribution inégale des connexions et des flux, ce qui peut avoir un impact sur la disponibilité de vos cibles. Par exemple, tous les clients situés derrière le même périphérique NAT ont la même adresse IP source. Par conséquent, l'ensemble du trafic provenant de ces clients est acheminé vers la même cible.
- L'équilibreur de charge peut réinitialiser les sessions permanentes d'un groupe cible si l'état de l'une de ses cibles change ou si vous enregistrez ou annulez l'enregistrement des cibles au groupe cible.
- Lorsque l'attribut `stickiness` est activé pour un groupe cible, les contrôles de santé passifs ne sont pas pris en charge. Pour plus d'informations, consultez [la section Contrôles de santé pour vos groupes cibles](#).
- Les sessions permanentes ne sont pas prises en charge pour les écouteurs TLS.

Pour activer les sessions permanentes à l'aide de la console

1. Ouvrez la console Amazon EC2 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 Attributes, choisissez Edit.
5. Sous Configuration de sélection de la cible, activez Permanence.
6. Sélectionnez Enregistrer les modifications.

Pour activer les sessions persistantes à l'aide du AWS CLI

Utilisez la commande [modify-target-group-attributes](#) avec l'attribut `stickiness.enabled`.

Création d'un groupe cible pour votre Network Load Balancer

Vous enregistrez les cibles pour votre Network Load Balancer avec un groupe cible. Par défaut, l'équilibreur de charge envoie des demandes à des cibles enregistrées à l'aide du port et du protocole que vous avez spécifiés pour le groupe cible. Vous pouvez remplacer ce port lorsque vous enregistrez chaque cible auprès du groupe cible.

Une fois que vous avez créé un groupe cible, vous pouvez ajouter des balises.

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 plus d'informations, consultez [Règles d'un écouteur](#). Vous pouvez spécifier le même groupe cible dans plusieurs écouteurs, mais ces écouteurs doivent appartenir au même Network Load Balancer. Pour utiliser un groupe cible avec un équilibreur de charge, vous devez vérifier que le groupe cible n'est pas utilisé par un écouteur pour un autre équilibreur de charge.

Vous pouvez ajouter ou supprimer des cibles dans votre groupe cible à tout moment. Pour plus d'informations, consultez [Enregistrer des cibles auprès de votre groupe cible](#). Vous pouvez aussi modifier les paramètres de vérification de l'état de votre groupe cible. Pour plus d'informations, consultez [Modifier les paramètres de vérification de l'état d'un groupe cible](#).

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

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, sélectionnez Groupes cibles.
3. Sélectionnez Créer un groupe cible.
4. Sous le panneau Configuration de base, procédez comme suit :
 - a. Pour Choisir un type de cible, sélectionnez Instances pour enregistrer les cibles par ID d'instance, Adresses IP pour enregistrer les cibles par adresse IP ou Application Load Balancer pour enregistrer un Application Load Balancer en tant que cible.
 - 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. Pour Protocole, choisissez un protocole comme suit :
 - Si l'écouteur est un protocole TCP, choisissez TCP ou TCP_UDP.

- Si l'écouteur est un protocole TLS, choisissez TCP ou TLS.
 - Si l'écouteur est un protocole UDP, choisissez UDP ou TCP_UDP.
 - Si l'écouteur protocole est TCP_UDP, choisissez TCP_UDP.
- d. (Facultatif) Pour Port, modifiez la valeur par défaut en fonction des besoins.
- e. Pour Type d'adresse IP, choisissez IPv4 ou IPv6. Cette option n'est disponible que si le type de cible est Instances ou Adresses IP et si le protocole est TCP ou TLS.
- Vous devez associer un groupe cible IPv6 à un équilibreur de charge à double pile. Toutes les cibles du groupe cible doivent avoir le même type d'adresse IP. Vous ne pouvez pas modifier le type d'adresse IP d'un groupe cible après l'avoir créé.
- f. Pour un VPC, sélectionnez le cloud privé virtuel (VPC) avec les cibles à enregistrer.
5. Pour le panneau Surveillances de l'état, modifiez les paramètres par défaut selon vos besoins. Pour les Paramètres avancés de surveillance de l'état, choisissez le port de surveillance de l'état, le nombre, le délai d'expiration, l'intervalle et spécifiez les codes de réussite. Si les surveillances de l'état dépassent consécutivement le Seuil de défektivité, l'équilibreur de charge met la cible hors service. Lorsque les surveillances de l'état dépassent consécutivement le Seuil de défektivité, l'équilibreur de charge remet la cible en service. Pour plus d'informations, consultez [Surveillance de l'état de vos groupes cibles](#).
6. (Facultatif) Pour ajouter une balise, choisissez Balises, puis Ajouter une balise et saisissez la clé et la valeur de la balise.
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 les instances, saisissez les ports, puis choisissez Inclure comme étant en attente ci-dessous.
- Remarque : une adresse IPv6 principale doit être attribuée aux instances pour qu'elles soient enregistrées auprès d'un groupe cible IPv6.
- Si le type de cible est Adresses IP, sélectionnez le réseau, saisissez les adresses 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 commande [create-target-group](#) pour créer le groupe cible, la commande [add-tags](#) pour baliser le groupe cible et la commande [register-targets](#) pour ajouter des cibles.

Surveillance de l'état de vos groupes cibles

Vous pouvez enregistrer vos cibles auprès d'un ou de plusieurs groupes cibles. L'équilibreur de charge 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.

Les Network Load Balancers utilisent des surveillances de l'état actives et passives pour déterminer si une cible est disponible pour traiter des demandes. Par défaut, chaque nœud d'équilibreur de charge achemine les demandes uniquement vers les cibles saines dans sa zone de disponibilité. Si vous activez l'équilibrage de charge entre zones permet, chaque nœud d'équilibreur de charge achemine les demandes vers les cibles saines dans toutes les zones de disponibilité activées. Pour plus d'informations, consultez [Equilibrage de charge entre zones](#).

Avec les vérifications de l'état passives, l'équilibreur de charge observe la façon dont les cibles répondent aux connexions. Les vérifications de l'état passives permettent l'équilibreur de charge de détecter une cible non saine avant que celle-ci soit signalée comme étant non saine par les vérifications de l'état actives. Vous ne pouvez pas désactiver, configurer ou surveiller les vérifications de l'état passives. Les contrôles de santé passifs ne sont pas pris en charge pour le trafic UDP, et les groupes cibles pour lesquels la fonctionnalité d'adhérence est activée. Pour plus d'informations, consultez la section [Sessions persistantes](#).

Si une cible devient défectueuse, l'équilibreur de charge envoie un RST TCP pour les paquets reçus sur les connexions client associées à la cible, sauf si la cible défectueuse déclenche le mode fail-open pour l'équilibreur de charge.

Si les groupes cibles n'ont pas une cible saine dans une zone de disponibilité activée, nous supprimons l'adresse IP du sous-réseau correspondant à partir de DNS pour que les demandes ne puissent pas être acheminées vers cette zone de disponibilité. Si toutes les cibles échouent aux surveillances de l'état en même temps dans toutes les zones de disponibilité activées, l'équilibreur de charge passe en mode fail-open. Les équilibreurs de charge réseau échoueront également à s'ouvrir lorsque vous avez un groupe cible vide. Ce mode a pour effet d'autoriser le trafic à destination de toutes les cibles dans toutes les zones de disponibilité activées, quel que soit leur état de santé.

Si un groupe cible est configuré avec des surveillances de l'état HTTPS, ses cibles enregistrées échouent aux surveillances si elles ne prennent en charge que le protocole TLS 1.3. Ces cibles doivent prendre en charge une version antérieure de TLS, telle que TLS 1.2.

Pour les demandes de vérification de l'état HTTP ou HTTPS, l'en-tête de l'hôte contient l'adresse IP du nœud d'équilibrage de charge et le port de l'écouteur, et non l'adresse IP de la cible et le port de vérification de l'état.

Si vous ajoutez un écouteur TLS à votre Network Load Balancer, nous effectuons un test de connectivité de l'écouteur. Comme la résiliation TLS met également fin à la connexion TCP, une nouvelle connexion TCP est établie entre votre équilibreur de charge et vos cibles. Par conséquent, les connexions TCP pour ce test peuvent être envoyées par votre équilibreur de charge aux cibles enregistrées auprès de votre écouteur TLS. Vous pouvez identifier ces connexions TCP car elles possèdent l'adresse IP source de votre Network Load Balancer et elles ne contiennent pas de paquets de données.


Pour un service UDP, la disponibilité des cibles peut être testée à l'aide de surveillances de l'état non UDP sur votre groupe cible. Vous pouvez utiliser n'importe quelle surveillance de l'état disponible (TCP, HTTP ou HTTPS) et n'importe quel port de votre cible pour vérifier la disponibilité d'un service UDP. Si le service recevant la surveillance de l'état échoue, votre cible est considérée comme indisponible. Pour améliorer la précision des surveillances de l'état pour un service UDP, configurez le service à l'écoute sur le port de surveillance de l'état pour suivre le statut de votre service UDP et faites échouer la surveillance si le service n'est pas disponible.

Paramètres de surveillance de l'état

Vous configurez les vérifications de l'état actives pour les cibles d'un groupe cible en utilisant les paramètres suivants. Si les bilans de santé dépassent le `UnhealthyThreshold` nombre de défaillances consécutives, l'équilibreur de charge met la cible hors service. Lorsque les bilans de santé dépassent le `HealthyThreshold` nombre de réussites consécutives, l'équilibreur de charge remet la cible en service.

Paramètre	Description	Par défaut
<code>HealthCheckProtocole</code>	Protocole utilisé par l'équilibreur de charge lors des vérifications de l'état des cibles. Les protocoles possibles sont HTTP, HTTPS et TCP. La valeur par défaut est le protocole TCP. Si le type de cible est <code>alb</code> , les protocoles de surveillance de l'état pris en charge sont HTTP et HTTPS.	TCP

Paramètre	Description	Par défaut
HealthCheckPort	Port utilisé par l'équilibreur de charge lors des vérifications de l'état des cibles. La valeur par défaut consiste à utiliser le port sur lequel chaque cible reçoit le trafic depuis l'équilibreur de charge.	Port sur lequel chaque cible reçoit le trafic depuis l'équilibreur de charge.
HealthCheckParcours	[Contrôles de santé HTTP/HTTPS] Le chemin du contrôle de santé qui est la destination des cibles pour les bilans de santé. La valeur par défaut est /.	/
HealthCheckTimeoutSeconds	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 secondes. Cette valeur doit être de 6 secondes pour les surveillances de l'état HTTP et de 10 secondes pour les surveillances TCP et HTTPS.	6 secondes pour les surveillances de l'état HTTP et 10 secondes pour les surveillances TCP et HTTPS.

Paramètre	Description	Par défaut
HealthCheckIntervalSeconds	Durée approximative, en secondes, entre les vérifications de l'état d'une cible. La plage est comprise entre 5 et 300 secondes. Le durée par défaut est 30 secondes.	30 secondes
	<div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px;"><p> Important</p><p>Les surveillances de l'état pour un Network Load Balancer sont distribuées et utilisent un mécanisme de consensus pour déterminer l'état des cibles. Par conséquent, des cibles reçoivent plus de vérifications de l'état que le nombre configuré. Pour réduire l'impact sur vos cibles si vous utilisez des vérifications d'état HTTP, utilisez une destination plus simple sur les cibles, par exemple, un fichier HTML statique, ou basculez vers des vérifications d'état TCP.</p></div>	
HealthyThresholdCompter	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.	5
UnhealthyThresholdCompter	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.	2

Paramètre	Description	Par défaut
Matcher	[Vérifications de l'état HTTP/HTTPS] Les codes HTTP à utiliser lors de la recherche d'une réponse de réussite provenant d'une cible. La plage est comprise entre 200 et 599. La valeur par défaut est comprise entre 200 et 399.	200-399

État de santé d'une cible

Avant que l'équilibreur de charge 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 l'équilibreur de charge.

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

Valeur	Description
<code>initial</code>	<p>L'équilibreur de charge 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 un bilan de santé, a échoué au bilan de santé ou est à l'arrêt.</p> <p>Code motif connexe : <code>Target.FailedHealthChecks</code></p>

Valeur	Description
<code>draining</code>	L'enregistrement de la cible est en cours d'annulation et le drainage de la connexion est en cours. Code motif connexe : <code>Target.DeregistrationInProgress</code>
<code>unhealthy.draining</code>	La cible n'a pas répondu aux examens de santé ou a échoué aux examens de santé et entre dans une période de grâce. La cible prend en charge les connexions existantes et n'acceptera aucune nouvelle connexion pendant cette période de grâce. Code motif connexe : <code>Target.FailedHealthChecks</code>
<code>unavailable</code>	L'état cible n'est pas disponible. Code motif connexe : <code>Elb.InternalError</code>
<code>unused</code>	La cible n'est pas enregistrée auprès d'un groupe cible, le groupe cible n'est pas utilisé dans une règle d'écoute ou la cible se trouve dans une zone de disponibilité non activée. Codes de motif connexes : <code>Target.NotRegistered</code> <code>Target.NotInUse</code> <code>Target.InvalidState</code> <code>Target.IpUnusable</code>

Codes de motif de vérification de l'état

Si l'état d'une cible correspond à une valeur autre que `Healthy`, l'API renvoie un code de motif et une description du problème, et la console affiche la même description dans une info-bulle. Notez que les codes de motif qui commencent par `Elb` proviennent de l'équilibreur de charge et que ceux qui commencent par `Target` proviennent de la 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>	<p>La cible est à l'état arrêté.</p> <p>La cible est à l'état résilié.</p> <p>La cible est à l'état résilié ou arrêté.</p> <p>La cible est à un état non valide.</p>
<code>Target.IpUnusable</code>	L'adresse IP ne peut pas être utilisée en tant que cible, car elle est utilisée par un équilibreur de charge
<code>Target.NotInUse</code>	<p>Le groupe cible n'est pas configuré de façon à recevoir le trafic de l'équilibreur de charge</p> <p>La cible est dans une zone de disponibilité qui n'est pas activée pour l'équilibreur de charge</p>
<code>Target.NotRegistered</code>	La cible n'est pas enregistrée auprès du groupe cible

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 console Amazon EC2 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. Le panneau Détails affiche le nombre total de cibles, ainsi que le nombre de cibles pour chaque état.
5. Dans l'onglet Cible, la colonne Statut d'état indique le statut de chaque cible.
6. Si le statut d'une cible est une valeur autre que `Healthy`, la colonne Détails de l'état de santé contient des informations supplémentaires.

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

Utilisez la commande [describe-target-health](#). 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](#).

Modifier les paramètres de vérification de l'état d'un groupe cible

Vous pouvez modifier les paramètres de vérification de l'état de votre groupe cible à tout moment.

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

1. Ouvrez la console Amazon EC2 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 Health checks, choisissez Edit.
5. Sur la page Modifier les paramètres de vérification 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 commande [modify-target-group](#).

Équilibrage de charge entre zones pour groupes cibles

Les nœuds de votre équilibreur de charge distribuent les requêtes des clients à des cibles enregistrées. Lorsque l'équilibrage de charge entre zones est activé, chaque nœud d'équilibreur de charge distribue le trafic entre les cibles enregistrées dans toutes les zones de disponibilité enregistrées. Lorsque l'équilibrage de charge entre zones est désactivé, chaque nœud d'équilibreur de charge distribue le trafic entre les cibles enregistrées dans sa zone de disponibilité uniquement. Cela peut être utilisé si les domaines de défaillance zonaux sont préférés aux domaines régionaux, afin de garantir qu'une zone saine n'est pas affectée par une zone défectueuse, ou pour améliorer la latence globale.

Avec les Network Load Balancers, l'équilibrage de charge entre zones est désactivé par défaut au niveau de l'équilibreur de charge, mais vous pouvez l'activer à tout moment. Pour les groupes cibles, le paramètre par défaut est d'utiliser le paramètre d'équilibreur de charge, mais vous pouvez le remplacer en activant ou en désactivant explicitement l'équilibrage de charge entre zones au niveau du groupe cible.

Considérations

- Lorsque vous activez l'équilibrage de charge entre zones pour un Network Load Balancer, des frais de transfert de données EC2 s'appliquent. Pour plus d'informations, voir [Comprendre les frais de transfert de données](#) dans le Guide de l'utilisateur AWS sur les exportations de données
- Le paramètre du groupe cible détermine le comportement d'équilibrage de charge du groupe cible. Par exemple, si l'équilibrage de charge entre zones est activé au niveau de l'équilibreur de charge et désactivé au niveau du groupe cible, le trafic envoyé au groupe cible n'est pas acheminé entre les zones de disponibilité.
- Lorsque l'équilibrage de charge entre zones est désactivé, assurez-vous de disposer d'une capacité cible suffisante dans chacune des zones de disponibilité de l'équilibreur de charge, afin que chaque zone puisse répondre à la charge de travail qui lui est associée.
- Lorsque l'équilibrage de charge entre zones est désactivé, assurez-vous que tous les groupes cibles participent aux mêmes zones de disponibilité. Une zone de disponibilité vide est considérée comme défectueuse.

Modification de l'équilibrage de charge entre zones d'un équilibreur de charge

Vous pouvez activer ou désactiver l'équilibrage de charge entre zones à tout moment au niveau de l'équilibreur de charge.

Pour modifier l'équilibrage de charge entre zones d'un équilibreur de charge à l'aide de la console

1. Ouvrez la console Amazon EC2 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 nom de l'équilibreur de charge afin d'ouvrir sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sur la page Modifier les attributs de l'équilibreur de charge, activez ou désactivez l'Équilibrage de charge entre zones.
6. Sélectionnez Enregistrer les modifications.

Pour modifier l'équilibrage de charge entre zones de votre équilibreur de charge à l'aide du AWS CLI

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

Modification de l'équilibrage de charge entre zones pour un groupe cible

Le paramètre d'équilibrage de charge entre zones au niveau du groupe cible remplace le paramètre au niveau de l'équilibreur de charge.

Vous pouvez activer ou désactiver l'équilibrage de charge entre zones au niveau du groupe cible si le type de groupe cible est `instance` ou `ip`. Si le type de groupe cible est `alb`, le groupe cible hérite toujours du paramètre d'équilibrage de charge entre zones de l'équilibreur de charge.

Pour modifier l'équilibrage de charge entre zones d'un groupe cible à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Répartition de charge, sélectionnez Groupes cibles.
3. Sélectionnez le nom du groupe cible pour ouvrir sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.

5. Sur la page Modifier les attributs du groupe cible, sélectionnez Activé pour Équilibrage de charge entre zones.
6. Sélectionnez Enregistrer les modifications.

Pour modifier l'équilibrage de charge entre zones pour un groupe cible à l'aide du AWS CLI

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

État du groupe cible

Par défaut, un groupe cible est considéré comme sain tant qu'il possède au moins une cible saine. Si votre flotte est importante, il ne suffit pas d'avoir une seule cible saine desservant le trafic. Au lieu de cela, vous pouvez spécifier un nombre ou un pourcentage minimal de cibles qui doivent être saines, ainsi que les actions entreprises par l'équilibreur de charge lorsque les cibles saines tombent en dessous du seuil spécifié. Cela améliore la disponibilité.

Actions d'état défectueux

Vous pouvez configurer des seuils sains pour les actions suivantes :

- **Basculement DNS** : lorsque les cibles saines d'une zone tombent en dessous du seuil, nous marquons les adresses IP du nœud d'équilibreur de charge de la zone comme défectueuses dans DNS. Par conséquent, lorsque les clients résolvent le nom DNS de l'équilibreur de charge, le trafic est acheminé uniquement vers les zones saines.
- **Basculement du routage** : lorsque les cibles saines d'une zone tombent en dessous du seuil, l'équilibreur de charge envoie le trafic vers toutes les cibles disponibles pour le nœud d'équilibreur de charge, y compris les cibles défectueuses. Cela augmente les chances de réussite d'une connexion client, en particulier lorsque les cibles échouent temporairement aux surveillances de l'état, et réduit le risque de surcharge des cibles saines.

Exigences et considérations

- Si vous spécifiez les deux types de seuils pour une action (nombre et pourcentage), l'équilibreur de charge réalise l'action lorsque l'un des seuils est dépassé.

- Si vous spécifiez des seuils pour les deux actions, le seuil de basculement DNS doit être supérieur ou égal au seuil de basculement du routage, afin que le basculement DNS se produise pendant ou avant le basculement du routage.
- Si vous spécifiez le seuil sous forme de pourcentage, nous calculons la valeur de manière dynamique, en fonction du nombre total de cibles enregistrées auprès des groupes cibles.
- Le nombre total de cibles est déterminé selon que la répartition de charge entre zones est activé ou non. Si la répartition de charge entre zones est désactivé, chaque nœud envoie du trafic uniquement aux cibles de sa propre zone, ce qui signifie que les seuils s'appliquent séparément au nombre de cibles dans chaque zone activée. Si l'équilibrage de charge entre zones est activé, chaque nœud envoie du trafic à toutes les cibles de toutes les zones activées, ce qui signifie que les seuils spécifiés s'appliquent au nombre total de cibles dans toutes les zones activées. Pour plus d'informations, consultez [Équilibrage de charge entre zones](#).
- Avec le basculement DNS, nous supprimons les adresses IP des zones défectueuses du nom d'hôte DNS de l'équilibreur de charge. Toutefois, le cache DNS du client local peut contenir ces adresses IP jusqu'à ce que le time-to-live (TTL) de l'enregistrement DNS expire (60 secondes).
- En cas de basculement DNS, cela a un impact sur tous les groupes cibles associés à l'équilibreur de charge. Assurez-vous de disposer d'une capacité suffisante dans les zones restantes pour gérer ce trafic supplémentaire, en particulier si la répartition de charge entre zones est désactivé.
- Avec le basculement DNS, si toutes les zones d'équilibreur de charge sont considérées comme défectueuses, l'équilibreur de charge envoie le trafic vers toutes les zones, y compris les zones défectueuses.
- Il existe des facteurs autres que le fait de savoir s'il existe suffisamment de cibles saines susceptibles d'entraîner un basculement DNS, tels que l'état de la zone.

Exemple

Les exemples suivants montrent comment les paramètres d'état du groupe cible sont appliqués.

Scénario

- Un équilibreur de charge qui prend en charge deux zones de disponibilité, A et B
- Chaque zone de disponibilité contient 10 cibles enregistrées
- Les paramètres d'état du groupe cible sont les suivants :
 - Basculement DNS : 50 %
 - Basculement du routage : 50 %

- Six cibles échouent dans la zone de disponibilité B

Si la répartition de charge entre zones est désactivée

- Le nœud d'équilibreur de charge de chaque zone de disponibilité ne peut envoyer du trafic qu'aux 10 cibles de sa zone de disponibilité.
- Il existe 10 cibles saines dans la zone de disponibilité A, ce qui correspond au pourcentage requis de cibles saines. L'équilibreur de charge continue de répartir le trafic entre les 10 cibles saines.
- Il n'y a que quatre cibles saines dans la zone de disponibilité B, soit 40 % des cibles du nœud d'équilibreur de charge dans la zone de disponibilité B. Comme ce pourcentage est inférieur au pourcentage requis de cibles saines, l'équilibreur de charge prend les mesures suivantes :
 - Basculement DNS : la zone de disponibilité B est marquée comme défectueuse dans DNS. Comme les clients ne peuvent pas résoudre le nom de l'équilibreur de charge vers le nœud d'équilibreur de charge de la zone de disponibilité B et que la zone de disponibilité A est saine, les clients envoient de nouvelles connexions à la zone de disponibilité A.
 - Basculement du routage : lorsque de nouvelles connexions sont envoyées explicitement à la zone de disponibilité B, l'équilibreur de charge distribue le trafic à toutes les cibles de la zone de disponibilité B, y compris les cibles défectueuses. Cela permet d'éviter les pannes parmi les cibles saines restantes.

Si la répartition de charge entre zones est activée

- Chaque nœud d'équilibreur de charge peut envoyer du trafic vers les 20 cibles enregistrées dans les deux zones de disponibilité.
- Il y a 10 cibles saines dans la zone de disponibilité A et 4 cibles saines dans la zone de disponibilité B, pour un total de 14 cibles saines. Cela représente 70 % des cibles pour les nœuds d'équilibreur de charge dans les deux zones de disponibilité, ce qui correspond au pourcentage requis de cibles saines.
- L'équilibreur de charge répartit le trafic entre les 14 cibles saines des deux zones de disponibilité.

Modification des paramètres d'état du groupe cible

Vous pouvez modifier les paramètres d'état de votre groupe cible comme suit.

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

1. Ouvrez la console Amazon EC2 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 Attributes, choisissez Edit.
5. Vérifiez si la répartition de charge entre zones est activé ou désactivé. Mettez à jour ce paramètre si nécessaire pour vous assurer que vous disposez d'une capacité suffisante pour gérer le trafic supplémentaire en cas de défaillance d'une zone.
6. Développez Exigences en matière d'état du groupe cible.
7. Pour Type de configuration, nous vous recommandons de choisir Configuration unifiée, qui définit le même seuil pour les deux actions.
8. Pour Exigences en matière d'état sain, exécutez l'une des actions suivantes :
 - Choisissez Nombre minimum de cibles saines, puis saisissez un nombre compris entre 1 et le nombre maximal de cibles pour votre groupe cible.
 - Choisissez Pourcentage minimum de cibles saines, puis saisissez un nombre compris entre 1 et 100.
9. Sélectionnez Enregistrer les modifications.

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

Utilisez la commande [modify-target-group-attributes](#). L'exemple suivant définit à 50 % le seuil d'état sain pour les deux actions présentant un état défectueux.

```
aws elbv2 modify-target-group-attributes \  
--target-group-arn arn:aws:elasticloadbalancing:region:123456789012:targetgroup/my-  
targets/73e2d6bc24d8a067 \  
--attributes  
Key=target_group_health.dns_failover.minimum_healthy_targets.percentage,Value=50 \  
  
Key=target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage,Value=50
```

Interruption de connexion pour des cibles défectueuses

La terminaison de connexion est activée par défaut. Lorsque la cible d'un Network Load Balancer échoue aux tests de santé configurés et est jugée défectueuse, l'équilibreur de charge met fin

aux connexions établies et arrête d'acheminer les nouvelles connexions vers la cible. Lorsque la terminaison de connexion est désactivée, la cible est toujours considérée comme défaillante et ne recevra pas de nouvelles connexions, mais les connexions établies restent actives, ce qui leur permet de se fermer correctement.

La terminaison de connexion pour les cibles défectueuses peut être définie individuellement pour chaque groupe cible.

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

1. Ouvrez la console Amazon EC2 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 Attributes, choisissez Edit.
5. Sous Gestion des états non sains de la cible, choisissez d'activer ou de désactiver l'option Interrompre les connexions lorsque les cibles deviennent défectueuses.
6. Sélectionnez Enregistrer les modifications.

Pour modifier le paramètre de terminaison de connexion à l'aide du AWS CLI

Utilisez la commande [modify-target-group-attributes](#) avec l'attribut `target_health_state.unhealthy.connection_termination.enabled`.

Intervalle de vidange malsain

Important

La terminaison de connexion doit être désactivée avant d'activer un intervalle de vidange défectueux.

Les cibles dans `unhealthy.draining` cet état sont considérées comme défectueuses. Elles ne reçoivent pas de nouvelles connexions, mais conservent les connexions établies pendant l'intervalle configuré. L'intervalle de connexion défaillant détermine le temps pendant lequel la cible reste dans `unhealthy.draining` cet état avant qu'il ne le devienne `unhealthy`. Si la cible passe les tests de santé pendant l'intervalle de connexion défaillant, son état `healthy` redevient normal. Si un désenregistrement est déclenché, l'état cible devient actif `draining` et le délai de désenregistrement commence à courir.

L'intervalle de vidange insalubre peut être défini individuellement pour chaque groupe cible.

Pour modifier l'intervalle de vidange défectueux à l'aide de la console

1. Ouvrez la console Amazon EC2 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 Attributes, choisissez Edit.
5. Sous Gestion de l'état malsain de Target, assurez-vous que l'option Mettre fin aux connexions lorsque les cibles deviennent défectueuses est désactivée.
6. Entrez une valeur pour Intervalle de vidange insalubre.
7. Sélectionnez Enregistrer les modifications.

Pour modifier l'intervalle de vidange insalubre à l'aide du AWS CLI

Utilisez la commande [modify-target-group-attributes](#) avec l'attribut `target_health_state.unhealthy.draining_interval_seconds`.

Utiliser le basculement DNS Route 53 pour votre équilibreur de charge

Si vous utilisez Route 53 pour acheminer des requêtes DNS vers votre équilibreur de charge, vous pouvez également configurer le basculement DNS pour ce dernier à l'aide de Route 53. Dans une configuration de basculement, Route 53 vérifie l'état de santé des cibles du groupe cible pour l'équilibreur de charge afin de déterminer si celles-ci sont disponibles. Si aucune cible saine n'est enregistrée auprès de l'équilibreur de charge, ou si l'équilibreur de charge lui-même est défectueux, Route 53 achemine le trafic vers une autre ressource disponible, par exemple, un équilibreur de charge sain ou un site Web statique dans Amazon S3.

Par exemple, supposons que vous ayez une application web pour `www.example.com`, et que vous vouliez que des instances redondantes s'exécutent derrière deux équilibreurs de charge situés dans des Régions différentes. Vous souhaitez que le trafic soit principalement acheminé vers l'équilibreur de charge d'une Région, et vous voulez utiliser l'équilibreur de charge de l'autre Région en secours pendant les pannes. Si vous configurez le basculement DNS, vous pouvez spécifier vos équilibreurs de charge principal et secondaire (Backup). Route 53 dirige le trafic vers l'équilibreur de charge principal s'il est disponible ou, dans le cas contraire, vers l'équilibreur de charge secondaire.

Utiliser Évaluer l'état de la cible

- Lorsque l'option Évaluer l'état de la cible est définie sur Yes sur un enregistrement d'alias pour un Network Load Balancer, Route 53 évalue l'état de santé de la ressource spécifiée par la valeur `alias target`. Pour un Network Load Balancer, Route 53 utilise les surveillances de l'état du groupe cible associées à l'équilibreur de charge.
- Lorsque tous les groupes cibles d'un Network Load Balancer sont sains, Route 53 indique que l'enregistrement d'alias est sain. Si un groupe cible contient au moins une cible saine, la surveillance de l'état du groupe cible est réussie. Route 53 renvoie ensuite les enregistrements conformément à votre stratégie de routage. Si la stratégie de routage de basculement est utilisée, Route 53 renvoie l'enregistrement principal.
- Si l'un des groupes cibles d'un Network Load Balancer est défectueux, l'enregistrement de l'alias échoue la surveillance de l'état de Route 53 (fail-open). Si vous utilisez l'option Évaluer l'état de la cible, cela échouera à la stratégie de routage de basculement.
- Si tous les groupes cibles d'un Network Load Balancer sont vides (aucune cible), Route 53 considère que l'enregistrement est défectueux (fail-open). Si vous utilisez l'option Évaluer l'état de la cible, cela échouera à la stratégie de routage de basculement.

Pour de plus amples informations, consultez [Configuration du basculement DNS](#) dans le Guide du développeur Amazon Route 53.

Enregistrer des cibles auprès de votre groupe cible

Lorsque votre cible est prête à traiter les demandes, vous l'inscrivez auprès d'un ou plusieurs groupes cibles. Le type de cible du groupe cible détermine la façon dont vous enregistrez les cibles. Par exemple, vous pouvez enregistrer des ID d'instance, des adresses IP ou un Application Load Balancer. Votre Network Load Balancer commence à acheminer les demandes vers les cibles dès que le processus d'enregistrement est terminé et que la cible a réussi les surveillances 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 plus d'informations, consultez [Surveillance de l'état de vos groupes cibles](#).

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 l'équilibreur de charge 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.

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 plus d'informations, consultez [Délai d'annulation d'enregistrement](#).

Si vous enregistrez des objectifs par ID d'instance, vous pouvez utiliser votre équilibreur de charge avec un groupe Auto Scaling. Après avoir attaché un groupe cible à un groupe Auto Scaling et que ce groupe monte en puissance, les instances lancées par le groupe Auto Scaling sont automatiquement enregistrées avec le groupe cible. Si vous détachez l'équilibreur de charge du groupe Auto Scaling, l'enregistrement des instances est annulé automatiquement dans le groupe cible. Pour plus d'informations, veuillez consulter [Attacher un équilibreur de charge à votre groupe Auto Scaling](#) (langue française non garantie) dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.

Groupes de sécurité cibles

Avant d'ajouter des cibles à votre groupe cible, configurez les groupes de sécurité associés aux cibles pour qu'ils acceptent le trafic provenant de votre Network Load Balancer.

Recommandations pour les groupes de sécurité cibles si un groupe de sécurité est associé à l'équilibreur de charge

- Pour autoriser le trafic client : ajoutez une règle qui fait référence au groupe de sécurité associé à l'équilibreur de charge.
- Pour autoriser le PrivateLink trafic : si vous avez configuré l'équilibreur de charge pour évaluer les règles entrantes relatives au trafic envoyé AWS PrivateLink, ajoutez une règle qui accepte le trafic provenant du groupe de sécurité de l'équilibreur de charge sur le port de trafic. Sinon, ajoutez une règle qui accepte le trafic provenant des adresses IP privées de l'équilibreur de charge sur le port de trafic.
- Pour accepter les surveillances de l'état de l'équilibreur de charge : ajoutez une règle qui accepte le trafic de surveillance de l'état provenant des groupes de sécurité de l'équilibreur de charge sur le port de surveillance.

Recommandations pour les groupes de sécurité cibles si aucun groupe de sécurité n'est associé à l'équilibreur de charge

- Pour autoriser le trafic client : si votre équilibreur de charge préserve les adresses IP client, ajoutez une règle qui accepte le trafic provenant des adresses IP de clients approuvés sur le port de trafic. Sinon, ajoutez une règle qui accepte le trafic provenant des adresses IP privées de l'équilibreur de charge sur le port de trafic.
- Pour autoriser PrivateLink le trafic : ajoutez une règle qui accepte le trafic provenant des adresses IP privées de l'équilibreur de charge sur le port de trafic.
- Pour accepter les surveillances de l'état de l'équilibreur de charge : ajoutez une règle qui accepte le trafic de surveillance de l'état provenant des adresses IP privées de l'équilibreur de charge sur le port de surveillance.

Comment fonctionne la préservation des adresses IP client

Les Network Load Balancers ne préservent pas les adresses IP client, sauf si vous définissez l'attribut `preserve_client_ip.enabled` sur `true`. De plus, avec les équilibreurs de charge réseau à double pile, nous préservons les adresses IP des clients lors de la traduction des adresses IPv4 en IPv6. Toutefois, lors de la traduction d'adresses IPv6 en IPv4, l'adresse IP source est toujours l'adresse IP privée du Network Load Balancer.

Pour rechercher les adresses IP privées de l'équilibreur de charge à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Network Interfaces (Interfaces réseau).
3. Dans le champ de recherche, saisissez le nom de votre Network Load Balancer. Il existe une interface réseau par sous-réseau d'équilibreur de charge.
4. Dans l'onglet Détails de chaque interface réseau, copiez l'adresse depuis Adresse privée IPv4.

Pour plus d'informations, consultez [Groupes de sécurité de votre Network Load Balancer](#).

Listes ACL réseau

Lorsque vous enregistrez des instances EC2 comme cibles, vous devez vous assurer que les réseaux ACL pour les réseaux pour vos instances permettent le trafic sur le port d'écoute et le port de vérification de l'état. La liste de contrôle des accès (ACL) réseau par défaut pour un VPC

autorise tout le trafic entrant et sortant. Si vous créez des listes de contrôle des accès (ACL) réseau personnalisées, vérifiez qu'elles autorisent le trafic approprié.

Les listes ACL réseau associées aux sous-réseaux de vos instances doivent autoriser le trafic suivant pour un équilibreur de charge accessible sur Internet.

Règles recommandées pour les sous-réseaux d'instance

Inbound

Source	Protocole	Plage de ports	Commentaire
<i>Adresses IP client</i>	<i>écouteur</i>	<i>écouteur</i>	Autoriser le trafic client (type de cible instance)
<i>Bloc d'adresse du VPC</i>	<i>écouteur</i>	<i>écouteur</i>	Autoriser le trafic client (type de cible ip)
<i>Bloc d'adresse du VPC</i>	<i>vérification_état</i>	<i>vérification_état</i>	Autoriser le trafic de vérification de l'état depuis l'équilibreur de charge.

Outbound

Destination (Destination)	Protocole	Plage de ports	Commentaire
<i>Adresses IP client</i>	<i>écouteur</i>	<i>écouteur</i>	Autoriser les réponses aux clients (type de cible instance)
<i>Bloc d'adresse du VPC</i>	<i>écouteur</i>	<i>écouteur</i>	Autoriser les réponses aux clients (type de cible ip)
<i>Bloc d'adresse du VPC</i>	<i>vérification_état</i>	1024-65535	Autoriser le trafic de vérification de l'état

Les listes ACL réseau associées aux sous-réseaux de votre équilibreur de charge doivent autoriser le trafic suivant pour un équilibreur de charge accessible sur Internet.

Règles recommandées pour les sous-réseaux de l'équilibreur de charge

Inbound

Source	Protocole	Plage de ports	Commentaire
<i>Adresses IP client</i>	<i>écouteur</i>	<i>écouteur</i>	Autoriser le trafic client (type de cible instance)
<i>Bloc d'adresse du VPC</i>	<i>écouteur</i>	<i>écouteur</i>	Autoriser le trafic client (type de cible ip)
<i>Bloc d'adresse du VPC</i>	<i>vérification_état</i>	1024-65535	Autoriser le trafic de vérification de l'état

Outbound

Destination (Destination)	Protocole	Plage de ports	Commentaire
<i>Adresses IP client</i>	<i>écouteur</i>	<i>écouteur</i>	Autoriser les réponses aux clients (type de cible instance)
<i>Bloc d'adresse du VPC</i>	<i>écouteur</i>	<i>écouteur</i>	Autoriser les réponses aux clients (type de cible ip)
<i>Bloc d'adresse du VPC</i>	<i>vérification_état</i>	<i>vérification_état</i>	Autoriser le trafic de vérification de l'état
<i>Bloc d'adresse du VPC</i>	<i>vérification_état</i>	1024-65535	Autoriser le trafic de vérification de l'état

Pour un équilibreur de charge interne, les listes ACL réseau des sous-réseaux de vos instances et nœuds d'équilibreur de charge doivent autoriser le trafic entrant et sortant vers et depuis le CIDR VPC, sur le port d'écoute et les ports éphémères.

Sous-réseaux partagés

Les participants peuvent créer un Network Load Balancer dans un VPC partagé. Les participants ne peuvent pas enregistrer une cible exécutée dans un sous-réseau qui n'est pas partagé avec eux.

Les sous-réseaux partagés pour les équilibreurs de charge réseau sont pris en charge dans toutes les AWS régions, à l'exception des suivantes :

- Asie-Pacifique (Osaka) ap-northeast-3
- Asie-Pacifique (Hong Kong) ap-east-1
- Moyen-Orient (Bahreïn) me-south-1
- AWS Chine (Pékin) cn-north-1
- AWS Chine (Ningxia) cn-northwest-1

Enregistrer ou annuler l'enregistrement de cibles

Chaque groupe cible doit avoir au moins une cible enregistrée dans chaque zone de disponibilité qui est activée pour l'équilibreur de charge.

Le type de cible de votre groupe cible détermine la façon dont vous enregistrez les cibles auprès du groupe cible. Pour plus d'informations, consultez [Type de cible](#).

Exigences et considérations

- Vous ne pouvez pas enregistrer des instances par ID d'instance si elles utilisent l'un des types d'instance suivants : C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 ou T1.
- Lorsque vous enregistrez des cibles par ID d'instance pour un groupe cible IPv6, une adresse IPv6 principale doit être attribuée aux cibles. Pour en savoir plus, consultez les [adresses IPv6](#) dans le guide de l'utilisateur Amazon EC2
- Lorsque vous enregistrez des cibles par ID d'instance, les instances doivent se trouver dans le même Amazon VPC que le Network Load Balancer. Vous ne pouvez pas enregistrer des instances par ID d'instance si elles se trouvent dans un VPC appairé au VPC de l'équilibreur de charge (même région ou région différente). Vous pouvez enregistrer ces instances par adresse IP.

- Si vous enregistrez une cible par adresse IP et que l'adresse IP se trouve dans le même VPC que l'équilibreur de charge, ce dernier vérifie qu'elle provient d'un sous-réseau qu'elle peut atteindre.
- Pour les groupes cibles UDP et TCP_UDP, n'enregistrez pas les instances par adresse IP si elles se trouvent en dehors du VPC de l'équilibreur de charge ou si elles utilisent l'un des types d'instance suivants : C1, CC1, CC2, CG1, CG2, CR1, G1, G2, HI1, HS1, M1, M2, M3 ou T1. Les cibles situées en dehors du VPC de l'équilibreur de charge ou utilisant un type d'instance non pris en charge peuvent être en mesure de recevoir du trafic en provenance de l'équilibreur de charge, mais ne pas être en mesure de répondre.

Table des matières

- [Enregistrer ou annuler l'enregistrement de cibles par ID d'instance](#)
- [Enregistrer ou annuler l'enregistrement de cibles par adresse IP](#)
- [Enregistrer ou annuler l'enregistrement de cibles à l'aide de l' AWS CLI](#)

Enregistrer ou annuler l'enregistrement de cibles par ID d'instance

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

Pour enregistrer des cibles par ID d'instance ou en annuler l'enregistrement à l'aide de la console

1. Ouvrez la console Amazon EC2 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. Pour enregistrer des instances, choisissez Enregistrer les cibles. Sélectionnez une ou plusieurs instances, saisissez le port d'instance par défaut selon vos besoins, puis choisissez Inclure comme étant en attente ci-dessous. Lorsque vous avez terminé d'ajouter des instances, choisissez Enregistrer les cibles en attente.

Remarque :

- Une adresse IPv6 principale doit être attribuée aux instances pour qu'elles soient enregistrées auprès d'un groupe cible IPv6.

- Les AWS GovCloud (US) Region s ne prennent pas en charge l'attribution d'une adresse IPv6 principale à l'aide de la console. Vous devez utiliser l'API pour attribuer des adresses IPv6 principales dans AWS GovCloud (US) Region s.
6. Pour annuler l'enregistrement d'instances, sélectionnez-les, puis choisissez Annuler l'enregistrement.

Enregistrer ou annuler l'enregistrement de cibles par adresse IP

Cibles IPv4

Une adresse IP que vous inscrivez doit provenir d'un des blocs d'adresse CIDR suivants :

- Les sous-réseaux du VPC pour le groupe cible
- 10.0.0.0/8 (RFC 1918)
- 100.64.0.0/10 (RFC 6598)
- 172.16.0.0/12 (RFC 1918)
- 192.168.0.0/16 (RFC 1918)

Le type d'adresse IP ne peut pas être modifié après la création du groupe cible.

Lorsque vous lancez un Network Load Balancer dans un Amazon VPC partagé en tant que participant, vous ne pouvez enregistrer des cibles que dans des sous-réseaux partagés avec vous.

Cibles IPv6

- Les adresses IP que vous enregistrez doivent se trouver dans le bloc d'adresses CIDR VPC ou dans un bloc d'adresses CIDR VPC apparié.
- Le type d'adresse IP ne peut pas être modifié après la création du groupe cible.
- Vous pouvez associer des groupes cibles IPv6 uniquement à un équilibreur de charge à double pile doté d'écouteurs TCP ou TLS.

Pour enregistrer des cibles par adresse IP ou en annuler l'enregistrement à l'aide de la console

1. Ouvrez la console Amazon EC2 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. Pour enregistrer les adresses IP, sélectionnez Enregistrer les cibles. Pour chaque adresse IP, sélectionnez le réseau, la zone de disponibilité, l'adresse IP (IPv4 ou IPv6) et le port, puis choisissez Inclure comme étant en attente ci-dessous. Lorsque vous avez terminé de spécifier les adresses, choisissez Enregistrer les cibles en attente.
6. Pour annuler l'enregistrement d'adresses IP, sélectionnez-les, puis choisissez Annuler l'enregistrement. Si vous avez un grand nombre d'adresses IP enregistrées, vous pouvez ajouter un filtre ou modifier l'ordre de tri.

Enregistrer ou annuler l'enregistrement de cibles à l'aide de l' AWS CLI

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

Application Load Balancers en tant que cibles

Vous pouvez créer un groupe cible avec un seul Application Load Balancer comme cible et configurer votre Network Load Balancer pour y transférer le trafic. Dans ce scénario, l'Application Load Balancer prend en charge la décision d'équilibrage de charge dès que le trafic l'atteint. Cette configuration combine les fonctionnalités des deux équilibreurs de charge et offre les avantages suivants :

- Vous pouvez utiliser la fonctionnalité de routage basée sur les demandes de couche 7 de l'Application Load Balancer en combinaison avec des fonctionnalités prises en charge par le Network Load Balancer, telles que les services de point de terminaison (AWS PrivateLink) et les adresses IP statiques.
- Vous pouvez utiliser cette configuration pour les applications qui ont besoin d'un point de terminaison unique pour les protocoles multiples, comme les services multimédias utilisant le protocole HTTP pour la signalisation et le protocole RTP pour la diffusion de contenu.

Vous pouvez utiliser cette fonctionnalité avec un Application Load Balancer interne ou accessible sur Internet comme cible d'un Network Load Balancer interne ou accessible sur Internet.

Considérations

- Pour associer un Application Load Balancer en tant que cible d'un Network Load Balancer, il doit se trouver dans le même Amazon VPC au sein du même compte.

- Vous pouvez associer un Application Load Balancer en tant que cible de plusieurs Network Load Balancers. Pour ce faire, enregistrez l'Application Load Balancer auprès d'un groupe cible distinct pour chaque Network Load Balancer.
- Chaque Application Load Balancer que vous enregistrez auprès d'un Network Load Balancer réduit le nombre maximal de cibles par zone de disponibilité et par Network Load Balancer de 50 (si l'équilibrage de charge entre zones est désactivé) ou de 100 (si l'équilibrage de charge entre zones est activé). Vous pouvez désactiver l'équilibrage de charge entre zones dans les deux équilibreurs de charge afin de minimiser la latence et d'éviter les frais de transfert de données régionaux. Pour plus d'informations, consultez [Quotas de vos Network Load Balancers](#).
- Lorsque le type de groupe cible est a1b, vous ne pouvez pas modifier les attributs du groupe cible. Ces attributs utilisent toujours leurs valeurs par défaut.
- Après avoir enregistré un Application Load Balancer en tant que cible, vous ne pouvez pas le supprimer tant que vous n'avez pas annulé son enregistrement depuis tous les groupes cibles.

Étape 1 : créer l'Application Load Balancer

Avant de commencer, configurez les groupes cibles que cet Application Load Balancer utilisera. Assurez-vous de disposer d'un cloud privé virtuel (VPC) avec les cibles que vous allez enregistrer auprès du groupe cible. Ce VPC doit avoir au minimum un sous-réseau public dans chacune des zones de disponibilité utilisées par vos cibles.

Pour créer un Application Load Balancer à l'aide de la console

1. Ouvrez la console Amazon EC2 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. Choisissez Créer un équilibreur de charge.
4. Sous Application Load Balancer, choisissez Create (Créer).
5. Sur la page Créer un Application Load Balancer, sous Configuration de base, spécifiez le Nom de l'équilibreur de charge, son Schéma et le Type d'adresse IP.
6. Pour les Écouteurs, vous pouvez créer un écouteur HTTP ou HTTPS sur n'importe quel port. Cependant, vous devez vous assurer que le numéro de port de cet écouteur correspond au port du groupe cible dans lequel résidera cet Application Load Balancer.
7. Sous Zones de disponibilité, procédez comme suit :

- a. Pour le VPC, sélectionnez un cloud privé virtuel (VPC) avec des instances ou des adresses IP que vous avez incluses comme cibles de votre Application Load Balancer. Vous devez utiliser le même VPC que celui que vous utiliseriez pour votre Network Load Balancer dans [Étape 3 : créer un Network Load Balancer et configurer l'Application Load Balancer comme cible](#).
 - b. Sélectionnez au moins deux Zones de disponibilité et les sous-réseaux correspondants. Assurez-vous que ces zones de disponibilité correspondent à celles activées pour votre Network Load Balancer afin d'optimiser la disponibilité, la capacité de mise à l'échelle et les performances.
8. Vous pouvez Attribuer un groupe de sécurité à votre équilibreur de charge en créant un nouveau groupe de sécurité ou en sélectionnant un groupe existant.

Le groupe de sécurité que vous sélectionnez doit contenir une règle qui autorise le trafic vers le port d'écouteur de cet équilibreur de charge. Utilisez les blocs CIDR (plage d'adresses IP) des ordinateurs du client comme source de trafic dans les règles entrantes pour les groupes de sécurité. Cela permet aux clients d'envoyer du trafic via cet Application Load Balancer. Pour plus d'informations sur la configuration de groupes de sécurité pour un Application Load Balancer comme cible d'un Network Load Balancer, veuillez consulter [Groupes de sécurité pour votre Application Load Balancer](#) (langue française non garantie) dans le Guide de l'utilisateur des Application Load Balancers.

9. Pour Configurer le routage, sélectionnez le groupe cible que vous avez configuré pour cet Application Load Balancer. Si aucun groupe cible n'est disponible et que vous souhaitez en configurer un nouveau, veuillez consulter [Créer un groupe cible](#) dans le Guide de l'utilisateur des Application Load Balancers.
10. Examinez votre configuration, puis choisissez Create load balancer (Créer l'équilibreur de charge).

Pour créer l'Application Load Balancer à l'aide du AWS CLI

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

Étape 2 : créer le groupe cible avec l'Application Load Balancer comme cible

La création d'un groupe cible vous permet d'enregistrer un Application Load Balancer nouveau ou existant en tant que cible. Vous ne pouvez ajouter qu'un Application Load Balancer par groupe cible.

Le même Application Load Balancer peut également être utilisé dans un groupe cible distinct, en tant que cible de deux Network Load Balancers au maximum.

Pour créer un groupe cible et enregistrer l'Application Load Balancer en tant que cible, à l'aide de la console

1. Ouvrez la console Amazon EC2 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 Créer un groupe cible.
4. Sur la page Spécifier les informations de groupe, sous Configuration de base, sélectionnez Application Load Balancer.
5. Pour Nom du groupe cible, saisissez un nom pour le groupe cible d'Application Load Balancer.
6. Pour Protocole, seul le protocole TCP est autorisé. Sélectionnez le Port de votre groupe cible. Ce port du groupe cible doit correspondre au port d'écouteur de l'Application Load Balancer. Vous pouvez également ajouter ou modifier le port d'écouteur sur l'Application Load Balancer pour qu'il corresponde à ce port.
7. Pour VPC, sélectionnez le cloud privé virtuel (VPC) avec l'Application Load Balancer à enregistrer avec le groupe cible.
8. Pour Surveillances de l'état, choisissez HTTP ou HTTPS comme Protocole de surveillance de l'état. Les surveillances de l'état sont envoyées à l'Application Load Balancer et transmises à ses cibles en utilisant le port, le protocole et le chemin ping spécifiés. Assurez-vous que votre Application Load Balancer peut recevoir ces surveillances de l'état en disposant d'un écouteur doté d'un port et d'un protocole qui correspondent au port et au protocole de la surveillance de l'état.
9. (Facultatif) Ajoutez une ou plusieurs balises en fonction des besoins.
10. Choisissez Suivant.
11. Sur la page Enregistrer les cibles, choisissez l'Application Load Balancer que vous souhaitez enregistrer en tant que cible. L'Application Load Balancer que vous choisissez dans la liste doit avoir un écouteur sur le même port que le groupe cible que vous créez. Vous pouvez ajouter ou modifier un écouteur sur cet équilibreur de charge pour qu'il corresponde au port du groupe cible ou revenir à l'étape précédente et modifier le port spécifié pour le groupe cible. Si vous ne savez pas quel Application Load Balancer ajouter comme cible, ou si vous ne souhaitez pas l'ajouter à ce stade, vous pouvez choisir d'ajouter l'Application Load Balancer ultérieurement.
12. Sélectionnez Créer un groupe cible.

Pour créer un groupe cible et enregistrer l'Application Load Balancer en tant que cible à l'aide de l'AWS CLI

Utilisez les commandes [create-target-group](#) et [register-targets](#).

Étape 3 : créer un Network Load Balancer et configurer l'Application Load Balancer comme cible

Procédez comme suit pour créer le Network Load Balancer, puis configurer l'Application Load Balancer comme cible à l'aide de la console.

Pour créer votre Network Load Balancer et votre écouteur à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le panneau de navigation, sous Load Balancing (Équilibrage de charge), choisissez Load Balancers (Équilibreur de charge).
3. Choisissez Créer un équilibreur de charge.
4. Sous Network Load Balancer, choisissez Créer.
5. Configuration de base

Dans le panneau Configuration de base, configurez le Nom de l'équilibreur de charge, son Schéma et le Type d'adresse IP.

6. Mappage du réseau
 - a. Pour VPC, sélectionnez le même VPC que celui que vous avez utilisé pour votre cible Application Load Balancer. Si vous avez sélectionné Accessible via Internet pour Schéma, seuls les VPC dotés d'une passerelle Internet pourront être sélectionnés.
 - b. Pour les Mappages, sélectionnez une ou plusieurs zones de disponibilité et les sous-réseaux correspondants. Nous vous recommandons de sélectionner les mêmes zones de disponibilité que votre cible Application Load Balancer afin d'optimiser la disponibilité, la capacité de mise à l'échelle et les performances.

(Facultatif) Pour utiliser des adresses IP statiques, choisissez Utiliser une adresse IP Elastic dans les Paramètres IPv4 de chaque zone de disponibilité. Avec les adresses IP statiques, vous pouvez ajouter certaines adresses IP à une liste d'autorisation pour les pare-feu, ou vous pouvez coder en dur des adresses IP avec des clients.

7. Écouteurs et routage

- a. La valeur par défaut est un écouteur qui accepte le trafic TCP sur le port 80. Seuls les écouteurs TCP peuvent transférer le trafic vers un groupe cible d'Application Load Balancer. Pour Protocole, vous devez conserver la valeur TCP, mais vous pouvez modifier le Port si nécessaire.

Avec cette configuration, vous pouvez utiliser des écouteurs HTTPS sur l'Application Load Balancer pour mettre fin au trafic TLS.

- b. Pour Action par défaut, sélectionnez le groupe cible Application Load Balancer pour transférer le trafic. S'il ne figure pas dans la liste ou s'il n'est pas possible de sélectionner un groupe cible (car il est déjà utilisé par un autre Network Load Balancer), vous pouvez créer un groupe cible Application Load Balancer comme indiqué dans [Étape 2 : créer le groupe cible avec l'Application Load Balancer comme cible](#).

8. Balises

(Facultatif) Ajoutez des balises pour catégoriser votre équilibreur de charge. Pour plus d'informations, veuillez consulter [Balises](#).

9. Récapitulatif

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

Pour créer le Network Load Balancer à l'aide du AWS CLI

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

Étape 4 : (facultatif) créer un point de terminaison d'un VPC

Pour utiliser le Network Load Balancer que vous avez configuré à l'étape précédente comme point de terminaison pour la connectivité privée, vous pouvez activer AWS PrivateLink. Cela établit une connexion privée à votre équilibreur de charge en tant que service de point de terminaison.

Pour créer un service de point de terminaison d'un VPC à l'aide de votre Network Load Balancer

1. Dans le volet de navigation, choisissez Load Balancers (Équilibreurs de charge).
2. Sélectionnez le nom du Network Load Balancer afin d'ouvrir sa page de détails.
3. Dans l'onglet Intégrations, développez Services de point de terminaison d'un VPC (AWS PrivateLink).

4. Choisissez Créer un point de terminaison pour ouvrir la page Services de point de terminaison. Pour les étapes restantes, veuillez consulter [Créer un service de point de terminaison](#) dans le Guide AWS PrivateLink .

Balises pour votre groupe cible

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 console Amazon EC2 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

Vous pouvez supprimer un groupe cible s'il n'est pas référencé par les actions de transfert des règles d'écouteur. 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 instance EC2 enregistrée, vous pouvez l'arrêter ou la suspendre.

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

1. Ouvrez la console Amazon EC2 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 commande [delete-target-group](#).

Surveillance de vos Network Load Balancers

Vous pouvez utiliser les fonctions suivantes pour surveiller vos équilibreurs de charge, analyser les modèles de trafic et résoudre les problèmes liés à vos équilibreurs de charge et vos cibles.

CloudWatch métriques

Vous pouvez utiliser Amazon CloudWatch pour récupérer des statistiques sur les points de données de vos équilibreurs de charge 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 plus d'informations, consultez [CloudWatch métriques pour votre Network Load Balancer](#).

Journaux de flux VPC

Vous pouvez utiliser les journaux de flux VPC pour capturer des informations détaillées sur le trafic entrant ou sortant de votre Network Load Balancer. Pour plus d'informations, veuillez consulter [Journaux de flux VPC](#) dans le Guide de l'utilisateur Amazon VPC.

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

Il existe deux entrées pour chaque connexion via votre Network Load Balancer : une pour la connexion frontend entre le client et l'équilibreur de charge et l'autre pour la connexion backend entre l'équilibreur de charge et la cible. Si l'attribut de préservation des adresses IP client du groupe cible est activé, la connexion apparaît à l'instance comme une connexion provenant du client. Dans le cas contraire, l'adresse IP source de la connexion est l'adresse IP privée de l'équilibreur de charge. Si le groupe de sécurité de l'instance n'autorise pas les connexions depuis le client, mais que les ACL réseau pour le sous-réseau de l'équilibreur de charge les autorisent, les journaux de l'interface réseau pour l'équilibreur de charge indiquent « ACCEPT OK » pour les connexions frontales et backend, alors que les journaux de l'interface réseau pour l'instance indiquent « REJECT OK » pour la connexion.

Si un Network Load Balancer est associé à des groupes de sécurité, vos journaux de flux contiennent des entrées relatives au trafic autorisé ou rejeté par les groupes de sécurité. Pour les Network Load Balancers dotés d'écouteurs TLS, les entrées de vos journaux de flux reflètent uniquement les entrées rejetées.

Journaux d'accès

Vous pouvez utiliser des journaux d'accès pour capturer des informations détaillées sur les demandes TLS envoyées à votre équilibreur de charge. Les fichiers journaux sont stockés dans Amazon S3. Vous pouvez utiliser ces journaux d'accès pour analyser les modèles de trafic et résoudre les problèmes liés à vos cibles. Pour plus d'informations, consultez [Journaux d'accès de votre Network Load Balancer](#).

CloudTrail journaux

Vous pouvez l'utiliser AWS CloudTrail pour capturer des informations détaillées sur les appels passés à l'API Elastic Load Balancing 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 plus d'informations, consultez [Journalisation des appels d'API pour votre Network Load Balancer à l'aide d' AWS CloudTrail](#).

CloudWatch métriques pour votre Network Load Balancer

Elastic Load Balancing publie des points de données sur Amazon CloudWatch pour vos équilibreurs de charge 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 équilibreur de charge 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 les métriques CloudWatch uniquement lorsque les demandes transitent par l'équilibreur de charge. 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 par l'équilibreur de charge ou s'il n'existe pas de données pour une métrique, cette dernière n'est pas présentée. Pour les équilibreurs de charge réseau dotés de groupes de sécurité, le trafic rejeté par les groupes de sécurité n'est pas pris en compte dans les CloudWatch métriques.

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

Table des matières

- [Métriques des Network Load Balancers](#)
- [Dimensions de métriques des Network Load Balancers](#)
- [Statistiques des métriques Network Load Balancer](#)
- [Afficher CloudWatch les statistiques de votre équilibreur de charge](#)

Métriques des Network Load Balancers

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

Métrique	Description
ActiveFlowCount	<p>Nombre total de flux (ou connexions) simultanés provenant des clients vers des cibles. Cette métrique comprend les connexions dont l'état est SYN_SENT et ESTABLISHED. Les connexions TCP ne sont pas mises hors service au niveau de l'équilibreur de charge ; un client qui ouvre une connexion TCP avec une cible est donc comptabilisé comme un seul flux.</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
ActiveFlowCount_TCP	<p>Nombre total de flux (ou connexions) TCP simultanés provenant des clients vers des cibles. Cette métrique comprend les connexions dont l'état est SYN_SENT et ESTABLISHED. Les connexions TCP ne sont pas mises hors service au niveau de l'équilibreur de charge ; un client qui ouvre une connexion TCP avec une cible est donc comptabilisé comme un seul flux.</p>

Métrique	Description
	<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
ActiveFlowCount_TL S	<p>Nombre total de flux (ou connexions) TLS simultanés provenant des clients vers des cibles. Cette métrique comprend les connexions dont l'état est SYN_SENT et ESTABLISHED.</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
ActiveFlowCount_UD P	<p>Nombre total de flux (ou connexions) UDP 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

Métrique	Description
ClientTLSNegotiationErrorCount	<p>Nombre total de liaisons TLS qui ont échoué lors de la négociation entre un client et un écouteur TLS.</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
ConsumedLCUs	<p>Nombre d'unités de capacité d'équilibreur de charge (LCU) utilisées par votre équilibreur de charge. Vous ne payez que pour les unités LCU 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
ConsumedLCUs_TCP	<p>Nombre d'unités de capacité d'équilibreur de charge (LCU) utilisées par votre équilibreur de charge pour TCP. Vous ne payez que pour les unités LCU que vous utilisez par heure. Pour plus d'informations, consultez Tarification Elastic Load Balancing.</p> <p>Critères de notification : il existe une valeur différente de zéro.</p> <p>Statistics : All</p> <p>Dimensions</p> <ul style="list-style-type: none">• LoadBalancer

Métrique	Description
ConsumedLCUs_TLS	<p>Nombre d'unités de capacité d'équilibreur de charge (LCU) utilisées par votre équilibreur de charge pour TLS. Vous ne payez que pour les unités LCU que vous utilisez par heure. Pour plus d'informations, consultez Tarification Elastic Load Balancing.</p> <p>Critères de notification : il existe une valeur différente de zéro.</p> <p>Statistics : All</p> <p>Dimensions</p> <ul style="list-style-type: none">• LoadBalancer
ConsumedLCUs_UDP	<p>Nombre d'unités de capacité d'équilibreur de charge (LCU) utilisées par votre équilibreur de charge pour UDP. Vous ne payez que pour les unités LCU que vous utilisez par heure. Pour plus d'informations, consultez Tarification Elastic Load Balancing.</p> <p>Critères de notification : il existe une valeur différente de zéro.</p> <p>Statistics : All</p> <p>Dimensions</p> <ul style="list-style-type: none">• LoadBalancer

Métrique	Description
HealthyHostCount	<p>Nombre de cibles considérées saines. Cette métrique n'inclut aucun Application Load Balancer enregistré comme cible.</p> <p>Critères de notification : signalé si les surveillances 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
NewFlowCount	<p>Nombre total de nouveaux flux (ou connexions) établis entre les clients et les cibles pendant la période.</p> <p>Critères de notification : toujours signalé.</p> <p>Statistics : la statistique la plus utile est Sum.</p> <p>Dimensions</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer
NewFlowCount_TCP	<p>Nombre total de nouveaux flux (ou connexions) TCP 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"> • LoadBalancer • AvailabilityZone , LoadBalancer

Métrique	Description
NewFlowCount_TLS	<p>Nombre total de nouveaux flux (ou connexions) TLS 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">• LoadBalancer• AvailabilityZone , LoadBalancer
NewFlowCount_UDP	<p>Nombre total de nouveaux flux (ou connexions) UDP 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">• LoadBalancer• AvailabilityZone , LoadBalancer
PeakPacketsPerSecond	<p>Débit moyen de paquets le plus élevé (paquets traités par seconde), calculé toutes les 10 secondes pendant la fenêtre d'échantillonnage. Cette métrique inclut le trafic de surveillance de l'état.</p> <p>Critères de notification : il existe une valeur différente de zéro.</p> <p>Statistics : la statistique la plus utile est Maximum.</p> <p>Dimensions</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer

Métrique	Description
PortAllocationErrorCount	<p>Nombre total d'erreurs éphémères d'attribution de port lors d'une opération de traduction IP client. Une valeur différente de zéro indique l'interruption des connexions client.</p> <p>Remarque : un Network Load Balancer prend en charge 55 000 connexions simultanées ou environ 55 000 connexions par minute sur chaque cible unique (adresse IP et port) lors de la traduction des adresses IP client. Pour résoudre les erreurs d'attribution de port, ajoutez davantage de cibles au groupe cible.</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
ProcessedBytes	<p>Nombre total d'octets traités par l'équilibreur de charge, y compris les en-têtes TCP/IP. Ce nombre inclut le trafic vers et depuis les cibles, moins le trafic lié à la vérification de l'état.</p> <p>Critères de notification : toujours signalé.</p> <p>Statistics : la statistique la plus utile est Sum.</p> <p>Dimensions</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer

Métrique	Description
ProcessedBytes_TCP	<p>Nombre total d'octets traités par les écouteurs TCP.</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
ProcessedBytes_TLS	<p>Nombre total d'octets traités par les écouteurs TLS.</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
ProcessedBytes_UDP	<p>Nombre total d'octets traités par les écouteurs UDP.</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

Métrique	Description
ProcessedPackets	<p>Nombre total de paquets traités par l'équilibreur de charge. Ce nombre inclut le trafic vers et depuis les cibles, y compris le trafic lié à la surveillance 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">• LoadBalancer• AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Inbound_ICMP	<p>Nombre de nouveaux messages ICMP rejetés par les règles entrantes des groupes de sécurité de 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
SecurityGroupBlockedFlowCount_Inbound_TCP	<p>Nombre de nouveaux flux TCP rejetés par les règles entrantes des groupes de sécurité de 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

Métrique	Description
SecurityGroupBlockedFlowCount_Inbound_UDP	<p>Nombre de nouveaux flux UDP rejetés par les règles entrantes des groupes de sécurité de 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
SecurityGroupBlockedFlowCount_Outbound_ICMP	<p>Nombre de nouveaux messages ICMP rejetés par les règles sortantes des groupes de sécurité de 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
SecurityGroupBlockedFlowCount_Outbound_TCP	<p>Nombre de nouveaux flux TCP rejetés par les règles sortantes des groupes de sécurité de 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

Métrique	Description
SecurityGroupBlockedFlowCount_Outbound_UDP	<p>Nombre de nouveaux flux UDP rejetés par les règles sortantes des groupes de sécurité de 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
TargetTLSNegotiationErrorCount	<p>Nombre total de liaisons TLS qui ont échoué lors de la négociation entre un écouteur TLS et une cible.</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
TCP_Client_Reset_Count	<p>Nombre total de paquets de réinitialisation (RST) envoyés par un client à une cible. Les réinitialisations sont générées par le client et transférées par l'équilibreur de charge.</p> <p>Critères de notification : toujours signalé.</p> <p>Statistics : la statistique la plus utile est Sum.</p> <p>Dimensions</p> <ul style="list-style-type: none">• LoadBalancer• AvailabilityZone , LoadBalancer

Métrique	Description
TCP_ELB_Reset_Count	<p>Nombre total de paquets de réinitialisation (RST) générés par l'équilibreur de charge. Pour plus d'informations, consultez Dépannage.</p> <p>Critères de notification : toujours signalé.</p> <p>Statistics : la statistique la plus utile est Sum.</p> <p>Dimensions</p> <ul style="list-style-type: none"> • LoadBalancer • AvailabilityZone , LoadBalancer
TCP_Target_Reset_Count	<p>Nombre total de paquets de réinitialisation (RST) envoyés par une cible à un client. Les réinitialisations sont générées par la cible et transférées par l'équilibreur de charge.</p> <p>Critères de notification : toujours signalé.</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. Cette métrique n'inclut aucun Application Load Balancer enregistré comme cible.</p> <p>Critères de notification : signalé si les surveillances 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

Métrique	Description
UnhealthyRoutingFlowCount	<p>Nombre de flux (ou de connexions) acheminés à l'aide de l'action de basculement du routage (fail-open).</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

Dimensions de métriques des Network Load Balancers

Pour filtrer les métriques pour votre équilibreur de charge, utilisez les dimensions ci-dessous.

Dimension	Description
AvailabilityZone	Filtrer les données métriques par Zone de disponibilité.
LoadBalancer	Filtre les données métriques en fonction de l'équilibreur de charge. Spécifiez l'équilibreur de charge comme suit : net/load-balancer-name/1234567890123456 (partie finale de l'ARN de l'équilibreur de charge).
TargetGroup	Filtre les données métriques en fonction du groupe cible. Spécifiez le groupe cible comme suit : targetgroup/target-group-name/1234567890123456 (partie finale du groupe cible ARN).

Statistiques des métriques Network Load Balancer

CloudWatch fournit des statistiques basées sur les points de données métriques publiés par Elastic Load Balancing. Les statistiques sont des regroupements de données de métrique sur une période donnée. Lorsque vous demandez des statistiques, le flux de données renvoyé est identifié par le nom et la dimension de la métrique. Une dimension est une paire nom/valeur qui identifie une métrique de

manière unique. Par exemple, vous pouvez demander des statistiques pour toutes les instances EC2 saines derrière un équilibreur de charge, lancées dans une zone de disponibilité spécifique.

Les statistiques `Maximum` et `Minimum` reflètent les valeurs minimum et maximum des points de données signalés par les nœuds de l'équilibreur de charge individuel dans chaque fenêtre d'échantillonnage. L'augmentation du maximum de `HealthyHostCount` correspond à la baisse du minimum de `UnHealthyHostCount`. Il est recommandé de surveiller le `HealthyHostCount` maximal, en invoquant l'alarme lorsque le `HealthyHostCount` maximal tombe en dessous du minimum requis, ou s'il est égal à 0. Cela peut vous aider à identifier les cas où vos cibles sont devenues défectueuses. Il est également recommandé de surveiller le `UnHealthyHostCount` minimal en invoquant l'alarme lorsque le `UnHealthyHostCount` minimal est supérieur à 0. Cela vous permet d'être averti lorsqu'il n'y a plus de cibles enregistrées.

La statistique `Sum` est la valeur regroupée pour tous les nœuds d'équilibreur de charge. Étant donné que les métriques incluent plusieurs rapports par période, `Sum` ne s'applique qu'aux métriques qui sont regroupées pour tous les nœuds d'équilibreur de charge.

La statistique `SampleCount` est le nombre d'échantillons mesurés. Étant donné que les métriques sont collectées selon des intervalles de prélèvement et des événements, cette statistique n'est généralement pas utile. Par exemple, avec `HealthyHostCount`, `SampleCount` est basé sur le nombre d'échantillons que chaque nœud d'équilibreur de charge signale, et non sur le nombre d'hôtes sains.

Afficher CloudWatch les statistiques de votre équilibreur de charge

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

Vous pouvez également consulter les métriques de votre équilibreur de charge à l'aide de la CloudWatch console.

Pour afficher des métriques à l'aide de la console

1. Ouvrez la console Amazon EC2 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 équilibreur de charge , procédez comme suit :
 - a. Dans le volet de navigation, choisissez Load Balancers.
 - b. Sélectionnez votre équilibreur de charge, 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/](https://console.aws.amazon.com/cloudwatch/).
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Sélectionnez l'espace de nom NetworkELB.
4. (Facultatif) Pour afficher une métrique pour toutes les dimensions, saisissez 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/NetworkELB
```

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

Utilisez la commande [get-metric-statistics](#) pour obtenir les 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/NetworkELB \  
--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": "2017-04-18T22:00:00Z",  
      "Average": 0.0,  
      "Unit": "Count"  
    },  
    {  
      "Timestamp": "2017-04-18T04:00:00Z",  
      "Average": 0.0,  
      "Unit": "Count"  
    },  
    ...  
  ],  
  "Label": "UnHealthyHostCount"  
}
```

Journaux d'accès de votre Network Load Balancer

Elastic Load Balancing fournit des journaux d'accès qui capturent des informations détaillées sur les connexions TLS établies avec votre Network Load Balancer. Vous pouvez utiliser ces journaux d'accès pour analyser les modèles de trafic et résoudre des problèmes.

Important

Les journaux d'accès sont créés uniquement lorsque le Network Load Balancer dispose d'un écouteur TLS et qu'ils contiennent des informations uniquement sur les connexions TLS.

La journalisation des accès est une fonction facultative d'Elastic Load Balancing qui est désactivée par défaut. Une fois que vous avez activé la journalisation des accès pour votre équilibreur de charge, Elastic Load Balancing capture les journaux sous forme de fichiers compressés et les stocke dans le compartiment Amazon S3 que vous spécifiez. Vous pouvez désactiver la journalisation des accès à tout moment.

Vous pouvez activer le chiffrement côté serveur avec des clés de chiffrement gérées par Amazon S3 (SSE-S3) ou utiliser Key Management Service avec des clés gérées par le client (CMK SSE-KMS) pour votre compartiment S3. Tous les fichiers de journaux d'accès sont automatiquement chiffrés avant d'être stockés dans votre compartiment S3, puis déchiffrés lorsque vous y accédez. Aucune action de votre part n'est requise puisqu'il n'y a aucune différence dans la manière dont vous accédez aux fichiers journaux chiffrés ou déchiffrés. Chaque fichier journal est chiffré à l'aide d'une clé unique, elle-même chiffrée à l'aide d'une clé KMS qui fait l'objet d'une rotation régulière. Pour plus d'informations, consultez les sections [Spécification du chiffrement Amazon S3 \(SSE-S3\)](#) et [Spécification du chiffrement côté serveur avec AWS KMS \(SSE-KMS\) dans le guide de l'utilisateur Amazon S3](#).

L'utilisation des journaux d'accès n'implique aucun coût supplémentaire. Les coûts de stockage pour Amazon S3 vous sont facturés, mais pas la bande passante utilisée par Elastic Load Balancing pour envoyer les fichiers journaux à Amazon S3. Pour plus d'informations sur les coûts de stockage, consultez [Tarification Amazon S3](#).

Fichiers journaux d'accès

Elastic Load Balancing publie un fichier journal pour chaque nœud d'équilibreur de charge toutes les 5 minutes. La diffusion de journaux est cohérente à terme. L'équilibreur de charge peut fournir plusieurs journaux pour la même période. Cela se produit généralement si le site connaît un trafic dense.

Les noms de fichiers des journaux d'accès respectent le format suivant :

```
bucket[/prefix]/AWSLogs/aws-account-id/elasticloadbalancing/region/yyyy/mm/dd/aws-account-id_elasticloadbalancing_region_net.load-balancer-id_end-time_random-string.log.gz
```

bucket

Nom du compartiment S3.

prefix

Préfixe (hiérarchie logique) dans le compartiment. Si vous ne spécifiez pas de préfixe, les journaux sont placés à la racine du compartiment.

aws-account-id

L' Compte AWS identifiant du propriétaire.

region

Région pour votre équilibreur de charge et le compartiment S3.

aaaa/mm/jj

Date à laquelle le journal a été fourni.

load-balancer-id

ID de ressource de l'équilibreur de charge. Si l'ID de ressource contient des barres obliques (/), elles sont remplacées par des points (.).

end-time

Date et heure auxquelles l'intervalle de journalisation a pris fin. Par exemple, une heure de fin 20181220T2340Z contient des entrées pour les demandes effectuées entre 23h35 et 23h40.

random-string

Chaîne aléatoire générée par le système.

Voici un exemple de nom de fichier journal :

```
s3://my-bucket/prefix/AWSLogs/123456789012/elasticloadbalancing/us-east-2/2020/05/01/123456789012_elasticloadbalancing_us-east-2_net.my-loadbalancer.1234567890abcdef_20200501T0000Z_20sg8hgm.log.gz
```

Vous pouvez stocker vos fichiers journaux dans votre compartiment aussi longtemps que vous le souhaitez, mais vous pouvez également définir des règles de cycle de vie Amazon S3 pour archiver ou supprimer automatiquement les fichiers journaux. Pour plus d'informations, veuillez consulter [Gestion du cycle de vie de votre stockage](#) dans le Guide de l'utilisateur Amazon S3.

Entrées des journaux d'accès

Le tableau suivant décrit les champs d'une entrée de journal d'accès, dans l'ordre. Tous les champs sont délimités par des espaces. Lorsque de nouveaux champs sont insérés, ils sont ajoutés à la fin de l'entrée de journal. Lors du traitement des fichiers journaux, vous devez ignorer les champs situés à la fin de l'entrée de journal que vous n'attendiez pas.

Champ	Description
type	Le type d'écouteur. La valeur prise en charge est t1s.

Champ	Description
version	La version de l'entrée de journal. La version actuelle est 2.0.
time	Le temps enregistré à la fin de la connexion TLS, au format ISO 8601.
elb	ID de ressource de l'équilibreur de charge.
écouteur	L'ID de ressource de l'écouteur TLS pour la connexion.
client:port	Adresse IP et port du client.
destination:port	Adresse IP et port de la destination. Si le client se connecte directement à l'équilibreur de charge, la destination est l'écouteur. Si le client se connecte à l'aide d'un service de point de terminaison de VPC, la destination est le point de terminaison de VPC.
connection_time	Durée totale pour établir la connexion, du début à la fermeture, en millisecondes.
tls_handshake_time	Durée totale pour établir la liaison TLS après l'établissement de la connexion TCP, y compris les retards côté client, en millisecondes. Cette durée est incluse dans le champ connection_time.
received_bytes	Le nombre d'octets reçus par l'équilibreur de charge à partir du client, après déchiffrement.
sent_bytes	Le nombre d'octets envoyés par l'équilibreur de charge au client, après déchiffrement.
incoming_tls_alert	La valeur entière des alertes TLS reçues par l'équilibreur de charge à partir du client, le cas échéant. Sinon, cette valeur est définie sur -.
chosen_cert_arn	ARN du certificat mis à la disposition du client. Si aucun message Hello client valide n'est envoyé, cette valeur est définie sur -.
chosen_cert_serial	Réservé pour un usage futur. Cette valeur est toujours définie sur -.
tls_cipher	La suite de chiffrement négociée avec le client, au format OpenSSL. Si la négociation TLS n'est pas exécutée, cette valeur est définie sur -.

Champ	Description
tls_protocol_version	Le protocole TLS négocié avec le client, au format chaîne. Les valeurs possibles sont <code>tlsv10</code> , <code>tlsv11</code> , <code>tlsv12</code> et <code>tlsv13</code> . Si la négociation TLS n'est pas exécutée, cette valeur est définie sur <code>-</code> .
tls_named_group	Réservé pour un usage futur. Cette valeur est toujours définie sur <code>-</code> .
domain_name	Valeur de l'extension <code>server_name</code> dans le message Hello client. Ce champ est codé en URL. Si aucun message Hello client valide n'est envoyé ou que l'extension manque, cette valeur est définie sur <code>-</code> .
alpn_fe_protocol	Le protocole TLS négocié avec le client, au format chaîne. Les valeurs possibles sont <code>h2</code> , <code>http/1.1</code> et <code>http/1.0</code> . Si aucune stratégie ALPN n'est configurée dans l'écouteur TLS, si aucun protocole correspondant n'est trouvé ou si aucune liste de protocoles valide n'est envoyée, cette valeur est définie sur <code>-</code> .
alpn_be_protocol	Protocole d'application négocié avec la cible, au format chaîne. Les valeurs possibles sont <code>h2</code> , <code>http/1.1</code> et <code>http/1.0</code> . Si aucune stratégie ALPN n'est configurée dans l'écouteur TLS, si aucun protocole correspondant n'est trouvé ou si aucune liste de protocoles valide n'est envoyée, cette valeur est définie sur <code>-</code> .
alpn_client_preference_list	Valeur de l'extension <code>application_layer_protocol_negotiation</code> dans le message client Hello. Ce champ est codé en URL. Chaque protocole est entouré de guillemets doubles et les protocoles sont séparés par une virgule. Si aucune stratégie ALPN n'est configurée dans l'écouteur TLS, si aucun message client valide n'est envoyé ou si l'extension n'est pas présente, cette valeur est définie sur <code>-</code> . La chaîne est tronquée si elle dépasse 256 octets.
tls_connection_creation_time	Le temps enregistré au début de la connexion TLS, au format ISO 8601.

Exemple d'entrées de journal

Des modèles d'entrées de journal sont présentés ci-après : Notez que le texte ne s'affiche sur plusieurs lignes que pour en faciliter la lecture.

Voici un exemple pour un écouteur TLS sans stratégie ALPN.

```
tls 2.0 2018-12-20T02:59:40 net/my-network-loadbalancer/c6e77e28c25b2234
g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
- - - 2018-12-20T02:59:30
```

Voici un exemple pour un écouteur TLS avec une stratégie ALPN.

```
tls 2.0 2020-04-01T08:51:42 net/my-network-loadbalancer/c6e77e28c25b2234
g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
h2 h2 "h2","http/1.1" 2020-04-01T08:51:20
```

Conditions requises pour le compartiment

Lorsque vous activez la journalisation des accès, vous devez spécifier un compartiment S3 pour les journaux d'accès. Le compartiment peut être détenu par un compte différent de celui possédant l'équilibreur de charge. Le compartiment doit répondre aux critères suivants :

Prérequis

- Le compartiment doit se situer dans la même région que l'équilibreur de charge.
- Le préfixe que vous spécifiez ne doit pas inclure AWSLogs. Nous ajoutons la partie du nom de fichier commençant par AWSLogs après le nom du compartiment et le préfixe que vous avez spécifié.
- Le compartiment doit avoir une stratégie de compartiment qui octroie l'autorisation d'écrire les journaux d'accès dans votre compartiment. Les stratégies de compartiment sont une collection

d'instructions JSON écrites dans le langage d'access policy permettant de définir des autorisations d'accès pour votre compartiment. Voici un exemple de politique .

```
{
  "Version": "2012-10-17",
  "Id": "AWSLogDeliveryWrite",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3::my-bucket",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": ["012345678912"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:us-east-1:012345678912:*"]
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-bucket/AWSLogs/account-ID/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": ["012345678912"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:us-east-1:012345678912:*"]
        }
      }
    }
  ]
}
```

```
}
```

Dans la stratégie précédente, pour `aws:SourceAccount`, spécifiez la liste des numéros de comptes pour lesquels les journaux sont transmis à ce compartiment. Pour `aws:SourceArn`, spécifiez la liste des ARN de la ressource qui génère les journaux, dans le formulaire `arn:aws:logs:source-region:source-account-id:*`.

Chiffrement

Vous pouvez activer le chiffrement côté serveur pour votre compartiment de journaux d'accès Amazon S3 de l'une des manières suivantes :

- Clés gérées par Amazon S3 (SSE-S3)
- AWS KMS clés stockées dans AWS Key Management Service (SSE-KMS) †

† Avec les journaux d'accès de Network Load Balancer, vous ne pouvez pas utiliser de clés AWS gérées, vous devez utiliser des clés gérées par le client.

Pour plus d'informations, consultez les sections [Spécification du chiffrement Amazon S3 \(SSE-S3\)](#) et [Spécification du chiffrement côté serveur avec AWS KMS \(SSE-KMS\)](#) dans le guide de l'utilisateur Amazon S3.

La stratégie de clé doit permettre au service de chiffrer et de déchiffrer les journaux. Voici un exemple de politique .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ]
    }
  ]
}
```

```
    ],  
    "Resource": "*"    
  }  
]  
}
```

Activer la journalisation des accès

Lorsque vous activez la journalisation des accès pour votre équilibreur de charge, vous devez spécifier le compartiment S3 dans lequel l'équilibreur de charge stockera les journaux. Assurez-vous de posséder ce compartiment et d'avoir configuré la stratégie de compartiment requise pour ce dernier. Pour plus d'informations, consultez [Conditions requises pour le compartiment](#).

Pour activer la journalisation des accès à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Sélectionnez le nom de votre équilibreur de charge afin d'ouvrir sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Dans la page Modifier les attributs de l'équilibreur de charge, procédez comme suit :
 - a. Pour Surveillance, activez Journaux d'accès.
 - b. Choisissez Parcourir S3 et sélectionnez un compartiment à utiliser. Vous pouvez également saisir l'emplacement de votre compartiment S3, y compris tout préfixe.
 - c. Sélectionnez Enregistrer les modifications.

Pour activer la journalisation des accès à l'aide du AWS CLI

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

Désactiver la journalisation des accès

Vous pouvez désactiver la journalisation des accès pour votre équilibreur de charge à tout moment. Une fois que vous avez désactivé la journalisation des accès, vos journaux d'accès restent dans votre compartiment S3 jusqu'à ce que vous les supprimiez. Pour plus d'informations, veuillez consulter [Utilisation des compartiments](#) dans le Guide de l'utilisateur Amazon Simple Storage Service.

Pour désactiver la journalisation des accès à l'aide de la console

1. Ouvrez la console Amazon EC2 à l'adresse <https://console.aws.amazon.com/ec2/>.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Sélectionnez le nom de votre équilibreur de charge afin d'ouvrir sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Pour Surveillance, désactivez Journaux d'accès.
6. Sélectionnez Enregistrer les modifications.

Pour désactiver la journalisation des accès à l'aide du AWS CLI

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

Traitement des fichiers journaux d'accès

Les fichiers journaux d'accès sont compressés. Si vous ouvrez les fichiers à l'aide de la console Amazon S3, ils sont décompressés et les informations s'affichent. Si vous téléchargez les fichiers, vous devez les décompresser pour afficher les informations.

Si la demande est importante sur votre site web, votre équilibreur de charge peut générer des fichiers journaux avec des gigaoctets de données. Il se peut que vous ne puissiez pas traiter une telle quantité de données à l'aide du line-by-line traitement. Vous devrez donc peut-être utiliser des outils d'analyse qui proposent des solutions de traitement en parallèle. Par exemple, vous pouvez utiliser les outils d'analyse suivants pour analyser et traiter des journaux d'accès :

- Amazon Athena est un service de requête interactif qui facilite l'analyse des données dans Amazon S3 à l'aide du langage SQL standard. Pour plus d'informations, veuillez consulter [Interrogation des journaux du dispositif du Network Load Balancer](#) dans le Guide de l'utilisateur Amazon Athena.
- [Loggly](#)
- [Splunk](#)
- [Sumo Logic](#)

Journalisation des appels d'API pour votre Network Load Balancer à l'aide d' 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 Service AWS dans Elastic Load Balancing. CloudTrail capture tous les appels d'API pour Elastic Load Balancing sous forme d'événements. Les appels capturés incluent des appels provenant des appels de code AWS Management Console et destinés aux opérations de l'API 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 compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité se produit dans Elastic Load Balancing, elle est enregistrée dans un CloudTrail événement avec les autres Service AWS événements de l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section [Affichage des événements avec l'historique des CloudTrail événements](#).

Pour un enregistrement continu des événements survenus dans votre environnement Compte AWS, y compris ceux relatifs à Elastic Load Balancing, créez une trace. 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 en configurer d'autres Services AWS 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 notifications Amazon SNS 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 Network Load Balancers sont enregistrées CloudTrail et documentées dans la [version 2015-12-01 de référence de l'API Elastic Load Balancing](#). 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 requête a été effectuée par un autre Service AWS.

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

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 appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Les fichiers journaux incluent les événements de tous les appels d' AWS API relatifs à vos appels d'API Compte AWS, et pas uniquement à ceux d'Elastic Load Balancing. Vous pouvez trouver les appels d'API Elastic Load Balancing en recherchant les éléments `eventSource` avec 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 Network Load Balancer puis l'a supprimé à l'aide du `AWS CLI`. Vous pouvez identifier l'interface de ligne de commande à l'aide des éléments `userAgent`. Vous pouvez

identifier les appels d'API demandés à l'aide des éléments eventName. Il est possible de trouver des informations sur l'utilisateur (Alice) dans l'élément userIdentity.

Example Exemple : CreateLoadBalancer

```
{
  "eventVersion": "1.03",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:user/Alice",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Alice"
  },
  "eventTime": "2016-04-01T15:31:48Z",
  "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"],
    "securityGroups": ["sg-5943793c"],
    "name": "my-load-balancer",
    "scheme": "internet-facing",
    "type": "network"
  },
  "responseElements": {
    "loadBalancers": [{
      "type": "network",
      "ipAddressType": "ipv4",
      "loadBalancerName": "my-load-balancer",
      "vpcId": "vpc-3ac0fb5f",
      "securityGroups": ["sg-5943793c"],
      "state": {"code": "provisioning"},
      "availabilityZones": [
        {"subnetId": "subnet-8360a9e7", "zoneName": "us-west-2a"},
        {"subnetId": "subnet-b7d581c0", "zoneName": "us-west-2b"}
      ],
      "dnsName": "my-load-balancer-1836718677.us-west-2.elb.amazonaws.com",
      "canonicalHostedZoneId": "Z2P70J7HTTTPLU",
      "createdTime": "Apr 11, 2016 5:23:50 PM",
```

```

        "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/net/my-load-balancer/ffcddace1759e1d0",
        "scheme": "internet-facing"
    ]}
},
"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": "2016-04-01T15:31:48Z",
  "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/net/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"
}

```

Dépannage de votre Network Load Balancer

Les informations suivantes peuvent vous aider à résoudre les problèmes liés à votre Network Load Balancer.

Une cible enregistrée n'est pas en service

Si le passage à l'état InService d'une cible est plus long que prévu, les vérifications de l'état risquent d'échouer. Votre cible ne sera pas en service tant que la vérification de l'état correspondante ne sera pas concluante. Pour plus d'informations, consultez [Surveillance de l'état de vos groupes cibles](#).

Vérifiez si les vérifications de l'état de votre instance ont échoué, puis contrôlez les points suivants :

Un groupe de configuration n'autorise pas le trafic

Les groupes de sécurité associés à une instance doivent autoriser le trafic à partir de l'équilibreur de charge à l'aide du port et du protocole de vérification de l'état. Pour plus d'informations, consultez [Groupes de sécurité cibles](#).

Une liste de contrôle d'accès (ACL) réseau n'autorise pas le trafic

La liste ACL réseau associée aux sous-réseaux de vos instances et aux sous-réseaux de votre équilibreur de charge doit autoriser le trafic et les surveillances de l'état depuis l'équilibreur de charge. Pour plus d'informations, consultez [Listes ACL réseau](#).

Les demandes ne sont pas acheminées vers les cibles

Vérifiez les points suivants :

Un groupe de configuration n'autorise pas le trafic

Les groupes de sécurité associés aux instances doivent autoriser le trafic sur le port d'écoute à partir d'adresses IP du client (si les cibles sont spécifiées par ID d'instance) ou de nœuds d'équilibreur de charge (si les cibles sont spécifiées par adresse IP). Pour plus d'informations, consultez [Groupes de sécurité cibles](#).

Une liste de contrôle d'accès (ACL) réseau n'autorise pas le trafic

Les ACL réseau associées aux sous-réseaux pour votre VPC doivent autoriser l'équilibreur de charge et les cibles à communiquer dans les deux sens sur le port d'écoute. Pour plus d'informations, consultez [Listes ACL réseau](#).

Les cibles sont dans une zone de disponibilité qui n'est pas activée

Si vous enregistrez des cibles dans une zone de disponibilité mais que vous n'activez pas la zone de disponibilité, ces cibles enregistrées ne reçoivent pas le trafic de l'équilibreur de charge.

L'instance n'est pas dans un VPC appairé

Si vous disposez d'instances dans un VPC appairé au VPC de l'équilibreur de charge, vous devez les enregistrer à l'aide de votre équilibreur de charge par adresse IP et non par ID d'instance.

Les cibles reçoivent plus de demandes de vérification de l'état que prévu

Les surveillances de l'état pour un Network Load Balancer sont distribuées et utilisent un mécanisme de consensus pour déterminer l'état des cibles. Par conséquent, des cibles reçoivent plus de vérifications de l'état que le nombre configuré via le paramètre `HealthCheckIntervalSeconds`.

Les cibles reçoivent moins de demandes de vérification de l'état que prévu

Vérifiez si `net.ipv4.tcp_tw_recycle` est activé. Ce paramètre est connu pour entraîner des problèmes liés aux équilibreurs de charge. Le paramètre `net.ipv4.tcp_tw_reuse` est considéré comme un paramètre plus sûr.

Des cibles non saines reçoivent des demandes de l'équilibreur de charge.

Cela se produit lorsque toutes les cibles enregistrées sont défectueuses. S'il existe au moins une cible enregistrée saine, votre Network Load Balancer achemine les demandes uniquement vers ses cibles enregistrées saines.

Lorsqu'il n'existe que des cibles enregistrées défectueuses, le Network Load Balancer achemine les demandes vers toutes les cibles enregistrées : il s'agit du mode fail-open. Le Network Load Balancer procède ainsi au lieu de supprimer toutes les adresses IP du DNS lorsque toutes les cibles sont défectueuses et que les zones de disponibilité respectives n'ont pas de cible saine à laquelle envoyer une demande.

La cible échoue aux vérifications d'intégrité HTTP ou HTTPS en raison d'une incompatibilité d'en-tête d'hôte

L'en-tête d'hôte HTTP dans la demande de vérification de l'intégrité contient l'adresse IP du nœud d'équilibrage et le port de l'écouteur, et non l'adresse IP de la cible et le port de vérification de l'intégrité. Si vous mappez des requêtes entrantes par en-tête d'hôte, vous devez vous assurer que les vérifications d'intégrité correspondent à n'importe quel en-tête d'hôte HTTP. Une autre option consiste à ajouter un service HTTP distinct sur un port différent et à configurer le groupe cible afin qu'il utilise ce port pour les vérifications d'intégrité à la place. Vous pouvez aussi envisager d'utiliser des contrôles d'intégrité TCP.

Impossible d'associer un groupe de sécurité à un équilibreur de charge

Si le Network Load Balancer a été créé sans groupes de sécurité, il ne peut pas prendre en charge les groupes de sécurité après sa création. Vous ne pouvez associer un groupe de sécurité qu'à un équilibreur de charge lors de sa création ou à un équilibreur de charge existant créé à l'origine avec des groupes de sécurité.

Impossible de supprimer tous les groupes de sécurité

Si le Network Load Balancer a été créé avec des groupes de sécurité, au moins un groupe de sécurité doit lui être associé à tout moment. Vous ne pouvez pas supprimer tous les groupes de sécurité de l'équilibreur de charge en même temps.

Augmentation de la métrique TCP_ELB_Reset_Count

Pour chaque demande TCP effectuée par un client via un Network 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. Si un client ou une cible envoie des données après que le délai d'inactivité est écoulé, il reçoit un paquet TCP RST pour indiquer que la connexion n'est plus valide. Par ailleurs, si une cible devient défectueuse, l'équilibreur de charge envoie un TCP RST pour les paquets reçus sur les connexions client associées à la cible, sauf si la cible défectueuse déclenche le mode fail-open pour l'équilibreur de charge.

Si vous constatez une hausse de la métrique `TCP_ELB_Reset_Count` juste avant ou pendant l'augmentation de la métrique `UnhealthyHostCount`, il est probable que les paquets TCP RST aient été envoyés parce que la cible commençait à échouer, mais n'avait pas été signalée comme étant défectueuse. Si vous constatez des augmentations persistantes de `TCP_ELB_Reset_Count` sans que les cibles ne soient signalées comme défectueuses, vous pouvez consulter les journaux de flux VPC pour voir si les clients envoient des données sur des flux expirés.

Connexions expirées pour les demandes d'une cible vers son équilibreur de charge

Vérifiez si la préservation des adresses IP client est activée sur votre groupe cible. La boucle NAT, également appelée hairpinning, n'est pas prise en charge lorsque la préservation des adresses IP client est activée. Si une instance est un client d'un équilibreur de charge auprès duquel elle est enregistrée, et si la préservation des adresses IP client est activée, la connexion aboutit uniquement si la demande est acheminée vers une autre instance. Si la demande est acheminée vers la même instance à partir de laquelle elle a été envoyée, la connexion expire, car les adresses IP source et de destination sont identiques.

Si une instance doit envoyer des demandes à un équilibreur de charge auprès duquel elle est enregistrée, effectuez l'une des actions suivantes :

- Désactivez la préservation des adresses IP client.
- Assurez-vous que les conteneurs qui doivent communiquer sont sur des instances de conteneur différentes.

Diminution des performances lorsque des cibles sont déplacées vers un Network Load Balancer

Les Classic Load Balancers et les Application Load Balancers utilisent le multiplexage des connexions, mais pas les Network Load Balancers. Par conséquent, vos cibles peuvent recevoir plus

de connexions TCP derrière un Network Load Balancer. Assurez-vous que vos cibles sont prêtes à gérer le volume de demandes de connexion qu'elles sont susceptibles de recevoir.

Erreurs d'allocation de port lors de la connexion AWS PrivateLink

Si votre Network Load Balancer est associé à un service de point de terminaison d'un VPC, il prend en charge 55 000 connexions simultanées ou environ 55 000 connexions par minute sur chaque cible unique (adresse IP et port). Si vous dépassez ce nombre de connexions, il y a plus de risque d'erreurs d'attribution de port. Les erreurs d'attribution de ports peuvent être suivies à l'aide de la métrique `PortAllocationErrorCount`. Pour résoudre les erreurs d'attribution de port, ajoutez davantage de cibles au groupe cible. Pour plus d'informations, consultez [CloudWatch métriques pour votre Network Load Balancer](#).

Échec de connexion intermittent lorsque la préservation des adresses IP client est activée

Lorsque la préservation des adresses IP client est activée, vous pouvez rencontrer des limitations de connexion TCP/IP liées à la réutilisation observée des sockets sur les cibles. Ces limitations de connexion peuvent survenir lorsqu'un client, ou un périphérique NAT situé devant le client, utilise la même adresse IP source et le même port source pour se connecter simultanément à plusieurs nœuds d'équilibreur de charge. Si l'équilibreur de charge achemine ces connexions vers la même cible, celles-ci apparaissent à la cible comme si elles provenaient du même socket source, ce qui entraîne des erreurs de connexion. Dans ce cas, les clients peuvent réessayer (si la connexion échoue) ou se reconnecter (si la connexion est interrompue). Vous pouvez réduire ce type d'erreur de connexion en augmentant le nombre de ports éphémères sources ou en augmentant le nombre de cibles pour l'équilibreur de charge. Vous pouvez éviter ce type d'erreur de connexion en désactivant la préservation des adresses IP client ou en désactivant l'équilibrage de charge entre zones.

En outre, lorsque la préservation des adresses IP client est activée, la connectivité peut échouer si les clients qui se connectent au Network Load Balancer sont également connectés à des cibles situées derrière l'équilibreur de charge. Pour résoudre ce problème, vous pouvez désactiver la préservation des adresses IP client sur les groupes cibles concernés. Vous pouvez également demander à vos clients de se connecter uniquement au Network Load Balancer, ou uniquement aux cibles, mais pas aux deux.

Retards de connexion TCP

Lorsque l'équilibrage de charge entre zones et la préservation des adresses IP client sont activés, un client se connectant à différentes adresses IP sur le même équilibreur de charge peut être acheminé vers la même cible. Si le client utilise le même port source pour ces deux connexions, la cible recevra ce qui semble être une connexion dupliquée, ce qui peut entraîner des erreurs de connexion et des retards TCP lors de l'établissement de nouvelles connexions. Vous pouvez éviter ce type d'erreur de connexion en désactivant l'équilibrage de charge entre zones. Pour plus d'informations, consultez [Équilibrage de charge entre zones](#).

Défaillance potentielle lors du provisionnement de l'équilibreur de charge

L'une des raisons pour lesquelles un Network Load Balancer peut échouer lors de son provisionnement est que vous utilisez une adresse IP déjà attribuée ou allouée ailleurs (par exemple, attribuée comme adresse IP secondaire d'une instance EC2). Cette adresse IP empêche la configuration de l'équilibreur de charge, et son état est `failed`. Vous pouvez résoudre ce problème en annulant l'allocation de l'adresse IP associée et en relançant le processus de création.

La résolution de noms DNS contient moins d'adresses IP que les zones de disponibilité activées

Dans l'idéal, votre Network Load Balancer fournit une adresse IP par zone de disponibilité activée, lorsqu'il possède au moins un hôte sain dans la zone de disponibilité. Lorsqu'aucun hôte sain n'est présent dans une zone de disponibilité donnée et que l'équilibrage de charge entre zones est désactivé, l'adresse IP du Network Load Balancer correspondant à cette zone de disponibilité est supprimée du DNS.

Supposons, par exemple, que votre Network Load Balancer dispose de trois zones de disponibilité activées, qui ont toutes au moins une instance cible enregistrée saine.

- Si les instances cibles enregistrées dans la zone de disponibilité A deviennent défectueuses, l'adresse IP correspondante de la zone de disponibilité A pour le Network Load Balancer est supprimée du DNS.
- Si deux des zones de disponibilité activées ne possèdent aucune instance cible enregistrée saine, les deux adresses IP respectives du Network Load Balancer seront supprimées du DNS.

- S'il n'y a aucune instance cible enregistrée saine dans toutes les zones de disponibilité activées, le mode fail-open est activé et le DNS fournira toutes les adresses IP des trois zones de disponibilité activées dans le résultat.

Résoudre les problèmes liés aux cibles défectueuses à l'aide de la carte des ressources

Si les tests de santé de vos cibles Network Load Balancer échouent, vous pouvez utiliser la carte des ressources pour détecter les cibles défectueuses et prendre des mesures en fonction du code de cause de l'échec. Pour plus d'informations, consultez [Carte des ressources du Network Load Balancer](#).

La carte des ressources fournit deux vues : Vue d'ensemble et Carte cible malsaine. L'option Vue d'ensemble est sélectionnée par défaut et affiche toutes les ressources de votre équilibreur de charge. La sélection de la vue Malhealthy Target Map affichera uniquement les cibles malsaines de chaque groupe cible associé au Network Load Balancer.

Note

L'option Afficher les détails des ressources doit être activée pour afficher le résumé du bilan de santé et les messages d'erreur pour toutes les ressources applicables dans la carte des ressources. Lorsque cette option n'est pas activée, vous devez sélectionner chaque ressource pour en afficher les détails.

La colonne Groupes cibles affiche un résumé des cibles saines et malsaines pour chaque groupe cible. Cela peut aider à déterminer si toutes les cibles échouent aux tests de santé ou si seules des cibles spécifiques échouent. Si toutes les cibles d'un groupe cible échouent aux tests de santé, vérifiez les paramètres du bilan de santé du groupe cible. Sélectionnez le nom d'un groupe cible pour ouvrir sa page détaillée dans un nouvel onglet.

La colonne Targets affiche le TargetID et l'état actuel du bilan de santé pour chaque cible. Lorsqu'une cible n'est pas saine, le code de la raison de l'échec du contrôle de santé s'affiche. Lorsqu'une cible échoue à un bilan de santé, vérifiez qu'elle dispose de ressources suffisantes. Sélectionnez l'ID d'une cible pour ouvrir sa page détaillée dans un nouvel onglet.

La sélection d'Exporter vous permet d'exporter la vue actuelle de la carte des ressources de votre Network Load Balancer au format PDF.

Vérifiez que les tests de santé de votre instance échouent, puis, en fonction du code de cause de l'échec, vérifiez les problèmes suivants :

- Malsain : le délai imparti pour la demande a expiré
 - Vérifiez que les groupes de sécurité et les listes de contrôle d'accès réseau (ACL) associés à vos cibles et à Network Load Balancer ne bloquent pas la connectivité.
 - Vérifiez que la cible dispose d'une capacité suffisante pour accepter les connexions depuis le Network Load Balancer.
 - Les réponses au bilan de santé du Network Load Balancer peuvent être consultées dans les journaux des applications de chaque cible. Pour plus d'informations, consultez [la section Codes de raison du contrôle de santé](#).
- Malsain : FailedHealthChecks
 - Vérifiez que la cible écoute le trafic sur le port de contrôle de santé.

Lors de l'utilisation d'un écouteur TLS

Vous choisissez la politique de sécurité à utiliser pour les connexions frontales. La politique de sécurité utilisée pour les connexions dorsales est automatiquement sélectionnée en fonction de la stratégie de sécurité frontale utilisée.

- Si votre écouteur TLS utilise une politique de sécurité TLS 1.3 pour les connexions frontales, la politique de ELBSecurityPolicy-TLS13-1-0-2021-06 sécurité est utilisée pour les connexions dorsales.
- Si votre écouteur TLS n'utilise pas de stratégie de sécurité TLS 1.3 pour les connexions frontales, la stratégie de ELBSecurityPolicy-2016-08 sécurité est utilisée pour les connexions dorsales.

Pour plus d'informations, consultez la section [Politiques de sécurité](#).

- Vérifiez que la cible fournit un certificat de serveur et une clé au format correct spécifié par la politique de sécurité.
- Vérifiez que la cible prend en charge un ou plusieurs chiffrements correspondants, ainsi qu'un protocole fourni par le Network Load Balancer pour établir des handshakes TLS.

Quotas de vos Network Load Balancers

Votre Compte AWS dispose de quotas par défaut, anciennement appelés limites, pour chaque service AWS. 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 afficher les quotas de vos Network Load Balancers ouvrez la [console Service Quotas](#). Dans le panneau de navigation, choisissez Services AWS et sélectionnez Elastic Load Balancing. Vous pouvez également utiliser la commande [describe-account-limits](#) (AWS CLI) pour Elastic Load Balancing.

Pour demander une augmentation de quota, consultez [Demande d'augmentation de quota](#) dans le Guide de l'utilisateur Service Quotas. Si le quota n'est pas encore disponible dans Service Quotas, utilisez le [formulaire d'augmentation de limite Elastic Load Balancing](#).

Équilibreur de charge

Les quotas de votre Compte AWS concernant les Network Load Balancers sont les suivants.

Nom	Par défaut	Ajustable
Certificats par Network Load Balancer	25	Oui
Écouteurs par Network Load Balancer	50	Non
ENI Network Load Balancer par VPC	1 200 ¹	Oui
Équilibreurs de charge réseau par région	50	Oui
Groupes cibles par action et par Network Load Balancer	1	Non
Cibles par zone de disponibilité et par Network Load Balancer	500 ^{2, 3}	Oui
Cibles par Network Load Balancer	3 000 ³	Oui

¹ Chaque Network Load Balancer utilise une interface réseau par zone. Le quota est défini au niveau du VPC. Lors du partage de sous-réseaux ou de VPC, l'utilisation est calculée pour tous les locataires.

² Si une cible est enregistrée avec N groupes cibles, cela compte comme N cibles pour atteindre cette limite. Chaque Application Load Balancer étant une cible du Network Load Balancer compte comme 50 cibles si l'équilibrage de charge entre zones est désactivé ou 100 cibles si l'équilibrage de charge entre zones est activé.

³ Si l'équilibrage de charge entre zones est activé, le maximum est de 500 cibles par équilibreur de charge, quel que soit le nombre de zones de disponibilité.

Groupes cibles

Les quotas suivants sont destinés aux groupes cibles.

Nom	Par défaut	Ajustable
Groupes cibles par région	3 000 ¹	Oui
Cibles par groupe cible et par région (instances ou adresses IP)	1 000	Oui
Cibles par groupe cible et par région (Application Load Balancers)	1	Non

* Ce quota est partagé par les Application Load Balancers et les Network Load Balancers.

Historique du document pour les Network Load Balancers

Le tableau suivant décrit les versions des Network Load Balancers.

Modification	Description	Date
Certificats RSA 3072 bits et ECDSA 256/384/521 bits	Cette version ajoute la prise en charge des certificats RSA 3072 bits et des certificats ECDSA (Elliptic Curve Digital Signature Algorithm) 256, 384 et 521 bits via (ACM). AWS Certificate Manager	19 janvier 2024
Terminaison TLS FIPS 140-3	Cette version ajoute des politiques de sécurité qui utilisent les modules cryptographiques FIPS 140-3 lors de la terminaison des connexions TLS.	20 novembre 2023
Affinité DNS zonale	Cette version permet aux clients de résoudre le DNS de l'équilibreur de charge pour recevoir une adresse IP dans la même zone de disponibilité (AZ) dans laquelle ils se trouvent.	12 octobre 2023
Désactiver la terminaison d'une connexion cible défectueuse	Cette version ajoute la prise en charge du maintien de connexions actives aux cibles qui échouent aux tests de santé.	12 octobre 2023
Fin de connexion UDP par défaut	Cette version ajoute la prise en charge de la résiliation des	12 octobre 2023

	connexions UDP à la fin du délai de désenregistrement par défaut.	
Enregistrer les cibles à l'aide d'IPv6	Cette version ajoute la prise en charge de l'enregistrement des instances en tant que cibles lorsqu'elles sont adressées par IPv6.	2 octobre 2023
Groupes de sécurité de votre Network Load Balancer	Cette version permet d'associer des groupes de sécurité à vos Network Load Balancers lors de leur création.	10 août 2023
État du groupe cible	Cette version permet de configurer le nombre ou le pourcentage minimal de cibles qui doivent être saines, ainsi que les actions entreprises par l'équilibreur de charge lorsque le seuil n'est pas atteint.	17 novembre 2022
Configuration d'une surveillance de l'état	Cette version apporte des améliorations à la configuration de la surveillance de l'état.	17 novembre 2022
Équilibrage de charge entre zones	Cette version ajoute la prise en charge de la configuration de l'équilibrage de charge entre zones au niveau du groupe cible.	17 novembre 2022
Groupes cibles IPv6	Cette version ajoute la prise en charge de la configuration de groupes cibles IPv6 pour les équilibreurs de charge réseau.	23 novembre 2021

Équilibreurs de charge internes IPv6	Cette version ajoute la prise en charge de la configuration de groupes cibles IPv6 pour les équilibreurs de charge réseau.	23 novembre 2021
TLS 1.3	Cette version ajoute des stratégies de sécurité prenant en charge la version 1.3 de TLS.	14 octobre 2021
Application Load Balancers en tant que cibles	Cette version permet de configurer un Application Load Balancer en tant que cible d'un Network Load Balancer.	27 septembre 2021
Préservation des adresses IP client	Cette version permet de configurer la préservation des adresses IP client.	4 février 2021
Stratégie de sécurité pour la confidentialité persistante prenant en charge la version 1.2 de TLS	Cette version ajoute une stratégie de sécurité pour la confidentialité persistante (FS, Forward Secrecy) prenant en charge TLS version 1.2.	24 novembre 2020
Mode double pile	Cette version ajoute la prise en charge du mode double pile, qui permet aux clients de se connecter à l'équilibreur de charge en utilisant à la fois des adresses IPv4 et des adresses IPv6.	13 novembre 2020

Fin de connexion en cas d'annulation d'enregistrement	Cette version permet d'interrompre les connexions aux cibles dont l'enregistrement a été annulé après la fin du délai d'expiration de l'annulation d'enregistrement.	13 novembre 2020
Stratégies ALPN	Cette version ajoute la prise en charge des listes de préférences ALPN (Application-Layer Protocol Negotiation).	27 mai 2020
Sessions permanentes	Cette version prend désormais en charge les sessions permanentes basées sur les adresses IP source et le protocole.	28 février 2020
Sous-réseaux partagés	Cette version permet de spécifier des sous-réseaux partagés avec vous par un autre Compte AWS.	26 novembre 2019
Adresses IP privées	Cette version vous permet de fournir une adresse IP privée à partir de la plage d'adresses IPv4 du sous-réseau que vous spécifiez lorsque vous activez une zone de disponibilité pour un équilibreur de charge interne.	25 novembre 2019

Ajout de sous-réseaux	Cette version ajoute la prise en charge de l'activation de zones de disponibilité supplémentaires après la création de votre équilibreur de charge.	25 novembre 2019
Politiques de sécurité pour FS	Cette version ajoute la prise en charge de trois politiques de sécurité de confidentialité prédéfinies supplémentaires.	8 octobre 2019
Prise en charge de SNI	Cette version ajoute la prise en charge de Server Name Indication (SNI).	12 septembre 2019
Protocole UDP	Cette version ajoute la prise en charge du protocole TLS.	24 juin 2019
Disponible dans une nouvelle région	Cette version ajoute la prise en charge des équilibreurs de charge réseau dans la région Asie-Pacifique (Osaka).	12 juin 2019
Protocole TLS	Cette version ajoute la prise en charge du protocole TLS.	24 janvier 2019
Équilibrage de charge entre zones	Cette version ajoute la prise en charge pour l'activation de l'équilibrage de charge entre zones.	le 22 février 2018
Protocole proxy	Cette version ajoute la prise en charge de l'activation du protocole proxy.	17 novembre 2017

[Adresses IP en tant que cibles](#)

Cette version prend en charge l'enregistrement d'adresses IP en tant que cibles.

21 septembre 2017

[Nouveau type d'équilibreur de charge](#)

Cette version d'Elastic Load Balancing introduit les Network Load Balancers.

7 septembre 2017

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.