Équilibreurs de charge classiques

Elastic Load Balancing

Elastic Load Balancing: Équilibreurs de charge classiques

Table of Contents

Qu'est-ce qu'un Classic Load Balancer ? 1
Présentation du Classic Load Balancer 1
Avantages 2
Comment démarrer 3
Tarification 3
Didacticiel : Création d'un Classic Load Balancer 4
Avant de commencer 4
Créez un Classic Load Balancer à l'aide du AWS Management Console 4
Équilibreurs de charge accessibles sur Internet 8
Noms DNS publics pour votre équilibreur de charge 8
Créer un équilibreur de charge accessible sur Internet 9
Équilibreurs de charge internes 10
Nom DNS public de votre équilibreur de charge 11
Créer un équilibreur de charge interne 12
Prérequis 12
Créez un équilibreur de charge interne à l'aide du AWS Management Console 12
Créez un équilibreur de charge interne à l'aide du AWS CLI 15
Instances enregistrées 18
Bonnes pratiques pour vos instances 18
Préparation de votre VPC et de vos instances EC2 19
Configurer la surveillance de l'état 20
Configuration d'une surveillance de l'état 21
Mettre à jour la configuration de surveillance de l'état 23
Vérifier l'état de santé de vos instances 24
Résoudre des problèmes de surveillance de l'état 24
Configurer des groupes de sécurité 24
Groupes de sécurité pour les équilibreurs de charge dans un VPC 25
Groupes de sécurité pour des instances dans un VPC 28
ACL réseau pour des équilibreurs de charge dans un VPC 29
Ajouter ou supprimer des sous-réseaux 32
Prérequis 33
Ajouter un sous-réseau 33
Supprimer un sous-réseau 34
Enregistrer ou annuler l'enregistrement des instances 35

Enregistrer une Instance ... 36
Afficher les instances enregistrées auprès de l'équilibreur de charge ... 37
Déterminer l'équilibreur de charge pour une instance enregistrée ... 38
Annuler l'enregistrement d'une instance ... 38
Écouteurs ... 40
Protocoles ... 41
Protocole TCP/SSL ... 41
Protocole HTTP/HTTPS ... 42
Écouteurs HTTPS/SSL ... 42
Certificats de serveur SSL ... 42
Négociation SSL ... 43
Authentification de serveur principal ... 43
Configurations d'Écouteur ... 43
En-têtes X-forwarded ... 46
X-Forwarded-For ... 47
X-Forwarded-Proto ... 47
X-Forwarded-Port ... 48
Écouteurs HTTPS ... 49
Certificats SSL/TLS ... 50
Créez ou importez un certificat SSL/TLS à l'aide de AWS Certificate Manager ... 51
Importation d'un certificat SSL/TLS à l'aide d'IAM ... 51
Configurations de négociation SSL ... 51
Stratégies de sécurité ... 52
Protocoles SSL ... 53
Préférence pour l'ordre des serveurs ... 53
Chiffrements SSL ... 54
Politiques de sécurité SSL prédéfinies ... 57
Création d'un équilibreur de charge HTTPS ... 62
Prérequis ... 62
Créez un équilibreur de charge HTTPS/SSL à l'aide du AWS Management Console ... 63
Créer un équilibreur de charge HTTPS/SSL à l'aide de l'interface AWS CLI ... 67
Configurer un Écouteur HTTPS ... 79
Prérequis ... 80
Ajouter un Écouteur HTTPS à l'aide de la console ... 80
Ajoutez un écouteur HTTPS à l'aide du AWS CLI ... 82
Remplacer le certificat SSL ... 84

Remplacer le certificat SSL à l'aide de la console 84
Remplacer le certificat SSL à l'aide de l'interface AWS CLI 86
Mettre à jour la configuration de négociation SSL 86
Mettre à jour la configuration de négociation SSL à l'aide de la console 87
Mettez à jour la configuration de négociation SSL à l'aide du AWS CLI 88
Configurer votre équilibreur de charge 93
Configurer le délai d'inactivité 93
Configurer le délai d'inactivité à l'aide de la console 94
Configurer le délai d'inactivité à l'aide de l'interface AWS CLI 94
Configurer la répartition de charge entre zones 95
Activer la répartition de charge entre zones 96
Désactiver la répartition de charge entre zones 97
Configurer le drainage de la connexion 99
Activer le drainage de la connexion 100
Désactiver le drainage de la connexion 101
Configurer le protocole proxy 102
En-tête du protocole proxy 102
Prérequis pour l'activation du protocole proxy 103
Activer le protocole proxy à l'aide de l'interface AWS CLI 103
Désactiver le protocole proxy à l'aide de l'interface AWS CLI 105
Configurer des sessions permanentes 106
Permanence de session basée sur la durée 108
Permanence des sessions contrôlées par application 111
Configurer le mode d'atténuation de désynchronisation 113
Classifications 114
Modes 116
Modifier le mode d'atténuation de désynchronisation 116
Baliser votre équilibreur de charge 117
Restrictions liées aux étiquettes 117
Ajouter une balise 118
Supprimer une balise 118
Configurer un nom de domaine 119
Associer votre nom de domaine personnalisé au nom de votre équilibreur de charge 120
Utiliser le basculement DNS Route 53 pour votre équilibreur de charge 120
Dissocier votre nom de domaine personnalisé de votre équilibreur de charge 121
Contrôler votre équilibreur de charge 123

CloudWatch métriques 123
Métriques Classic Load Balancer 124
Dimensions de métriques pour les Classic Load Balancers 134
Statistiques pour les métriques Classic Load Balancer 134
Afficher CloudWatch les statistiques de votre équilibreur de charge 135
Journaux d'accès 137
Fichiers journaux d'accès 138
Entrées des journaux d'accès 140
Traitement des journaux d'accès 144
Activer les journaux d'accès 145
Désactiver les journaux d'accès 153
CloudTrail journaux 154
Informations sur Elastic Load Balancing dans CloudTrail 155
Présentation des entrées du fichier journal Elastic Load Balancing 156
Résoudre les problèmes liés à votre équilibreur de charge 159
Erreurs d'API 161
CertificateNotTrouvé : Non défini 161
OutofService: une erreur passagère s'est produite 161
Erreurs HTTP 162
HTTP 400 : BAD_REQUEST 163
HTTP 405 : METHOD_NOT_ALLOWED 163
HTTP 408 : Délai d'attente des demandes 163
HTTP 502 : Passerelle erronée 164
HTTP 503 : Service indisponible 164
HTTP 504 : Délai de passerelle expiré 165
Métriques de code de réponse 165
HTTPCode_ELB_4XX 166
HTTPCode_ELB_5XX 166
HTTPCode_Backend_2XX 166
HTTPCode_Backend_3XX 167
HTTPCode_Backend_4XX 167
HTTPCode_Backend_5XX 167
Surveillance de l'état 168
Erreur de page cible de vérification de l'état 168
La connexion aux instances a expiré 169
L'authentification par clé publique échoue 170

L'instance ne reçoit pas le trafic provenant de l'équilibreur de charge 170
Des ports sur l'instance ne sont pas ouverts 171
Les instances d'un groupe Auto Scaling ne réussissent pas la surveillance de l'état ELB 171
Connectivité du client 172
Les clients ne peuvent pas se connecter à un équilibreur de charge accessible sur Internet 172
Les requêtes envoyées à un domaine personnalisé ne sont pas reçues par l'équilibreur de charge 172
Les requêtes HTTPS envoyées à l'équilibreur de charge renvoient « NET::ERR_CERT_COMMON_NAME_INVALID » 173
Enregistrement d'instance 173
L'enregistrement d'une instance EC2 prend trop de temps 174
Impossible d'enregistrer une instance lancée à partir d'une AMI payante 174
Quotas 175
Historique de la documentation 176
..... clxxxvi

Qu'est-ce qu'un Classic 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 Classic Load Balancers. Pour plus d'informations sur les autres équilibreurs de charge, consultez le Guide de l'utilisateur des Application Load Balancers, le Guide de l'utilisateur des dispositifs d'équilibrage de charge de réseau et le Guide de l'utilisateur pour les Gateway Load Balancers.

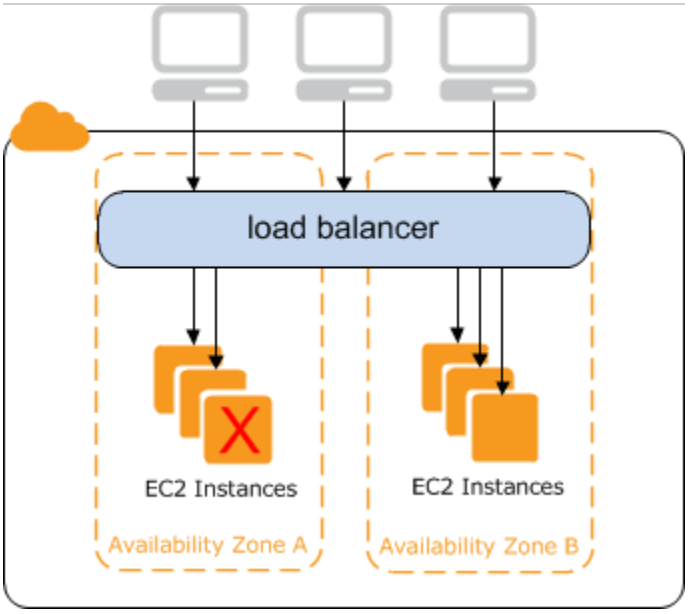
Présentation du Classic Load Balancer

L'équilibreur de charge distribue le trafic applicatif entrant sur plusieurs instances EC2 dans plusieurs zones de disponibilité. Cela augmente la tolérance aux pannes de vos applications. Elastic Load Balancing détecte les instances non saines et achemine uniquement le trafic vers des instances saines.

Votre équilibreur de charge constitue un point de contact unique pour les clients. La disponibilité de votre application s'en trouve accrue. Vous pouvez ajouter et supprimer des instances 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.

Un écouteur vérifie les demandes de connexion des clients à l'aide du protocole et du port que vous configurez, et transmet les demandes à une ou plusieurs instances enregistrées en utilisant le protocole et le numéro de port que vous configurez. Vous ajoutez un ou plusieurs écouteurs à l'équilibreur de charge.

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



Pour garantir que vos instances enregistrées puissent traiter la charge de demandes dans chaque zone de disponibilité, il est important de conserver environ le même nombre d'instances dans chaque zone de disponibilité enregistrée auprès de l'équilibreur de charge. Par exemple, si vous avez dix instances dans la zone de disponibilité us-west-2a et deux instances dans la zone de disponibilité us-west-2b, les demandes sont réparties de manière uniforme entre les deux zones de disponibilité. En conséquence, les deux instances dans us-west-2b traitent la même quantité de trafic que les dix instances dans us-west-2a. Vous devriez plutôt avoir six instances dans chaque zone de disponibilité.

Par défaut, l'équilibreur de charge répartit le trafic uniformément entre les zones de disponibilité qui vous activez pour votre équilibreur de charge. Afin de répartir le trafic de manière uniforme entre toutes les instances enregistrées dans toutes les zones de disponibilité activées, activez l'équilibrage de charge entre zones sur votre équilibreur de charge. Cependant, nous vous recommandons de conserver des nombres approximativement équivalents d'instances dans chaque zone de disponibilité pour une meilleure tolérance aux pannes.

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

Avantages

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

- Prise en charge des écouteurs TCP et SSL

- Prise en charge des sessions permanentes à l'aide de cookies générés par l'application

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 savoir comment créer un Classic Load Balancer et enregistrer des instances EC2 auprès de celui-ci, consultez Didacticiel : Création d'un Classic Load Balancer.
- Pour savoir comment créer un équilibreur de charge HTTPS et enregistrer des instances EC2 auprès de celui-ci, consultez Création d'un Classic Load Balancer avec un Écouteur HTTPS.
- Pour apprendre à utiliser les différentes fonctions prises en charge par Elastic Load Balancing, consultez Configurer votre Classic Load Balancer.

Tarification

Avec votre équilibreur de charge, vous payez uniquement en fonction de votre utilisation. Pour plus d'informations, consultez Tarification Elastic Load Balancing.

Didacticiel : Création d'un Classic Load Balancer

Ce didacticiel fournit une introduction pratique aux équilibreurs de charge classiques via une interface Web. AWS Management Console Vous allez créer un équilibreur de charge qui reçoit le trafic HTTP public et l'envoie à vos instances EC2.

Tâches

- Avant de commencer
- Créez un Classic Load Balancer à l'aide du AWS Management Console

Avant de commencer

- Suivez les étapes de Préparation de votre VPC et de vos instances EC2.
- Lancez les instances EC2 que vous avez l'intention d'enregistrer auprès de votre équilibreur de charge. Assurez-vous que les groupes de sécurité pour ces instances autorisent l'accès HTTP sur le port 80.
- Installez un serveur web, comme Apache ou Internet Information Services (IIS), sur chaque instance, saisissez son nom DNS dans le champ d'adresse d'un navigateur web connecté à Internet et vérifiez que le navigateur affiche la page par défaut du serveur.

Créez un Classic Load Balancer à l'aide du AWS Management Console

Utilisez la procédure suivante pour créer votre Classic Load Balancer. Fournissez des informations de configuration de base pour votre équilibreur de charge, comme un nom et un schéma. Fournissez ensuite des informations sur votre réseau et sur l'écouteur qui achemine le trafic vers vos instances.

Pour créer un Classic 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 sélectionner la même Région que celle que vous avez sélectionnée pour vos instances EC2.
3. Dans le panneau de navigation, sous Load Balancing (Équilibrage de charge), choisissez Load Balancers (Équilibreurs de charge).

4. Sélectionnez Create Load Balancer (Créer un équilibreur de charge).
5. Développez la section Classic Load Balancer, puis choisissez Create.
6. Configuration de base
   a. Pour Load Balancer name, saisissez un nom pour l'équilibreur de charge.

      Le nom de votre Classic Load Balancer doit être unique dans l'ensemble de vos Classic Load Balancers pour la région, ne peut contenir que 32 caractères au maximum, ne peut comporter que des caractères alphanumériques et des traits d'union, et ne doit pas commencer ou se terminer par un trait d'union.
   b. Pour Scheme, sélectionnez Internet-facing.
7. Mappage du réseau
   a. Pour VPC, sélectionnez le même VPC que celui que vous avez sélectionné pour vos instances.
   b. Pour Mappings, sélectionnez d'abord une Zone de disponibilité, puis choisissez un sous-réseau public parmi ses sous-réseaux disponibles. Vous ne pouvez sélectionner qu'un seul sous-réseau par zone de disponibilité. Afin d'améliorer la disponibilité de votre équilibreur de charge, sélectionnez plusieurs zones de disponibilité et sous-réseaux.
8. Groupes de sécurité
   - Pour Security groups, sélectionnez un groupe de sécurité existant configuré pour autoriser le trafic HTTP requis sur le port 80.
9. Écouteurs et routage
   a. Pour Listener, assurez-vous que le protocole est `HTTP` et le port est `80`.
   b. Pour Instance, assurez-vous que le protocole est `HTTP` et le port est `80`.
10. Surveillance de l'état
    a. Pour Ping Protocol, assurez-vous que le protocole est `HTTP`.
    b. Pour Ping Port, assurez-vous que le port est `80`.
    c. Pour Ping Path, assurez-vous que le chemin est `/`.
    d. Pour Advanced health check settings, utilisez les valeurs par défaut.
11. Instances
    a. Sélectionnez Add instances pour afficher l'écran de sélection des instances.

b. Sous Available instances, vous pouvez sélectionner parmi les instances actuellement disponibles pour l'équilibreur de charge, en fonction des paramètres réseau actuels.

c. Lorsque vous êtes satisfait de vos sélections, sélectionnez Confirm pour ajouter les instances à enregistrer dans l'équilibreur de charge.

12. Attributs

- Pour Enable cross-zone load balancing, Enable connection draining et Timeout (draining interval) conservez les valeurs par défaut.

13. Balises d'équilibreur de charge (facultatif)

a. Le champ Key est obligatoire.

b. Le champ Value est facultatif.

c. Pour ajouter une autre balise, sélectionnez Add new tag puis entrez vos valeurs dans le champ Key et éventuellement le champ Value.

d. Pour supprimer une balise existante, sélectionner Remove en regard de la balise à supprimer.

14. Résumé et création

a. Si vous devez modifier des paramètres, sélectionnez Edit en regard du paramètre à modifier.

b. Une fois que vous êtes satisfait de tous les paramètres affichés dans le résumé, sélectionnez Create load balancer pour commencer à créer votre équilibreur de charge.

c. Sur la dernière page de création, sélectionnez View load balancer pour afficher votre équilibreur de charge dans la console Amazon EC2.

15. Vérification

a. Sélectionnez votre nouvel équilibreur de charge.

b. Sous l'onglet Target instances, vérifiez la colonne Health status. Une fois qu'au moins l'une de vos instances EC2 est en service, vous pouvez tester votre équilibreur de charge.

c. Dans la section Détails, copiez les équilibreurs de charge DNS name qui ressemblerait à `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`.

d. Collez le nom DNS de votre nouvel équilibreur de charge dans le champ d'adresse d'un navigateur web public connecté à Internet. Si votre équilibreur de charge fonctionne correctement, vous voyez la page par défaut de votre serveur.

16. Supprimer (facultatif)

a. Si vous avez un enregistrement CNAME 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.

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

c. Sélectionnez l'équilibreur de charge.

d. Sélectionnez Actions, Delete load balancer.

e. Lorsque vous êtes invité à confirmer, tapez `confirm`, puis sélectionnez Delete.

f. Une fois que vous avez supprimé un équilibreur de charge, les instances EC2 enregistrées auprès de l'équilibreur de charge continuent de s'exécuter. Vous serez facturé pour chaque heure partielle ou complète pendant laquelle elles continuent de s'exécuter. Lorsque vous n'avez plus besoin d'une instance EC2, vous pouvez l'arrêter ou la résilier pour éviter des frais supplémentaires.

Classic Load Balancers accessibles sur Internet

Un équilibreur de charge accessible sur Internet possède un nom DNS publiquement résolu. Il peut router les demandes de clients via Internet vers les instances EC2 qui sont enregistrées auprès de l'équilibreur de charge.

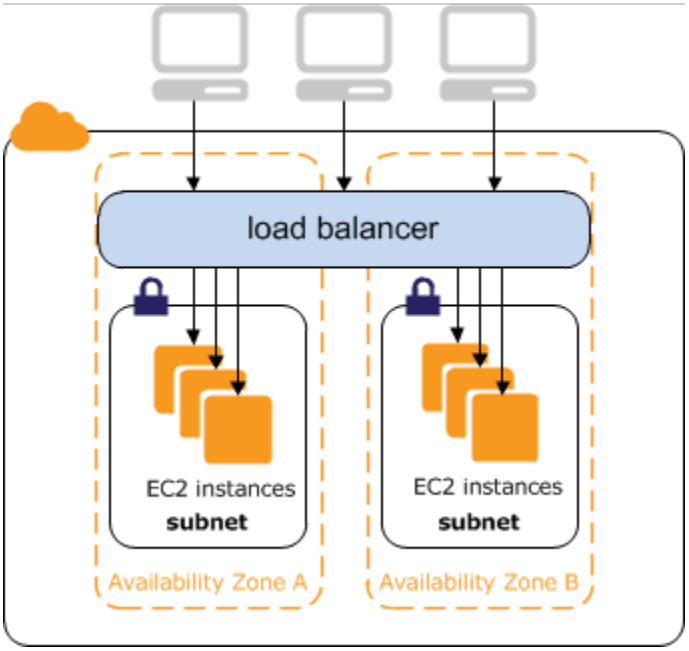


Table des matières

- Noms DNS publics pour votre équilibreur de charge
- Créer un équilibreur de charge accessible sur Internet

Noms DNS publics pour votre équilibreur de charge

Lorsque votre équilibreur de charge est créé, il reçoit un nom DNS public que les clients peuvent utiliser pour envoyer des demandes. Les serveurs DNS résolvent le nom DNS de votre équilibreur de charge aux adresses IP publiques des nœuds d'équilibreur de charge pour votre équilibreur de charge. Chaque nœud d'équilibreur de charge est connecté aux instances principales à l'aide d'adresses IP privées.

La console affiche un nom DNS public au format suivant :

```
name-1234567890.region.elb.amazonaws.com
```

Créer un équilibreur de charge accessible sur Internet

Lorsque vous créez un équilibreur de charge dans un VPC, vous pouvez le définir en tant qu'équilibreur de charge interne ou accessible sur Internet. Vous créez un équilibreur de charge accessible sur Internet dans un sous-réseau public.

Lorsque vous créez votre équilibreur de charge, vous configurez des écouteurs et des vérifications de l'état, et vous enregistrez des instances principales. Vous configurez un écouteur en spécifiant un protocole et un port pour les connexions frontales (du client vers l'équilibreur de charge), et un protocole et un port pour les connexions principales (de l'équilibreur de charge vers les instances principales). Vous pouvez configurer plusieurs écouteurs pour votre équilibreur de charge.

Pour créer un équilibreur de charge accessible sur Internet de base, consultez Didacticiel : Création d'un Classic Load Balancer.

Pour créer un équilibreur de charge avec un écouteur HTTPS, consultez Création d'un Classic Load Balancer avec un Écouteur HTTPS.

Internal Classic Load Balancers internes

Lorsque vous créez un équilibreur de charge dans un VPC, vous devez choisir entre un équilibreur de charge interne et un équilibreur de charge accessible sur Internet.

Les nœuds d'un équilibreur de charge accessible sur Internet ont des adresses IP publiques. Le nom DNS d'un équilibreur de charge accessible sur Internet peut être publiquement résolu en adresses IP publiques des nœuds. Les équilibreurs de charge accessibles sur Internet peuvent donc acheminer des demandes de clients via Internet. Pour plus d'informations, consultez Classic Load Balancers accessibles sur Internet.

Les nœuds d'un équilibreur de charge interne ont des adresses IP privées uniquement. Le nom DNS d'un équilibreur de charge interne est publiquement résolu en adresses IP privées des nœuds. Les équilibreurs de charge internes peuvent donc acheminer uniquement des demandes de clients avec un accès au VPC de l'équilibreur de charge.

Si votre application possède plusieurs niveaux, par exemple, des serveurs web qui doivent être connectés à Internet et des serveurs de base de données qui sont connectés uniquement aux serveurs web, vous pouvez concevoir une architecture utilisant à la fois un équilibreur de charge interne et un équilibreur de charge accessible sur Internet. Créez un équilibreur de charge accessible sur Internet et enregistrez les serveurs Web auprès de celui-ci. Créez un équilibreur de charge interne et enregistrez les serveurs de base de données auprès de celui-ci. Les serveurs web reçoivent les demandes de l'équilibreur de charge accessible sur Internet et les envoient pour les serveurs de base de données à l'équilibreur de charge interne. Les serveurs de base de données reçoivent les demandes de l'équilibreur de charge interne.

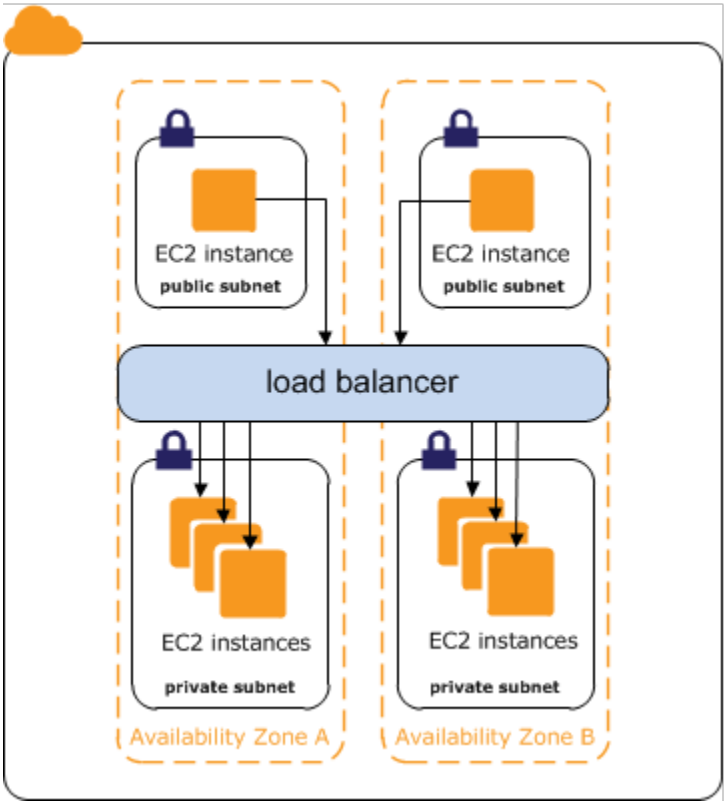


Table des matières

- Nom DNS public de votre équilibreur de charge
- Création d'un Classic Load Balancer interne

Nom DNS public de votre équilibreur de charge

Lorsqu'un équilibreur de charge interne est créé, il reçoit un nom DNS public au format suivant :

```
internal-name-123456789.region.elb.amazonaws.com
```

Les serveurs DNS résolvent le nom DNS de votre équilibreur de charge aux adresses IP privées des nœuds d'équilibreur de charge pour votre équilibreur de charge interne. Chaque nœud d'équilibreur de charge est connecté aux adresses IP privées des instances principales à l'aide d'interfaces réseau Elastic. Si l'équilibrage de charge entre zones est activé, chaque nœud est connecté à chaque instance principale, quelle que soit la zone de disponibilité. Sinon, chaque nœud est connecté uniquement aux instances qui sont dans sa zone de disponibilité.

Création d'un Classic Load Balancer interne

Vous pouvez créer un équilibreur de charge interne pour répartir le trafic vers vos instances EC2 depuis les clients ayant accès au VPC de l'équilibreur de charge.

Table des matières

- Prérequis
- Créez un équilibreur de charge interne à l'aide du AWS Management Console
- Créez un équilibreur de charge interne à l'aide du AWS CLI

Prérequis

- Si vous n'avez pas encore créé de VPC pour votre équilibreur de charge, vous devez le créer avant de démarrer. Pour plus d’informations, consultez Préparation de votre VPC et de vos instances EC2.
- Lancez les instances EC2 que vous avez l'intention d'enregistrer auprès de votre équilibreur de charge interne. Veiller à les lancer dans des sous-réseaux privés dans le VPC destiné à l'équilibreur de charge.

Créez un équilibreur de charge interne à l'aide du AWS Management Console

Utilisez la procédure suivante pour créer votre Classic Load Balancer interne. Fournissez des informations de configuration de base pour votre équilibreur de charge, comme un nom et un schéma. Fournissez ensuite des informations sur votre réseau et sur l'écouteur qui achemine le trafic vers vos instances.

Pour créer un Classic Load Balancer interne 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 sélectionner la même Région que celle que vous avez sélectionnée pour vos instances EC2.
3. Dans le panneau de navigation, sous Load Balancing (Équilibrage de charge), choisissez Load Balancers (Équilibreurs de charge).
4. Sélectionnez Create Load Balancer (Créer un équilibreur de charge).

5. Développez la section Classic Load Balancer, puis choisissez Create.
6. Configuration de base
   a. Pour Load Balancer name, saisissez un nom pour l'équilibreur de charge.

      Le nom de votre Classic Load Balancer doit être unique dans l'ensemble de vos Classic Load Balancers pour la région, ne peut contenir que 32 caractères au maximum, ne peut comporter que des caractères alphanumériques et des traits d'union, et ne doit pas commencer ou se terminer par un trait d'union.
   b. Pour Scheme, sélectionnez Internal.
7. Mappage du réseau
   a. Pour VPC, sélectionnez le même VPC que celui que vous avez sélectionné pour vos instances.
   b. Pour Mappings, sélectionnez d'abord une Zone de disponibilité, puis choisissez un sous-réseau parmi ses sous-réseaux disponibles. Vous ne pouvez sélectionner qu'un seul sous-réseau par zone de disponibilité. Afin d'améliorer la disponibilité de votre équilibreur de charge, sélectionnez plusieurs zones de disponibilité et sous-réseaux.
8. Pour Security groups, sélectionnez un groupe de sécurité existant configuré pour autoriser le trafic HTTP requis sur le port 80. Vous pouvez également créer un nouveau groupe de sécurité si votre application utilise des protocoles et des ports différents.
9. Écouteurs et routage
   a. Pour Listener, assurez-vous que le protocole est `HTTP` et le port est `80`.
   b. Pour Instance, assurez-vous que le protocole est `HTTP` et le port est `80`.
10. Surveillance de l'état
    a. Pour Ping Protocol, la valeur par défaut est `HTTP`.
    b. Pour Ping Port, la valeur par défaut est `80`.
    c. Pour Ping Path, la valeur par défaut est `/`.
    d. Pour Advanced health check settings, utilisez les valeurs par défaut ou saisissez des valeurs spécifiques à votre application.
11. Instances
    a. Sélectionnez Add instances pour afficher l'écran de sélection des instances.

b. Sous Available instances, vous pouvez sélectionner parmi les instances actuellement disponibles pour l'équilibreur de charge, en fonction des paramètres réseau sélectionnés précédemment.

c. Lorsque vous êtes satisfait de vos sélections, sélectionnez Confirm pour ajouter les instances à enregistrer dans l'équilibreur de charge.

12. Attributs

- Pour Enable cross-zone load balancing, Enable connection draining et Timeout (draining interval) conservez les valeurs par défaut.

13. Balises d'équilibreur de charge (facultatif)

a. Le champ Key est obligatoire.

b. Le champ Value est facultatif.

c. Pour ajouter une autre balise, sélectionnez Add new tag puis entrez vos valeurs dans le champ Key et éventuellement le champ Value.

d. Pour supprimer une balise existante, sélectionner Remove en regard de la balise à supprimer.

14. Résumé et création

a. Si vous devez modifier des paramètres, sélectionnez Edit en regard du paramètre à modifier.

b. Une fois que vous êtes satisfait de tous les paramètres affichés dans le résumé, sélectionnez Create load balancer pour commencer à créer votre équilibreur de charge.

c. Sur la dernière page de création, sélectionnez View load balancer pour afficher votre équilibreur de charge dans la console Amazon EC2.

15. Vérification

a. Sélectionnez votre nouvel équilibreur de charge.

b. Sous l'onglet Target instances, vérifiez la colonne Health status. Une fois qu'au moins l'une de vos instances EC2 est en service, vous pouvez tester votre équilibreur de charge.

c. Dans la section Détails, copiez les équilibreurs de charge DNS name qui ressemblerait à `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`.

d. Collez le nom DNS de votre nouvel équilibreur de charge dans le champ d'adresse d'un navigateur web public connecté à Internet. Si votre équilibreur de charge fonctionne correctement, vous voyez la page par défaut de votre serveur.

16. Supprimer (facultatif)

    a. Si vous avez un enregistrement CNAME 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.

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

    c. Sélectionnez l'équilibreur de charge.

    d. Sélectionnez Actions, Delete load balancer.

    e. Lorsque vous êtes invité à confirmer, tapez `confirm`, puis sélectionnez Delete.

    f. Une fois que vous avez supprimé un équilibreur de charge, les instances EC2 enregistrées auprès de l'équilibreur de charge continuent de s'exécuter. Vous serez facturé pour chaque heure partielle ou complète pendant laquelle elles continuent de s'exécuter. Lorsque vous n'avez plus besoin d'une instance EC2, vous pouvez l'arrêter ou la résilier pour éviter des frais supplémentaires.

Créez un équilibreur de charge interne à l'aide du AWS CLI

Par défaut, Elastic Load Balancing crée un équilibreur de charge accessible sur Internet. Utilisez la procédure suivante pour créer un équilibreur de charge interne et enregistrer vos instances EC2 auprès de l'équilibreur de charge interne nouvellement créé.

Pour créer un équilibreur de charge interne

1. Utilisez la create-load-balancercommande avec l'`--scheme`option définie sur`internal`, comme suit :

```
aws elb create-load-balancer --load-balancer-name my-internal-loadbalancer --
listeners Protocol=HTTP,LoadBalancerPort=80,InstanceProtocol=HTTP,InstancePort=80
 --subnets subnet-4e05f721 --scheme internal --security-groups sg-b9ffedd5
```

   Voici un exemple de réponse. Notez que le nom indique qu'il s'agit d'un équilibreur de charge interne.

```
{
    "DNSName": "internal-my-internal-loadbalancer-786501203.us-
west-2.elb.amazonaws.com"
}
```

2. Utilisez la commande register-instances-with-load-balancer suivante pour ajouter des instances :

```
aws elb register-instances-with-load-balancer --load-balancer-name my-internal-loadbalancer --instances i-4f8cf126 i-0bb7ca62
```

Voici un exemple de réponse :

```
{
    "Instances": [
        {
            "InstanceId": "i-4f8cf126"
        },
        {
            "InstanceId": "i-0bb7ca62"
        }
    ]
}
```

3. (Facultatif) Utilisez la describe-load-balancerscommande suivante pour vérifier l'équilibreur de charge interne :

```
aws elb describe-load-balancers --load-balancer-name my-internal-loadbalancer
```

La réponse inclut les champs DNSName et Scheme qui indiquent qu'il s'agit d'un équilibreur de charge interne.

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "DNSName": "internal-my-internal-loadbalancer-1234567890.us-
west-2.elb.amazonaws.com",
            "SecurityGroups": [
                "sg-b9ffedd5"
            ],
            "Policies": {
                "LBCookieStickinessPolicies": [],
                "AppCookieStickinessPolicies": [],
                "OtherPolicies": []
            },
            "LoadBalancerName": "my-internal-loadbalancer",
```

```
            "CreatedTime": "2014-05-22T20:32:19.920Z",
            "AvailabilityZones": [
                "us-west-2a"
            ],
            "Scheme": "internal",
            ...
        }
    ]
}
```

Instances enregistrées pour votre Classic Load Balancer

Une fois que vous avez créé votre Classic Load Balancer, vous devez enregistrez vos instances EC2 après de l'équilibreur de charge. Vous pouvez sélectionner des instances EC2 d'une ou de plusieurs zones de disponibilité au sein de la même Région que l'équilibreur de charge. Elastic Load Balancing Balancer effectue régulièrement des surveillances de l'état sur les instances EC2 enregistrées et répartit automatiquement les demandes entrantes vers le nom DNS de votre équilibreur de charge sur les instances EC2 saines enregistrées.

Table des matières

- Bonnes pratiques pour vos instances
- Préparation de votre VPC et de vos instances EC2
- Configurer les vérifications de l'état pour votre Classic Load Balancer
- Configurer des groupes de sécurité pour votre Classic Load Balancer
- Ajouter ou supprimer des sous-réseaux pour votre Classic Load Balancer
- Enregistrer ou annuler l'enregistrement des instances EC2 pour votre Classic Load Balancer

Bonnes pratiques pour vos instances

- Installez un serveur web, comme Apache ou Internet Information Services (IIS), sur toutes les instances que vous prévoyez d'enregistrer auprès de votre équilibreur de charge.
- Pour les écouteurs HTTP et HTTPS, nous vous recommandons d'activer l'option keep-alive sur vos instances EC2, ce qui permet à l'équilibreur de charge de réutiliser les connexions vers vos instances pour plusieurs demandes de client. Cela réduit la charge sur votre serveur web et améliore le débit de l'équilibreur de charge. Le délai d'expiration keep-alive doit être d'au moins 60 secondes pour que l'équilibreur de charge soit responsable de la fermeture de la connexion à votre instance.
- Elastic Load Balancing prend en charge la détection de la MTU (unité de transmission maximale) du chemin. Pour vous assurer que la détection de la MTU du chemin peut fonctionner correctement, vous devez vérifier que le groupe de sécurité pour votre instance autorise les messages de fragmentation ICMP (type 3, code 4) requis. Pour plus d'informations, consultez Path MTU Discovery dans le guide de l'utilisateur Amazon EC2.

Préparation de votre VPC et de vos instances EC2

Nous vous recommandons de lancer vos instances et de créer votre équilibreur de charge dans un Virtual Private Cloud (VPC). Si vous avez un nouveau AWS compte ou si vous prévoyez d'utiliser une région que vous n'avez jamais utilisée auparavant, vous disposez d'un VPC par défaut. Vous pouvez utiliser un VPC par défaut, si vous avez un, ou créer votre propre VPC.

Équilibreurs de charge dans un VPC

Amazon Virtual Private Cloud (Amazon VPC) vous permet de définir un environnement réseau virtuel dans une section privée et isolée du AWS cloud. Dans ce cloud privé virtuel (VPC), vous pouvez lancer des AWS ressources telles que des équilibreurs de charge et des instances EC2. Pour de plus amples informations, consultez le Guide de l'utilisateur Amazon VPC.

Sous-réseaux pour votre équilibreur de charge

Pour vous assurer que votre équilibreur de charge peut se mettre à l'échelle correctement, vérifiez que chaque sous-réseau pour votre équilibreur de charge dispose d'un bloc d'adresses CIDR, avec au moins un masque de bits `/27` (par exemple, `10.0.0.0/27`), et d'au moins 8 adresses IP disponibles. Votre équilibreur de charge utilise ces adresses IP pour établir des connexions avec les instances et pour monter en puissance la charge si nécessaire. Si le nombre d'adresses IP est insuffisant, l'équilibreur de charge risque de ne pas pouvoir monter en puissance, ce qui entraînera des erreurs 503 dues à une capacité insuffisante.

Créez un sous-réseau dans chaque zone de disponibilité où vous voulez lancer des instances. En fonction de votre application, vous pouvez lancer vos instances dans des sous-réseaux publics, des sous-réseaux privés ou une combinaison des deux. Un sous-réseau public dispose d'une route vers une passerelle Internet. Notez que les VPC par défaut comportent par défaut un sous-réseau public par zone de disponibilité.

Lorsque vous créez un équilibreur de charge, vous devez ajouter un ou plusieurs sous-réseaux publics à celui-ci. Si vos instances sont dans des sous-réseaux privés, créez des sous-réseaux publics dans les mêmes zones de disponibilité que les sous-réseaux avec vos instances ; vous ajouterez ces sous-réseaux publics à l'équilibreur de charge.

Groupes de sécurité

Vous devez vous assurer que l'équilibreur de charge est en mesure de communiquer avec vos instances sur le port d'écoute et le port de vérification de l'état. Pour plus d’informations, consultez Groupes de sécurité pour les équilibreurs de charge dans un VPC. Le groupe de sécurité de vos

instances doit autoriser le trafic dans les deux sens, sur les deux ports de chaque sous-réseau attaché à votre équilibreur de charge. Pour plus d'informations, consultez Groupes de sécurité pour des instances dans un VPC.

Listes ACL réseau

Les ACL réseau pour votre VPC doivent autoriser le trafic dans les deux sens sur le port d'écoute et le port de vérification de l'état. Pour plus d'informations, consultez ACL réseau pour des équilibreurs de charge dans un VPC.

Configurer les vérifications de l'état pour votre Classic Load Balancer

Votre Classic Load Balancer envoie périodiquement des demandes à ses cibles enregistrées pour tester leur état. Ces tests sont appelés vérifications de l'état. L'état des instances qui sont saines au moment de la vérification de l'état est `InService`. L'état des instances qui sont défectueuses au moment de la vérification de l'état est `OutOfService`. L'équilibreur de charge effectue des vérifications de l'état sur toutes les instances enregistrées, que l'instance soit saine ou non.

L'équilibreur de charge n'achemine les demandes que vers les instances saines. Lorsque l'équilibreur de charge détermine qu'une instance est défectueuse, il arrête d'acheminer les demandes vers celle-ci. L'équilibreur de charge recommence à acheminer les demandes vers l'instance lorsque cette dernière a été restaurée à un état sain.

L'équilibreur de charge vérifie l'état de santé des instances enregistrées à l'aide de la configuration de surveillance de l'état par défaut fournie par Elastic Load Balancing ou d'une surveillance de l'état que vous configurez.

Si vous avez associé votre groupe Auto Scaling à un Classic Load Balancer, vous pouvez utiliser la surveillance de l'état de l'équilibreur de charge pour déterminer l'état de santé des instances de votre groupe Auto Scaling. Par défaut, un groupe Auto Scaling détermine périodiquement l'état de santé de chaque instance. Pour plus d'informations, consultez Surveillances de l'état Elastic Load Balancing dans votre groupe Auto Scaling dans le manuel Guide de l'utilisateur Amazon EC2 Auto Scaling.

Table des matières

- Configuration d'une surveillance de l'état
- Mettre à jour la configuration de surveillance de l'état
- Vérifier l'état de santé de vos instances

- Résoudre des problèmes de surveillance de l'état

Configuration d'une surveillance de l'état

Une configuration de l'état contient les informations utilisées par un équilibreur de charge pour déterminer l'état de santé des instances enregistrées. Le tableau suivant décrit les champs de configuration d'une vérification de l'état.

Champ	Description
Protocole	Protocole à utiliser pour se connecter à l'instance. Valeurs valides : `TCP`, `HTTP`, `HTTPS` et `SSL` Valeur par défaut pour la console : `HTTP` Valeur par défaut pour la CLI/l'API : `TCP`
Port	Port à utiliser pour se connecter à l'instance, par exemple, une paire `protocol:port` . Si l'équilibreur de charge ne peut pas se connecter à l'instance sur le port indiqué dans le délai de réponse configuré, l'instance est considérée comme défectueuse. Protocoles : `TCP`, `HTTP`, `HTTPS` et `SSL` Plage de ports : 1 à 65535 Valeur par défaut pour la console : `HTTP:80` Valeur par défaut pour la CLI/l'API : `TCP:80`
Chemin	Destination pour les demandes HTTP ou HTTPS. Une demande HTTP ou HTTPS GET est émise vers l'instance sur le port et le chemin. Si l'équilibreur de charge reçoit une réponse autre que « 200 OK » dans le délai de réponse, l'instance est considérée comme

Champ	Description
	défectueuse. Si la réponse inclut un corps, votre application doit définir l'en-tête Content-Length sur une valeur supérieure ou égale à zéro, ou spécifier Transfer-Encoding avec une valeur définie sur « chunked ». Par défaut : `/index.html`
Response Timeout	Délai d'attente avant de recevoir une réponse de la vérification de l'état, en secondes. Valeurs valides : 2 à 60 Par défaut: 5
HealthCheck Intervalle	Intervalle de temps entre les vérifications de l'état d'une instance individuelle, en secondes. Valeurs valides : 5 à 300 Valeur par défaut : 30
Unhealthy Threshold	Nombre de vérifications de l'état en échec consécutives devant avoir lieu avant de déclarer une instance EC2 comme défectueuse. Valeurs valides : 2 à 10 Par défaut: 2
Healthy Threshold	Nombre de vérifications de l'état réussies consécutives devant avoir lieu avant de déclarer une instance EC2 défectueuse. Valeurs valides : 2 à 10 Par défaut: 10

L'équilibreur de charge envoie une demande de surveillance de l'état à chaque instance enregistrée toutes les `Interval` secondes, en utilisant le port, le protocole et le chemin spécifiés. Chaque demande de vérification de l'état est indépendante et dure pendant la totalité de l'intervalle. Le temps nécessaire pour que l'instance réponde n'affecte pas l'intervalle pour la vérification de l'état suivante. Si les bilans de santé dépassent le UnhealthyThresholdnombre de défaillances consécutives, l'équilibreur de charge met l'instance hors service. Lorsque le nombre de tests de santé dépasse le HealthyThresholdnombre de réussites consécutives, l'équilibreur de charge remet l'instance en service.

Une vérification de l'état HTTP/HTTPS réussit si l'instance renvoie un code de réponse 200 dans l'intervalle de vérification de l'état. Une vérification de l'état TCP réussit si la connexion TCP aboutit. Une vérification de l'état SSL réussit si la liaison SSL aboutit.

Mettre à jour la configuration de surveillance de l'état

Vous pouvez mettre à jour la configuration de vérification de l'état de l'équilibreur de charge à tout moment.

Pour mettre à jour la configuration de vérification de l'état pour 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 panneau de navigation, sous Load Balancing (Équilibrage de charge), 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 Health checks, choisissez Edit.
5. Sur la page Edit health check settings, sous Health checks, mettez à jour la configuration si nécessaire.
6. Lorsque vous êtes satisfait de vos sélections, sélectionnez Save changes.

Pour mettre à jour la configuration du contrôle de santé de votre équilibreur de charge à l'aide du AWS CLI

Utilisez la commande configure-health-check suivante :

```
aws elb configure-health-check --load-balancer-name my-load-balancer --health-check
 Target=HTTP:80/path,Interval=30,UnhealthyThreshold=2,HealthyThreshold=2,Timeout=3
```

Vérifier l'état de santé de vos instances

Vous pouvez vérifier l'état de santé de vos instances enregistrées.

Pour vérifier l'état de santé de vos instances 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 le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Dans la section Details, Status indique le nombre d'instances en service.
5. Sous l'onglet Target instances, dans le tableau Target instances, la colonne Health status indique le statut spécifique de chaque instance enregistrée.

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

Utilisez la commande describe-instance-health suivante :

```
aws elb describe-instance-health --load-balancer-name my-load-balancer
```

Résoudre des problèmes de surveillance de l'état

Vos instances enregistrées peuvent ne pas réussir la vérification de l'état de l'équilibreur de charge pour plusieurs raisons. Les raisons les plus fréquentes de l'échec d'une vérification de l'état sont quand des instances EC2 ferment des connexions vers l'équilibreur de charge ou quand la réponse des instances EC2 dépasse le délai imparti. Pour plus d'informations sur les causes potentielles et les étapes vous pouvez suivre pour résoudre les problèmes de vérification de l'état en échec, consultez Résoudre les problèmes liés à un Classic Load Balancer : surveillance de l'état de santé.

Configurer des groupes de sécurité pour votre Classic Load Balancer

Un groupe de sécurité fonctionne comme un pare-feu qui contrôle le trafic autorisé vers et depuis une ou plusieurs instances. Lorsque vous démarrez une instance EC2, vous pouvez lui associer un ou plusieurs groupes de sécurité. Pour chaque groupe de sécurité, vous ajoutez une ou plusieurs règles

pour autoriser le trafic. Vous pouvez modifier les règles d'un groupe de sécurité à tout moment. Les nouvelles règles sont appliquées automatiquement à toutes les instances associées au groupe de sécurité. Pour plus d'informations, consultez les groupes de sécurité Amazon EC2 dans le guide de l'utilisateur Amazon EC2.

Table des matières

- Groupes de sécurité pour les équilibreurs de charge dans un VPC
- Groupes de sécurité pour des instances dans un VPC
- ACL réseau pour des équilibreurs de charge dans un VPC

Groupes de sécurité pour les équilibreurs de charge dans un VPC

Lorsque vous utilisez le AWS Management Console pour créer un équilibreur de charge dans un VPC, vous pouvez choisir un groupe de sécurité existant pour le VPC ou créer un nouveau groupe de sécurité pour le VPC. Si vous sélectionnez un groupe de sécurité existant, celui-ci doit autoriser le trafic dans les deux sens vers les ports d'écoute et de vérification de l'état pour l'équilibreur de charge. Si vous choisissez de créer un groupe de sécurité, la console ajoute automatiquement des règles pour autoriser tout le trafic sur ces ports.

[VPC autre que celui par défaut] Si vous utilisez AWS CLI l'API ou créez un équilibreur de charge dans un VPC autre que celui par défaut, mais que vous ne spécifiez aucun groupe de sécurité, votre équilibreur de charge est automatiquement associé au groupe de sécurité par défaut du VPC.

[VPC par défaut] Si vous utilisez l'API AWS CLI or pour créer un équilibreur de charge dans votre VPC par défaut, vous ne pouvez pas choisir de groupe de sécurité existant pour votre équilibreur de charge. Au lieu de cela, Elastic Load Balancing fournit un groupe de sécurité avec des règles pour autoriser tout le trafic sur les ports spécifiés pour l'équilibreur de charge. Elastic Load Balancing crée un seul groupe de sécurité de ce type par AWS compte, avec un nom de la forme default_elb_ *id* (par exemple,). `default_elb_fc5fbed3-0405-3b7d-a328-ea290EXAMPLE` Les équilibreurs de charge suivants que vous créez dans le VPC par défaut utilisent également ce groupe de sécurité. Vérifiez les règles du groupe de sécurité pour vous assurer qu'elles autorisent le trafic sur les ports d'écoute et de vérification de l'état pour le nouvel équilibreur de charge. Lorsque vous supprimez votre équilibreur de charge, ce groupe de sécurité n'est pas supprimé automatiquement.

Si vous ajoutez un port d'écoute à un équilibreur de charge existant, vous devez vérifier vos groupes de sécurité pour vous assurer qu'ils autorisent le trafic sur le nouveau port d'écoute dans les deux sens.

Table des matières

- Règles recommandées pour les groupes de sécurité d'équilibreur de charge
- Gérer les groupes de sécurité à l'aide de la console
- Gérez les groupes de sécurité à l'aide du AWS CLI

Règles recommandées pour les groupes de sécurité d'équilibreur de charge

Les groupes de sécurité pour vos équilibreurs de charge doivent permettre à ces derniers de communiquer avec vos instances. Les règles recommandées dépendent du type d'équilibreur de charge (accessible sur Internet ou interne).

Le tableau suivant montre les règles recommandées pour un équilibreur de charge accessible sur Internet.

Inbound			
Source	Protocol	Port Range	Comment
0.0.0.0/0	TCP	*écouteur*	Autoriser tout le trafic entrant sur le port d'écoute de l'équilibreur de charge
Outbound			
Destination	Protocol	Port Range	Comment
groupe_sécurité_instances	TCP	*écouteur_instances*	Autoriser le trafic sortant vers les instances sur le port d'écoute des instances
groupe_sécurité_instances	TCP	*vérification_état*	Autoriser le trafic sortant vers les instances sur le port de vérification de l'état

Le tableau suivant montre les règles recommandées pour un équilibreur de charge interne.

Inbound			
Source	Protocol	Port Range	Comment
Bloc d'adresse du VPC	TCP	*écouteur*	Autoriser le trafic entrant à partir du CIDR VPC vers le port d'écoute de l'équilibreur de charge
Outbound			
Destination	Protocol	Port Range	Comment
groupe_sécurité_instances	TCP	*écouteur_instances*	Autoriser le trafic sortant vers les instances sur le port d'écoute des instances
groupe_sécurité_instances	TCP	*vérification_état*	Autoriser le trafic sortant vers les instances sur le port de vérification de l'état

Gérer les groupes de sécurité à l'aide de la console

Utilisez la procédure suivante pour modifier les groupes de sécurité associés à votre équilibreur de charge dans un VPC.

Pour mettre à jour un groupe de sécurité attribué à 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 panneau de navigation, sous Load Balancing (Équilibrage de charge), 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 Security, choisissez Edit.
5. Sur la page Edit security groups, Sous Security groups ajoutez ou supprimez des groupes de sécurité selon les besoins.

   Vous pouvez ajouter jusqu'à cinq groupes de sécurité.
6. Lorsque vous avez terminé, choisissez Save changes (Enregistrer les modifications).

Gérez les groupes de sécurité à l'aide du AWS CLI

Utilisez la commande apply-security-groups-to-load-balancer suivante pour associer un groupe de sécurité à un équilibreur de charge dans un VPC. Les groupes de sécurité spécifiés remplacent les groupes de sécurité associés.

```
aws elb apply-security-groups-to-load-balancer --load-balancer-name my-loadbalancer --
security-groups sg-53fae93f
```

Voici un exemple de réponse :

```
{
  "SecurityGroups": [
     "sg-53fae93f"
  ]
}
```

Groupes de sécurité pour des instances dans un VPC

Les groupes de sécurité pour vos instances doivent permettre à celles-ci de communiquer avec l'équilibreur de charge. Le tableau suivant montre les règles recommandées.

Inbound			
Source	Protocol	Port Range	Comment
groupe_sécurité_équilibreur_de_charge	TCP	*écouteur_instances*	Autoriser le trafic depuis l'équilibreur de charge sur le

			port d'écoute des instances
groupe_sécurité_équilibreur_de_charge	TCP	*vérification_état*	Autoriser le trafic depuis l'équilibreur de charge sur le port de vérification de l'état

Nous vous recommandons également de permettre au trafic ICMP entrant de prendre en charge la détection de la MTU du chemin. Pour plus d'informations, consultez Path MTU Discovery dans le guide de l'utilisateur Amazon EC2.

ACL réseau pour des équilibreurs de charge dans un VPC

La liste de contrôle des accès (ACL) réseau par défaut pour le VPC autorise tout le trafic entrant et sortant. Si vous créez des ACL réseau personnalisées, vous devez ajouter des règles qui autorisent l'équilibreur de charge et les instances à communiquer.

Les règles recommandées pour le sous-réseau pour votre équilibreur de charge dépendent du type d'équilibreur de charge (accessible sur Internet ou interne).

Voici les règles recommandées pour un équilibreur de charge accessible sur Internet.

Inbound			
Source	Protocol	Port	Comment
0.0.0.0/0	TCP	*écouteur*	Autoriser tout le trafic entrant sur le port d'écoute de l'équilibreur de charge
Bloc d'adresse du VPC	TCP	1024-65535	Autoriser le trafic entrant depuis le CIDR VPC sur les ports éphémères
Outbound			

Destination	Protocol	Port	Comment
Bloc d'adresse du VPC	TCP	*écouteur_instances*	Autoriser tout le trafic sortant sur le port d'écoute des instances
Bloc d'adresse du VPC	TCP	*vérification_état*	Autoriser tout le trafic sortant sur le port de vérification de l'état
0.0.0.0/0	TCP	1024-65535	Autoriser tout le trafic sortant sur les ports éphémères

Voici les règles recommandées pour un équilibreur de charge interne.

Inbound

Source	Protocol	Port	Comment
Bloc d'adresse du VPC	TCP	*écouteur*	Autoriser le trafic entrant à partir du CIDR VPC vers le port d'écoute de l'équilibreur de charge
Bloc d'adresse du VPC	TCP	1024-65535	Autoriser le trafic entrant depuis le CIDR VPC sur les ports éphémères

Outbound

Destination	Protocol	Port	Comment
Bloc d'adresse du VPC	TCP	*écouteur_instances*	Autoriser le trafic sortant vers le

			CIDR VPC sur le port d'écoute des instances
Bloc d'adresse du VPC	TCP	*vérification_état*	Autoriser le trafic sortant vers le CIDR VPC sur le port de vérification de l'état
Bloc d'adresse du VPC	TCP	1024-65535	Autoriser le trafic sortant vers le CIDR VPC sur les ports éphémères

Les règles recommandées pour le sous-réseau pour vos instances dépendent de si le sous-réseau est privé ou public. Les règles suivantes sont pour un sous-réseau privé. Si vos instances sont dans un sous-réseau public, modifiez la source et la destination du CIDR du VPC en `0.0.0.0/0`.

Inbound

Source	Protocol	Port	Comment
Bloc d'adresse du VPC	TCP	*écouteur_instances*	Autoriser le trafic entrant depuis le CIDR VPC sur le port d'écoute des instances
Bloc d'adresse du VPC	TCP	*vérification_état*	Autoriser le trafic entrant depuis le CIDR VPC sur le port de vérification de l'état

Outbound

Destination	Protocol	Port	Comment

Bloc d'adresse du VPC	TCP	1024-65535	Autoriser le trafic sortant vers le CIDR VPC sur les ports éphémères

Ajouter ou supprimer des sous-réseaux pour votre Classic Load Balancer

Lorsque vous ajoutez un sous-réseau à votre équilibreur de charge, Elastic Load Balancer crée un nœud d'équilibreur de charge dans la zone de disponibilité. Les nœuds d'équilibreur de charge acceptent le trafic des clients et transmettent les demandes entrantes aux instances saines enregistrées dans une ou plusieurs zones de disponibilité. Pour les équilibreurs de charge dans un VPC, nous vous recommandons d'ajouter un sous-réseau par zone de disponibilité pour au moins deux zones de disponibilité. Cela permet d'améliorer la disponibilité de votre équilibreur de charge. Notez que vous pouvez modifier à tout moment les sous-réseaux pour votre équilibreur de charge.

Sélectionnez des sous-réseaux dans les mêmes zones de disponibilité que vos instances. Si votre équilibreur de charge est accessible sur Internet, vous devez sélectionner des sous-réseaux publics pour que vos instances principales reçoivent le trafic à partir de l'équilibreur de charge (même si les instances principales sont dans des sous-réseaux privés). Si votre équilibreur de charge est un équilibreur de charge interne, nous vous recommandons de sélectionner des sous-réseaux privés. Pour plus d'informations sur les sous-réseaux pour votre équilibreur de charge, consultez Préparation de votre VPC et de vos instances EC2.

Une fois que vous avez ajouté un sous-réseau, l'équilibreur de charge commence à acheminer les demandes vers les instances enregistrées de la zone de disponibilité correspondante. Par défaut, l'équilibreur de charge achemine les demandes de façon uniforme dans les zones de disponibilité pour ses sous-réseaux. Pour acheminer les demandes de manière uniforme vers les instances enregistrées dans les zones de disponibilité pour ses sous-réseaux, activez l'équilibrage de charge entre zones. Pour plus d'informations, consultez Configurer la répartition de charge entre zones pour votre Classic Load Balancer.

Vous pouvez souhaiter enlever temporairement un sous-réseau de votre équilibreur de charge lorsque sa zone de disponibilité n'a pas d'instances saines enregistrées ou lorsque vous voulez dépanner ou mettre à jour les instances enregistrées. Une fois que vous avez retiré un sous-réseau, l'équilibreur de charge arrête d'acheminer les demandes vers les instances enregistrées de sa

zone de disponibilité mais continue de les acheminer vers les instances enregistrées des zones de disponibilité des autres sous-réseaux.

Table des matières

- Prérequis
- Ajouter un sous-réseau
- Supprimer un sous-réseau

Prérequis

Lorsque vous mettez à jour les sous-réseaux pour votre équilibreur de charge, vous devez respecter les exigences suivantes :

- L'équilibreur de charge doit avoir au moins un sous-réseau en permanence.
- Vous pouvez ajouter au plus un seul sous-réseau par zone de disponibilité.
- Vous ne pouvez pas ajouter de sous-réseau Zone locale.

Comme il existe des API distinctes pour ajouter ou supprimer des sous-réseaux dans un équilibreur de charge, vous devez prendre en compte soigneusement l'ordre des opérations en remplaçant les sous-réseaux actuels par de nouveaux sous-réseaux de façon à répondre à ces exigences. En outre, vous devez ajouter temporairement un sous-réseau d'une autre zone de disponibilité si vous avez besoin de remplacer tous les sous-réseaux pour votre équilibreur de charge. Par exemple, si votre équilibreur de charge a une seule zone de disponibilité et que vous avez besoin de remplacer son sous-réseau par un autre sous-réseau, vous devez d'abord ajouter un sous-réseau depuis une deuxième zone de disponibilité. Ensuite, vous pouvez supprimer le sous-réseau de la zone de disponibilité d'origine (en gardant toujours au moins un sous-réseau), ajouter un nouveau sous-réseau depuis la zone de disponibilité d'origine (sans dépasser un sous-réseau par zone de disponibilité), puis supprimer le sous-réseau de la deuxième zone de disponibilité (si celle-ci est uniquement nécessaire pour effectuer l'échange).

Ajouter un sous-réseau

Vous pouvez étendre la disponibilité de votre équilibreur de charge à un sous-réseau supplémentaire. Enregistrez les instances de ce sous-réseau auprès de l'équilibreur de charge, puis attachez un sous-réseau à l'équilibreur de charge depuis la même zone de disponibilité que les instances. Pour

plus d'informations, consultez Enregistrer ou annuler l'enregistrement des instances EC2 pour votre Classic Load Balancer.

Ajouter un sous-réseau à 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 panneau de navigation, sous Load Balancing (Équilibrage de charge), choisissez Load Balancers (Équilibreurs de charge).
3. Choisissez le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Sous l'ongletNetwork mapping, choisissez Edit subnets.
5. Sur la page Edit subnets, dans la section Network mapping, sélectionnez la zone de disponibilité à activer, puis choisissez le sous-réseau à ajouter dans cette zone de disponibilité.
6. Lorsque vous avez terminé, choisissez Save changes (Enregistrer les modifications).

Ajouter un sous-réseau à votre équilibreur de charge à l'aide de la CLI

Utilisez la commande attach-load-balancer-to-subnets suivante pour ajouter deux sous-réseaux à votre équilibreur de charge :

```
aws elb attach-load-balancer-to-subnets --load-balancer-name my-load-balancer --
subnets subnet-dea770a9 subnet-fb14f6a2
```

La réponse répertorie tous les sous-réseaux pour l'équilibreur de charge. Par exemple :

```
{
    "Subnets": [
        "subnet-5c11033e",
        "subnet-dea770a9",
        "subnet-fb14f6a2"
    ]
}
```

Supprimer un sous-réseau

Vous pouvez supprimer un sous-réseau de votre équilibreur de charge. Notez qu'après que vous avez supprimé un sous-réseau, les instances de ce sous-réseau restent enregistrées auprès de l'équilibreur de charge. Pour plus d'informations, consultez Enregistrer ou annuler l'enregistrement des instances EC2 pour votre Classic Load Balancer.

Pour supprimer un sous-réseau de 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 panneau de navigation, sous Load Balancing (Équilibrage de charge), choisissez Load Balancers (Équilibreurs de charge).
3. Choisissez le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Sous l'ongletNetwork mapping, choisissez Edit subnets.
5. Sur la page Edit subnets, dans la section Network mapping, sélectionnez un sous-réseau différent pour une zone de disponibilité déjà activée, ou désélectionnez une zone de disponibilité pour la supprimer ainsi que le sous-réseau associé.
6. Lorsque vous avez terminé, choisissez Save changes (Enregistrer les modifications).

Pour supprimer un sous-réseau à l'aide du AWS CLI

Utilisez la commande detach-load-balancer-from-subnets suivante pour supprimer les sous-réseaux indiqués de l'équilibreur de charge spécifié :

```
aws elb detach-load-balancer-from-subnets --load-balancer-name my-loadbalancer --
subnets subnet-450f5127
```

La réponse répertorie les sous-réseaux restants pour l'équilibreur de charge. Par exemple :

```
{
    "Subnets": [
        "subnet-15aaab61"
    ]
}
```

Enregistrer ou annuler l'enregistrement des instances EC2 pour votre Classic Load Balancer

L'enregistrement d'une instance EC2 l'ajoute à votre équilibreur de charge. L'équilibreur de charge surveille en permanence l'état de santé des instances enregistrées dans ses zones de disponibilité activées et achemine les demandes vers les instances saines. Si la demande sur vos instances augmente, vous pouvez enregistrer des instances supplémentaires auprès de l'équilibreur de charge pour répondre à la demande.

L'annulation de l'enregistrement d'une instance EC2 supprime celle-ci de votre équilibreur de charge. L'équilibreur de charge arrête d'acheminer les demandes vers une instance dès que l'enregistrement de celle-ci a été annulé. Si la demande diminue, ou si vous avez besoin d'intervenir sur vos instances, vous pouvez annuler l'enregistrement d'instances auprès de l'équilibreur de charge. Une instance dont l'enregistrement a été annulé continue de s'exécuter, mais ne reçoit plus de trafic provenant de l'équilibreur de charge, et vous pouvez l'enregistrer à nouveau auprès de l'équilibreur de charge lorsque vous êtes prêt.

Lorsque vous annulez l'enregistrement d'une instance, Elastic Load Balancing attend que les demandes en cours soient terminées si un drainage de la connexion est activé. Pour plus d'informations, consultez Configurer le drainage de la connexion pour votre Classic Load Balancer.

Si votre équilibreur de charge est attaché à un groupe Auto Scaling, les instances du groupe sont automatiquement enregistrées auprès de l'équilibreur de charge. Si vous détachez un équilibreur de charge de votre groupe Auto Scaling, l'enregistrement des instances du groupe est annulé.

Elastic Load Balancing enregistre votre instance EC2 auprès de votre équilibreur de charge à l'aide de son adresse IP.

[EC2-VPC] Lorsque vous enregistrez une instance avec une interface réseau Elastic (ENI) attachée, l'équilibreur de charge achemine les demandes vers l'adresse IP principale de l'interface principale (eth0) de l'instance.

Table des matières

- Enregistrer une Instance
- Afficher les instances enregistrées auprès de l'équilibreur de charge
- Déterminer l'équilibreur de charge pour une instance enregistrée
- Annuler l'enregistrement d'une instance

Enregistrer une Instance

Lorsque vous êtes prêt, enregistrez votre instance auprès de votre équilibreur de charge. Si l'instance est dans une zone de disponibilité qui est activée pour l'équilibreur de charge, l'instance est prête à recevoir le trafic à partir de l'équilibreur de charge dès qu'elle réussit le nombre requis de vérifications de l'état.

Pour enregistrer vos instances 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 le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Sous l'onglet Target instances, sélectionnez Manage instances.
5. Sur la page Manage instance, dans le tableau Available instances, sélectionnez les instances à enregistrer auprès de votre équilibreur de charge.
6. Assurez-vous que les instances devant être enregistrées sont renseignées dans le tableau Review selected instances.
7. Sélectionnez Enregistrer les modifications.

Pour enregistrer vos instances à l'aide du AWS CLI

Utilisez la commande register-instances-with-load-balancer suivante :

```
aws elb register-instances-with-load-balancer --load-balancer-name my-loadbalancer --instances i-4e05f721
```

Voici un exemple de réponse qui répertorie les instances enregistrées auprès de l'équilibreur de charge :

```
{
    "Instances": [
        {
            "InstanceId": "i-315b7e51"
        },
        {
            "InstanceId": "i-4e05f721"
        }
    ]
}
```

Afficher les instances enregistrées auprès de l'équilibreur de charge

Utilisez la commande describe-load-balancers suivante pour répertorier les instances enregistrées auprès de l'équilibreur de charge spécifié :

```
aws elb describe-load-balancers --load-balancer-names my-load-balancer --output text --
query "LoadBalancerDescriptions[*].Instances[*].InstanceId"
```

Voici un exemple de sortie :

```
i-e905622e
i-315b7e51
i-4e05f721
```

Déterminer l'équilibreur de charge pour une instance enregistrée

Utilisez la commande describe-load-balancers suivante pour obtenir le nom de l'équilibreur de charge auprès duquel l'instance spécifiée est enregistrée :

```
aws elb describe-load-balancers --output text --query "LoadBalancerDescriptions[?
Instances[?InstanceId=='i-e905622e']].[LoadBalancerName]"
```

Voici un exemple de sortie :

```
my-load-balancer
```

Annuler l'enregistrement d'une instance

Vous pouvez annuler l'enregistrement d'une instance auprès de votre équilibreur de charge si vous n'avez plus besoin de la capacité, ou si vous devez intervenir sur l'instance.

Si votre équilibreur de charge est attaché à un groupe Auto Scaling, détacher l'instance du groupe annule également son enregistrement auprès de l'équilibreur de charge. Pour de plus amples informations, consultez Détacher les instances EC2 de votre groupe Auto Scaling dans le Guide de l'utilisateur Amazon EC2 Auto Scaling.

Pour annuler l'enregistrement de vos instances 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 le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Sous l'onglet Target instances, sélectionnez Manage instances.

5. Sur la page Manage instances, dans le tableau Available instances, désélectionnez les instances à désenregistrer auprès de votre équilibreur de charge.
6. Assurez-vous que les instances devant être désenregistrées sont renseignées dans le tableau Review selected instances.
7. Sélectionnez Enregistrer les modifications.

Pour désenregistrer vos instances à l'aide du AWS CLI

Utilisez la commande deregister-instances-from-load-balancer suivante :

```
aws elb deregister-instances-from-load-balancer --load-balancer-name my-loadbalancer --instances i-4e05f721
```

Voici un exemple de réponse qui répertorie les instances enregistrées restantes auprès de l'équilibreur de charge :

```
{
    "Instances": [
        {
            "InstanceId": "i-315b7e51"
        }
    ]
}
```

Écouteurs de votre Classic Load Balancer

Avant de commencer à utiliser Elastic Load Balancing, vous devez configurer un ou plusieurs Écouteurs pour votre Classic Load Balancer. Un écouteur est un processus qui vérifie les demandes de connexion. Il est configuré avec un protocole et un port pour les connexions frontales (du client vers l'équilibreur de charge), et un protocole et un port pour les connexions principales (de l'équilibreur de charge vers l'instance principale).

Elastic Load Balancing prend en charge les protocoles suivants :

- HTTP
- HTTPS (HTTP sécurisé)
- TCP
- SSL (TCP sécurisé)

Le protocole HTTPS utilise le protocole SSL pour établir une connexion sécurisée sur la couche HTTP. Vous pouvez également utiliser le protocole SSL pour établir une connexion sécurisée sur la couche TCP.

Si la connexion frontale utilise TCP ou SSL, vos connexions principales peuvent utiliser TCP ou SSL. Si la connexion frontale utilise HTTP ou HTTPS, vos connexions principales peuvent utiliser HTTP ou HTTPS.

Les instances principales peuvent écouter sur les ports 1 à 65535.

Les équilibreurs de charge peuvent écouter sur les ports suivants : 1-65535

Table des matières

- Protocoles
- Écouteurs HTTPS/SSL
- Configurations d'Écouteur pour Classic Load Balancers
- En-têtes HTTP et Classic Load Balancers

Protocoles

La communication pour une application web classique passe par des couches de matériels et de logiciels. Chaque couche fournit une fonction de communication spécifique. Le contrôle sur la fonction de communication est transmis d'une couche à la couche suivante, dans l'ordre. OSI (Open System Interconnection) définit une infrastructure de modèle pour l'implémentation d'un format standard de communication, appelé protocole, dans ces couches. Pour plus d'informations, consultez Modèle OSI dans Wikipedia.

Lorsque vous utilisez Elastic Load Balancing, vous devez avoir une compréhension de base des couches 4 et 7. La couche 4 est la couche de transport qui décrit la connexion TCP (Transmission Control Protocol) entre le client et votre instance principale, via l'équilibreur de charge. La couche 4 est le niveau le plus bas configurable pour votre équilibreur de charge. La couche 7 est la couche d'application qui décrit l'utilisation des connexions HTTP (Hypertext Transfer Protocol) et HTTPS (HTTP sécurisé) depuis les clients vers l'équilibreur de charge, et depuis l'équilibreur de charge vers votre instance principale.

Le protocole SSL (Secure Sockets Layer) est principalement utilisé pour chiffrer des données confidentielles sur des réseaux non sécurisés comme Internet. Le protocole SSL établit une connexion sécurisée entre un client et le serveur principal, et garantit que toutes les données transmises entre le client et votre serveur sont privées et complètes.

Protocole TCP/SSL

Lorsque vous utilisez TCP (couche 4) pour les connexions frontales et principales, votre équilibreur de charge transmet la demande aux instances principales sans modifier les en-têtes. Une fois que votre équilibreur de charge a reçu une demande, il tente d'ouvrir une connexion TCP vers l'instance principale sur le port spécifié dans la configuration de l'écouteur.

Comme les équilibreurs de charge interceptent le trafic entre les clients et vos instances principales, les journaux d'accès pour votre instance principale contiennent l'adresse IP de l'équilibreur de charge, et non celle client d'origine. Vous pouvez activer le protocole proxy, qui ajoute un en-tête avec les informations de connexion du client, comme l'adresse IP source, l'adresse IP de destination et des numéros de port. L'en-tête est ensuite envoyé à l'instance principale dans le cadre de la demande. Vous pouvez analyser la première ligne de la demande pour extraire les informations de connexion. Pour plus d’informations, consultez Configurer la prise en charge du protocole proxy pour votre Classic Load Balancer.

En utilisant cette configuration, vous ne recevez pas de cookies pour la permanence des sessions ou d'en-têtes X-Forwarded.

Protocole HTTP/HTTPS

Lorsque vous utilisez le protocole HTTP (couche 7) pour les connexions frontales et dorsales, votre équilibreur de charge analyse les en-têtes de la demande avant de l'envoyer aux instances principales.

Pour chaque instance enregistrée et saine derrière un équilibreur de charge HTTP/HTTPS, Elastic Load Balancing ouvre et gère une ou plusieurs connexions TCP. Ces connexions permettent de s'assurer qu'il existe toujours une connexion établie prête à recevoir les demandes HTTP/HTTPS.

Les demandes HTTP et les réponses HTTP utilisent des champs d'en-tête pour envoyer des informations concernant les messages HTTP. Elastic Load Balancing prend en charge les en-têtes `X-Forwarded-For`. Comme les équilibreurs de charge interceptent le trafic entre les clients et les serveurs, vos journaux d'accès au serveur contiennent uniquement l'adresse IP de l'équilibreur de charge. Pour voir l'adresse IP du client, utilisez l'en-tête de demande `X-Forwarded-For`. Pour plus d'informations, consultez X-Forwarded-For.

Lorsque vous utilisez HTTP/HTTPS, vous pouvez activer les sessions permanentes sur votre équilibreur de charge. Une session permanente lie la session d'un utilisateur à une instance principale spécifique. Il est ainsi possible de garantir que toutes les demandes provenant de l'utilisateur pendant la session sont adressées à la même instance principale. Pour plus d'informations, consultez Configurer des sessions permanentes pour votre Classic Load Balancer.

Toutes les extensions HTTP ne sont pas prises en charge dans l'équilibreur de charge. Vous devrez peut-être utiliser un écouteur TCP si l'équilibreur de charge ne peut pas mettre fin à la demande en raison de méthodes inattendues, de codes de réponse ou d'autres implémentations HTTP 1.0/1.1 non standard.

Écouteurs HTTPS/SSL

Vous pouvez créer un équilibreur de charge avec les fonctions de sécurité suivantes.

Certificats de serveur SSL

Si vous utilisez HTTPS ou SSL pour vos connexions front-end, vous devez déployer un certificat X.509 (certificat de serveur SSL) sur votre équilibreur de charge. L'équilibreur de charge déchiffre les

demandes des clients avant de les envoyer aux instances principales (terminaison SSL). Pour plus d'informations, consultez Certificats SSL/TLS pour les Classic Load Balancers.

Si vous ne voulez pas que l'équilibreur de charge gère la terminaison SSL (opération connue sous le nom de déchargement SSL), vous pouvez utiliser le protocole TCP pour les connexions front-end et back-end et déployer des certificats sur les instances enregistrées qui traitent les demandes.

Négociation SSL

Elastic Load Balancing fournit des configurations de négociation SSL prédéfinies qui sont utilisées pour la négociation SSL lorsqu'une connexion est établie entre un client et votre équilibreur de charge. Les configurations de négociation SSL assurent la compatibilité avec un grand nombre de clients et utilisent des algorithmes de chiffrement à force élevée appelés chiffrements. Cependant, certains cas d'utilisation peuvent avoir besoin que toutes les données sur le réseau soient chiffrées et autoriser uniquement des chiffrements spécifiques. Certaines normes de conformité en matière de sécurité (comme, PCI, SOX, etc.) peuvent avoir besoin d'un jeu de protocoles et de chiffrements spécifiques des clients pour garantir que les normes de sécurité sont respectées. Dans de tels cas, vous pouvez créer une configuration de négociation SSL personnalisée selon vos besoins spécifiques. Vos chiffrements et protocoles devraient prendre effet dans les 30 secondes. Pour plus d'informations, consultez Configurations de négociation SSL pour Classic Load Balancers.

Authentification de serveur principal

Si vous utilisez une connexion HTTPS ou SSL pour vos connexions back-end, vous pouvez activer l'authentification de vos instances enregistrées. Vous pouvez ensuite utiliser le processus d'authentification pour vous assurer que ces instances acceptent uniquement les communications chiffrées et que chaque instance enregistrée possède la clé publique qui convient.

Pour plus d'informations, consultez Configurer l'authentification de serveur principal.

Configurations d'Écouteur pour Classic Load Balancers

Les tableaux suivants récapitulent les paramètres d'Écouteur que vous pouvez utiliser pour configurer vos Classic Load Balancers.

Équilibreur de charge HTTP/HTTPS

Cas d'utilisation	Protocole frontal	Options frontales	Protocole principal	Options principales	Remarques
Équilibreur de charge HTTP de base	HTTP	NA	HTTP	NA	• Prend en charge les en-têtes X-Forwarded
Sécuriser le site Web ou votre application à l'aide d'Elastic Load Balancing pour décharger le déchiffrement SSL	HTTPS	Négociation SSL	HTTP	NA	• Prend en charge les en-têtes X-Forwarded • Nécessite un certificat SSL déployé sur l'équilibreur de charge
Site Web ou application sécurisés à l'aide du end-to-end chiffrement	HTTPS	Négociation SSL	HTTPS	Authentification principale	• Prend en charge les en-têtes X-Forwarded • Nécessite des certificats SSL déployés sur l'équilibreur de charge et les instances enregistrées

Équilibreur de charge TCP/SSL

Cas d'utilisation	Protocole frontal	Options frontales	Protocole principal	Options principales	Remarques
Équilibreur de charge TCP de base	TCP	NA	TCP	NA	• Prend en charge l'en-tête de protocole proxy
Sécuriser le site Web ou votre application à l'aide d'Elastic Load Balancing pour décharger le déchiffrement SSL	SSL	Négociation SSL	TCP	NA	• Nécessite un certificat SSL déployé sur l'équilibreur de charge • Prend en charge l'en-tête de protocole proxy
Site Web ou application sécurisés à l'aide du end-to-end chiffrement avec Elastic Load Balancing	SSL	Négociation SSL	SSL	Authentification principale	• Nécessite des certificats SSL déployés sur l'équilibreur de charge et les instances enregistrées • N'insère pas d'en-

Cas d'utilisation	Protocole frontal	Options frontales	Protocole principal	Options principales	Remarques
					têtes SNI sur les connexions SSL principales • Ne prend pas en charge l'en-tête de protocole proxy

En-têtes HTTP et Classic Load Balancers

Les demandes HTTP et les réponses HTTP utilisent des champs d'en-tête pour envoyer des informations concernant les messages HTTP. Les champs d'en-tête sont des paires nom-valeur dont les noms et les valeurs sont séparés par un signe deux points, et qui sont séparées entre elles par un retour chariot (CR) et un saut de ligne (LF). Un ensemble standard de champs d'en-tête HTTP est défini dans la section du RFC 2616 concernant les en-têtes de message. Des en-têtes HTTP non standard couramment utilisés par les applications sont également disponibles (et ajoutés automatiquement). Certains des en-têtes HTTP non standard ont un préfixe `X-Forwarded`. Les Classic Load Balancers prennent en charge les en-têtes `X-Forwarded` suivants.

Pour plus d'informations sur les connexions HTTP, consultez la section Demande de routage dans le Guide de l'utilisateur Elastic Load Balancing.

Prérequis

- Vérifiez que les paramètres de votre écouteur prennent en charge les en-têtes X-Forwarded. Pour plus d'informations, consultez Configurations d'Écouteur pour Classic Load Balancers.
- Configurez votre serveur web pour consigner les adresses IP client.

En-têtes X-Forwarded

- X-Forwarded-For
- X-Forwarded-Proto
- X-Forwarded-Port

X-Forwarded-For

L'en-tête de demande `X-Forwarded-For` est automatiquement ajouté et vous aide à identifier l'adresse IP d'un client lorsque vous utilisez un équilibreur de charge HTTP ou HTTPS. Comme les équilibreurs de charge interceptent le trafic entre les clients et les serveurs, vos journaux d'accès au serveur contiennent uniquement l'adresse IP de l'équilibreur de charge. Pour voir l'adresse IP du client, utilisez l'en-tête de demande `X-Forwarded-For`. Elastic Load Balancing stocke l'adresse IP du client dans l'en-tête de demande `X-Forwarded-For` et transmet l'en-tête à votre serveur. Si l'en-tête de demande `X-Forwarded-For` n'est pas inclus dans la demande, l'équilibreur de charge en crée un avec l'adresse IP du client comme valeur de la demande. Sinon, l'équilibreur de charge ajoute l'adresse IP du client à l'en-tête existant et transmet l'en-tête à votre serveur. L'en-tête de demande `X-Forwarded-For` peut contenir plusieurs adresses IP séparées par des virgules. L'adresse la plus à gauche est l'adresse IP du client où la demande a été effectuée pour la première fois. Ceci est suivi de tous les identificateurs de proxy ultérieurs, dans une chaîne.

L'en-tête de demande `X-Forwarded-For` a le format suivant :

```
X-Forwarded-For: client-ip-address
```

Voici un exemple d'en-tête de demande `X-Forwarded-For` pour un client avec l'adresse IP `203.0.113.7`.

```
X-Forwarded-For: 203.0.113.7
```

Voici un exemple d'en-tête de demande `X-Forwarded-For` pour un client avec l'adresse IPv6 `2001:DB8::21f:5bff:febf:ce22:8a2e`.

```
X-Forwarded-For: 2001:DB8::21f:5bff:febf:ce22:8a2e
```

X-Forwarded-Proto

L'en-tête de demande `X-Forwarded-Proto` vous permet d'identifier le protocole (HTTP ou HTTPS) utilisé par un client pour se connecter à votre équilibreur de charge. Les journaux d'accès de votre

serveur contiennent uniquement le protocole utilisé entre le serveur et l'équilibreur de charge ; ils ne comportent aucune information sur le protocole utilisé entre le client et l'équilibreur de charge. Pour déterminer le protocole utilisé entre le client et l'équilibreur de charge, utilisez l'en-tête de demande `X-Forwarded-Proto`. Elastic Load Balancing stocke le protocole utilisé entre le client et l'équilibreur de charge dans l'en-tête de demande `X-Forwarded-Proto` et transmet en même temps l'en-tête à votre serveur.

Votre application ou site web peut utiliser le protocole stocké dans l'en-tête de demande `X-Forwarded-Proto` pour générer une réponse qui effectue une redirection vers l'URL appropriée.

L'en-tête de demande `X-Forwarded-Proto` a le format suivant :

```
X-Forwarded-Proto: originatingProtocol
```

L'exemple suivant contient un en-tête de demande `X-Forwarded-Proto` pour une demande provenant du client en tant que demande HTTPS :

```
X-Forwarded-Proto: https
```

X-Forwarded-Port

L'en-tête de demande `X-Forwarded-Port` vous permet d'identifier le port de destination utilisé par le client pour se connecter à l'équilibreur de charge.

Écouteurs HTTPS pour votre Classic Load Balancer

Vous pouvez créer un équilibreur de charge qui utilise le protocole SSL/TLS pour les connexions chiffrées (transfert de charge SSL). Cette fonction permet de chiffrer le trafic entre votre équilibreur de charge et les clients qui initient des sessions HTTPS, ainsi que pour les connexions entre votre équilibreur de charge et vos instances EC2.

Elastic Load Balancing utilise des configurations de négociation SSL (Secure Sockets Layer), également qualifiées de politiques de sécurité, pour négocier des connexions entre les clients et l'équilibreur de charge. Lorsque vous utilisez HTTPS/SSL pour vos connexions front-end, vous pouvez utiliser une stratégie de sécurité prédéfinie ou une stratégie de sécurité personnalisée. Vous devez déployer un certificat SSL sur votre équilibreur de charge. L'équilibreur de charge utilise ce certificat pour mettre fin à la connexion, puis déchiffrer les demandes des clients avant de les envoyer aux instances. L'équilibreur de charge utilise une suite de chiffrement statique pour les connexions back-end. Le cas échéant, vous pouvez choisir d'activer l'authentification sur vos instances.

Les Classic Load Balancers ne prennent pas en charge Server Name Indication (SNI). Vous pouvez plutôt utiliser l'une des autres solutions suivantes :

- Déployez un certificat sur l'équilibreur de charge et ajoutez un nom SAN (Subject Alternative Name) pour chaque site supplémentaire. Les noms SAN vous permettent de protéger plusieurs noms d'hôte à l'aide d'un seul certificat. Demandez à votre fournisseur de certificat de plus amples informations sur le nombre de noms SAN qu'il prend en charge par certificat, et sur comment ajouter et supprimer des noms SAN.
- Utilisez des écouteurs TCP sur le port 443 pour les connexions frontale et principales. L'équilibreur de charge transmet la demande en l'état pour que vous puissiez gérer la terminaison HTTPS sur l'instance EC2.

Les Classic Load Balancers ne prennent pas en charge l'authentification TLS mutuelle (mTLS). Pour la prise en charge de mTLS, créez un écouteur TCP. L'équilibreur de charge transmet la demande en l'état pour que vous puissiez implémenter mTLS sur l'instance EC2.

Table des matières

- Certificats SSL/TLS pour les Classic Load Balancers
- Configurations de négociation SSL pour Classic Load Balancers
- Création d'un Classic Load Balancer avec un Écouteur HTTPS

- Configurer un Écouteur HTTPS pour votre Classic Load Balancer
- Remplacer le certificat SSL pour votre Classic Load Balancer
- Mettre à jour la configuration de négociation SSL de votre Classic Load Balancer

Certificats SSL/TLS pour les Classic Load Balancers

Si vous utilisez le protocole HTTPS (SSL ou TLS) pour votre écouteur front-end, vous devez déployer un certificat SSL/TLS sur votre équilibreur de charge. L'équilibreur de charge utilise le certificat pour mettre fin à la connexion, puis déchiffrer les demandes des clients avant de les envoyer aux instances.

Les protocoles SSL et TLS utilisent un certificat X.509 (certificat de serveur SSL/TLS) pour authentifier le client et l'application back-end. Un certificat X.509 est une forme numérique d'identification émise par une autorité de certification (CA). Il contient les informations d'identification, une période de validité, une clé publique, un numéro de série et la signature numérique de l'émetteur.

Vous pouvez créer un certificat à l'aide AWS Certificate Manager d'un outil prenant en charge les protocoles SSL et TLS, comme OpenSSL. Vous spécifierez ce certificat lorsque vous créerez ou mettrez à jour un écouteur HTTPS pour votre équilibreur de charge. Lorsque vous créez un certificat à utiliser avec votre équilibreur de charge, vous devez spécifier un nom de domaine.

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. S'ils ne correspondent pas, le trafic ne sera pas chiffré, car la connexion TLS ne peut pas être vérifiée.

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 apparaîtra 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 .

Créez ou importez un certificat SSL/TLS à l'aide de AWS Certificate Manager

Nous vous recommandons d'utiliser AWS Certificate Manager (ACM) pour créer ou importer des certificats pour votre équilibreur de charge. ACM s'intègre à Elastic Load Balancing afin que vous puissiez déployer le certificat sur votre équilibreur de charge. Pour que vous puissiez déployer un certificat sur votre équilibreur de charge, le certificat doit être dans la même Région que l'équilibreur de charge. Pour plus d'informations, consultez Demander un certificat public ou Importation de certificats dans le AWS Certificate Manager Guide de l'utilisateur.

Pour permettre à un utilisateur de déployer le certificat sur votre équilibreur de charge avec AWS Management Console, vous devez accorder l'accès à l'action d'API `ListCertificates` d'ACM. Pour plus d'informations, consultez la section Liste des certificats dans le AWS Certificate Manager Guide de l'utilisateur.

> **Important**
>
> Vous ne pouvez pas installer des certificats avec des clés EC ou des clés RSA 4096 bits sur votre équilibreur de charge via l'intégration à ACM. Vous devez charger des certificats avec des clés EC ou des clés RSA 4096 bits dans IAM pour les utiliser avec votre équilibreur de charge.

Importation d'un certificat SSL/TLS à l'aide d'IAM

Si vous n'utilisez pas ACM, vous pouvez utiliser des outils SSL/TLS comme OpenSSL pour créer une demande de signature de certificat (CSR), puis faire signer la CSR par une CA afin de générer un certificat et charger celui-ci dans IAM. Pour de plus amples informations, veuillez consulter Utilisation des certificats de serveur dans le Guide de l'utilisateur IAM.

Configurations de négociation SSL pour Classic Load Balancers

Elastic Load Balancing utilise une configuration de négociation Secure Socket Layer (SSL) (ou politique de sécurité) pour négocier des connexions SSL entre un client et l'équilibreur de charge. Une stratégie de sécurité est une combinaison de protocoles SSL, de chiffrements SSL et de l'option de préférence pour l'ordre des serveurs. Pour plus d'informations sur la configuration d'une connexion SSL pour votre équilibreur de charge, consultez Écouteurs de votre Classic Load Balancer.

Table des matières

- Stratégies de sécurité
- Protocoles SSL
- Préférence pour l'ordre des serveurs
- Chiffrements SSL
- Politiques de sécurité SSL prédéfinies pour les Classic Load Balancers

Stratégies de sécurité

Une stratégie de sécurité détermine les chiffrements et les protocoles pris en charge lors des négociations SSL entre un client et un équilibreur de charge. Vous pouvez configurer vos Classic Load Balancers pour qu'ils utilisent des stratégies de sécurité prédéfinies ou personnalisées.

Notez qu'un certificat fourni par AWS Certificate Manager (ACM) contient une clé publique RSA. Vous devez inclure une suite de chiffrement utilisant RSA dans votre politique de sécurité si vous utilisez un certificat fourni par ACM, sinon, la connexion TLS échouera.

Politiques de sécurité prédéfinies

Les noms des stratégies de sécurité prédéfinies les plus récentes comportent des informations de version basées sur l'année et le mois de la mise à disposition de celles-ci. Par exemple, la stratégie de sécurité prédéfinie par défaut est `ELBSecurityPolicy-2016-08`. Chaque fois qu'une nouvelle stratégie de sécurité prédéfinie est mise à disposition, vous pouvez mettre à jour votre configuration pour l'utiliser.

Pour plus d'informations sur les protocoles et les chiffrements activés pour les stratégies de sécurité prédéfinies, consultez Politiques de sécurité SSL prédéfinies.

Politiques de sécurité personnalisées

Vous pouvez créer une configuration de négociation personnalisée avec les chiffrements et les protocoles dont vous avez besoin. Par exemple, certaines normes de conformité en matière de sécurité (comme PCI et SOC) peuvent avoir besoin d'un jeu de protocoles et de chiffrements spécifique pour garantir que les normes de sécurité sont respectées. Dans de tels cas, vous pouvez créer une stratégie de sécurité personnalisée afin de répondre à ces normes.

Pour plus d'informations sur la création d'une stratégie personnalisée, consultez Mettre à jour la configuration de négociation SSL de votre Classic Load Balancer.

Protocoles SSL

Le protocole SSL 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.

Secure Sockets Layer (SSL) et Transport Layer Security (TLS) sont des protocoles cryptographiques utilisés pour chiffrer les données confidentielles sur des réseaux non sécurisés, comme Internet. Le protocole TLS est une version plus récente du protocole SSL. Dans la documentation Elastic Load Balancing, nous faisons référence aux protocoles SSL et TLS en tant que protocole SSL.

Protocole recommandé

Nous recommandons le protocole TLS 1.2, qui est utilisé dans la politique de sécurité prédéfinie ELB SecurityPolicy -TLS-1-2-2017-01. Vous pouvez également utiliser le protocole TLS 1.2 dans vos politiques de sécurité personnalisées. La politique de sécurité par défaut prend en charge le protocole TLS 1.2 et les versions antérieures de TLS. Elle est donc moins sécurisée que celle d'SecurityPolicyELB -TLS-1-2-2017-01.

Protocole obsolète

Si vous aviez activé précédemment le protocole SSL 2.0 dans une politique personnalisée, nous vous recommandons de mettre à jour votre politique de sécurité vers l'une des politiques de sécurité prédéfinies.

Préférence pour l'ordre des serveurs

Elastic Load Balancing prend en charge l'option Préférence pour l'ordre des serveurs pour négocier des connexions entre un client et un équilibreur de charge. Pendant le processus de négociation de connexion SSL, 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. Par défaut, le premier chiffrement sur la liste du client qui correspond à l'un des chiffrements de l'équilibreur de charge est sélectionné pour la connexion SSL. Si l'équilibreur de charge est configuré pour prendre en charge la préférence pour l'ordre des serveurs, il sélectionne le premier chiffrement de sa liste figurant dans la liste de chiffrements du client. L'équilibreur de charge peut ainsi déterminer quel chiffrement est utilisé pour la connexion SSL. Si vous n'autorisez pas la préférence pour l'ordre des serveurs, l'ordre de chiffrements présenté par le client est utilisé pour négocier des connexions entre le client et l'équilibreur de charge.

Chiffrements SSL

Un chiffrement SSL est un algorithme de chiffrement qui utilise des clés de chiffrement pour créer un message codé. Les protocoles SSL utilisent plusieurs chiffrements SSL pour chiffrer les données sur Internet.

Notez qu'un certificat fourni par AWS Certificate Manager (ACM) contient une clé publique RSA. Vous devez inclure une suite de chiffrement utilisant RSA dans votre politique de sécurité si vous utilisez un certificat fourni par ACM, sinon, la connexion TLS échouera.

Elastic Load Balancing prend en charge les chiffrements suivants pour une utilisation avec des Elastic Load Balancers. Un sous-ensemble de ces chiffrements sont utilisés par les stratégies SSL prédéfinies. Tous ces chiffrements sont disponibles pour être utilisés dans une stratégie personnalisée. Nous vous recommandons d'utiliser uniquement les chiffrements inclus dans la stratégie de sécurité par défaut (ceux avec un astérisque). Beaucoup d'autres chiffrements ne sont pas sûrs et doivent être utilisés à vos risques et périls.

Chiffrements

- ECDHE-ECDSA-AES128-GCM-SHA256 *
- ECDHE-RSA-AES128-GCM-SHA256 *
- ECDHE-ECDSA-AES128-SHA256 *
- ECDHE-RSA-AES128-SHA256 *
- ECDHE-ECDSA-AES128-SHA *
- ECDHE-RSA-AES128-SHA *
- DHE-RSA-AES128-SHA
- 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 *
- AES128-GCM-SHA256 *
- AES128-SHA256 *
- AES128-SHA *

- AES256-GCM-SHA384 *
- AES256-SHA256 *
- AES256-SHA *
- DHE-DSS-AES128-SHA
- CAMELLIA128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- ECDHE-RSA-RC4-SHA
- RC4-SHA
- ECDHE-ECDSA-RC4-SHA
- DHE-DSS-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-DSS-AES256-SHA256
- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- DHE-RSA-CAMELLIA256-SHA
- DHE-DSS-CAMELLIA256-SHA
- CAMELLIA256-SHA
- EDH-DSS-DES-CBC3-SHA
- DHE-DSS-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-DSS-AES128-SHA256
- DHE-RSA-CAMELLIA128-SHA
- DHE-DSS-CAMELLIA128-SHA
- ADH-AES128-GCM-SHA256
- ADH-AES128-SHA
- ADH-AES128-SHA256
- ADH-AES256-GCM-SHA384

- ADH-AES256-SHA
- ADH-AES256-SHA256
- ADH-CAMELLIA128-SHA
- ADH-CAMELLIA256-SHA
- ADH-DES-CBC3-SHA
- ADH-DES-CBC-SHA
- ADH-RC4-MD5
- ADH-SEED-SHA
- DES-CBC-SHA
- DHE-DSS-SEED-SHA
- DHE-RSA-SEED-SHA
- EDH-DSS-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- IDEA-CBC-SHA
- RC4-MD5
- SEED-SHA
- DES-CBC3-MD5
- DES-SRC-MD5
- RC2-SRC-MD5
- PSK-AES256-CBC-SHA
- PSK-3DES-EDE-CBC-SHA
- KRB5-DES-CBC3-SHA
- KRB5-DES-CBC3-MD5
- PSK-AES128-CBC-SHA
- PSK-RC4-SHA
- KRB5-RC4-SHA
- KRB5-RC4-MD5
- KRB5-DES-CBC-SHA
- KRB5-DES-CBC-MD5
- EXP-EDH-RSA-DES-CBC-SHA

- EXP-EDH-DSS-DES-CBC-SHA
- EXP-ADH-DES-CBC-SHA
- EXP-DES-CBC-SHA
- EXP-RC2-CBC-MD5
- EXP-KRB5-RC2-CBC-SHA
- EXP-KRB5-DES-CBC-SHA
- EXP-KRB5-RC2-SRC-MD5
- EXP-KRB5-DES-CBC-MD5
- EXP-ADH-RC4-MD5
- EXP-RC4-MD5
- EXP-KRB5-RC4-SHA
- EXP-KRB5-RC4-MD5

* Ce sont les chiffrements recommandés inclus dans la stratégie de sécurité par défaut.

Politiques de sécurité SSL prédéfinies pour les Classic Load Balancers

Vous pouvez choisir l'une des stratégies de sécurité prédéfinies pour vos écouteurs HTTPS/SSL. Nous vous recommandons la politique de sécurité par défaut `ELBSecurityPolicy-2016-08`, pour des raisons de compatibilité. Vous pouvez utiliser l'une des stratégies `ELBSecurityPolicy-TLS` afin de satisfaire les normes de sécurité et de conformité qui exigent la désactivation de certaines versions de protocole TLS. Vous pouvez également créer une politique de sécurité personnalisée. Pour plus d'informations, consultez Mettre à jour la configuration de négociation SSL.

Les chiffrements basés sur RSA et DSA sont spécifiques à l'algorithme de signature utilisé pour créer un certificat SSL. Veillez à créer un certificat SSL à l'aide de l'algorithme de signature basé sur les chiffrements qui sont activés pour votre stratégie de sécurité.

Si vous sélectionnez une politique qui est activée pour la préférence pour l'ordre des serveurs, l'équilibreur de charge utilise les chiffrements dans l'ordre dans lequel ils sont spécifiés ici pour négocier des connexions entre le client et l'équilibreur de charge. Sinon, l'équilibreur de charge utilise les chiffrements dans l'ordre dans lequel ils sont présentés par le client.

Le tableau suivant décrit les stratégies de sécurité prédéfinies les plus récentes pour les Classic Load Balancers, y compris leurs protocoles SSL activés, les chiffrements SSL et la politique par défaut,

`ELBSecurityPolicy-2016-08`. Le `ELBSecurityPolicy-` a été supprimé des noms de stratégie dans la ligne d'en-tête afin qu'ils correspondent.

> **Tip**
>
> Cette règle s'applique uniquement aux Classic Load Balancers. Pour plus d'informations s'appliquant aux autres équilibreurs de charge, consultez Politiques de sécurité pour les Application Load Balancers et Politiques de sécurité pour les dispositifs d'équilibrage de charge de réseau.

Politique de sécurité	2016-08	TLS-1-1-2017-01	TLS-1-2-2017-01	2015-05	2015-03	2015-02
Protocoles SSL						
Protocol-TLSv1	✓			✓	✓	✓
Protocol-TLSv1.1	✓	✓		✓	✓	✓
Protocol-TLSv1.2	✓	✓	✓	✓	✓	✓
Options SSL						
Préférence pour l'ordre des serveurs	✓	✓	✓	✓	✓	✓
Chiffrements SSL						
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓

Politique de sécurité	2016-08	TLS-1-1-2017-01	TLS-1-2-2017-01	2015-05	2015-03	2015-02
ECDHE-RSA-AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES128-SHA256	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES128-SHA	✓	✓		✓	✓	✓
ECDHE-RSA-AES128-SHA	✓	✓		✓	✓	✓
DHE-RSA-AES128-SHA					✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓

Politique de sécurité	2016-08	TLS-1-1-2017-01	TLS-1-2-2017-01	2015-05	2015-03	2015-02
ECDHE-RSA-AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA384	✓	✓	✓	✓	✓	✓
ECDHE-RSA-AES256-SHA	✓	✓		✓	✓	✓
ECDHE-ECDSA-AES256-SHA	✓	✓		✓	✓	✓
AES128-GCM-SHA256	✓	✓	✓	✓	✓	✓
AES128-SHA256	✓	✓	✓	✓	✓	✓
AES128-SHA	✓	✓		✓	✓	✓

Politique de sécurité	2016-08	TLS-1-1-2017-01	TLS-1-2-2017-01	2015-05	2015-03	2015-02
AES256-GCM-SHA384	✓	✓	✓	✓	✓	✓
AES256-SHA256	✓	✓	✓	✓	✓	✓
AES256-SHA	✓	✓		✓	✓	✓
DHE-DSS-AES128-SHA					✓	✓
DES-CBC3-SHA				✓	✓	

Politiques de sécurité prédéfinies

Voici les politiques de sécurité prédéfinies pour les Classic Load Balancers. Pour décrire une politique prédéfinie, utilisez la describe-load-balancer-policiescommande.

- ELB -2016-08 SecurityPolicy
- ELB -TLS-1-2-2017-01 SecurityPolicy
- ELB -TLS-1-1-2017-01 SecurityPolicy
- ELB -2015-05 SecurityPolicy
- ELB -2015-03 SecurityPolicy
- ELB -2015-02 SecurityPolicy
- ELB -2014-10 SecurityPolicy
- ELB -2014-01 SecurityPolicy
- ELB -2011-08 SecurityPolicy
- ElbSample-ELB ou DefaultNegotiationPolicy ElbSample-ELB DefaultCipherPolicy
- ELBSample-OpenSSL ou ELBSample-OpenSSL DefaultNegotiationPolicy DefaultCipherPolicy

Création d'un Classic Load Balancer avec un Écouteur HTTPS

Un équilibreur de charge prend les demandes des clients et les répartit sur les instances EC2 qui sont enregistrées auprès de l'équilibreur de charge.

Vous pouvez créer un équilibreur de charge qui écoute sur les ports HTTP (80) et HTTPS (443). Si vous spécifiez que l'écouteur HTTPS envoie des demandes aux instances sur le port 80, l'équilibreur de charge met fin aux demandes et à la communication depuis l'équilibreur de charge vers les instances n'est pas chiffrée. Si l'écouteur HTTPS envoie des demandes aux instances sur le port 443, la communication depuis l'équilibreur de charge vers les instances est chiffrée.

Si votre équilibreur de charge utilise une connexion chiffrée pour communiquer avec les instances, vous pouvez éventuellement activer l'authentification des instances. Cela garantit que l'équilibreur de charge communique avec une instance uniquement si la clé publique correspond à la clé que vous avez spécifiée à équilibreur de charge à cet effet.

Pour plus d'informations sur l'ajout d'écouteurs HTTPS à un équilibreur de charge existant, consultez Configurer un Écouteur HTTPS pour votre Classic Load Balancer.

Table des matières

- Prérequis
- Créez un équilibreur de charge HTTPS/SSL à l'aide du AWS Management Console
- Créer un équilibreur de charge HTTPS/SSL à l'aide de l'interface AWS CLI

Prérequis

Avant de commencer, vérifiez que vous avez répondu aux exigences suivantes :

- Suivez les étapes de Préparation de votre VPC et de vos instances EC2.
- Lancez les instances EC2 que vous avez l'intention d'enregistrer auprès de votre équilibreur de charge. Les groupes de sécurité pour ces instances doivent autoriser le trafic à partir de l'équilibreur de charge.
- Les instances EC2 doivent répondre à la cible de la vérification de l'état avec un code d'état HTTP 200. Pour plus d’informations, consultez Configurer les vérifications de l'état pour votre Classic Load Balancer.
- Si vous avez l'intention d'activer l'option keep-alive sur vos instances EC2, nous vous recommandons de définir les paramètres keep-alive au moins sur les valeurs de délai d'inactivité

de votre équilibreur de charge. Si vous voulez vous assurer que l'équilibreur de charge est responsable de la fermeture des connexions à votre instance, vérifiez que la valeur définie sur votre instance pour le délai keep-alive est supérieure à celle du paramètre de délai d'inactivité sur votre équilibreur de charge. Pour plus d'informations, consultez Configurer le délai d'inactivité des connexions de votre Classic Load Balancer.

- Si vous créez un écouteur sécurisé, vous devez déployer un certificat de serveur SSL sur votre équilibreur de charge. L'équilibreur de charge utilise le certificat pour mettre fin à la connexion, puis déchiffrer les demandes avant de les envoyer aux instances. Si vous n'avez pas de certificat SSL, vous pouvez créer en. Pour plus d'informations, consultez Certificats SSL/TLS pour les Classic Load Balancers.

Créez un équilibreur de charge HTTPS/SSL à l'aide du AWS Management Console

Dans cet exemple, vous configurez deux écouteurs pour votre équilibreur de charge. Le premier écouteur accepte les demandes HTTP sur le port 80 et les envoie aux instances sur le port 80 à l'aide de HTTP. Le deuxième écouteur accepte les demandes HTTPS sur le port 443 et les envoie aux instances à l'aide de HTTP sur le port 80 (ou à l'aide de HTTPS sur le port 443 si vous souhaitez configurer l'authentification d'instance principale).

Un écouteur est un processus qui vérifie les demandes de connexion. Il est configuré avec un protocole et un port pour les connexions frontales (du client vers l'équilibreur de charge), et un protocole et un port pour les connexions principales (de l'équilibreur de charge vers l'instance). Pour plus d'informations sur les ports, protocoles et configurations d'Écouteur pris en charge par Elastic Load Balancing, consultez Écouteurs de votre Classic Load Balancer.

Pour créer votre Classic Load Balancer sécurisé 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 sélectionner la même Région que celle que vous avez sélectionnée pour vos instances EC2.
3. Dans le panneau de navigation, sous Load Balancing (Équilibrage de charge), choisissez Load Balancers (Équilibreurs de charge).
4. Sélectionnez Create Load Balancer (Créer un équilibreur de charge).
5. Développez la section Classic Load Balancer, puis choisissez Create.
6. Configuration de base

a. Pour Load Balancer name, saisissez un nom pour l'équilibreur de charge.

   Le nom de votre Classic Load Balancer doit être unique dans l'ensemble de vos Classic Load Balancers pour la région, ne peut contenir que 32 caractères au maximum, ne peut comporter que des caractères alphanumériques et des traits d'union, et ne doit pas commencer ou se terminer par un trait d'union.

b. Pour Scheme, sélectionnez Internet-facing.

7. Mappage du réseau

   a. Pour VPC, sélectionnez le même VPC que celui que vous avez sélectionné pour vos instances.

   b. Pour Mappings, sélectionnez d'abord une Zone de disponibilité, puis choisissez un sous-réseau public parmi ses sous-réseaux disponibles. Vous ne pouvez sélectionner qu'un seul sous-réseau par zone de disponibilité. Afin d'améliorer la disponibilité de votre équilibreur de charge, sélectionnez plusieurs zones de disponibilité et sous-réseaux.

8. Groupes de sécurité

   • Pour Security groups, sélectionnez un groupe de sécurité existant configuré pour autoriser le trafic HTTP requis sur le port 80 et le trafic HTTP sur le port 443.

     S'il n'en existe pas, vous pouvez créer un nouveau groupe de sécurité avec les règles nécessaires.

9. Écouteurs et routage

   a. Conservez les paramètres par défaut de l'écouteur par défaut, puis sélectionnez Add listener.

   b. Pour Listener sur le nouvel écouteur, sélectionnez `HTTPS` car le protocole et le port seront mis à jour vers `443`. Par défaut, Instance utilise le protocole `HTTP` sur le port `80`.

   c. Si l'authentification back end est nécessaire, modifiez le protocole d'Instance par `HTTPS`. Cela mettra également à jour le port d'Instance vers `443`

10. Paramètres de l'écouteur sécurisé

    Lorsque vous utilisez HTTPS ou SSL pour votre écouteur frontal, vous devez déployer un certificat SSL sur votre équilibreur de charge. L'équilibreur de charge utilise le certificat pour mettre fin à la connexion, puis déchiffrer les demandes des clients avant de les envoyer aux instances. Vous devez également spécifier une politique de sécurité. Elastic Load Balancing

fournit des politiques de sécurité qui ont des configurations de négociation SSL prédéfinies, mais vous pouvez également créer votre propre politique de sécurité personnalisée. Si vous avez configuré HTTPS/SSL sur la connexion principale, vous pouvez activer l'authentification de vos instances.

a. Pour la politique de sécurité, vérifiez que la stratégie est définie sur ELB SecurityPolicy -2016-08. Nous vous recommandons de toujours utiliser la stratégie de sécurité prédéfinie la plus récente ou de créer une stratégie personnalisée. Consultez Update the SSL Negotiation Configuration.

b. Pour Default SSL/TLS certificate, les options suivantes sont disponibles :

- Si vous avez créé ou importé un certificat à l'aide de AWS Certificate Manager, sélectionnez From ACM, puis sélectionnez le certificat dans Select a certificate.
- Si vous avez importé un certificat à l'aide d'IAM, sélectionnez From IAM et puis sélectionnez votre certificat dans Select a certificate.
- Si vous avez un certificat à importer mais qu'ACM n'est pas disponible dans votre région, sélectionnez Import, puis sélectionnez To IAM. Tapez le nom du certificat dans le champ Certificate name. Dans Certificate private key, copiez et collez le contenu du fichier de clé privée (codé PEM). Dans Certificate body, copiez et collez le contenu du fichier de certificat de clé publique (codé PEM). Dans Certificate Chain (Chaîne de certificats), copiez et collez le contenu du fichier de chaîne de certificats (codé PEM), sauf si vous utilisez un certificat auto-signé et qu'il n'est pas important que les navigateurs acceptent implicitement le certificat.

c. (Facultatif) Si vous avez configuré l'écouteur HTTPS pour communiquer avec des instances à l'aide d'une connexion chiffrée, vous pouvez éventuellement configurer l'authentification des instances dans Backend authentication certificate.

> **Note**
>
> Si vous ne voyez pas la section Backend authentication certificate , retournez à Listeners and routing et sélectionnez HTTPS comme protocole pour Instance.

i. Pour Certificate name, tapez le nom du certificat de clé publique.

ii. Pour Certificate Body (PEM encoded), copiez et collez le contenu du certificat. L'équilibreur de charge communique avec une instance uniquement si la clé publique correspond à cette clé.

iii. Pour ajouter un autre certificat, choisissez Add new backend certificate. La limite est de cinq.

11. Surveillance de l'état

    a. Dans la section Ping target, sélectionnez un Ping Protocol et Ping Port. Vos instances EC2 doivent accepter le trafic sur le port de ping spécifié.

    b. Pour Ping Port, assurez-vous que le port est `80`.

    c. Pour Ping Path, remplacez la valeur par défaut par une seule barre oblique, (`/`). Cela indique à Elastic Load Balancing d'envoyer les demandes de surveillance de l'état à la page d'accueil par défaut pour votre serveur web, par exemple, `index.html`.

    d. Pour Advanced health check settings, utilisez les valeurs par défaut.

12. Instances

    a. Sélectionnez Add instances pour afficher l'écran de sélection des instances.

    b. Sous Available instances, vous pouvez sélectionner parmi les instances actuellement disponibles pour l'équilibreur de charge, en fonction des paramètres réseau sélectionnés précédemment.

    c. Lorsque vous êtes satisfait de vos sélections, sélectionnez Confirm pour ajouter les instances à enregistrer dans l'équilibreur de charge.

13. Attributs

    - Pour Enable cross-zone load balancing, Enable connection draining et Timeout (draining interval) conservez les valeurs par défaut.

14. Balises d'équilibreur de charge (facultatif)

    a. Le champ Key est obligatoire.

    b. Le champ Value est facultatif.

    c. Pour ajouter une autre balise, sélectionnez Add new tag puis entrez vos valeurs dans le champ Key et éventuellement le champ Value.

    d. Pour supprimer une balise existante, sélectionner Remove en regard de la balise à supprimer.

15. Résumé et création

a. Si vous devez modifier des paramètres, sélectionnez Edit en regard du paramètre à modifier.

b. Une fois que vous êtes satisfait de tous les paramètres affichés dans le résumé, sélectionnez Create load balancer pour commencer à créer votre équilibreur de charge.

c. Sur la dernière page de création, sélectionnez View load balancer pour afficher votre équilibreur de charge dans la console Amazon EC2.

16. Vérification

a. Sélectionnez votre nouvel équilibreur de charge.

b. Sous l'onglet Target instances, vérifiez la colonne Health status. Une fois qu'au moins l'une de vos instances EC2 est en service, vous pouvez tester votre équilibreur de charge.

c. Dans la section Détails, copiez les équilibreurs de charge DNS name qui ressemblerait à `my-load-balancer-1234567890.us-east-1.elb.amazonaws.com`.

d. Collez le nom DNS de votre nouvel équilibreur de charge dans le champ d'adresse d'un navigateur web public connecté à Internet. Si votre équilibreur de charge fonctionne correctement, vous voyez la page par défaut de votre serveur.

17. Supprimer (facultatif)

a. Si vous avez un enregistrement CNAME 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.

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

c. Sélectionnez l'équilibreur de charge.

d. Sélectionnez Actions, Delete load balancer.

e. Lorsque vous êtes invité à confirmer, tapez `confirm`, puis sélectionnez Delete.

f. Une fois que vous avez supprimé un équilibreur de charge, les instances EC2 enregistrées auprès de l'équilibreur de charge continuent de s'exécuter. Vous serez facturé pour chaque heure partielle ou complète pendant laquelle elles continuent de s'exécuter. Lorsque vous n'avez plus besoin d'une instance EC2, vous pouvez l'arrêter ou la résilier pour éviter des frais supplémentaires.

Créer un équilibreur de charge HTTPS/SSL à l'aide de l'interface AWS CLI

Utilisez les instructions suivantes pour créer un équilibreur de charge à l'aide de l'interface AWS CLI

Tâches

- Étape 1 : Configurer des Écouteurs
- Étape 2 : Configurer la politique de sécurité SSL
- Étape 3 : Configurer l'authentification d'instance principale (facultatif)
- Étape 4 : Configurer des surveillances de l'état (facultatif)
- Étape 5 : Enregistrer des instances EC2
- Étape 6 : Vérifier les instances
- Étape 7 : Supprimer votre équilibreur de charge (facultatif)

Étape 1 : Configurer des Écouteurs

Un écouteur est un processus qui vérifie les demandes de connexion. Il est configuré avec un protocole et un port pour les connexions frontales (du client vers l'équilibreur de charge), et un protocole et un port pour les connexions principales (de l'équilibreur de charge vers l'instance). Pour plus d'informations sur les ports, protocoles et configurations d'Écouteur pris en charge par Elastic Load Balancing, consultez Écouteurs de votre Classic Load Balancer.

Dans cet exemple, vous configurez deux écouteurs pour votre équilibreur de charge en spécifiant les ports et les protocoles à utiliser pour les connexions frontales et principales. Le premier écouteur accepte les demandes HTTP sur le port 80 et les envoie aux instances sur le port 80 à l'aide de HTTP. Le deuxième écouteur accepte les demandes HTTPS sur le port 443 et les envoie aux instances à l'aide de HTTP sur le port 80.

Comme le deuxième écouteur utilise HTTPS pour la connexion frontale, vous devez déployer un certificat de serveur SSL sur votre équilibreur de charge. L'équilibreur de charge utilise le certificat pour mettre fin à la connexion, puis déchiffrer les demandes avant de les envoyer aux instances.

Pour configurer des écouteurs pour votre équilibreur de charge

1. Obtenez l'Amazon Resource Name (ARN) du certificat SSL. Par exemple :

   ACM

   ```
   arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
   ```

   IAM

```
arn:aws:iam::123456789012:server-certificate/my-server-certificate
```

2. Utilisez la create-load-balancercommande suivante pour configurer l'équilibreur de charge avec les deux écouteurs :

```
aws elb create-load-balancer --load-balancer-name my-load-balancer --listeners
 "Protocol=http,LoadBalancerPort=80,InstanceProtocol=http,InstancePort=80"
 "Protocol=https,LoadBalancerPort=443,InstanceProtocol=http,InstancePort=80,SSLCertificateI
 --availability-zones us-west-2a
```

Voici un exemple de réponse :

```
{
  "DNSName": "my-loadbalancer-012345678.us-west-2.elb.amazonaws.com"
}
```

3. (Facultatif) Utilisez la describe-load-balancerscommande suivante pour afficher les détails de votre équilibreur de charge :

```
aws elb describe-load-balancers --load-balancer-name my-load-balancer
```

Étape 2 : Configurer la politique de sécurité SSL

Vous pouvez sélectionner l'une des stratégies de sécurité prédéfinies, ou créer votre propre stratégie de sécurité personnalisée. Sinon, Elastic Load Balancing configure votre équilibreur de charge avec la politique de sécurité prédéfinie par défaut, `ELBSecurityPolicy-2016-08`. Nous vous recommandons d'utiliser la stratégie de sécurité par défaut. Pour plus d'informations sur les stratégies de sécurité, consultez Configurations de négociation SSL pour Classic Load Balancers.

Pour vérifier que votre équilibreur de charge est associé à la stratégie de sécurité par défaut

Utilisez la commande describe-load-balancers suivante :

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

Voici un exemple de réponse. Notez que la stratégie `ELBSecurityPolicy-2016-08` est associée à l'équilibreur de charge sur le port 443.

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 80,
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": [
                        "ELBSecurityPolicy-2016-08"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
        }
    ]
}
```

Si vous préférez, vous pouvez configurer la stratégie de sécurité SSL pour votre équilibreur de charge au lieu d'utiliser la stratégie de sécurité par défaut.

(Facultatif) Pour utiliser une politique de sécurité SSL prédéfinie

1. Utilisez la describe-load-balancer-policiescommande suivante pour répertorier les noms des politiques de sécurité prédéfinies :

```
aws elb describe-load-balancer-policies
```

Pour plus d'informations sur la configuration des stratégies de sécurité prédéfinies, consultez Politiques de sécurité SSL prédéfinies.

2. Utilisez la create-load-balancer-policycommande suivante pour créer une politique de négociation SSL à l'aide de l'une des politiques de sécurité prédéfinies que vous avez décrites à l'étape précédente :

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
--policy-name my-SSLNegotiation-policy --policy-type-name SSLNegotiationPolicyType
--policy-attributes AttributeName=Reference-Security-
Policy,AttributeValue=predefined-policy
```

3. (Facultatif) Utilisez la describe-load-balancer-policiescommande suivante pour vérifier que la politique est créée :

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --
policy-name my-SSLNegotiation-policy
```

La réponse inclut la description de la stratégie.

4. Utilisez la commande set-load-balancer-policies-of-listener suivante pour activer la politique sur le port 443 de l'équilibreur de charge :

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

> **Note**
>
> La commande `set-load-balancer-policies-of-listener` remplace l'ensemble de stratégies actuel pour le port de programme d'équilibreur de charge indiqué par l'ensemble de stratégies spécifié. La liste `--policy-names` doit inclure toutes les stratégies à activer. Si vous omettez une stratégie actuellement activée, celle-ci est désactivée.

5. (Facultatif) Utilisez la describe-load-balancerscommande suivante pour vérifier que la politique est activée :

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

Voici un exemple de réponse montrant que la stratégie est activée sur le port 443.

```
{
    "LoadBalancerDescriptions": [
        {
            ....
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 80,
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": [
                        "my-SSLNegotiation-policy"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
        }
    ]
}
```

Lorsque vous créez une stratégie de sécurité personnalisée, vous devez activer au moins un protocole et un chiffrement. Les chiffrements DSA et RSA sont spécifiques à l'algorithme de signature et sont utilisés pour créer le certificat SSL. Si vous avez déjà votre certificat SSL, veillez à activer le chiffrement qui a été utilisé pour créer ce certificat. Le nom de votre stratégie personnalisée ne doit pas commencer par `ELBSecurityPolicy-` ou `ELBSample-`, car ces préfixes sont réservés pour les noms des stratégies de sécurité prédéfinies.

(Facultatif) Pour utiliser une politique de sécurité SSL personnalisée

1. Utilisez la create-load-balancer-policycommande pour créer une politique de négociation SSL à l'aide d'une politique de sécurité personnalisée. Par exemple :

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
 --policy-name my-SSLNegotiation-policy --policy-type-name
 SSLNegotiationPolicyType
 --policy-attributes AttributeName=Protocol-TLSv1.2,AttributeValue=true
 AttributeName=Protocol-TLSv1.1,AttributeValue=true
 AttributeName=DHE-RSA-AES256-SHA256,AttributeValue=true
 AttributeName=Server-Defined-Cipher-Order,AttributeValue=true
```

2. (Facultatif) Utilisez la describe-load-balancer-policiescommande suivante pour vérifier que la politique est créée :

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --
policy-name my-SSLNegotiation-policy
```

   La réponse inclut la description de la stratégie.

3. Utilisez la commande set-load-balancer-policies-of-listener suivante pour activer la politique sur le port 443 de l'équilibreur de charge :

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

   > **Note**
   >
   > La commande `set-load-balancer-policies-of-listener` remplace l'ensemble de stratégies actuel pour le port de programme d'équilibreur de charge indiqué par l'ensemble de stratégies spécifié. La liste `--policy-names` doit inclure toutes les stratégies à activer. Si vous omettez une stratégie actuellement activée, celle-ci est désactivée.

4. (Facultatif) Utilisez la describe-load-balancerscommande suivante pour vérifier que la politique est activée :

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

Voici un exemple de réponse montrant que la stratégie est activée sur le port 443.

```
{
    "LoadBalancerDescriptions": [
        {
            ....
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 80,
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": [
                        "my-SSLNegotiation-policy"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
        }
    ]
}
```

Étape 3 : Configurer l'authentification d'instance principale (facultatif)

Si vous configurez HTTPS/SSL sur la connexion principale, vous pouvez éventuellement configurer l'authentification de vos instances.

Lorsque vous configurez l'authentification d'instance principale, vous créez une stratégie de clé publique. Ensuite, vous utilisez cette stratégie de clé publique pour créer une stratégie

d'authentification d'instance principale. Enfin, vous définissez la stratégie d'authentification d'instance principale avec le port de l'instance pour le protocole HTTPS.

L'équilibreur de charge communique avec une instance uniquement si la clé publique que l'instance présente à l'équilibreur de charge correspond à une clé publique de la stratégie d'authentification pour votre équilibreur de charge.

Pour configurer l'authentification d'instance principale

1. Utilisez la commande suivante pour extraire la clé publique :

```
openssl x509 -in your X509 certificate PublicKey -pubkey -noout
```

2. Utilisez la create-load-balancer-policycommande suivante pour créer une politique de clé publique :

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer --policy-
name my-PublicKey-policy \
--policy-type-name PublicKeyPolicyType --policy-attributes
 AttributeName=PublicKey,AttributeValue=MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w
 0BAQUFADCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZ
 WF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIw
 EAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5
 jb20wHhcNMTEwNDI1MjA0NTIxWhcNMTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBh
 MCVVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBb
 WF6b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMx
 HzAdBgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wgZ8wDQYJKoZIhvcNAQE
 BBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ21uUSfwfEvySWtC2XADZ4nB+BLYgVI
 k60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9TrDHudUZg3qX4waLG5M43q7Wgc/MbQ
 ITxOUSQv7c7ugFFDzQGBzZswY6786m86gpEIbb3OhjZnzcvQAaRHhdlQWIMm2nr
 AgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4nUhVVxYUntneD9+h8Mg9q6q+auN
 KyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0FkbFFBjvSfpJIlJ00zbhNYS5f6Guo
 EDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTbNYiytVbZPQUQ5Yaxu2jXnimvw
 3rrszlaEXAMPLE=
```

> **Note**
>
> Pour spécifier une valeur de clé publique pour `--policy-attributes`, supprimez les première et dernière lignes de la clé publique (la ligne contenant « `-----BEGIN`

PUBLIC KEY----- » et la ligne contenant « -----END PUBLIC KEY----- »). Les espaces blancs AWS CLI ne sont pas autorisés dans--policy-attributes.

3. Utilisez la create-load-balancer-policycommande suivante pour créer une politique d'authentification d'instance principale à l'aide my-PublicKey-policy de.

```
aws elb create-load-balancer-policy --load-balancer-name my-
loadbalancer --policy-name my-authentication-policy --policy-type-
name BackendServerAuthenticationPolicyType --policy-attributes
 AttributeName=PublicKeyPolicyName,AttributeValue=my-PublicKey-policy
```

Vous pouvez éventuellement utiliser plusieurs stratégies de clé publique. L'équilibreur de charge essaie toutes les clés, une par une. Si la clé publique présentée par une instance correspond à l'une de ces clés publiques, l'instance est authentifiée.

4. Utilisez la for-backend-server commande set-load-balancer-policies- suivante pour my-authentication-policy définir le port d'instance pour HTTPS. Dans cet exemple, le port d'instance est le port 443.

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-
loadbalancer --instance-port 443 --policy-names my-authentication-policy
```

5. (Facultatif) Utilisez la describe-load-balancer-policiescommande suivante pour répertorier toutes les politiques de votre équilibreur de charge :

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer
```

6. (Facultatif) Utilisez la describe-load-balancer-policiescommande suivante pour afficher les détails de la politique :

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --
policy-names my-authentication-policy
```

Étape 4 : Configurer des surveillances de l'état (facultatif)

Elastic Load Balancing vérifie régulièrement l'état de santé de chaque instance EC2 enregistrée en fonction des vérifications de l'état que vous avez configurées. Si Elastic Load Balancing trouve une instance défectueuse, il arrête de lui envoyer du trafic et achemine le trafic vers les instances

saines. Pour plus d'informations, consultez Configurer les vérifications de l'état pour votre Classic Load Balancer.

Lorsque vous créez votre équilibreur de charge, Elastic Load Balancing utilise les paramètres par défaut pour les surveillances de l'état. Si vous préférez, vous pouvez modifier la configuration de vérification de l'état de votre équilibreur de charge au lieu d'utiliser les paramètres par défaut.

Pour configurer les vérifications de l'état pour vos instances

Utilisez la commande configure-health-check suivante :

```
aws elb configure-health-check --load-balancer-name my-loadbalancer --health-check
 Target=HTTP:80/ping,Interval=30,UnhealthyThreshold=2,HealthyThreshold=2,Timeout=3
```

Voici un exemple de réponse :

```
{
    "HealthCheck": {
        "HealthyThreshold": 2,
        "Interval": 30,
        "Target": "HTTP:80/ping",
        "Timeout": 3,
        "UnhealthyThreshold": 2
    }
}
```

Étape 5 : Enregistrer des instances EC2

Une fois que vous avez créé votre équilibreur de charge, vous devez enregistrez vos instances EC2 après de celui-ci. Vous pouvez sélectionner des instances EC2 d'une ou de plusieurs zones de disponibilité au sein de la même Région que l'équilibreur de charge. Pour plus d'informations, consultez Instances enregistrées pour votre Classic Load Balancer.

Utilisez la commande register-instances-with-load-balancer comme suit :

```
aws elb register-instances-with-load-balancer --load-balancer-name my-loadbalancer --
instances i-4f8cf126 i-0bb7ca62
```

Voici un exemple de réponse :

```
{
    "Instances": [
```

```
        {
            "InstanceId": "i-4f8cf126"
        },
        {
            "InstanceId": "i-0bb7ca62"
        }
    ]
}
```

Étape 6 : Vérifier les instances

Votre équilibreur de charge est utilisable dès que l'une de vos instances enregistrées est à l'état `InService`.

Pour vérifier l'état de vos instances EC2 nouvellement enregistrées, utilisez la describe-instance-healthcommande suivante :

```
aws elb describe-instance-health  --load-balancer-name my-loadbalancer --
instances i-4f8cf126 i-0bb7ca62
```

Voici un exemple de réponse :

```
{
    "InstanceStates": [
        {
            "InstanceId": "i-4f8cf126",
            "ReasonCode": "N/A",
            "State": "InService",
            "Description": "N/A"
        },
        {
            "InstanceId": "i-0bb7ca62",
            "ReasonCode": "Instance",
            "State": "OutOfService",
            "Description": "Instance registration is still in progress"
        }
    ]
}
```

Si le champ `State` pour une instance est `OutOfService`, c'est probablement parce que vos instances sont encore en cours d'enregistrement. Pour plus d'informations, consultez Résoudre les problèmes liés à un Classic Load Balancer : enregistrement d'instance.

Une fois que l'état d'au moins une de vos instances est `InService`, vous pouvez tester votre équilibreur de charge. Pour tester votre équilibreur de charge, copiez son nom DNS et collez-le dans le champ d'adresse d'un navigateur web connecté à Internet. Si votre équilibreur de charge fonctionne, vous voyez la page par défaut de votre serveur HTTP.

Étape 7 : Supprimer votre équilibreur de charge (facultatif)

La suppression d'un l'équilibreur de charge annule automatiquement l'enregistrement de ses instances EC2 associées. Dès que l'équilibreur de charge est supprimé, vous cessez d'être facturé pour cet équilibreur de charge. Toutefois, les instances EC2 continuent de s'exécuter et vous continuez à payer de frais.

Pour supprimer votre équilibreur de charge, utilisez la delete-load-balancercommande suivante :

```
aws elb delete-load-balancer --load-balancer-name my-loadbalancer
```

Pour arrêter vos instances EC2, utilisez la commande stop-instances. Pour mettre fin à vos instances EC2 (les résilier), utilisez la commande terminate-instances.

Configurer un Écouteur HTTPS pour votre Classic Load Balancer

Un écouteur est un processus qui vérifie les demandes de connexion. Il est configuré avec un protocole et un port pour les connexions frontales (du client vers l'équilibreur de charge), et un protocole et un port pour les connexions principales (de l'équilibreur de charge vers l'instance). Pour plus d'informations sur les ports, protocoles et configurations d'Écouteur pris en charge par Elastic Load Balancing, consultez Écouteurs de votre Classic Load Balancer.

Si vous disposez d'un équilibreur de charge avec un écouteur qui accepte les demandes HTTP sur le port 80, vous pouvez ajouter un écouteur qui accepte les demandes HTTPS sur le port 443. Si vous spécifiez que l'écouteur HTTPS envoie des demandes aux instances sur le port 80, l'équilibreur de charge met fin aux demandes SSL et à la communication depuis l'équilibreur de charge vers les instances non chiffrées. Si l'écouteur HTTPS envoie des demandes aux instances sur le port 443, la communication depuis l'équilibreur de charge vers les instances est chiffrée.

Si votre équilibreur de charge utilise une connexion chiffrée pour communiquer avec des instances, vous pouvez éventuellement activer l'authentification des instances. Cela garantit que l'équilibreur de charge communique avec une instance uniquement si la clé publique correspond à la clé que vous avez spécifiée à équilibreur de charge à cet effet.

Pour plus d'informations sur la création d'un nouvel écouteur HTTPS, consultez Création d'un Classic Load Balancer avec un Écouteur HTTPS.

Table des matières

- Prérequis
- Ajouter un Écouteur HTTPS à l'aide de la console
- Ajoutez un écouteur HTTPS à l'aide du AWS CLI

Prérequis

Pour activer la prise en charge de HTTPS pour un écouteur HTTPS, vous devez déployer un certificat de serveur SSL sur votre équilibreur de charge. L'équilibreur de charge utilise le certificat pour mettre fin à la connexion, puis déchiffrer les demandes avant de les envoyer aux instances. Si vous n'avez pas de certificat SSL, vous pouvez créer en. Pour plus d'informations, consultez Certificats SSL/TLS pour les Classic Load Balancers.

Ajouter un Écouteur HTTPS à l'aide de la console

Vous pouvez ajouter un écouteur HTTPS à un équilibreur de charge existant.

Pour ajouter un écouteur HTTPS à 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 panneau de navigation, sous Load Balancing (Équilibrage de charge), choisissez Load Balancers (Équilibreurs de charge).
3. Choisissez le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Sous l'onglet Listeners, choisissez Manage listeners.
5. Sur la page Manage listeners, dans la section Listeners, choisissez Add listener.
6. Pour Listener protocol, sélectionner HTTPS.

> **Important**
>
> Par défaut, le protocole d'instance est HTTP. Si vous souhaitez configurer l'authentification d'instance principale, modifiez le protocole d'instance en HTTPS.

7. Pour la politique de sécurité, la valeur par défaut recommandée ELB SecurityPolicy -2016-08 sera sélectionnée. Nous vous recommandons de toujours utiliser la stratégie de sécurité

prédéfinie la plus récente. Si vous devez utiliser une autre stratégie de sécurité prédéfinie ou créer une stratégie personnalisée, consultez Mettre à jour la configuration de négociation SSL.

8. Pour Default SSL cert, choisissez Edit, puis exécutez l'une des actions suivantes :

   - Si vous avez créé ou importé un certificat à l'aide de AWS Certificate Manager, choisissez From ACM, sélectionnez le certificat dans la liste, puis sélectionnez Enregistrer les modifications.

     > **Note**
     >
     > Cette option est disponible uniquement dans les Régions qui prennent en charge AWS Certificate Manager.

   - Si vous avez importé un certificat à l'aide d'IAM, choisissez From IAM, sélectionnez le certificat dans la liste, puis choisissez Save changes.
   - Si vous avez un certificat SSL à importer dans ACM, sélectionnez Import et To ACM. Dans Certificate private key, copiez et collez le contenu du fichier de clé privée codé PEM. Dans Certificate body, copiez et collez le contenu du fichier de certificat de clé publique codé PEM. Dans Certificate chain - optional, copiez et collez le contenu du fichier de chaîne de certificat codé PEM, sauf si vous utilisez un certificat auto-signé et qu'il n'est pas important que les navigateurs acceptent implicitement le certificat.
   - Si vous avez un certificat SSL à importer, mais qu'ACM n'est pas pris en charge dans cette région, sélectionnez Import et To IAM. Dans Certificate name, tapez le nom du certificat. Dans Certificate private key, copiez et collez le contenu du fichier de clé privée codé PEM. Dans Certificate body, copiez et collez le contenu du fichier de certificat de clé publique codé PEM. Dans Certificate chain - optional, copiez et collez le contenu du fichier de chaîne de certificat codé PEM, sauf si vous utilisez un certificat auto-signé et qu'il n'est pas important que les navigateurs acceptent implicitement le certificat.
   - Sélectionnez Enregistrer les modifications.

9. Pour Cookie stickiness, la valeur par défaut est Disabled. Pour modifier cela, choisissez Edit. Si vous choisissez Generated by load balancer, une Période d'expiration doit être spécifié. Si vous choisissez Generated by application, un Nom du cookie doit être spécifié. Après avoir fait votre sélection, choisissez Save changes.
10. (Facultatif) Choisissez Add listener pour ajouter des écouteurs supplémentaires.
11. Choisissez Save changes pour ajouter les écouteurs que vous venez de configurer.

12. (Facultatif) Pour configurer l'authentification des instances principales pour un équilibreur de charge existant, vous devez utiliser l'API AWS CLI ou une API, car cette tâche n'est pas prise en charge par la console. Pour plus d'informations, consultez Configurer l'authentification d'instance principale.

Ajoutez un écouteur HTTPS à l'aide du AWS CLI

Vous pouvez ajouter un écouteur HTTPS à un équilibreur de charge existant.

Pour ajouter un écouteur HTTPS à votre équilibreur de charge à l'aide du AWS CLI

1. Obtenez l'Amazon Resource Name (ARN) du certificat SSL. Par exemple :

   ACM

   ```
   arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
   ```

   IAM

   ```
   arn:aws:iam::123456789012:server-certificate/my-server-certificate
   ```

2. Utilisez la create-load-balancer-listenerscommande suivante pour ajouter un écouteur à votre équilibreur de charge qui accepte les requêtes HTTPS sur le port 443 et envoie les demandes aux instances sur le port 80 via HTTP :

   ```
   aws elb create-load-balancer-listeners --load-balancer-name my-load-balancer --
   listeners
    Protocol=HTTPS,LoadBalancerPort=443,InstanceProtocol=HTTP,InstancePort=80,SSLCertificateId
   ```

   Si vous souhaitez configurer l'authentification d'instance principale, utilisez la commande suivante pour ajouter un écouteur qui accepte les demandes HTTPS sur le port 443 et envoie les demandes aux instances sur le port 443 à l'aide de HTTPS :

   ```
   aws elb create-load-balancer-listeners --load-balancer-name my-load-balancer --
   listeners
    Protocol=HTTPS,LoadBalancerPort=443,InstanceProtocol=HTTPS,InstancePort=443,SSLCertificate
   ```

3. (Facultatif) Vous pouvez utiliser la describe-load-balancerscommande suivante pour afficher les détails mis à jour de votre équilibreur de charge :

```
aws elb describe-load-balancers --load-balancer-name my-load-balancer
```

Voici un exemple de réponse :

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 80,
                        "SSLCertificateId": "ARN",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": [
                        "ELBSecurityPolicy-2016-08"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "HTTP",
                        "InstanceProtocol": "HTTP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
        }
    ]
}
```

4. (Facultatif) Votre écouteur HTTPS a été créé à l'aide de la stratégie de sécurité par défaut. Si vous souhaitez définir une autre politique de sécurité prédéfinie ou une politique de sécurité personnalisée, utilisez les commandes create-load-balancer-policyet set-load-balancer-policies-of-listener. Pour plus d'informations, consultez Mettez à jour la configuration de négociation SSL à l'aide du AWS CLI.

5. (Facultatif) Pour configurer l'authentification des instances principales, utilisez la for-backend-server commande set-load-balancer-policies-. Pour plus d'informations, consultez Configurer l'authentification d'instance principale.

Remplacer le certificat SSL pour votre Classic Load Balancer

Si vous avez un écouteur HTTPS, vous avez déployé un certificat de serveur SSL sur votre équilibreur de charge lorsque vous avez créé l'écouteur. Chaque certificat est associé à une durée de validité. Vous devez veiller à renouveler ou remplacer le certificat avant la fin de la période de validité.

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. Une fois qu'un certificat déployé sur un équilibreur de charge est renouvelé, les nouvelles demandes utilisent le certificat renouvelé.

Pour remplacer un certificat, vous devez d'abord créer un nouveau certificat en suivant les mêmes étapes que celles que vous avez utilisées lorsque vous avez créé le certificat actuel. Vous pouvez ensuite remplacer le certificat. Une fois qu'un certificat déployé sur un équilibreur de charge est remplacé, les nouvelles demandes utilisent le nouveau certificat.

Notez que le renouvellement d'un certificat n'affecte pas les demandes déjà reçues par un nœud d'équilibreur de charge et qui sont en attente d'acheminement vers une cible saine.

Table des matières

- Remplacer le certificat SSL à l'aide de la console
- Remplacer le certificat SSL à l'aide de l'interface AWS CLI

Remplacer le certificat SSL à l'aide de la console

Vous pouvez remplacer le certificat déployé sur votre équilibreur de charge par un certificat fourni par ACM ou un certificat chargé sur IAM.

Pour remplacer le certificat SSL d'un équilibreur de charge HTTPS 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 le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Sous l'onglet Listeners, choisissez Manage listeners.
5. Sur la page Manage listeners, localisez l'écouteur à mettre à jour, choisissez Edit sous Default SSL cert et effectuez l'une des opérations suivantes :

   - Si vous avez créé ou importé un certificat à l'aide de AWS Certificate Manager, choisissez From ACM, sélectionnez le certificat dans la liste, puis sélectionnez Enregistrer les modifications.

     > **Note**
     >
     > Cette option est disponible uniquement dans les Régions qui prennent en charge AWS Certificate Manager.

   - Si vous avez importé un certificat à l'aide d'IAM, choisissez From IAM, sélectionnez le certificat dans la liste, puis choisissez Save changes.
   - Si vous avez un certificat SSL à importer dans ACM, sélectionnez Import et To ACM. Dans Certificate private key, copiez et collez le contenu du fichier de clé privée codé PEM. Dans Certificate body, copiez et collez le contenu du fichier de certificat de clé publique codé PEM. Dans Certificate chain - optional, copiez et collez le contenu du fichier de chaîne de certificat codé PEM, sauf si vous utilisez un certificat auto-signé et qu'il n'est pas important que les navigateurs acceptent implicitement le certificat.
   - Si vous avez un certificat SSL à importer, mais qu'ACM n'est pas pris en charge dans cette région, sélectionnez Import et To IAM. Dans Certificate name, tapez le nom du certificat. Dans Certificate private key, copiez et collez le contenu du fichier de clé privée codé PEM. Dans Certificate body, copiez et collez le contenu du fichier de certificat de clé publique codé PEM. Dans Certificate chain - optional, copiez et collez le contenu du fichier de chaîne de certificat codé PEM, sauf si vous utilisez un certificat auto-signé et qu'il n'est pas important que les navigateurs acceptent implicitement le certificat.
   - Sélectionnez Enregistrer les modifications.

Remplacer le certificat SSL à l'aide de l'interface AWS CLI

Vous pouvez remplacer le certificat déployé sur votre équilibreur de charge par un certificat fourni par ACM ou un certificat chargé sur IAM.

Pour remplacer un certificat SSL par un certificat fourni par ACM

1. Utilisez la commande request-certificate suivante pour demander un nouveau certificat :

```
aws acm request-certificate --domain-name www.example.com
```

2. Utilisez la commande set-load-balancer-listener-ssl-certificate suivante pour définir le certificat :

```
aws elb set-load-balancer-listener-ssl-certificate --load-balancer-
name my-load-balancer --load-balancer-port 443 --ssl-certificate-id
 arn:aws:acm:region:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

Pour remplacer un certificat SSL par un certificat chargé dans IAM

1. Si vous avez un certificat SSL mais que vous ne l'avez pas chargé, consultez Chargement d'un certificat de serveur dans le Guide de l'utilisateur IAM.
2. Utilisez la get-server-certificatecommande suivante pour obtenir l'ARN du certificat :

```
aws iam get-server-certificate --server-certificate-name my-new-certificate
```

3. Utilisez la commande set-load-balancer-listener-ssl-certificate suivante pour définir le certificat :

```
aws elb set-load-balancer-listener-ssl-certificate --load-balancer-
name my-load-balancer --load-balancer-port 443 --ssl-certificate-id
 arn:aws:iam::123456789012:server-certificate/my-new-certificate
```

Mettre à jour la configuration de négociation SSL de votre Classic Load Balancer

Elastic Load Balancing fournit des politiques de sécurité qui ont des configurations de négociation SSL prédéfinies à utiliser pour négocier des connexions SSL entre les clients et votre équilibreur de

charge. Si vous utilisez le protocole HTTPS/SSL pour votre écouteur, vous pouvez utiliser l'une des stratégies de sécurité prédéfinies ou votre propre stratégie de sécurité personnalisée.

Pour plus d'informations sur les stratégies de sécurité, consultez Configurations de négociation SSL pour Classic Load Balancers. Pour plus d'informations sur les configurations des politiques de sécurité fournies par Elastic Load Balancing, consultez Politiques de sécurité SSL prédéfinies.

Si vous créez un Écouteur HTTPS/SSL sans associer une politique de sécurité, Elastic Load Balancing associe la politique de sécurité prédéfinie par défaut, `ELBSecurityPolicy-2016-08`, à votre équilibreur de charge.

Si vous possédez déjà un équilibreur de charge avec une configuration de négociation SSL qui n'utilise pas les derniers protocoles et chiffrements, nous vous recommandons de mettre à jour votre équilibreur de charge pour utiliser ELB -2016-08. SecurityPolicy Si vous préférez, vous pouvez créer une configuration personnalisée. Nous vous recommandons vivement de tester les nouvelles stratégies de sécurité avant de mettre à niveau la configuration de votre équilibreur de charge.

Les exemples suivants vous montrent comment mettre à jour la configuration de négociation SSL pour un écouteur HTTPS/SSL. Notez que la modification n'affecte pas les demandes reçues par un nœud d'équilibreur de charge et qui sont en attente de routage vers une instance saine ; la configuration mise à jour sera utilisée avec les nouvelles demandes reçues.

Table des matières

- Mettre à jour la configuration de négociation SSL à l'aide de la console
- Mettez à jour la configuration de négociation SSL à l'aide du AWS CLI

Mettre à jour la configuration de négociation SSL à l'aide de la console

Par défaut, Elastic Load Balancing associe la dernière politique prédéfinie à votre équilibreur de charge. Lorsqu'une nouvelle stratégie prédéfinie est ajoutée, nous vous recommandons de mettre à jour votre équilibreur de charge pour utiliser la nouvelle stratégie prédéfinie. Vous pouvez également sélectionner une autre stratégie de sécurité prédéfinie ou créer une stratégie personnalisée.

Pour mettre à jour la configuration de négociation SSL pour un équilibreur de charge HTTPS/SSL 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 le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Sous l'onglet Listeners, choisissez Manage listeners.
5. Sur la page Manage listeners, localisez l'écouteur à mettre à jour, choisissez Edit sous Security policy sélectionnez une stratégie de sécurité à l'aide de l'une des options suivantes :
   - (Recommandé) Conservez la politique par défaut, ELB SecurityPolicy -2016-08, puis choisissez Enregistrer les modifications.
   - Sélectionnez une stratégie prédéfinie autre que celle par défaut, puis choisissez Save changes.
   - Sélectionnez Custom et activez au moins un protocole et un chiffrement comme suit :
     a. Pour SSL Protocols, sélectionnez un ou plusieurs protocoles à activer.
     b. Pour SSL Options, sélectionnez Server Order Preference afin d'utiliser l'ordre indiqué dans le tableau Politiques de sécurité SSL prédéfinies pour la négociation SSL.
     c. Pour SSL Ciphers, sélectionnez un ou plusieurs chiffrements à activer. Si vous avez déjà un certificat SSL, vous devez activer le chiffrement qui a été utilisé pour créer le certificat, car les chiffrements DSA et RSA sont spécifiques à l'algorithme de signature.
     d. Sélectionnez Enregistrer les modifications.

Mettez à jour la configuration de négociation SSL à l'aide du AWS CLI

Vous pouvez utiliser la stratégie de sécurité prédéfinie par défaut, `ELBSecurityPolicy-2016-08`, une autre stratégie de sécurité prédéfinie ou une stratégie de sécurité personnalisée.

Pour utiliser une stratégie de sécurité SSL prédéfinie

1. Utilisez la describe-load-balancer-policiescommande suivante pour répertorier les politiques de sécurité prédéfinies fournies par Elastic Load Balancing. La syntaxe que vous utilisez dépend du système d'exploitation et du shell que vous utilisez.

   Linux

   ```
   aws elb describe-load-balancer-policies --query 'PolicyDescriptions[?
   PolicyTypeName==`SSLNegotiationPolicyType`].{PolicyName:PolicyName}' --output table
   ```

   Windows

```
aws elb describe-load-balancer-policies --query "PolicyDescriptions[?
PolicyTypeName==`SSLNegotiationPolicyType`].{PolicyName:PolicyName}" --output table
```

Voici un exemple de sortie :

```
-----------------------------------------
|      DescribeLoadBalancerPolicies      |
+----------------------------------------+
|               PolicyName               |
+----------------------------------------+
|  ELBSecurityPolicy-2016-08             |
|  ELBSecurityPolicy-TLS-1-2-2017-01     |
|  ELBSecurityPolicy-TLS-1-1-2017-01     |
|  ELBSecurityPolicy-2015-05             |
|  ELBSecurityPolicy-2015-03             |
|  ELBSecurityPolicy-2015-02             |
|  ELBSecurityPolicy-2014-10             |
|  ELBSecurityPolicy-2014-01             |
|  ELBSecurityPolicy-2011-08             |
|  ELBSample-ELBDefaultCipherPolicy      |
|  ELBSample-OpenSSLDefaultCipherPolicy  |
+----------------------------------------+
```

Pour déterminer quels chiffrements sont activés pour une stratégie, utilisez la commande suivante :

```
aws elb describe-load-balancer-policies --policy-names ELBSecurityPolicy-2016-08 --
output table
```

Pour plus d'informations sur la configuration des stratégies de sécurité prédéfinies, consultez Politiques de sécurité SSL prédéfinies.

2. Utilisez la create-load-balancer-policycommande pour créer une politique de négociation SSL à l'aide de l'une des politiques de sécurité prédéfinies décrites à l'étape précédente. Par exemple, la commande suivante utilise la stratégie de sécurité prédéfinie par défaut :

```
aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
--policy-name my-SSLNegotiation-policy  --policy-type-name SSLNegotiationPolicyType
--policy-attributes AttributeName=Reference-Security-
Policy,AttributeValue=ELBSecurityPolicy-2016-08
```

Si vous dépassez la limite du nombre de politiques pour l'équilibreur de charge, utilisez la delete-load-balancer-policycommande pour supprimer les politiques non utilisées.

3. (Facultatif) Utilisez la describe-load-balancer-policiescommande suivante pour vérifier que la politique est créée :

```
aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --
policy-name my-SSLNegotiation-policy
```

La réponse inclut la description de la stratégie.

4. Utilisez la commande set-load-balancer-policies-of-listener suivante pour activer la politique sur le port 443 de l'équilibreur de charge :

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

> **Note**
>
> La commande `set-load-balancer-policies-of-listener` remplace l'ensemble de stratégies actuel pour le port de programme d'équilibreur de charge indiqué par l'ensemble de stratégies spécifié. La liste `--policy-names` doit inclure toutes les stratégies à activer. Si vous omettez une stratégie actuellement activée, celle-ci est désactivée.

5. (Facultatif) Utilisez la describe-load-balancerscommande suivante pour vérifier que la nouvelle politique est activée pour le port de l'équilibreur de charge :

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

La réponse montre que la stratégie est activée sur le port 443.

```
...
  {
      "Listener": {
          "InstancePort": 443,
          "SSLCertificateId": "ARN",
          "LoadBalancerPort": 443,
          "Protocol": "HTTPS",
```

```
            "InstanceProtocol": "HTTPS"
        },
        "PolicyNames": [
            "my-SSLNegotiation-policy"
        ]
    }
...
```

Lorsque vous créez une stratégie de sécurité personnalisée, vous devez activer au moins un protocole et un chiffrement. Les chiffrements DSA et RSA sont spécifiques à l'algorithme de signature et sont utilisés pour créer le certificat SSL. Si vous avez déjà un certificat SSL, veillez à activer le chiffrement qui a été utilisé pour créer le certificat. Le nom de votre stratégie personnalisée ne doit pas commencer par `ELBSecurityPolicy-` ou `ELBSample-`, car ces préfixes sont réservés pour les noms des stratégies de sécurité prédéfinies.

Pour utiliser une stratégie de sécurité SSL personnalisée

1. Utilisez la create-load-balancer-policycommande pour créer une politique de négociation SSL à l'aide d'une politique de sécurité personnalisée. Par exemple :

   ```
   aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer
    --policy-name my-SSLNegotiation-policy --policy-type-name
    SSLNegotiationPolicyType
    --policy-attributes AttributeName=Protocol-TLSv1.2,AttributeValue=true
    AttributeName=Protocol-TLSv1.1,AttributeValue=true
    AttributeName=DHE-RSA-AES256-SHA256,AttributeValue=true
    AttributeName=Server-Defined-Cipher-Order,AttributeValue=true
   ```

   Si vous dépassez la limite du nombre de politiques pour l'équilibreur de charge, utilisez la delete-load-balancer-policycommande pour supprimer les politiques non utilisées.

2. (Facultatif) Utilisez la describe-load-balancer-policiescommande suivante pour vérifier que la politique est créée :

   ```
   aws elb describe-load-balancer-policies --load-balancer-name my-loadbalancer --
   policy-name my-SSLNegotiation-policy
   ```

   La réponse inclut la description de la stratégie.

3. Utilisez la commande set-load-balancer-policies-of-listener suivante pour activer la politique sur le port 443 de l'équilibreur de charge :

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-SSLNegotiation-policy
```

> **Note**
>
> La commande `set-load-balancer-policies-of-listener` remplace l'ensemble de stratégies actuel pour le port de programme d'équilibreur de charge indiqué par l'ensemble de stratégies spécifié. La liste `--policy-names` doit inclure toutes les stratégies à activer. Si vous omettez une stratégie actuellement activée, celle-ci est désactivée.

4. (Facultatif) Utilisez la describe-load-balancerscommande suivante pour vérifier que la nouvelle politique est activée pour le port de l'équilibreur de charge :

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

La réponse montre que la stratégie est activée sur le port 443.

```
...
  {
      "Listener": {
          "InstancePort": 443,
          "SSLCertificateId": "ARN",
          "LoadBalancerPort": 443,
          "Protocol": "HTTPS",
          "InstanceProtocol": "HTTPS"
      },
      "PolicyNames": [
          "my-SSLNegotiation-policy"
      ]
  }
...
```

Configurer votre Classic Load Balancer

Table des matières

- Configurer le délai d'inactivité des connexions de votre Classic Load Balancer
- Configurer la répartition de charge entre zones pour votre Classic Load Balancer
- Configurer le drainage de la connexion pour votre Classic Load Balancer
- Configurer la prise en charge du protocole proxy pour votre Classic Load Balancer
- Configurer des sessions permanentes pour votre Classic Load Balancer
- Configurer le mode d'atténuation de désynchronisation pour votre Classic Load Balancer
- Baliser votre Classic Load Balancer
- Configurer un nom de domaine personnalisé pour votre Classic Load Balancer

Configurer le délai d'inactivité des connexions de votre Classic Load Balancer

Pour chaque demande effectuée par un client via un Classic Load Balancer, l'équilibreur de charge gère deux connexions. La connexion frontale est placée entre le client et l'équilibreur de charge. La connexion principale est placée entre l'équilibreur de charge et une instance EC2 enregistrée. L'équilibreur de charge dispose d'un délai d'inactivité configuré qui s'applique à ses connexions. Si aucune donnée n'a été envoyée ou reçue avant que la période d'inactivité soit écoulée, l'équilibreur de charge ferme la connexion. Pour vous assurer que opérations longues comme les chargements de fichiers ont le temps de se terminer, envoyez au moins 1 octet de données avant la fin de chaque période d'inactivité, et augmentez la durée du délai d'inactivité si nécessaire.

Si vous utilisez les écouteurs HTTP et HTTPS, nous vous recommandons d'activer l'option HTTP keep-alive pour vos instances. Vous pouvez activer keep-alive dans les paramètres de serveur Web pour vos instances Keep-alive, lorsqu'il est activé, permet à l'équilibreur de charge de réutiliser les connexions principales jusqu'à ce que le délai d'expiration Keep-alive expire. Pour vous assurer que l'équilibreur de charge est responsable de la fermeture des connexions à votre instance, vérifiez que la valeur que vous définissez pour le délai HTTP keep-alive est supérieure à celle du paramètre de délai d'inactivité sur votre équilibreur de charge.

Notez que les sondes TCP keep-alive n'empêchent pas l'équilibreur de charge de mettre fin à la connexion, car elles n'envoient pas des données dans la charge utile.

Table des matières

- Configurer le délai d'inactivité à l'aide de la console
- Configurer le délai d'inactivité à l'aide de l'interface AWS CLI

Configurer le délai d'inactivité à l'aide de la console

Par défaut, Elastic Load Balancing définit le délai d'inactivité de votre équilibreur de charge à 60 secondes. Utilisez la procédure suivante pour définir une valeur de délai d'inactivité différente.

Pour configurer le paramètre de délai d'inactivité de 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 panneau de navigation, sous Load Balancing (Équilibrage de charge), 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 Attributes, choisissez Edit.
5. Sur la page Edit load balancer attributes, dans la section Traffic configuration, tapez une valeur pour Idle timeout. La plage pour le délai d'inactivité est de 1 à 4 000 secondes.
6. Sélectionnez Enregistrer les modifications.

Configurer le délai d'inactivité à l'aide de l'interface AWS CLI

Utilisez la modify-load-balancer-attributescommande suivante pour définir le délai d'inactivité de votre équilibreur de charge :

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes "{\"ConnectionSettings\":{\"IdleTimeout\":30}}"
```

Voici un exemple de réponse :

```
{
    "LoadBalancerAttributes": {
        "ConnectionSettings": {
            "IdleTimeout": 30
        }
    },
```

```
    "LoadBalancerName": "my-loadbalancer"
}
```

Configurer la répartition de charge entre zones pour votre Classic Load Balancer

Avec l'équilibrage de charge entre zones, chaque nœud de l'équilibreur de charge pour votre Classic Load Balancer répartit les demandes uniformément entre les instances enregistrées dans toutes les zones de disponibilité activées. Si l'équilibrage de charge entre zones est désactivé, chaque nœud de l'équilibreur de charge répartit les demandes uniformément entre les instances enregistrées dans sa zone de disponibilité uniquement. Pour de plus amples informations, consultez Répartition de charge entre zones dans le Guide de l'utilisateur Elastic Load Balancing.

L'équilibrage de charge entre zones réduit la nécessité de maintenir un nombre équivalent d'instances dans chaque zone de disponibilité activée et améliore la capacité de votre application à gérer la perte d'une ou plusieurs instances. Cependant, nous vous recommandons de conserver des nombres approximativement équivalents d'instances dans chaque zone de disponibilité activée pour une tolérance aux pannes accrue.

Pour les environnements où les clients mettent en cache les recherches DNS, des demandes entrantes peuvent favoriser une des zones de disponibilité. Avec la répartition de charge entre zones, ce déséquilibre dans la charge de demandes est réparti entre toutes les instances disponibles dans la Région, ce qui réduit l'impact du comportement anormal de clients.

Lorsque vous créez un Classic Load Balancer, les valeurs par défaut pour la répartition de charge entre zones dépend de la manière dont vous créez l'équilibreur de charge. Avec l'API ou l'interface de ligne de commande, l'équilibrage de charge entre zones est désactivé par défaut. Avec le AWS Management Console, l'option permettant d'activer l'équilibrage de charge entre zones est sélectionnée par défaut. Après avoir créé un Classic Load Balancer, vous pouvez activer ou désactiver la répartition de charge entre zones à tout moment.

Table des matières

- Activer la répartition de charge entre zones
- Désactiver la répartition de charge entre zones

Activer la répartition de charge entre zones

Vous pouvez activer la répartition de charge entre zones à tout moment pour votre Classic Load Balancer.

Pour activer l'équilibrage de charge entre zones 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 le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sur la page Edit load balancer attributes, dans la section Availability Zone routing configuration, activer Cross-zone load balancing.
6. Sélectionnez Enregistrer les modifications.

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

1. Utilisez la modify-load-balancer-attributescommande suivante pour définir l'`CrossZoneLoadBalancing`attribut de votre équilibreur de charge sur `true` :

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --
load-balancer-attributes "{\"CrossZoneLoadBalancing\":{\"Enabled\":true}}"
```

   Voici un exemple de réponse :

```
{
   "LoadBalancerAttributes": {
     "CrossZoneLoadBalancing": {
         "Enabled": true
       }
   },
   "LoadBalancerName": "my-loadbalancer"
 }
```

2. (Facultatif) Utilisez la describe-load-balancer-attributescommande suivante pour vérifier que l'équilibrage de charge entre zones est activé pour votre équilibreur de charge :

```
aws elb describe-load-balancer-attributes --load-balancer-name my-loadbalancer
```

Voici un exemple de réponse :

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "CrossZoneLoadBalancing": {
            "Enabled": true
        },
        "ConnectionSettings": {
            "IdleTimeout": 60
        },
        "AccessLog": {
            "Enabled": false
        }
    }
}
```

Désactiver la répartition de charge entre zones

Vous pouvez désactiver l'option d'équilibrage de charge entre zones à tout moment pour votre équilibreur de charge.

Pour désactiver l'équilibrage de charge entre zones 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 le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sur la page Edit load balancer attributes, dans la section Availability Zone routing configuration, désactiver Cross-zone load balancing.
6. Sélectionnez Enregistrer les modifications.

Pour désactiver l'équilibrage de charge entre zones, définissez l'attribut `CrossZoneLoadBalancing` de votre équilibreur de charge sur `false`.

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

1. Utilisez la commande modify-load-balancer-attributes suivante :

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --
load-balancer-attributes "{\"CrossZoneLoadBalancing\":{\"Enabled\":false}}"
```

   Voici un exemple de réponse :

```
{
   "LoadBalancerAttributes": {
     "CrossZoneLoadBalancing": {
         "Enabled": false
       }
   },
   "LoadBalancerName": "my-loadbalancer"
 }
```

2. (Facultatif) Utilisez la describe-load-balancer-attributescommande suivante pour vérifier que l'équilibrage de charge entre zones est désactivé pour votre équilibreur de charge :

```
aws elb describe-load-balancer-attributes --load-balancer-name my-loadbalancer
```

   Voici un exemple de réponse :

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        },
        "CrossZoneLoadBalancing": {
            "Enabled": false
        },
        "ConnectionSettings": {
            "IdleTimeout": 60
        },
        "AccessLog": {
```

```
            "Enabled": false
        }
    }
}
```

Configurer le drainage de la connexion pour votre Classic Load Balancer

Pour vous assurer qu'un Classic Load Balancer cesse d'envoyer des demandes aux instances dont l'enregistrement est en cours d'annulation ou qui sont défectueuses, tout en maintenant les connexions existantes ouvertes, utilisez le drainage de la connexion. Cela permet à l'équilibreur de charge de terminer les demandes en cours effectuées sur des instances dont l'enregistrement est en cours d'annulation ou qui sont défectueuses.

Lorsque vous activez le drainage de la connexion, vous pouvez spécifier une durée maximale pendant laquelle l'équilibreur de charge conserve des connexions actives avant de signaler que l'enregistrement de l'instance est en cours d'annulation. Le délai d'attente maximal peut être défini sur une valeur comprise entre 1 et 3 600 secondes (la valeur par défaut est de 300 secondes). Lorsque le délai d'attente maximal est atteint, l'équilibreur de charge force la fermeture des connexions vers l'instance dont l'enregistrement est en cours d'annulation.

Pendant que les demandes en cours sont servies, l'équilibreur de charge indique que l'état d'une instance dont l'enregistrement est en cours d'annulation est `InService: Instance deregistration currently in progress`. Lorsque l'instance dont l'enregistrement est en cours d'annulation a fini de traiter toutes les demandes en cours, ou lorsque le délai d'attente maximal est atteint, l'équilibreur de charge indique que l'état de l'instance est `OutOfService: Instance is not currently registered with the LoadBalancer`.

Si une instance devient défectueuse, l'équilibreur de charge indique que l'état de l'instance est `OutOfService`. Si des demandes en cours sont effectuées vers l'instance défectueuse, elles sont achevées. Le délai d'attente maximal ne s'applique pas aux connexions vers des instances saines.

Si vos instances font partie d'un groupe Auto Scaling et que le drainage de la connexion est activé pour l'équilibreur de charge, Auto Scaling attend la fin des demandes en cours ou que le délai maximal expire (le premier des deux) avant de mettre fin aux instances à cause d'un événement de dimensionnement ou d'un remplacement des vérifications de l'état.

Vous pouvez désactiver le drainage de la connexion si vous voulez que votre équilibreur de charge ferme immédiatement les connexions vers les instances dont l'enregistrement est en cours d'annulation ou qui deviennent défectueuses. Lorsque le drainage de connexion est désactivé, les demandes en cours effectuées vers des instances dont l'enregistrement est en cours d'annulation ou qui sont défectueuses ne sont pas achevées.

Table des matières

- Activer le drainage de la connexion
- Désactiver le drainage de la connexion

Activer le drainage de la connexion

Vous pouvez activer le drainage de la connexion à tout moment pour votre équilibreur de charge.

Pour activer le drainage de la 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 Load Balancing (Équilibrage de charge), 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 Attributes, choisissez Edit.
5. Sur la page Edit load balancer attributes, dans la section Traffic configuration, sélectionnezEnable connection draining.
6. (Facultatif) Pour Timeout (draining interval), saisissez une valeur comprise entre 1 et 3 600 secondes. Sinon, la valeur par défaut de 300 secondes est utilisée.
7. Sélectionnez Enregistrer les modifications.

Pour activer le drainage des connexions à l'aide du AWS CLI

Utilisez la commande modify-load-balancer-attributes suivante :

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-balancer-attributes "{\"ConnectionDraining\":{\"Enabled\":true,\"Timeout\":300}}"
```

Voici un exemple de réponse :

```
{
```

```
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": true,
            "Timeout": 300
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

Désactiver le drainage de la connexion

Vous pouvez désactiver le drainage de la connexion à tout moment pour votre équilibreur de charge.

Pour désactiver le drainage de la 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 Load Balancing (Équilibrage de charge), 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 Attributes, choisissez Edit.
5. Sur la page Edit load balancer attributes, dans la section Traffic configuration, désélectionnez Enable connection draining.
6. Sélectionnez Enregistrer les modifications.

Pour désactiver le drainage des connexions à l'aide du AWS CLI

Utilisez la commande modify-load-balancer-attributes suivante :

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-
balancer-attributes "{\"ConnectionDraining\":{\"Enabled\":false}}"
```

Voici un exemple de réponse :

```
{
    "LoadBalancerAttributes": {
        "ConnectionDraining": {
            "Enabled": false,
            "Timeout": 300
        }
```

```
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

Configurer la prise en charge du protocole proxy pour votre Classic Load Balancer

Le protocole proxy est un protocole Internet utilisé pour exécuter des informations de connexion de la source demandant la connexion à la destination pour laquelle la connexion a été demandée. Elastic Load Balancing utilise le protocole proxy version 1, qui utilise un format d'en-tête lisible par l'homme.

Par défaut, lorsque vous utilisez le protocole TCP (Transmission Control Protocol) ou SSL (Secure Sockets Layer) pour les connexions frontales et principales, votre Classic Load Balancer transfère les demandes aux instances sans modifier les en-têtes de demande. Si vous activez le protocole proxy, un en-tête compréhensible par les utilisateurs est ajouté à l'en-tête de demande avec des informations de connexion telles que l'adresse IP source, l'adresse IP de destination et les numéros de ports. L'en-tête est ensuite envoyé à l'instance dans le cadre de la demande.

> **Note**
>
> AWS Management Console Ne prend pas en charge l'activation du protocole proxy.

Table des matières

- En-tête du protocole proxy
- Prérequis pour l'activation du protocole proxy
- Activer le protocole proxy à l'aide de l'interface AWS CLI
- Désactiver le protocole proxy à l'aide de l'interface AWS CLI

En-tête du protocole proxy

L'en-tête du protocole proxy vous aide à identifier l'adresse IP d'un client lorsque votre équilibreur de charge utilise TCP pour les connexions principales. Comme des équilibreurs de charge interceptent le trafic entre les clients et vos instances, les journaux d'accès de votre instance contiennent l'adresse IP de l'équilibreur de charge, et non celle du client d'origine. Vous pouvez analyser la première ligne de la demande pour extraire l'adresse IP et le numéro de port de votre client.

L'adresse du proxy dans l'en-tête pour IPv6 est l'adresse IPv6 publique de votre équilibreur de charge. Cette adresse IPv6 correspond à l'adresse IP qui est résolue à partir du nom DNS de votre équilibreur de charge, qui commence par `ipv6` ou `dualstack`. Si le client se connecte à IPv4, l'adresse du proxy dans l'en-tête est l'adresse IPv4 privée de l'équilibreur de charge, qui n'est pas résolue via une recherche DNS.

La ligne du protocole proxy est une ligne unique qui se termine par un retour chariot et un saut de ligne (`"\r\n"`), au format suivant :

```
PROXY_STRING + single space + INET_PROTOCOL + single space + CLIENT_IP + single space +
 PROXY_IP + single space + CLIENT_PORT + single space + PROXY_PORT + "\r\n"
```

Exemple : IPv4

Voici un exemple de ligne de protocole proxy pour IPv4.

```
PROXY TCP4 198.51.100.22 203.0.113.7 35646 80\r\n
```

Prérequis pour l'activation du protocole proxy

Avant de commencer, vous devez exécuter les actions suivantes :

- Vérifiez que votre équilibreur de charge n'est pas situé derrière un serveur proxy avec le protocole proxy activé. Si le protocole proxy est activé sur le serveur proxy et l'équilibreur de charge, l'équilibreur de charge ajoute un autre en-tête à la demande, qui a déjà un en-tête du serveur proxy. En fonction de la configuration de votre instance, cette duplication peut entraîner des erreurs.
- Vérifiez que vos instances peuvent traiter les informations du protocole proxy.
- Vérifiez que les paramètres de votre Écouteur prennent en charge le protocole proxy. Pour plus d'informations, consultez Configurations d'Écouteur pour Classic Load Balancers.

Activer le protocole proxy à l'aide de l'interface AWS CLI

Pour activer le protocole proxy, vous devez créer une politique de type `ProxyProtocolPolicyType`, puis activer la stratégie sur le port d'instance.

Utilisez la procédure suivante pour créer une nouvelle stratégie pour votre équilibreur de charge de type `ProxyProtocolPolicyType`, définissez la stratégie nouvellement créée sur l'instance sur le port `80` et vérifiez que la stratégie est activée.

Pour activer le protocole proxy pour votre équilibreur de charge

1. (Facultatif) Utilisez la commande describe-load-balancer-policy-types suivante pour répertorier les politiques prises en charge par Elastic Load Balancing :

   ```
   aws elb describe-load-balancer-policy-types
   ```

   La réponse inclut les noms et les descriptions des types de stratégie pris en charge. Voici la sortie affichée pour le type `ProxyProtocolPolicyType` :

   ```
   {
       "PolicyTypeDescriptions": [
           ...
           {
               "PolicyAttributeTypeDescriptions": [
                   {
                       "Cardinality": "ONE",
                       "AttributeName": "ProxyProtocol",
                       "AttributeType": "Boolean"
                   }
               ],
               "PolicyTypeName": "ProxyProtocolPolicyType",
               "Description": "Policy that controls whether to include the IP address
    and port of the originating
   request for TCP messages. This policy operates on TCP/SSL listeners only"
           },
           ...
       ]
   }
   ```

2. Utilisez la create-load-balancer-policycommande suivante pour créer une politique qui active le protocole proxy :

   ```
   aws elb create-load-balancer-policy --load-balancer-name my-loadbalancer --policy-
   name my-ProxyProtocol-policy --policy-type-name ProxyProtocolPolicyType --policy-
   attributes AttributeName=ProxyProtocol,AttributeValue=true
   ```

3. Utilisez la for-backend-server commande set-load-balancer-policies- suivante pour activer la politique nouvellement créée sur le port spécifié. Notez que cette commande remplace l'ensemble actuel de stratégies activées. Par conséquent, l'option `--policy-names` doit spécifier la stratégie que vous ajoutez à la liste (par exemple, `my-ProxyProtocol-policy`) et les stratégies actuellement activées (par exemple, `my-existing-policy`).

```
aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 80 --policy-names my-ProxyProtocol-policy my-existing-policy
```

4. (Facultatif) Utilisez la describe-load-balancerscommande suivante pour vérifier que le protocole proxy est activé :

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

La réponse inclut les informations suivantes qui montrent que la stratégie `my-ProxyProtocol-policy` est associée au port `80`.

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "BackendServerDescriptions": [
                {
                    "InstancePort": 80,
                    "PolicyNames": [
                        "my-ProxyProtocol-policy"
                    ]
                }
            ],
            ...
        }
    ]
}
```

Désactiver le protocole proxy à l'aide de l'interface AWS CLI

Vous pouvez désactiver les stratégies associées à votre instance, puis les activer ultérieurement.

Pour désactiver la politique de protocole proxy

1. Utilisez la for-backend-server commande set-load-balancer-policies- suivante pour désactiver la politique du protocole proxy en l'omettant dans l'`--policy-names`option, mais en incluant les autres politiques qui doivent rester activées (par exemple,`my-existing-policy`).

   ```
   aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 80 --policy-names my-existing-policy
   ```

   S'il n'existe aucune autre stratégie à activer, spécifiez une chaîne vide avec l'option `--policy-names` comme suit :

   ```
   aws elb set-load-balancer-policies-for-backend-server --load-balancer-name my-loadbalancer --instance-port 80 --policy-names "[]"
   ```

2. (Facultatif) Utilisez la describe-load-balancerscommande suivante pour vérifier que la politique est désactivée :

   ```
   aws elb describe-load-balancers --load-balancer-name my-loadbalancer
   ```

   La réponse inclut les informations suivantes qui montrent qu'aucun port n'est associé à la stratégie .

   ```
   {
       "LoadBalancerDescriptions": [
           {
               ...
               "BackendServerDescriptions": [],
               ...
           }
       ]
   }
   ```

Configurer des sessions permanentes pour votre Classic Load Balancer

Par défaut, un Classic Load Balancer achemine chaque demande de façon indépendante vers l'instance enregistrée ayant la plus petite charge. Cependant, vous pouvez utiliser la fonction de

session permanente (aussi appelée affinité de session), qui permet à l'équilibreur de charge de lier la session d'un utilisateur à une instance spécifique. Il est ainsi possible de garantir que toutes les demandes de l'utilisateur pendant la session sont adressées à la même instance.

La clé de la gestion des sessions permanentes consiste à déterminer combien de temps votre équilibreur de charge doit acheminer systématiquement les demandes de l'utilisateur vers la même instance. Si votre application a son propre cookie de session, vous pouvez configurer Elastic Load Balancing pour que le cookie de session suive la durée spécifiée par le cookie de session de l'application. Si votre application n'a pas son propre cookie de session, vous pouvez configurer Elastic Load Balancing pour créer un cookie de session en spécifiant votre propre durée de permanence.

Elastic Load Balancing crée un cookie AWSELB, nommé, qui est utilisé pour mapper la session à l'instance.

Prérequis

- Un équilibreur de charge HTTP/HTTPS
- Au moins une instance saine dans chaque zone de disponibilité.

Compatibilité

- Le RFC pour la propriété path d'un cookie autorise les traits de soulignement. Cependant, l'URI Elastic Load Balancing encode les traits de soulignement en `%5F` car certains navigateurs, comme Internet Explorer 7, s'attendent à ce que les traits de soulignement soient encodés par l'URI en `%5F`. En raison de l'impact potentiel sur les navigateurs qui fonctionnent actuellement, Elastic Load Balancing continue à encoder les traits de soulignement dans l'URI. Par exemple, si le cookie a la propriété `path=/my_path`, Elastic Load Balancing change cette propriété dans la demande transmise en `path=/my%5Fpath`.
- Vous ne pouvez pas définir l'indicateur `secure` ou `HttpOnly` sur vos cookies de permanence de sessions basée sur la durée. Toutefois, ces cookies ne contiennent pas des données sensibles. Notez que si vous définissez le `secure` drapeau ou le `HttpOnly` drapeau sur un cookie de persistance de session contrôlé par une application, il est également défini sur le cookie. AWSELB
- Si le champ `Set-Cookie` d'un cookie d'application contient un point-virgule de fin, l'équilibreur de charge ignore le cookie.

Table des matières

- Permanence de session basée sur la durée
- Permanence des sessions contrôlées par application

Permanence de session basée sur la durée

L'équilibreur de charge utilise un cookie spécial pour suivre l'instance de chaque demande adressée à chaque auditeur. AWSELB Lorsque l'équilibreur de charge reçoit une demande, il vérifie d'abord si ce cookie est présent dans la demande. Si tel est le cas, la demande est envoyée à l'instance spécifiée dans le cookie. S'il n'y a pas de cookie, l'équilibreur de charge choisit une instance à partir de l'algorithme d'équilibrage de charge existant. Un cookie est inséré dans la réponse pour lier les demandes suivantes provenant du même utilisateur à cette instance. La configuration de la stratégie de permanence de session définit l'expiration d'un cookie, ce qui établit la durée de validité de chaque cookie. L'équilibreur de charge n'actualise pas le délai d'expiration du cookie et ne vérifie pas si le cookie a expiré avant de l'utiliser. Après l'expiration d'un cookie, la session n'est plus permanente. Le client doit supprimer le cookie de son magasin de cookies lorsque celui-ci est expiré.

Avec les demandes CORS (partage des ressources cross-origin), certains navigateurs nécessitent `SameSite=None; Secure` pour activer la permanence. Dans ce cas, Elastic Load Balancing crée un deuxième cookie d'adhérence AWSELBCORS, qui inclut les mêmes informations que le cookie d'adhérence d'origine, plus cet attribut. `SameSite` Les clients reçoivent les deux cookies.

Si une instance est défaillante ou devient défectueuse, l'équilibreur de charge s'arrête d'acheminer les demandes vers cette celle-ci et choisit une nouvelle instance saine en fonction de l'algorithme d'équilibrage de charge existant. La demande est acheminée vers la nouvelle instance comme s'il n'existait pas de cookie et que la session n'était plus permanente.

Si un client bascule vers un écouteur avec un port backend différent, la permanence est perdue.

Pour activer des sessions permanentes basées sur la durée pour 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 panneau de navigation, sous Load Balancing (Équilibrage de charge), choisissez Load Balancers (Équilibreurs de charge).
3. Choisissez le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Sous l'onglet Listeners, choisissez Manage listeners.

5. Sur la page Manage listeners, localisez l'écouteur à mettre à jour et choisissez Edit sous Cookie stickiness.
6. Sélectionnez Generated by load balancer.
7. (Facultatif) Pour Expiration period, saisissez la période d'expiration du cookie, en secondes. Si vous ne spécifiez pas de période d'expiration, la session permanente dure pendant la durée de la session de navigateur.
8. Sélectionnez Enregistrer les modifications.

Pour activer des sessions permanentes basées sur la durée pour un équilibreur de charge à l'aide de l'interface AWS CLI

1. Utilisez la commande create-lb-cookie-stickiness-policy suivante pour créer une politique de conservation des cookies générée par l'équilibreur de charge avec une période d'expiration des cookies de 60 secondes :

```
aws elb create-lb-cookie-stickiness-policy --load-balancer-name my-loadbalancer --
policy-name my-duration-cookie-policy --cookie-expiration-period 60
```

2. Utilisez la commande set-load-balancer-policies-of-listener suivante pour activer le maintien de la session pour l'équilibreur de charge spécifié :

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-duration-cookie-policy
```

> **Note**
>
> La commande `set-load-balancer-policies-of-listener` remplace l'ensemble actuel de politiques associées au port de l'équilibreur de charge spécifié. Chaque fois que vous utilisez cette commande, spécifiez l'option `--policy-names` pour répertorier toutes les stratégies à activer.

3. (Facultatif) Utilisez la describe-load-balancerscommande suivante pour vérifier que la politique est activée :

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

La réponse inclut les informations suivantes qui montrent que la stratégie est activée pour l'écouteur sur le port spécifié :

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 443,
                        "SSLCertificateId": "arn:aws:iam::123456789012:server-
certificate/my-server-certificate",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTPS"
                    },
                    "PolicyNames": [
                        "my-duration-cookie-policy",
                        "ELBSecurityPolicy-2016-08"
                    ]
                },
                ...
            ],
            ...
            "Policies": {
                "LBCookieStickinessPolicies": [
                 {
                        "PolicyName": "my-duration-cookie-policy",
                        "CookieExpirationPeriod": 60
                    }

                ],
                "AppCookieStickinessPolicies": [],
                "OtherPolicies": [
                    "ELBSecurityPolicy-2016-08"
                ]
            },
            ...
        }
    ]
}
```

Permanence des sessions contrôlées par application

L'équilibreur de charge utilise un cookie spécial pour associer la session à l'instance qui a traité la demande initiale, mais suit la durée de vie du cookie d'application spécifié dans la configuration de la stratégie. L'équilibreur de charge n'insère un nouveau cookie de permanence que si la réponse de l'application inclut un nouveau cookie d'application. Le cookie de permanence de l'équilibreur de charge n'est pas mis à jour à chaque demande. Si le cookie d'application est explicitement supprimé ou expire, la session cesse d'être permanente jusqu'à l'émission d'un nouveau cookie.

Les attributs suivants, définis par les instances principales, sont envoyés aux clients dans le cookie : `path`, `port`, `domain`, `secure`, `httponly`, `discard`, `max-age`, `expires`, `version`, `comment`, `commenturl` et `samesite`.

Si une instance est défaillante ou devient défectueuse, l'équilibreur de charge s'arrête d'acheminer les demandes vers cette celle-ci et choisit une nouvelle instance saine en fonction de l'algorithme d'équilibrage de charge existant. L'équilibreur de charge traite désormais la session comme étant liée à la nouvelle instance saine et continue d'acheminer les demandes vers cette instance, même si l'instance en échec est récupérée.

Pour activer la permanence de session contrôlée par application 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 le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Sous l'onglet Listeners, choisissez Manage listeners.
5. Sur la page Manage listeners, localisez l'écouteur à mettre à jour et choisissez Edit sous Cookie stickiness.
6. Sélectionnez Generated by application.
7. Pour Cookie Name, tapez le nom du cookie de votre application.
8. Sélectionnez Enregistrer les modifications.

Pour activer le caractère permanent des sessions contrôlé par l'application à l'aide du AWS CLI

1. Utilisez la commande create-app-cookie-stickiness-policy suivante pour créer une politique de conservation des cookies générée par l'application :

```
aws elb create-app-cookie-stickiness-policy --load-balancer-name my-loadbalancer --
policy-name my-app-cookie-policy --cookie-name my-app-cookie
```

2. Utilisez la commande set-load-balancer-policies-of-listener suivante pour activer le maintien de la session pour un équilibreur de charge :

```
aws elb set-load-balancer-policies-of-listener --load-balancer-name my-loadbalancer
 --load-balancer-port 443 --policy-names my-app-cookie-policy
```

> **Note**
>
> La commande `set-load-balancer-policies-of-listener` remplace l'ensemble actuel de politiques associées au port de l'équilibreur de charge spécifié. Chaque fois que vous utilisez cette commande, spécifiez l'option `--policy-names` pour répertorier toutes les stratégies à activer.

3. (Facultatif) Utilisez la describe-load-balancerscommande suivante pour vérifier que la politique persistante est activée :

```
aws elb describe-load-balancers --load-balancer-name my-loadbalancer
```

4. La réponse inclut les informations suivantes qui montrent que la stratégie est activée pour l'écouteur sur le port spécifié :

```
{
    "LoadBalancerDescriptions": [
        {
            ...
            "ListenerDescriptions": [
                {
                    "Listener": {
                        "InstancePort": 443,
                        "SSLCertificateId": "arn:aws:iam::123456789012:server-
certificate/my-server-certificate",
                        "LoadBalancerPort": 443,
                        "Protocol": "HTTPS",
                        "InstanceProtocol": "HTTPS"
                    },
                    "PolicyNames": [
                        "my-app-cookie-policy",
```

```
                        "ELBSecurityPolicy-2016-08"
                    ]
                },
                {
                    "Listener": {
                        "InstancePort": 80,
                        "LoadBalancerPort": 80,
                        "Protocol": "TCP",
                        "InstanceProtocol": "TCP"
                    },
                    "PolicyNames": []
                }
            ],
            ...
            "Policies": {
                "LBCookieStickinessPolicies": [],
                "AppCookieStickinessPolicies": [
                {
                        "PolicyName": "my-app-cookie-policy",
                        "CookieName": "my-app-cookie"
                    }

                ],
                "OtherPolicies": [
                    "ELBSecurityPolicy-2016-08"
                ]
            },
            ...
        }
    ]
}
```

Configurer le mode d'atténuation de désynchronisation pour votre Classic Load Balancer

Le mode d'atténuation de désynchronisation protège votre application contre les problèmes dus à HTTP Desync. L'équilibreur de charge classe chaque demande en fonction de son niveau de menace, autorise les demandes sécurisées, puis atténue les risques comme spécifié par le mode d'atténuation que vous spécifiez. Les modes d'atténuation de désynchronisation sont Moniteur, Défensif et Le plus strict. La valeur par défaut est le mode Défensif, qui fournit une

atténuation durable contre la désynchronisation HTTP tout en maintenant la disponibilité de votre application. Vous pouvez passer au mode Le plus strict pour vous assurer que votre application reçoit uniquement les requêtes conformes à la RFC 7230.

La bibliothèque http_desync_guardian analyse les requêtes HTTP pour empêcher les attaques HTTP Desync. Pour de plus amples informations, consultez HTTP Desync Guardian sur github.

Table des matières

- Classifications
- Modes
- Modifier le mode d'atténuation de désynchronisation

> **Tip**
>
> Cette configuration s'applique uniquement aux Classic Load Balancers. Pour plus d'informations s'appliquant aux Application Load Balancers, consultez Mode d'atténuation de désynchronisation pour les Application Load Balancers.

Classifications

Les classifications sont les suivantes.

- Conformité : la requête est conforme à la RFC 7230 et ne présente aucune menace de sécurité connue.
- Acceptable : la requête n'est pas conforme à la RFC 7230 mais ne présente aucune menace de sécurité connue.
- Ambiguë : la requête n'est pas conforme à la RFC 7230 mais présente un risque, car divers serveurs web et proxys pourraient la traiter différemment.
- Sévère : la requête présente un risque de sécurité élevé. L'équilibreur de charge bloque la requête, sert une réponse 400 au client et ferme la connexion client.

Les listes suivantes décrivent les problèmes pour chaque classification.

Acceptable

- Un en-tête contient un caractère non ASCII ou de contrôle.

- La version de requête contient une valeur incorrecte.
- Il existe un en-tête Content-Length avec une valeur de 0 pour une requête GET ou HEAD.
- L'URI de la requête contient un espace qui n'est pas encodé par URL.

Ambigu

- L'URI de requête contient des caractères de contrôle.
- La requête contient à la fois un en-tête Transfer-Encoding et un en-tête Content-Length.
- Il existe plusieurs en-têtes Content-Length avec la même valeur.
- Un en-tête est vide ou il y a une ligne avec seulement des espaces.
- Il existe un en-tête qui peut être normalisé en Transfer-Encoding ou Content-Length à l'aide de techniques de normalisation de texte courantes.
- Il existe un en-tête Content-Length pour une requête GET ou HEAD.
- Il existe un en-tête Transfer-Encoding pour une requête GET ou HEAD.

Sévère

- L'URI de la requête contient un caractère nul ou un retour chariot.
- L'en-tête Content-Length contient une valeur qui ne peut pas être analysée ou n'est pas un nombre valide.
- Un en-tête contient un caractère nul ou un retour chariot.
- L'en-tête Transfer-Encoding contient une valeur incorrecte.
- La méthode de la requête est mal formée.
- La version de la requête est mal formée.
- Il existe plusieurs en-têtes Content-Length avec des valeurs différentes.
- Il existe plusieurs en-têtes segmentés Transfer-Encoding:.

Si une requête n'est pas conforme à la RFC 7230, l'équilibreur de charge incrémente la métrique `DesyncMitigationMode_NonCompliant_Request_Count`. Pour plus d'informations, consultez Métriques Classic Load Balancer.

Modes

Le tableau suivant décrit la façon dont les Classic Load Balancers traitent les requêtes en fonction du mode et de la classification.

Classification	Mode Moniteur	Mode Défensif	Mode Le plus strict
Conforme	Autorisé	Autorisé	Autorisé
Acceptable	Autorisé	Autorisé	Bloqué
Ambigu	Autorisé	Autorisé[1]	Bloqué
Sévère	Autorisé	Bloqué	Bloqué

[1] Achemine les requêtes mais ferme les connexions client et cible.

Modifier le mode d'atténuation de désynchronisation

Pour mettre à jour le mode d'atténuation de désynchronisation 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 le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sur la page Edit load balancer attributes, sous Traffic configuration, choisissez Defensive - recommended, Strictest, ou Monitor.
6. Sélectionnez Enregistrer les modifications.

Pour mettre à jour le mode d'atténuation de la désynchronisation à l'aide du AWS CLI

Utilisez la modify-load-balancer-attributescommande avec l'`elb.http.desyncmitigationmode`attribut défini sur `monitor`ou `defensive`, ou `strictest`.

```
aws elb modify-load-balancer-attributes --load-balancer-name my-load-balancer --load-balancer-attributes file://attribute.json
```

Voici le contenu de `attribute.json`.

```
{
    "AdditionalAttributes": [
        {
            "Key": "elb.http.desyncmitigationmode",
            "Value": "strictest"
        }
    ]
}
```

Baliser votre Classic Load Balancer

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

Vous pouvez ajouter plusieurs balises à chaque Classic Load Balancer. Les clés de balise doivent être uniques pour 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.

Table des matières

- Restrictions liées aux étiquettes
- Ajouter une balise
- Supprimer une balise

Restrictions liées aux étiquettes

Les restrictions de base suivantes s'appliquent aux balises :

- 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.

Ajouter une balise

Vous pouvez ajouter des balises à votre équilibreur de charge à tout moment.

Pour ajouter une balise 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 (Équilibrage de charge), 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 Balises, choisissez Gérer les balises.
5. Sur la page Manage tags, pour chaque balise, choisissez Add new tag, puis spécifiez une clé et une valeur.
6. Une fois que vous avez terminé d'ajouter des balises, choisissez Save changes.

Pour ajouter un tag à l'aide du AWS CLI

Utilisez la commande add-tags suivante pour ajouter la balise spécifiée :

```
aws elb add-tags --load-balancer-name my-loadbalancer --tag "Key=project,Value=lima"
```

Supprimer une balise

Vous pouvez supprimer des balises de votre équilibreur de charge lorsque que vous avez fini de les utiliser.

Pour supprimer une balise 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 (Équilibrage de charge), 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 Balises, choisissez Gérer les balises.
5. Sur la page Manage tags, choisissez Remove en regard de chaque balise à supprimer.
6. Une fois que vous avez terminé de supprimer des balises, choisissez Save changes.

Pour supprimer une étiquette à l'aide du AWS CLI

Utilisez la commande remove-tags suivante pour supprimer la balise avec la clé spécifiée :

```
aws elb remove-tags --load-balancer-name my-loadbalancer --tag project
```

Configurer un nom de domaine personnalisé pour votre Classic Load Balancer

Chaque Classic Load Balancer reçoit un nom DNS (Domain Name System, système de noms de domaine) par défaut. Ce nom DNS inclut le nom de la AWS région dans laquelle l'équilibreur de charge est créé. Par exemple, si vous créez un équilibreur de charge nommé `my-loadbalancer` dans la Région USA Ouest (Oregon), celui-ci reçoit un nom DNS tel que `my-loadbalancer-1234567890.us-west-2.elb.amazonaws.com`. Pour accéder au site web sur vos instances, vous collez ce nom DNS dans le champ d'adresse d'un navigateur web. Toutefois, ce nom DNS n'est pas facile à mémoriser et à utiliser pour vos clients.

Si vous préférez utiliser un nom DNS convivial pour votre équilibreur de charge, comme `www.example.com`, plutôt que le nom DNS par défaut, vous pouvez créer un nom de domaine personnalisé et l'associer au nom DNS pour 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.

Table des matières

- Associer votre nom de domaine personnalisé au nom de votre équilibreur de charge
- Utiliser le basculement DNS Route 53 pour votre équilibreur de charge
- Dissocier votre nom de domaine personnalisé de votre équilibreur de charge

Associer votre nom de domaine personnalisé au nom de votre équilibreur de charge

Tout d'abord, si vous ne l'avez pas déjà fait, enregistrez votre nom de domaine. L'ICANN (Internet Corporation for Assigned Names and Numbers) gère les noms de domaine sur Internet. Vous enregistrez un nom de domaine à l'aide d'un serveur d'inscriptions de noms de domaine, une organisation accréditée par l'ICANN qui gère le registre des noms de domaine. Le site Web pour votre serveur d'inscriptions vous fournira des instructions détaillées et des informations de tarification pour l'enregistrement de votre nom de domaine. Pour plus d'informations, consultez les ressources suivantes :

- Pour utiliser Amazon Route 53 pour enregistrer un nom de domaine, consultez Enregistrement de noms de domaines à l'aide de Route 53 dans le Guide du développeur Amazon Route 53.
- Pour une liste des serveurs d'inscriptions accrédités, consultez la page Accredited Registrar Directory.

Utilisez ensuite votre service DNS, par exemple, votre serveur d'inscriptions de domaine, pour créer un enregistrement CNAME afin d'acheminer les demandes vers votre équilibreur de charge. Pour plus d'informations, consultez la documentation de votre service DNS.

Vous pouvez également utiliser Route 53 comme service DNS. Vous créez une zone hébergée, qui contient des informations sur l'acheminement du trafic sur Internet pour votre domaine, et un jeu d'enregistrements de ressources d'alias, qui achemine les requêtes pour votre nom de domaine vers votre équilibreur de charge. Route 53 ne facture pas les requêtes DNS pour des jeux d'enregistrements d'alias, et vous pouvez utiliser des jeux d'enregistrements d'alias pour acheminer des requêtes DNS vers votre équilibreur de charge pour la zone apex de votre domaine (par exemple, `example.com`). Pour plus d'informations sur le transfert de services DNS pour des domaines existants vers Route 53, consultez Configuration de Route 53 en tant que service DNS dans le Guide du développeur Amazon Route 53.

Pour finir, créez une zone hébergée et un jeu d'enregistrements d'alias pour votre domaine à l'aide de Route 53. Pour de plus amples informations, consultez Acheminement du trafic vers un équilibreur de charge dans le Guide du développeur Amazon Route 53.

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 instances EC2 enregistrées pour l'équilibreur de charge afin de déterminer si celles-ci sont disponibles. Si aucune instances EC2 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 Classic Load Balancer, Route 53 évalue l'état de santé de la ressource spécifiée par la valeur `alias target`. Pour un Classic Load Balancer, Route 53 utilise les surveillances de l'état de l'instance associées à l'équilibreur de charge.
- Tant que l'une des instances enregistrées dans un Classic Load Balancer est saine, Route 53 indique que l'enregistrement d'alias est sain. 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.
- Lorsque toutes les instances enregistrées dans un Classic Load Balancer sont défectueuses, Route 53 indique que l'enregistrement d'alias est défectueux. 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 secondaire.

Pour de plus amples informations, consultez Configuration du basculement DNS dans le Guide du développeur Amazon Route 53.

Dissocier votre nom de domaine personnalisé de votre équilibreur de charge

Vous pouvez dissocier votre nom de domaine personnalisé d'une instance d'équilibreur de charge en supprimant d'abord les jeux d'enregistrements de ressources de votre zone hébergée, puis

en supprimant la zone hébergée. Pour de plus amples informations, consultez Modification des enregistrements et Suppression d'une zone hébergée publique dans le Guide du développeur Amazon Route 53.

Contrôler votre Classic Load Balancer

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 instances principales.

CloudWatch métriques

Elastic Load Balancing publie CloudWatch sur Amazon des points de données concernant vos équilibreurs de charge et vos instances principales. CloudWatch vous permet de récupérer des statistiques sur ces points de données 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 statistiques pour votre Classic Load Balancer.

Journaux d'accès Elastic Load Balancing

Les journaux d'accès Elastic Load Balancing capturent des informations détaillées pour les demandes exécutées vers votre équilibreur de charge et les stockent en tant que fichiers journaux dans le compartiment Amazon S3 que vous spécifiez. Chaque journal contient des détails tels que le moment où une demande a été reçue, l'adresse du client IP, les latences, le chemin de demande et les réponses du serveur. Vous pouvez utiliser ces journaux d'accès pour analyser les modèles de trafic et résoudre les problèmes liés à vos applications principales. Pour plus d'informations, consultez Journaux d'accès pour votre Classic Load Balancer.

CloudTrail journaux

AWS CloudTrail vous permet de suivre les appels passés à l'API Elastic Load Balancing par ou au nom de votre AWS compte. CloudTrail stocke les informations dans des fichiers journaux du compartiment Amazon S3 que vous spécifiez. Vous pouvez utiliser ces fichiers journaux pour surveiller l'activité des équilibreurs de charge en déterminant quelles demandes ont été envoyées, les adresses IP sources d'où proviennent les demandes, qui a effectué la demande, quand, etc. Pour plus d'informations, consultez Journalisation des appels d'API pour votre Classic Load Balancer à l'aide de AWS CloudTrail.

CloudWatch statistiques pour votre Classic Load Balancer

Elastic Load Balancing publie des points de données sur Amazon CloudWatch pour vos équilibreurs de charge et vos instances principales. 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 d'instances EC2 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 plus d'informations sur Amazon CloudWatch, consultez le guide de CloudWatch l'utilisateur Amazon.

Table des matières

- Métriques Classic Load Balancer
- Dimensions de métriques pour les Classic Load Balancers
- Statistiques pour les métriques Classic Load Balancer
- Afficher CloudWatch les statistiques de votre équilibreur de charge

Métriques Classic Load Balancer

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

Métrique	Description
`BackendConnectionErrors`	Nombre de connexions qui n'ont pas pu être établies entre l'équilibreur de charge et les instances enregistrées. Étant donné que l'équilibreur de charge essaie de relancer la connexion lorsque des erreurs se produisent, ce nombre peut dépasser le taux de

Métrique	Description
	demande. Notez que ce nombre inclut également les erreurs de connexion associées à des vérifications de l'état. Critères de notification : il existe une valeur différente de zéro Statistics : la statistique la plus utile est `Sum`. Notez que `Average`, `Minimum` et `Maximum` sont présentés par nœud d'équilibreur de charge et ne sont généralement pas utiles. Toutefois, la différence entre le minimum et le maximum (ou pic par rapport à la moyenne ou moyenne par rapport au seuil) peut être utile pour déterminer si un nœud de l'équilibreur de charge représente un cas particulier. Exemple : supposons que votre équilibreur de charge comporte 2 instances dans us-west-2a et 2 instances dans us-west-2b, et que les tentatives de connexion à une instance dans us-west-2a génèrent des erreurs de connexion back-end. La somme pour us-west-2a inclut ces erreurs de connexion, contrairement à la somme pour us-west-2b. Par conséquent, la somme pour l'équilibreur de charge est égale à celle pour us-west-2a.
`DesyncMitigationMode_NonCompliant_Request_Count`	[Écouteur HTTP] Nombre de demandes qui ne sont pas conformes à la RFC 7230. Critères de notification : il existe une valeur différente de zéro Statistics : la statistique la plus utile est `Sum`.

Métrique	Description
`HealthyHostCount`	Nombre d'instances saines enregistrées auprès de votre équilibreur de charge. Une instance récemment enregistrée est considérée comme saine si elle a réussi la première vérification de l'état. Si l'équilibrage de charge entre zones est activé, le nombre d'instances saines pour la dimension `LoadBalancerName` est calculé sur toutes les zones de disponibilité. Sinon, il est calculé par zone de disponibilité. Critères de notification : il s'agit d'instances enregistrées Statistiques : les statistiques les plus utiles sont `Average` et `Maximum`. Ces statistiques sont déterminées par les nœuds de l'équilibreur de charge. Notez que certains nœuds de l'équilibreur de charge peuvent déterminer qu'une instance est défectueuse pendant une brève période, tandis que d'autres nœuds la considèrent comme saine. Exemple : supposons que votre équilibreur de charge comporte 2 instances dans us-west-2a et 2 instances dans us-west-2b ; us-west-2a contient une instance défectueuse, tandis que us-west-2b n'en contient pas. Avec la dimension `AvailabilityZone`, la moyenne est d'une instance saine et une instance défectueuse dans us-west-2, et de 2 instances saines et 0 instance défectueuse dans us-west-2 b.

Métrique	Description
`HTTPCode_Backend_2XX`, `HTTPCode_Backend_3XX`, `HTTPCode_Backend_4XX`, `HTTPCode_Backend_5XX`	[Écouteur HTTP] Nombre de codes de réponse HTTP générés par les instances enregistrées. Ce nombre n'inclut pas les codes de réponse générés par l'équilibreur de charge. Critères de notification : il existe une valeur différente de zéro Statistics : la statistique la plus utile est `Sum`. Notez que `Minimum`, `Maximum` et `Average` ont chacun la valeur 1. Exemple : supposons que votre équilibreur de charge comporte 2 instances dans us-west-2a et 2 instances dans us-west-2b, et que les demandes envoyées à une instance dans us-west-2a génèrent des réponses HTTP 500. La somme pour us-west-2a inclut ces réponses d'erreur, contrairement à la somme pour us-west-2b. Par conséquent, la somme pour l'équilibreur de charge est égale à celle pour us-west-2a.
`HTTPCode_ELB_4XX`	[Écouteur HTTP] Nombre de codes d'erreur client HTTP 4XX générés par l'équilibreur de charge. Des erreurs client sont générées lorsqu'une demande est mal formulée ou incomplète. Critères de notification : il existe une valeur différente de zéro Statistics : la statistique la plus utile est `Sum`. Notez que `Minimum`, `Maximum` et `Average` ont chacun la valeur 1. Exemple : supposons que votre équilibreur de charge ait activé us-west-2a et us-west-2b, et que les demandes du client incluent une URL de demande incorrecte. Les erreurs client risquent donc d'augmenter dans toutes les zones de disponibilité. La somme pour l'équilibreur de charge est la somme des valeurs pour les zones de disponibilité.

Métrique	Description
HTTPCode_ELB_5XX	[Écouteur HTTP] Nombre de codes d'erreur serveur HTTP 5XX générés par l'équilibreur de charge. Ce nombre n'inclut pas les codes de réponse générés par les instances enregistrées. Cette métrique est présentée si aucune instance saine n'est enregistr ée sur l'équilibreur de charge, ou si le taux de demande dépasse la capacité des instances (débordement) ou de l'équilibreur de charge. Critères de notification : il existe une valeur différente de zéro Statistics : la statistique la plus utile est Sum. Notez que Minimum, Maximum et Average ont chacun la valeur 1. Exemple : supposons que votre équilibreur de charge ait activé us-west-2a et us-west-2b, et que les instances dans us-west-2a connaissent une latence élevée et mettent du temps à répondre aux demandes. Par conséquent, la file d'attente des hausses pour les nœuds de l'équilibreur de charge dans us-west-2a se remplit et les clients reçoivent une erreur 503. Si us-west-2b continue à répondre normalement, la somme pour l'équilibreur de charge est égale à celle pour us-west-2a.

Métrique	Description
`Latency`	[Écouteur HTTP] Durée totale écoulée, en secondes, du moment où l'équilibreur de charge a envoyé la demande à une instance enregistrée au moment où l'instance a commencé à envoyer les en-têtes de réponse. [Écouteur TCP] Délai total, en secondes, avant que l'équilibreur de charge parvienne à établir une connexion à une instance enregistr ée. Critères de notification : il existe une valeur différente de zéro Statistics : la statistique la plus utile est `Average`. Utilisez `Maximum` pour déterminer si des demandes prennent beaucoup plus de temps que la moyenne. Notez que `Minimum` n'est généralement pas utile. Exemple : supposons que l'équilibreur de charge comporte 2 instances dans us-west-2a et 2 instances dans us-west-2b, et que les demandes envoyées à une instance dans us-west-2a aient une latence plus élevée. La moyenne pour us-west-2a est supérieure à la moyenne pour us-west-2b.

Métrique	Description
`RequestCount`	Nombre de demandes terminées ou de connexions effectuées au cours de l'intervalle spécifié (1 ou 5 minutes). [Écouteur HTTP] Nombre de demandes reçues et acheminées, y compris les réponses d'erreur HTTP provenant des instances enregistrées. [Écouteur TCP] Nombre de connexions effectuées aux instances enregistrées. Critères de notification : il existe une valeur différente de zéro Statistics : la statistique la plus utile est `Sum`. Notez que `Minimum`, `Maximum` et `Average` retournent tous la valeur 1. Exemple : supposons que votre équilibreur de charge comporte 2 instances dans us-west-2a et 2 instances dans us-west-2 b, et que 100 demandes soient envoyées à l'équilibreur de charge. 60 demandes sont envoyées à us-west-2a, chaque instance recevant 30 demandes, et 40 demandes sont envoyées à us-west-2b, chaque instance recevant 20 demandes. Avec la dimension `AvailabilityZone` , us-west-2a contient une somme de 60 demandes et us-west-2b, une somme de 40 demandes. Avec la dimension `LoadBalancerName` , la somme est de 100 demandes.

Métrique	Description
`SpilloverCount`	Nombre total de demandes qui ont été rejetées en raison de la saturation de la file d'attente des hausses. [Écouteur HTTP] L'équilibreur de charge renvoie un code d'erreur HTTP 503. [Écouteur TCP] L'équilibreur de charge ferme la connexion. Critères de notification : il existe une valeur différente de zéro Statistics : la statistique la plus utile est `Sum`. Notez que `Average`, `Minimum` et `Maximum` sont présentés par nœud d'équilibreur de charge et ne sont généralement pas utiles. Exemple : supposons que votre équilibreur de charge ait activé us-west-2a et us-west-2b, et que les instances dans us-west-2a connaissent une latence élevée et mettent du temps à répondre aux demandes. Par conséquent, la file d'attente des hausses pour le nœud d'équilibreur de charge dans us-west-2a se remplit, ce qui entraîne un débordement. Si us-west-2b continue à répondre normalement, la somme pour l'équilibreur de charge sera la même que celle pour us-west-2a.

Métrique	Description
`SurgeQueueLength`	Nombre total de demandes (écouteur HTTP) ou de connexions (écouteur TCP) qui sont en attente de routage vers une instance saine. La taille maximale de la file d'attente est 1 024. Les demandes ou connexions supplémentaires sont rejetées lorsque la file d'attente est saturée. Pour plus d'informations, consultez `SpilloverCount` . Critères de notification : il existe une valeur différente de zéro. Statistiques : la statistique la plus utile est `Maximum`, car elle représente le pic des demandes placées en file d'attente. La statistique `Average` peut être utile, associée à `Minimum` et `Maximum`, pour déterminer la plage des demandes placées en file d'attente. Notez que `Sum` n'est pas utile. Exemple : supposons que votre équilibreur de charge ait activé us-west-2a et us-west-2b, et que les instances dans us-west-2a connaissent une latence élevée et mettent du temps à répondre aux demandes. Par conséquent, la file d'attente des hausses pour les nœuds de l'équilibreur de charge dans us-west-2a se remplit et les clients connaîtront probablement une augmentat ion des temps de réponse. Si le problème persiste, l'équilibreur de charge présentera certainement des débordements (voir la métrique `SpilloverCount`). Si us-west-2b continue à répondre normalement, `max` pour l'équilibreur de charge sera le même que `max` pour us-west-2a.

Métrique	Description
`UnHealthyHostCount`	Nombre d'instances défaillantes enregistrées auprès de votre équilibreur de charge. Une instance est considérée comme défectueuse une fois qu'elle a dépassé le seuil de défectuosité configuré pour les vérifications de l'état. Une instance défectueuse est considérée comme à nouveau saine lorsqu'elle atteint le seuil de bonne santé configuré pour les vérifications de l'état. Critères de notification : il s'agit d'instances enregistrées Statistiques : les statistiques les plus utiles sont `Average` et `Minimum`. Ces statistiques sont déterminées par les nœuds de l'équilibreur de charge. Notez que certains nœuds de l'équilib reur de charge peuvent déterminer qu'une instance est défectueu se pendant une brève période, tandis que d'autres nœuds la considèrent comme saine. Exemple : voir `HealthyHostCount` .

Les métriques suivantes vous permettent d'estimer vos coûts si vous migrez un Classic Load Balancer vers un Application Load Balancer. Ces mesures sont destinées à un usage informatif uniquement, et non à être utilisées avec des CloudWatch alarmes. Notez que si votre Classic Load Balancer possède plusieurs Écouteurs, ces métriques sont agrégées parmi les Écouteurs.

Ces estimations sont basées sur un équilibreur de charge équipé d'une règle par défaut et d'un certificat d'une taille de 2K. Si vous utilisez un certificat d'une taille de 4K ou supérieure, nous vous recommandons d'estimer vos coûts de la manière suivante : créez un Application Load Balancer basé sur votre Classic Load Balancer à l'aide de l'outil de migration et surveillez la métrique `ConsumedLCUs` pour l'Application Load Balancer. Pour de plus amples informations, consultez Migrer d'un Classic Load Balancer vers un Application Load Balancer dans le Guide de l'utilisateur Elastic Load Balancing.

Métrique	Description
`EstimatedALBActive ConnectionCount`	

Métrique	Description
	Estimation du nombre de connexions TCP simultanées et actives entre les clients et l'équilibreur de charge et entre l'équilibreur de charge et les cibles.
`EstimatedALBConsumedLCUs`	Estimation du nombre d'unités de capacité d'équilibreur de charge (LCU) utilisées par un Application Load Balancer. Vous ne payez que pour les unités LCU que vous utilisez par heure. Pour plus d'informations, consultez Tarification Elastic Load Balancing.
`EstimatedALBNewConnectionCount`	Estimation du nombre de nouvelles connexions TCP établies entre les clients et l'équilibreur de charge et entre l'équilibreur de charge et les cibles.
`EstimatedProcessedBytes`	Estimation du nombre d'octets traités par un Application Load Balancer.

Dimensions de métriques pour les Classic Load Balancers

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

Dimension	Description
`AvailabilityZone`	Filtre les données des métriques par la zone de disponibilité spécifiée.
`LoadBalancerName`	Filtre les données des métriques par l'équilibreur de charge spécifié.

Statistiques pour les métriques Classic 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.

Le statistiques `Minimum` et `Maximum` reflètent les valeurs minimum et maximum signalées par les différents nœuds d'équilibreur de charge. Par exemple, supposons qu'il existe 2 nœuds d'équilibreur de charge. Un nœud a `HealthyHostCount` avec 2 pour `Minimum`, 10 pour `Maximum` et 6 pour `Average`, tandis que l'autre nœud a `HealthyHostCount` avec 1 pour `Minimum`, 5 pour `Maximum` et 3 pour `Average`. Par conséquent, l'équilibreur de charge a 1 pour `Minimum`, 10 pour `Maximum` et environ 4 pour `Average`.

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, comme `RequestCount`, `HTTPCode_ELB_XXX`, `HTTPCode_Backend_XXX`, `BackendConnectionErrors` et `SpilloverCount`.

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.

Un centile indique la position relative d'une valeur dans un ensemble de données. Vous pouvez spécifier un centile en utilisant jusqu'à deux décimales (par exemple, p95.45). Par exemple, le 95e centile signifie que 95 % des données sont inférieures à cette valeur et que 5 % des données lui sont supérieures. Les centiles sont souvent utilisés pour isoler les anomalies. Par exemple, supposons qu'une application sert la majorité des demandes à partir d'un cache en 1 à 2 ms, mais en 100 à 200 ms si le cache est vide. Le valeur maximale reflète le cas plus lent, environ 200 ms. La moyenne n'indique pas la distribution des données. Les percentiles offrent une vue plus descriptive de performances de l'application. En utilisant le 99e percentile comme déclencheur ou CloudWatch alarme Auto Scaling, vous pouvez faire en sorte que le traitement de 1 % des demandes ne prenne pas plus de 2 ms.

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. Dans le panneau de navigation, sous Load Balancing (Équilibrage de charge), choisissez Load Balancers (Équilibreurs de charge).
3. Choisissez le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Sélectionnez l'onglet Monitoring (Surveillance).
5. Pour obtenir une vue plus grande d'une seule métrique, passez le curseur sur son graphique, puis choisissez l'icône `Maximize`. Les mesures suivantes sont disponibles :

   - Hôtes sains — `HealthyHostCount`
   - Hôtes non sains — `UnHealthyHostCount`
   - Latence moyenne — `Latency`
   - Requêtes — `RequestCount`
   - Erreurs de connexion backend — `BackendConnectionErrors`
   - Longueur de file d'attente des hausses — `SurgeQueueLength`
   - Décompte de débordement — `SpilloverCount`
   - HTTP 2XXs — `HTTPCode_Backend_2XX`
   - HTTP 3XXs — `HTTPCode_Backend_3XX`
   - HTTP 4XXs — `HTTPCode_Backend_4XX`
   - HTTP 5XXs — `HTTPCode_Backend_5XX`
   - ELB HTTP 4XXs — `HTTPCode_ELB_4XX`
   - ELB HTTP 5XXs — `HTTPCode_ELB_5XX`
   - Nombre estimé d'octets traités — `EstimatedProcessedBytes`
   - Estimation des LCU consommées par ALB — `EstimatedALBConsumedLCUs`
   - Nombre estimé de connexions actives ALB — `EstimatedALBActiveConnectionCount`
   - Nombre estimé de nouvelles connexions ALB — `EstimatedALBNewConnectionCount`

Pour afficher les métriques à l'aide de la CloudWatch console

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Sélectionnez l'espace de noms ELB.
4. Effectuez l’une des actions suivantes :
   - Sélectionnez une dimension de métrique pour afficher les métriques par équilibreur de charge, par zone de disponibilité ou pour l'ensemble des équilibreurs de charge.
   - Pour afficher une métrique pour toutes les dimensions, saisissez son nom dans le champ de recherche.
   - Pour afficher les métriques pour un seul équilibreur de charge, saisissez son nom dans le champ de recherche.
   - Pour afficher les métriques pour une seule zone de disponibilité, saisissez son nom dans le champ de recherche.

Journaux d'accès pour votre Classic Load Balancer

Elastic Load Balancing fournit des journaux d'accès qui capturent des informations détaillées sur les demandes envoyées à votre équilibreur de charge. Chaque journal contient des informations comme l'heure à laquelle la demande a été reçue, l'adresse IP du client, les latences, les chemins de demande et les réponses du serveur. Vous pouvez utiliser ces journaux d'accès pour analyser les modèles de trafic et résoudre des problèmes.

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

Tous les fichiers journaux des accès sont automatiquement chiffrés avec SSE-S3 avant d'être stockés dans votre compartiment S3, puis déchiffrés lorsque vous y accédez. Vous n'avez pas besoin d'intervenir ; le chiffrement et le déchiffrement sont effectués de manière transparente. 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 la section Protection des données à l'aide du chiffrement côté serveur avec les clés de chiffrement gérés par Amazon S3 (SSE-S3) dans le Guide de l'utilisateur Amazon Simple Storage Service.

L'utilisation des journaux d'accès n'implique aucun coût supplémentaire. Les coûts de stockage pour Amazon S3 vous seront 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.

Table des matières

- Fichiers journaux d'accès
- Entrées des journaux d'accès
- Traitement des journaux d'accès
- Activer les journaux d'accès pour votre Classic Load Balancer
- Désactiver les journaux d'accès pour votre Classic Load Balancer

Fichiers journaux d'accès

Elastic Load Balancing publie un fichier journal pour chaque nœud d'équilibreur de charge à l'intervalle que vous spécifiez. Vous pouvez spécifier un intervalle de publication de 5 minutes ou de 60 minutes lorsque vous activez le journal d'accès pour votre équilibreur de charge. Par défaut, Elastic Load Balancing publie les journaux à un intervalle de 60 minutes. Si l'intervalle est défini sur 5 minutes, les journaux sont publiés à 1 h 05, 1 h 10, 1 h 15, et ainsi de suite. Le démarrage de la livraison des journaux est différé de jusqu'à 5 minutes si l'intervalle est défini sur 5 minutes et jusqu'à 15 minutes si l'intervalle est défini sur 60 minutes. Vous pouvez modifier l'intervalle de publication à tout moment.

L'équilibreur de charge peut fournir plusieurs journaux pour la même période. Cela se produit généralement si le site connaît un trafic dense, dispose de plusieurs nœuds d'équilibreur de charge et a un intervalle court pour la publication des journaux.

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_load-balancer-name_end-time_ip-address_random-string.log
```

bucket

Nom du compartiment S3.

prefix

(Facultatif) Préfixe (hiérarchie logique) pour le compartiment. Le préfixe que vous spécifiez ne doit pas inclure la chaîne `AWSLogs`. Pour plus d'informations, consultez Organisation des objets à l'aide de préfixes.

`AWSLogs`

Nous ajoutons la partie du nom de fichier commençant par `AWSLogs` après le nom du compartiment et le préfixe facultatif que vous avez spécifié.

aws-account-id

L'identifiant du AWS compte 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-name

Le nom de l'équilibreur de charge.

end-time

Date et heure auxquelles l'intervalle de journalisation a pris fin. Par exemple, une heure de fin de 20140215T2340Z contient des entrées pour les demandes effectuées entre 23 h 35 et 23 h 40, si l'intervalle de publication est de 5 minutes.

ip-address

Adresse IP du nœud d'équilibreur de charge qui a traité la demande. Pour un équilibreur de charge, il s'agit d'une adresse IP privée.

random-string

Chaîne aléatoire générée par le système.

Voici un exemple de nom de fichier journal avec un préfixe « my-app » :

```
s3://my-loadbalancer-logs/my-app/AWSLogs/123456789012/elasticloadbalancing/
us-west-2/2018/02/15/123456789012_elasticloadbalancing_us-west-2_my-
loadbalancer_20180215T2340Z_172.160.001.192_20sg8hgm.log
```

Voici un exemple de nom de fichier journal sans préfixe :

```
s3://my-loadbalancer-logs/AWSLogs/123456789012/elasticloadbalancing/
us-west-2/2018/02/15/123456789012_elasticloadbalancing_us-west-2_my-
loadbalancer_20180215T2340Z_172.160.001.192_20sg8hgm.log
```

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, consultez la section Gestion du cycle de vie des objets dans le Guide de l'utilisateur Amazon Simple Storage Service.

Entrées des journaux d'accès

Elastic Load Balancing consigne toutes les demandes envoyées à l'équilibreur de charge, y compris celles qui ne sont jamais parvenues aux instances principales. Par exemple, si un client envoie une demande incorrecte ou qu'il n'existe aucune instance saine pour répondre, les demandes sont quand-même consignées.

> **Important**
>
> Elastic Load Balancing consigne les demandes dans la mesure du possible. Il est recommandé d'utiliser les journaux d'accès pour comprendre la nature des demandes, et non comme comptabilisation complète de toutes les demandes.

Syntaxe

Chaque entrée contient les détails d'une seule demande adressée à l'équilibreur de charge. Tous les champs de l'entrée de journal sont séparés par des espaces. Chaque entrée du fichier journal a le format suivant :

```
timestamp elb client:port backend:port request_processing_time backend_processing_time
 response_processing_time elb_status_code backend_status_code received_bytes sent_bytes
 "request" "user_agent" ssl_cipher ssl_protocol
```

Le tableau suivant décrit les champs d'une entrée de journal d'accès.

Champ	Description
time	Date et heure auxquelles l'équilibreur de charge a reçu les demandes, au format ISO 8601.
elb	Nom de l'équilibreur de charge
client:port	Adresse IP et port du client demandeur.
backend:port	Adresse IP et port de l'instance enregistrée qui a traité cette demande. Si l'équilibreur de charge ne peut pas envoyer la demande à une instance enregistrée, ou si l'instance ferme la connexion avant qu'une réponse puisse être envoyée, cette valeur est définie sur `-`. Cette valeur peut également être définie sur `-` si l'instance enregistrée ne répond pas avant le délai d'inactivité.
request_processing_time	[Écouteur HTTP] Durée totale écoulée, en secondes, du moment où l'équilibreur de charge a reçu la demande au moment où il l'a envoyée à une instance enregistrée. [Écouteur TCP] Durée totale écoulée, en secondes, du moment où l'équilibreur de charge a accepté une connexion TCP/SSL à partir d'un client au moment où il envoie le premier octet de données à une instance enregistrée. Cette valeur est définie sur `-1` si l'équilibreur de charge ne peut pas envoyer la demande à une instance enregistrée. Cela peut se produire si l'instance enregistrée ferme la connexion avant la fin du délai d'inactivité ou si le client envoie une demande incorrecte. En outre, pour les auditeurs TCP, cela peut se produire si le client établit une connexion avec l'équilibreur de charge, mais n'envoie pas de données. Cette valeur peut également être définie sur `-1` si l'instance enregistrée ne répond pas avant le délai d'inactivité.
backend_processing_time	[Écouteur HTTP] Durée totale écoulée, en secondes, du moment où l'équilibreur de charge a envoyé la demande à une instance enregistr

Champ	Description
	ée au moment où l'instance a commencé à envoyer les en-têtes de réponse. [Écouteur TCP] Délai total, en secondes, avant que l'équilibreur de charge parvienne à établir une connexion à une instance enregistrée. Cette valeur est définie sur `-1` si l'équilibreur de charge ne peut pas envoyer la demande à une instance enregistrée. Cela peut se produire si l'instance enregistrée ferme la connexion avant la fin du délai d'inactivité ou si le client envoie une demande incorrecte. Cette valeur peut également être définie sur `-1` si l'instance enregistrée ne répond pas avant le délai d'inactivité.
response_processing_time	[Écouteur HTTP] Durée totale écoulée (en secondes) du moment où l'équilibreur de charge a reçu l'en-tête de réponse de l'instance enregistrée au moment où il a commencé à envoyer la réponse au client. Cette durée inclut le temps en file d'attente sur l'équilibreur de charge et le temps d'acquisition de la connexion entre l'équilibreur de charge et le client. [Écouteur TCP] Durée totale écoulée (en secondes) du moment où l'équilibreur de charge a reçu le premier octet de l'instance enregistrée au moment où il a commencé à envoyer la réponse au client. Cette valeur est définie sur `-1` si l'équilibreur de charge ne peut pas envoyer la demande à une instance enregistrée. Cela peut se produire si l'instance enregistrée ferme la connexion avant la fin du délai d'inactivité ou si le client envoie une demande incorrecte. Cette valeur peut également être définie sur `-1` si l'instance enregistrée ne répond pas avant le délai d'inactivité.
elb_status_code	[Écouteur HTTP] Code d'état de la réponse de l'équilibreur de charge.
backend_status_code	[Écouteur HTTP] Code d'état de la réponse de l'instance enregistrée.

Champ	Description
received_bytes	Taille de la demande, en octets, reçue du client (demandeur). [Écouteur HTTP] La valeur inclut le corps de la demande, mais pas les en-têtes. [Écouteur TCP] La valeur inclut le corps de la demande et les en-têtes.
sent_bytes	Taille de la réponse, en octets, envoyée au client (demandeur). [Écouteur HTTP] La valeur inclut le corps de la réponse, mais pas les en-têtes. [Ecouteur TCP] La valeur inclut le corps de la demande et les en-têtes.
de la demande	Ligne de demande du client placée entre guillemets et consignée au format suivant : Méthode HTTP + Protocole://en-tête hôte:port + Chemin + Version HTTP. L'équilibreur de charge conserve en l'état l'URL envoyée par le client lors de l'enregistrement de l'URI de la demande. Il ne définit pas le type de contenu pour le fichier journal d'accès. Lorsque vous traitez ce champ, tenez compte de la façon dont le client a envoyé l'URL. [Écouteur TCP] L'URL est constituée de trois tirets, séparés par un espace, et se termine par un espace (« --- »).
user_agent	[Écouteur HTTP/HTTPS] Chaîne Agent utilisateur qui identifie le client qui a envoyé la demande. La chaîne se compose d'un ou plusieurs identificateurs, et du produit/[version]. Si la chaîne dépasse 8 Ko, elle est tronquée.
ssl_cipher	[Écouteur HTTPS/SSL] Chiffrement SSL. Cette valeur est enregistrée uniquement si la connexion SSL/TLS entrante a été établie après une négociation réussie. Sinon, la valeur est définie sur -.
ssl_protocol	[Écouteur HTTPS/SSL] Protocole SSL. Cette valeur est enregistrée uniquement si la connexion SSL/TLS entrante a été établie après une négociation réussie. Sinon, la valeur est définie sur -.

Exemples

Exemple d'entrée HTTP

Voici un exemple d'entrée de journal pour un écouteur HTTP (port 80 vers port 80) :

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.000073
 0.001048 0.000057 200 200 0 29 "GET http://www.example.com:80/ HTTP/1.1" "curl/7.38.0"
 - -
```

Exemple d'entrée HTTPS

Voici un exemple d'entrée de journal pour un écouteur HTTPS (port 443 vers port 80) :

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80
 0.000086 0.001048 0.001337 200 200 0 57 "GET https://www.example.com:443/ HTTP/1.1"
 "curl/7.38.0" DHE-RSA-AES128-SHA TLSv1.2
```

Exemple d'entrée TCP

Voici un exemple d'entrée de journal pour un écouteur TCP (port 8080 vers port 80) :

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.001069
 0.000028 0.000041 - - 82 305 "- - - " "-" - -
```

Exemple d'entrée SSL

Voici un exemple d'entrée de journal pour un écouteur SSL (port 8443 vers port 80) :

```
2015-05-13T23:39:43.945958Z my-loadbalancer 192.168.131.39:2817 10.0.0.1:80 0.001065
 0.000015 0.000023 - - 57 502 "- - - " "-" ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2
```

Traitement des journaux d'accès

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 de plus amples d'informations, consultez Interrogation des journaux Classic Load Balancer dans le Guide de l'utilisateur Amazon Athena.
- Loggly
- Splunk
- Sumo Logic

Activer les journaux d'accès pour votre Classic Load Balancer

Pour activer les journaux d'accès pour votre équilibreur de charge, vous devez spécifier le nom du compartiment Amazon S3 dans lequel l'équilibreur de charge stockera les journaux. Vous devez également attacher une politique de compartiment à ce compartiment, laquelle accorde à Elastic Load Balancing l'autorisation d'écrire dans le compartiment.

Tâches

- Étape 1 : Créer un compartiment S3
- Étape 2 : Attacher une politique à votre compartiment S3
- Étape 3 : configurer des journaux d'accès
- Étape 4 : vérifier les autorisations du compartiment
- Résolution des problèmes

Étape 1 : Créer un compartiment S3

Lorsque vous activez les journaux d'accès, vous devez spécifier un compartiment S3 pour les fichiers de journaux d'accès. Le compartiment doit répondre aux critères suivants :

Prérequis

- Le compartiment doit se situer dans la même région que l'équilibreur de charge. Le compartiment et l'équilibreur de charge peuvent être détenus par des comptes différents.
- La seule option de chiffrement côté serveur qui soit prise en charge est celle des clés gérées par Amazon S3 (SSE-S3). Pour plus d'informations, veuillez consulter la rubrique Clés de chiffrement gérées par Amazon S3 (SSE-S3).

Pour créer un compartiment S3 vide à l'aide de la console Amazon S3

1. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.
2. Choisissez Créer un compartiment.
3. Sur la page Créer un compartiment, procédez de la façon suivante :

   a. Pour Nom du compartiment, saisissez le nom de votre compartiment. Ce nom doit être unique parmi tous les noms de compartiment existants dans Amazon S3. Dans certaines régions, des restrictions supplémentaires peuvent être appliquées aux noms de compartiment. Pour de plus amples informations, consultez Limites et restrictions applicables aux compartiments dans le Guide de l'utilisateur Amazon Simple Storage Service.

   b. Pour AWS Region (Région), sélectionnez la région où vous avez créé votre équilibreur de charge.

   c. Pour le chiffrement par défaut, choisissez des clés gérées par Amazon S3 (SSE-S3).

   d. Choisissez Créer un compartiment.

Étape 2 : Attacher une politique à votre compartiment S3

Votre compartiment S3 doit avoir une politique de compartiment qui accorde à Elastic Load Balancing l'autorisation d'écrire les journaux d'accès dans le 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. Chaque instruction comporte des informations relatives à une seule autorisation et contient une série d'éléments.

Si vous utilisez un compartiment existant qui comporte déjà une politique attachée, vous pouvez ajouter la déclaration pour le journaux d'accès Elastic Load Balancing à la politique. Si vous procédez ainsi, nous vous recommandons d'évaluer l'ensemble d'autorisations résultant pour vous s'assurer que celles-ci sont appropriées pour les utilisateurs qui ont besoin d'accéder au compartiment pour trouver des journaux d'accès.

Stratégies de compartiment disponibles

La politique de compartiment que vous allez utiliser dépend Région AWS du compartiment.

Régions disponibles à partir d'août 2022 ou ultérieurement

Cette politique accorde des autorisations au service de livraison de journaux spécifié. Utilisez cette politique pour les équilibreurs de charge dans les zones de disponibilité et les zones locales des régions suivantes :

- Asie-Pacifique (Hyderabad)
- Asie-Pacifique (Melbourne)
- Canada Ouest (Calgary)
- Europe (Espagne)
- Europe (Zurich)
- Israël (Tel Aviv)
- Moyen-Orient (EAU)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::bucket-name/prefix/AWSLogs/aws-account-id/*"
    }
  ]
}
```

Régions disponibles avant août 2022

Cette politique accorde des autorisations à l'ID de compte Elastic Load Balancing spécifié. Utilisez cette politique pour les équilibreurs de charge dans les zones de disponibilité ou les zones locales des régions de la liste ci-dessous.

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

```
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "my-s3-arn"
    }
  ]
}
```

Remplacez *elb-account-id* par l'ID du Compte AWS Elastic Load Balancing pour votre région :

- USA Est (Virginie du Nord) : 127311923021
- USA Est (Ohio) : 033677994240
- USA Ouest (Californie du Nord) : 027434742980
- USA Ouest (Oregon) : 797873946194
- Afrique (Le Cap) : 098369216593
- Asie-Pacifique (Hong Kong) : 754344448648
- Asie-Pacifique (DJakarta) – 589379963580
- Asie-Pacifique (Mumbai) : 718504428378
- Asie-Pacifique (Osaka) : 383597477331
- Asie-Pacifique (Séoul) : 600734575887
- Asie-Pacifique (Singapour) : 114774131450
- Asie-Pacifique (Sydney) : 783225319266
- Asie-Pacifique (Tokyo) : 582318560864
- Canada (Centre) : 985666609251
- Europe (Francfort) : 054676820928
- Europe (Irlande) : 156460612806
- Europe (Londres) : 652711504416
- Europe (Milan) : 635631232127
- Europe (Paris) : 009996457667
- Europe (Stockholm) : 897822967062
- Moyen-Orient (Bahreïn) : 076674570225

- Amérique du Sud (São Paulo) : 507241528517

Remplacez *my-s3-arn* par l'ARN de l'emplacement de vos journaux d'accès. L'ARN que vous spécifiez dépend de votre intention de spécifier ou non un préfixe lorsque vous activez les journaux d'accès à l'étape 3.

- Exemple d'ARN avec un préfixe

```
arn:aws:s3:::bucket-name/prefix/AWSLogs/aws-account-id/*
```

- Exemple d'ARN sans préfixe

```
arn:aws:s3:::bucket-name/AWSLogs/aws-account-id/*
```

AWS GovCloud (US) Regions

Cette politique accorde des autorisations à l'ID de compte Elastic Load Balancing spécifié. Utilisez cette politique pour les équilibreurs de charge situés dans les zones de disponibilité ou les zones locales des AWS GovCloud (US) régions de la liste ci-dessous.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws-us-gov:iam::elb-account-id:root"
      },
      "Action": "s3:PutObject",
      "Resource": "my-s3-arn"
    }
  ]
}
```

Remplacez *elb-account-id*par l'ID du Compte AWS Elastic Load Balancing pour votre Compte AWS région :

- AWS GovCloud (US-Ouest) — 048591011584
- AWS GovCloud (USA Est) — 190560391635

Remplacez *my-s3-arn* par l'ARN de l'emplacement de vos journaux d'accès. L'ARN que vous spécifiez dépend de votre intention de spécifier ou non un préfixe lorsque vous activez les journaux d'accès à l'étape 3.

- Exemple d'ARN avec un préfixe

```
arn:aws-us-gov:s3:::bucket-name/prefix/AWSLogs/aws-account-id/*
```

- Exemple d'ARN sans préfixe

```
arn:aws-us-gov:s3:::bucket-name/AWSLogs/aws-account-id/*
```

Pour associer une politique de compartiment de journaux d'accès à votre compartiment à l'aide de la console Amazon S3

1. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.
2. Sélectionnez le nom du compartiment pour ouvrir sa page de détails.
3. Choisissez Permissions (Autorisations), Bucket policy (Politique de compartiment), puis Edit (Modifier).
4. Mettez à jour la politique de compartiment pour accorder les autorisations requises.
5. Sélectionnez Enregistrer les modifications.

Étape 3 : configurer des journaux d'accès

Utilisez la procédure suivante pour configurer des journaux d'accès afin de capturer et de diffuser des fichiers journaux vers votre compartiment S3.

Prérequis

Le compartiment doit répondre aux exigences décrites à l'étape 1 et vous devez y associer une politique de compartiment comme décrit à l'étape 2. Si vous spécifiez un préfixe, celui-ci ne doit pas inclure la chaîne « AWSLogs ».

Pour configurer les journaux d'accès pour 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 panneau de navigation, sous Load Balancing (Équilibrage de charge), choisissez Load Balancers (Équilibreurs de charge).

3. Sélectionnez le nom de votre équilibreur de charge afin d'ouvrir sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sur la page Edit load balancer attributes, dans la section Monitoring, procédez comme suit :

   a. Activer Access logs.

   b. Pour S3 URI, saisissez l'URI S3 de vos fichiers journaux. L'URI que vous spécifiez varie selon que vous utilisez ou non un préfixe.

      - URI avec un préfixe : `s3://bucket-name/prefix`
      - URI sans préfixe : `s3://bucket-name`

   c. Conservez Logging interval à `60 minutes - default`.

   d. Sélectionnez Enregistrer les modifications.

Pour configurer les journaux d'accès pour votre équilibreur de charge à l'aide du AWS CLI

Commencez par créer un fichier .json qui permet à Elastic Load Balancing de capturer et fournir des journaux de toutes les 60 minutes au compartiment S3 que vous avez créé pour les journaux :

```
{
  "AccessLog": {
    "Enabled": true,
    "S3BucketName": "my-loadbalancer-logs",
    "EmitInterval": 60,
    "S3BucketPrefix": "my-app"
  }
}
```

Spécifiez ensuite le fichier .json dans la modify-load-balancer-attributescommande comme suit :

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-
balancer-attributes file://my-json-file.json
```

Voici un exemple de réponse.

```
{
    "LoadBalancerAttributes": {
        "AccessLog": {
            "Enabled": true,
```

```
            "EmitInterval": 60,
            "S3BucketName": "my-loadbalancer-logs",
            "S3BucketPrefix": "my-app"
        }
    },
    "LoadBalancerName": "my-loadbalancer"
}
```

Pour gérer le compartiment S3 pour vos journaux d'accès

Assurez-vous de désactiver les journaux d'accès avant de supprimer le compartiment que vous avez configuré pour ces derniers. Sinon, si un nouveau bucket portant le même nom et la politique de bucket requise est créé dans un compartiment Compte AWS dont vous n'êtes pas le propriétaire, Elastic Load Balancing pourrait écrire les journaux d'accès à votre équilibreur de charge dans ce nouveau bucket.

Étape 4 : vérifier les autorisations du compartiment

Une fois que les journaux d'accès sont activés pour votre équilibreur de charge, Elastic Load Balancing valide le compartiment S3 et crée un fichier de test pour s'assurer que la politique de compartiment spécifie les autorisations requises. Vous pouvez utiliser la console S3 pour vérifier que le fichier test a été créé. Le fichier test n'est pas un fichier journal d'accès réel ; il ne contient pas de modèles d'enregistrement.

Pour vérifier qu'Elastic Load Balancing a créé un fichier test dans votre compartiment S3

1. Ouvrez la console Amazon S3 sur https://console.aws.amazon.com/s3/.
2. Sélectionnez le nom du compartiment S3 que vous avez spécifié pour les journaux d'accès.
3. Accédez au fichier test, `ELBAccessLogTestFile`. L'emplacement varie selon que vous utilisez ou non un préfixe.
   - Emplacement avec un préfixe : *`my-bucket`*`/`*`prefix`*`/AWSLogs/`*`123456789012`*`/ELBAccessLogTestFile`
   - Emplacement sans préfixe : *`my-bucket`*`/AWSLogs/`*`123456789012`*`/ELBAccessLogTestFile`

Résolution des problèmes

Accès refusé pour le compartiment : ***bucket-name***. Veuillez vérifier l'autorisation de S3bucket

Si vous recevez une erreur, les éléments suivants sont des causes possibles :

- La politique de compartiment n'accorde pas à Elastic Load Balancing l'autorisation d'écrire des journaux d'accès dans le compartiment. Vérifiez que vous utilisez la bonne politique en matière de compartiments pour la région. Vérifiez que l'ARN de la ressource utilise le même nom de compartiment que celui que vous avez spécifié lorsque vous avez activé les journaux d'accès. Vérifiez que l'ARN de la ressource n'inclut pas de préfixe si vous n'en avez pas spécifié lorsque vous avez activé les journaux d'accès.
- Le compartiment utilise une option de chiffrement côté serveur non prise en charge. Le compartiment doit utiliser des clés gérées par Amazon S3 (SSE-S3).

Désactiver les journaux d'accès pour votre Classic Load Balancer

Vous pouvez désactiver les journaux d'accès pour votre équilibreur de charge à tout moment. Après avoir désactivé les journaux d'accès, ces derniers restent dans votre compartiment Amazon S3 jusqu'à ce que vous les supprimiez. Pour plus d'informations sur la gestion d'un compartiment S3, consultez la section Utilisation des compartiments dans le Guide de l'utilisateur Amazon Simple Storage Service.

Pour désactiver les journaux d'accès pour 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 panneau de navigation, sous Load Balancing (Équilibrage de charge), choisissez Load Balancers (Équilibreurs de charge).
3. Sélectionnez le nom de votre équilibreur de charge afin d'ouvrir sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sur la page Edit load balancer attributes, dans la section Monitoring, désactiver Access logs.

Pour désactiver les journaux d'accès à l'aide du AWS CLI

Utilisez la modify-load-balancer-attributescommande suivante pour désactiver les journaux d'accès :

```
aws elb modify-load-balancer-attributes --load-balancer-name my-loadbalancer --load-
balancer-attributes "{\"AccessLog\":{\"Enabled\":false}}"
```

Voici un exemple de réponse :

```
{
    "LoadBalancerName": "my-loadbalancer",
    "LoadBalancerAttributes": {
        "AccessLog": {
            "S3BucketName": "my-loadbalancer-logs",
            "EmitInterval": 60,
            "Enabled": false,
            "S3BucketPrefix": "my-app"
        }
    }
}
```

Journalisation des appels d'API pour votre Classic Load Balancer à l'aide de AWS CloudTrail

Elastic Load Balancing est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Elastic Load Balancing. CloudTrail capture tous les 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.

Pour surveiller d'autres actions pour votre équilibreur de charge, par exemple, quand un client exécute une demande vers votre équilibreur de charge, utilisez les journaux d'accès. Pour plus d’informations, consultez Journaux d'accès pour votre Classic Load Balancer.

Informations sur Elastic Load Balancing dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans Elastic Load Balancing, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez afficher, 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 de votre AWS compte, y compris ceux relatifs à Elastic Load Balancing, créez un historique. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à toutes les AWS régions. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

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

Toutes les actions Elastic Load Balancing pour les Classic Load Balancers sont enregistrées CloudTrail et documentées dans la version 2012-06-01 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 demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

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 inclut 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 des événements pour tous les appels d' AWS API pour votre AWS compte, et pas uniquement pour les appels d'API 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 Classic 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": "AIDAJDPLRKLG7UEXAMPLE",
        "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 botocore/1.4.1",
    "requestParameters": {
        "subnets": ["subnet-12345678","subnet-76543210"],
        "loadBalancerName": "my-load-balancer",
        "listeners": [{
           "protocol": "HTTP",
           "loadBalancerPort": 80,
           "instanceProtocol": "HTTP",
           "instancePort": 80
        }]
    },
    "responseElements": {
        "dNSName": "my-loadbalancer-1234567890.elb.amazonaws.com"
    },
    "requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
    "eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2012-06-01",
    "recipientAccountId": "123456789012"
}
```

Example Exemple : DeleteLoadBalancer

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJDPLRKLG7UEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-08T12:39:25Z",
    "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 botocore/1.4.1",
    "requestParameters": {
        "loadBalancerName": "my-load-balancer"
    },
    "responseElements": null,
```

```
    "requestID": "f0f17bb6-b9ba-11e3-9b20-999fdEXAMPLE",
    "eventID": "4f99f0e8-5cf8-4c30-b6da-3b69fEXAMPLE"
    "eventType": "AwsApiCall",
    "apiVersion": "2012-06-01",
    "recipientAccountId": "123456789012"
}
```

Résoudre les problèmes liés à votre Classic Load Balancer

Les tableaux suivants répertorient les ressources de résolution des problèmes qui pourront vous être utiles lors de l'utilisation d'un Classic Load Balancer.

Erreurs d'API

Erreur
CertificateNotTrouvé : Non défini
OutofService: une erreur passagère s'est produite

Erreurs HTTP

Erreur
HTTP 400 : BAD_REQUEST
HTTP 405 : METHOD_NOT_ALLOWED
HTTP 408 : Délai d'attente des demandes
HTTP 502 : Passerelle erronée
HTTP 503 : Service indisponible
HTTP 504 : Délai de passerelle expiré

Métriques de code de réponse

Métrique de code de réponse
HTTPCode_ELB_4XX
HTTPCode_ELB_5XX
HTTPCode_Backend_2XX

Métrique de code de réponse
HTTPCode_Backend_3XX
HTTPCode_Backend_4XX
HTTPCode_Backend_5XX

Problèmes de surveillance de l'état

Problème
Erreur de page cible de vérification de l'état
La connexion aux instances a expiré
L'authentification par clé publique échoue
L'instance ne reçoit pas le trafic provenant de l'équilibreur de charge
Des ports sur l'instance ne sont pas ouverts
Les instances d'un groupe Auto Scaling ne réussissent pas la surveillance de l'état ELB

Problèmes de connectivité

Problème
Les clients ne peuvent pas se connecter à un équilibreur de charge accessible sur Internet
Les requêtes envoyées à un domaine personnalisé ne sont pas reçues par l'équilibreur de charge
Les requêtes HTTPS envoyées à l'équilibreur de charge renvoient « NET::ERR_CERT_COMMON_NAME_INVALID »

Problèmes d'enregistrement d'instance

Problème
L'enregistrement d'une instance EC2 prend trop de temps
Impossible d'enregistrer une instance lancée à partir d'une AMI payante

Résoudre les problèmes liés à un Classic Load Balancer : erreurs d'API

Voici des messages d'erreur renvoyés par l'API Elastic Load Balancing, les causes potentielles et les étapes que vous pouvez suivre pour résoudre les problèmes.

Messages d'erreur

- CertificateNotTrouvé : Non défini
- OutofService: une erreur passagère s'est produite

CertificateNotTrouvé : Non défini

Cause 1 : la propagation du certificat vers toutes les Régions est retardée lorsque ce certificat est créé à l'aide de la AWS Management Console. Lorsque ce retard a lieu, le message d'erreur apparaît lors de la dernière étape du processus de création de l'équilibreur de charge.

Solution 1 : attendez environ 15 minutes, puis réessayez. Si le problème persiste, accédez au Centre AWS Support pour obtenir de l'aide.

Cause 2 : Si vous utilisez directement l'API AWS CLI or, vous pouvez recevoir cette erreur si vous fournissez un Amazon Resource Name (ARN) pour un certificat qui n'existe pas.

Solution 2 : utilisez l'action AWS Identity and Access Management (IAM) GetServerCertificate pour obtenir l'ARN du certificat et vérifier que vous avez fourni la bonne valeur pour l'ARN.

OutofService: une erreur passagère s'est produite

Cause : un problème interne temporaire s'est produit au sein du service Elastic Load Balancing ou du réseau sous-jacent. Ce problème temporaire peut également se produire lorsqu'Elastic Load

Balancing interroge l'état de santé de l'équilibreur de charge et des instances enregistrées de ce dernier.

Solution : relancez l'appel d'API. Si le problème persiste, accédez au Centre AWS Support pour obtenir de l'aide.

Résoudre les problèmes liés à un Classic Load Balancer : erreurs HTTP

La méthode HTTP (également appelée verbe) spécifie l'action à exécuter sur la ressource qui reçoit une demande HTTP. Les méthodes standard pour les demandes HTTP sont définies dans la section du RFC 2616 concernant les définitions de méthode. Les méthodes standard incluent GET, POST, PUT, HEAD et OPTIONS. Certaines applications web ont besoin (et parfois introduisent) de méthodes qui sont des extensions de méthodes HTTP/1.1. Les exemples courants de méthodes étendues HTTP incluent PATCH, REPORT, MKCOL, PROPFIND, MOVE et LOCK. Elastic Load Balancing accepte toutes les méthodes HTTP standard et non standard.

Les demandes et les réponses HTTP utilisent des champs d'en-tête pour envoyer des informations concernant les messages HTTP. Les champs d'en-tête sont des paires nom-valeur dont les noms et les valeurs sont séparés par un signe deux points, et qui sont séparées entre elles par un retour chariot (CR) et un saut de ligne (LF). Un ensemble standard de champs d'en-tête HTTP est défini dans la section du RFC 2616 concernant les en-têtes de message. Pour plus d’informations, consultez En-têtes HTTP et Classic Load Balancers.

Lorsqu'un équilibreur de charge reçoit une demande HTTP, il vérifie que cette dernière est correcte et contrôle la longueur de la méthode. La longueur totale de la méthode dans une demande HTTP vers un équilibreur de charge ne doit pas dépasser 127 caractères. Si la demande HTTP réussit les deux contrôles, l'équilibreur de charge l'envoie à l'instance EC2. Si le champ de méthode de la demande est incorrect, l'équilibreur de charge répond par une erreur HTTP 400 : BAD_REQUEST. Si la longueur de la méthode dans la demande dépasse 127 caractères, l'équilibreur de charge répond par une erreur HTTP 405 : METHOD_NOT_ALLOWED.

L'instance EC2 traite une demande valide en implémentant la méthode dans la demande et en envoyant une réponse au client. Vos instances doivent être configurées pour traiter les méthodes prises en charge et non prises en charge.

Voici des messages d'erreur renvoyés par votre équilibreur de charge, les causes potentielles et les étapes que vous pouvez suivre pour résoudre les problèmes.

Messages d'erreur

- HTTP 400 : BAD_REQUEST
- HTTP 405 : METHOD_NOT_ALLOWED
- HTTP 408 : Délai d'attente des demandes
- HTTP 502 : Passerelle erronée
- HTTP 503 : Service indisponible
- HTTP 504 : Délai de passerelle expiré

HTTP 400 : BAD_REQUEST

Description : indique que le client a envoyé une demande incorrecte.

Cause 1 : le client a envoyé une demande incorrecte qui ne respecte pas les spécifications HTTP. Par exemple, une demande ne peut pas comporter d'espace dans l'URL.

Cause 2 : le client utilise la méthode HTTP CONNECT, qui n'est pas prise en charge par Elastic Load Balancing.

Solution : connectez-vous directement à votre instance et saisissez les détails de la demande du client. Vérifiez que les demandes sont correctes dans les en-têtes et l'URL. Vérifiez que la demande respecte les spécifications HTTP. Vérifiez que la méthode HTTP CONNECT n'est pas utilisés.

HTTP 405 : METHOD_NOT_ALLOWED

Description : indique que la longueur de la méthode n'est pas valide.

Cause : la longueur de la méthode dans l'en-tête de la demande dépasse 127 caractères.

Solution : vérifiez la longueur de la méthode.

HTTP 408 : Délai d'attente des demandes

Description : indique que le client a annulé la demande ou n'a pas pu envoyer une demande complète.

Cause 1 : une interruption du réseau ou une structure de demande incorrecte, comme des en-têtes partiellement formés, une taille de contenu spécifiée ne correspondant pas à la taille de contenu réelle transmise, etc.

Solution 1 : inspectez le code qui constitue la demande et essayez de l'envoyer directement à vos instances enregistrées (ou à un environnement de développement/test) où vous aurez plus de contrôle pour examiner la demande réelle.

Cause 2 : la connexion au client est fermée (l'équilibreur de charge n'a pas pu envoyer une réponse)

Solution 2 : vérifiez que le client ne ferme pas la connexion avant l'envoi d'une réponse en utilisant un renifleur de paquets sur la machine sur laquelle vous effectuez la demande.

HTTP 502 : Passerelle erronée

Description : indique que l'équilibreur de charge n'a pas pu analyser la réponse envoyée à partir d'une instance enregistrée.

Cause : réponse incorrecte d'une instance ou problème éventuel lié à l'équilibreur de charge.

Solution : vérifiez que la réponse envoyée à partir de l'instance est conforme aux spécifications HTTP. Accédez au Centre AWS Support pour obtenir de l'aide.

HTTP 503 : Service indisponible

Description : indique que l'équilibreur de charge ou les instances enregistrées sont à l'origine de l'erreur.

Cause 1 : capacité insuffisante dans l'équilibreur de charge pour traiter la demande.

Solution 1 : il doit s'agir d'un problème temporaire qui ne devrait pas durer plus de quelques minutes. Si le problème persiste, accédez au Centre AWS Support pour obtenir de l'aide.

Cause 2 : aucune instance n'est enregistrée.

Solution 2 : enregistrez au moins une instance dans chaque zone de disponibilité dans laquelle votre équilibreur de charge est configuré pour répondre. Vérifiez cela en consultant les `HealthyHostCount` indicateurs contenus dans CloudWatch. Si vous ne pouvez pas vérifier qu'une instance est enregistrée dans chaque zone de disponibilité, nous vous recommandons d'activer l'équilibrage de charge entre zones. Pour plus d’informations, consultez Configurer la répartition de charge entre zones pour votre Classic Load Balancer.

Cause 3 : il n'y a aucune instance saine.

Solution 3 : vérifiez que vous avez des instances saines dans chaque zone de disponibilité dans laquelle votre équilibreur de charge est configuré pour répondre. Vérifiez ceci en examinant la métrique `HealthyHostCount`.

Cause 4 : la file d'attente des hausses est saturée.

Solution 4 : assurez-vous que vos instances ont une capacité suffisante pour gérer le taux de demandes. Vérifiez ceci en examinant la métrique `SpilloverCount`.

HTTP 504 : Délai de passerelle expiré

Description : indique que l'équilibreur de charge a fermé une connexion parce qu'une demande ne s'est pas achevée avant la fin du délai d'inactivité.

Cause 1 : le délai de réponse de l'application est supérieur au délai d'inactivité configuré.

Solution 1 : surveillez les métriques `HTTPCode_ELB_5XX` et `Latency`. Si ces métriques augmentent, cela peut être dû au fait que l'application ne répond pas avant la fin du délai d'inactivité. Pour plus d'informations sur les demandes qui dépassent le délai imparti, activez les journaux d'accès sur l'équilibreur de charge et vérifiez les codes de réponse 504 dans les journaux générés par Elastic Load Balancing. Si nécessaire, vous pouvez augmenter votre capacité ou le délai d'inactivité configuré afin que les opérations longues (par exemple, le chargement d'un fichier volumineux) puissent se terminer. Pour plus d'informations, consultez Configurer le délai d'inactivité des connexions de votre Classic Load Balancer et Comment résoudre les problèmes de latence élevée liés à Elastic Load Balancing.

Cause 2 : des instances enregistrées ferment la connexion à Elastic Load Balancing.

Solution 2 : activez les paramètres keep-alive sur vos instances EC2 et veillez à ce que le délai d'attente keep-alive ait une valeur supérieure ou égale aux paramètres de délai d'inactivité de votre équilibreur de charge.

Résoudre les problèmes liés à un Classic Load Balancer : métriques de code de réponse

Votre équilibreur de charge envoie des métriques à Amazon CloudWatch pour les codes de réponse HTTP envoyés aux clients, en identifiant la source des erreurs comme étant l'équilibreur de charge ou les instances enregistrées. Vous pouvez utiliser les métriques renvoyées par votre équilibreur de charge CloudWatch pour résoudre les problèmes. Pour plus d’informations, consultez CloudWatch statistiques pour votre Classic Load Balancer.

Vous trouverez ci-dessous les mesures du code de réponse renvoyées par CloudWatch votre équilibreur de charge, les causes potentielles et les mesures que vous pouvez prendre pour résoudre les problèmes.

Métriques de code de réponse

- HTTPCode_ELB_4XX
- HTTPCode_ELB_5XX
- HTTPCode_Backend_2XX
- HTTPCode_Backend_3XX
- HTTPCode_Backend_4XX
- HTTPCode_Backend_5XX

HTTPCode_ELB_4XX

Cause : demande incorrecte ou annulée par le client.

Solutions

- veuillez consulter HTTP 400 : BAD_REQUEST.
- veuillez consulter HTTP 405 : METHOD_NOT_ALLOWED.
- veuillez consulter HTTP 408 : Délai d'attente des demandes.

HTTPCode_ELB_5XX

Cause : l'équilibreur de charge ou l'instance enregistrée est à l'origine de l'erreur, ou l'équilibreur de charge ne peut pas analyser la réponse.

Solutions

- veuillez consulter HTTP 502 : Passerelle erronée.
- veuillez consulter HTTP 503 : Service indisponible.
- veuillez consulter HTTP 504 : Délai de passerelle expiré.

HTTPCode_Backend_2XX

Cause : réponse de réussite normale des instances enregistrées.

Solution : aucune.

HTTPCode_Backend_3XX

Cause : réponse de redirection envoyée par les instances enregistrées.

Solution : affichez les journaux d'accès ou d'erreurs sur votre instance afin de déterminer la cause. Envoyez les demandes directement à l'instance (sans passer par l'équilibreur de charge) pour afficher les réponses.

HTTPCode_Backend_4XX

Cause : réponse d'erreur de client envoyée par les instances enregistrées.

Solution : affichez les journaux d'accès ou d'erreurs sur vos instances afin de déterminer la cause. Envoyez les demandes directement à l'instance (sans passer par l'équilibreur de charge) pour afficher les réponses.

> **Note**
>
> Si le client annule une demande HTTP qui a été lancée avec un en-tête `Transfer-Encoding: chunked`, un problème connu a lieu avec lequel l'équilibreur de charge transmet la demande à l'instance, même si le client a annulé à la demande. Cela peut entraîner des erreurs de serveur backend.

HTTPCode_Backend_5XX

Cause : réponse d'erreur de serveur envoyée par les instances enregistrées.

Solution : affichez les journaux d'accès ou les journaux d'erreurs sur vos instances afin de déterminer la cause. Envoyez les demandes directement à l'instance (sans passer par l'équilibreur de charge) pour afficher les réponses.

> **Note**
>
> Si le client annule une demande HTTP qui a été lancée avec un en-tête `Transfer-Encoding: chunked`, un problème connu a lieu avec lequel l'équilibreur de charge transmet la demande à l'instance, même si le client a annulé à la demande. Cela peut entraîner des erreurs de serveur backend.

Résoudre les problèmes liés à un Classic Load Balancer : surveillance de l'état de santé

Votre équilibreur de charge vérifie l'état de santé de ses instances enregistrées à l'aide de la configuration de surveillance de l'état par défaut fournie par Elastic Load Balancing ou d'une surveillance de l'état personnalisée que vous spécifiez. La configuration de la vérification de l'état contient des informations comme le protocole, le port de ping, le chemin de ping, le délai de réponse et l'intervalle de vérification de l'état. Une instance est considérée comme saine si elle retourne un code de réponse 200 dans l'intervalle de vérification de l'état. Pour plus d'informations, consultez Configurer les vérifications de l'état pour votre Classic Load Balancer.

Si l'état actuel de tout ou partie de vos instances est `OutOfService` et que le champ de description affiche le message `Instance has failed at least the Unhealthy Threshold number of health checks consecutively`, les instances n'ont pas réussi la vérification de l'état de l'équilibreur de charge. Voici les problèmes à rechercher, les causes potentielles et les étapes que vous pouvez suivre pour résoudre les problèmes.

Problèmes

- Erreur de page cible de vérification de l'état
- La connexion aux instances a expiré
- L'authentification par clé publique échoue
- L'instance ne reçoit pas le trafic provenant de l'équilibreur de charge
- Des ports sur l'instance ne sont pas ouverts
- Les instances d'un groupe Auto Scaling ne réussissent pas la surveillance de l'état ELB

Erreur de page cible de vérification de l'état

Problème : une demande HTTP GET envoyée à l'instance sur le port de ping et le chemin de ping spécifiés (par exemple, HTTP:80/index.html) reçoit un code de réponse autre que 200.

Cause 1 : aucune page cible n'est configurée sur l'instance.

Solution 1 : créez une page cible (par exemple, `index.html`) sur chaque instance enregistrée et spécifiez son chemin comme chemin de ping.

Cause 2 : la valeur de l'en-tête Content-Length dans la réponse n'est pas définie.

Solution 2 : si la réponse inclut un corps, définissez la valeur de l'en-tête Content-Length sur une valeur supérieure ou égale à zéro, ou définissez la valeur de Transfer-Encoding sur « chunked ».

Cause 3 : l'application n'est pas configurée pour recevoir des demandes de l'équilibreur de charge ou pour renvoyer un code de réponse 200.

Solution 3 : vérifiez l'application sur votre instance pour enquêter sur la cause.

La connexion aux instances a expiré

Problème : des demandes de vérification de l'état de votre équilibreur de charge à vos instances EC2 dépassent le délai imparti, ou échouent par intermittence.

Tout d'abord, vérifiez le problème en vous connectant directement à l'instance. Nous vous recommandons de vous connecter à votre instance à partir du réseau en utilisant l'adresse IP privée de l'instance.

Utilisez la commande suivante pour une connexion TCP :

```
telnet private-IP-address-of-the-instance port
```

Utilisez la commande suivante pour une connexion HTTP ou HTTPS :

```
curl -I private-IP-address-of-the-instance:port/health-check-target-page
```

Si vous utilisez une connexion HTTP/HTTPS et obtenez une réponse autre que 200, consultez Erreur de page cible de vérification de l'état. Si vous pouvez vous connecter directement à l'instance, vérifiez les points suivants :

Cause 1 : l'instance ne peut pas répondre dans le délai de réponse configuré.

Solution 1 : ajustez les paramètres de délai de réponse dans la configuration de vérification de l'état de votre équilibreur de charge.

Cause 2 : l'instance est soumise à une charge importante et dépasse votre délai de réponse configuré pour répondre.

Solution 2 :

- Vérifiez dans le graphique de surveillance si l'UC est sur-utilisée. Pour plus d'informations, consultez Obtenir des statistiques pour une instance EC2 spécifique dans le guide de l'utilisateur Amazon EC2.

- Vérifiez l'utilisation d'autres ressources d'application, comme la mémoire ou les limites en vous connectant à vos instances EC2.
- Si nécessaire, ajoutez des instances supplémentaires ou activez Auto Scaling. Pour plus d'informations, consultez le Guide de l'utilisateur Amazon EC2 Auto Scaling.

Cause 3 : si vous utilisez une connexion HTTP ou HTTPS et que la vérification de l'État est effectuée sur une page cible spécifiée dans le champ de chemin de ping (par exemple, `HTTP:80/index.html`), la page cible peut prendre plus de temps pour répondre que votre délai d'attente configuré.

Solution 3 : utilisez une page cible de vérification de l'état plus simple ou ajustez les paramètres d'intervalle de vérification de l'état.

L'authentification par clé publique échoue

Problème : un équilibreur de charge configuré pour utiliser le protocole HTTPS ou SSL avec l'authentification principale activée ne réussit pas l'authentification par clé publique.

Cause : la clé publique sur le certificat SSL ne correspond pas à la clé publique configurée sur l'équilibreur de charge. Utilisez la commande `s_client` pour afficher la liste des certificats de serveur dans la chaîne de certificats. Pour de plus amples informations, veuillez consulter s_client dans la documentation OpenSSL.

Solution : vous devez peut-être mettre à jour votre certificat SSL. Si votre certificat SSL est à jour, essayez de le réinstaller sur votre équilibreur de charge. Pour plus d'informations, consultez Remplacer le certificat SSL pour votre Classic Load Balancer.

L'instance ne reçoit pas le trafic provenant de l'équilibreur de charge

Problème : le groupe de sécurité pour l'instance bloque le trafic provenant de l'équilibreur de charge.

Effectuez une capture de paquet sur l'instance pour vérifier le problème. Utilisez la commande suivante :

```
# tcpdump port health-check-port
```

Cause 1 : le groupe de sécurité associé à l'instance n'autorise pas le trafic provenant de l'équilibreur de charge.

Solution 1 : modifiez le groupe de sécurité de l'instance pour autoriser le trafic provenant de l'équilibreur de charge. Ajoutez une règle pour autoriser tout le trafic à partir du groupe de sécurité de l'équilibreur de charge.

Cause 2 : le groupe de sécurité de votre équilibreur de charge dans un VPC n'autorise pas le trafic vers les instances EC2.

Solution 2 : modifiez le groupe de sécurité de votre équilibreur de charge pour autoriser le trafic vers les sous-réseaux et les instances EC2.

Pour plus d'informations sur la gestion des groupes de sécurité, consultez Groupes de sécurité pour les équilibreurs de charge dans un VPC.

Des ports sur l'instance ne sont pas ouverts

Problème : la vérification de l'état envoyée à l'instance EC2 par l'équilibreur de charge est bloquée par le port ou un pare-feu.

Vérifiez le problème en utilisant la commande suivante :

```
netstat –ant
```

Cause : le port de vérification de l'état ou le port d'écouteur spécifié (s'ils sont configurés différemment) n'est pas ouvert. Les ports spécifiés pour la vérification de l'état et le port d'écoute doivent être ouverts et à l'écoute.

Solution : ouvrez le port d'écoute et le port spécifié dans votre configuration de vérification de l'état (s'ils sont configurés différemment) sur vos instances pour recevoir le trafic de l'équilibreur de charge.

Les instances d'un groupe Auto Scaling ne réussissent pas la surveillance de l'état ELB

Problème : les instances de votre groupe Auto Scaling réussissent la surveillance de l'état Auto Scaling par défaut, mais pas la surveillance de l'état ELB.

Cause : Auto Scaling utilise des contrôles de statut EC2 afin de détecter les problèmes matériels et logiciels liés aux instances, mais l'équilibreur de charge effectue des vérifications de l'état en envoyant une demande à l'instance et en attendant un code de réponse 200 ou en établissant une connexion TCP (pour une vérification de l'état basée sur TCP) avec l'instance.

Une instance peut ne pas réussir la vérification de l'état ELB, parce qu'une application s'exécutant sur l'instance connaît des problèmes faisant que l'équilibreur de charge considère l'instance comme étant hors service. Cette instance peut réussir la vérification de l'état Auto Scaling. Elle ne sera pas remplacée par la politique Auto Scaling car elle est considérée comme saine selon le contrôle de statut EC2.

Solution : utilisez la surveillance de l'état ELB pour votre groupe Auto Scaling. Lorsque vous utilisez la surveillance de l'état ELB, Auto Scaling détermine l'état de santé de vos instances en vérifiant les résultats de la surveillance de l'état de l'instance et de la surveillance de l'état ELB. Pour plus d'informations, consultez Ajout de surveillances de l'état dans votre groupe Auto Scaling dans le manuel Guide de l'utilisateur Amazon EC2 Auto Scaling.

Résolution des problèmes liés à un Classic Load Balancer : connectivité client

Les clients ne peuvent pas se connecter à un équilibreur de charge accessible sur Internet

Si l'équilibreur de charge ne répond pas aux requêtes, vérifiez les points suivants :

Votre équilibreur de charge accessible sur Internet est attaché à un sous-réseau privé

- Vous devez spécifier des sous-réseaux publics pour votre équilibreur de charge. Un sous-réseau public dispose d'une route vers une passerelle Internet pour Virtual Private Cloud (VPC).

Un groupe de sécurité ou une liste ACL n'autorise pas le trafic

- Le groupe de sécurité de l'équilibreur de charge et toutes les listes ACL réseau des sous-réseaux de l'équilibreur de charge doivent autoriser le trafic entrant depuis les clients et le trafic sortant vers les clients sur les ports d'écoute. Pour plus d’informations, consultez Groupes de sécurité pour les équilibreurs de charge dans un VPC.

Les requêtes envoyées à un domaine personnalisé ne sont pas reçues par l'équilibreur de charge

Si l'équilibreur de charge ne reçoit pas les requêtes envoyées à un domaine personnalisé, vérifiez les points suivants :

Le nom de domaine personnalisé ne correspond pas à l'adresse IP de l'équilibreur de charge

- Confirmez l'adresse IP à laquelle le nom de domaine personnalisé correspond à l'aide d'une interface de ligne de commande.
  - Linux, macOS ou Unix : vous pouvez utiliser la commande `dig` dans Terminal. Par exemple, `dig example.com`
  - Windows : vous pouvez utiliser la commande `nslookup` dans Command Prompt. Par exemple, `nslookup example.com`
- Vérifiez à quelle adresse IP le nom DNS de l'équilibreur de charge correspond à l'aide d'une interface de ligne de commande.
- Comparez les résultats des deux sorties. Les adresses IP doivent correspondre.

Les requêtes HTTPS envoyées à l'équilibreur de charge renvoient « NET::ERR_CERT_COMMON_NAME_INVALID »

Si des requêtes HTTPS reçoivent `NET::ERR_CERT_COMMON_NAME_INVALID` de l'équilibreur de charge, vérifiez les causes possibles suivantes :

- Le nom de domaine utilisé dans la requête HTTPS ne correspond pas au nom alternatif spécifié dans le certificat ACM associé aux écouteurs.
- Le nom DNS par défaut de l'équilibreur de charge est utilisé. Le nom DNS par défaut ne peut pas être utilisé pour effectuer des requêtes HTTPS, car aucun certificat public ne peut être demandé pour le domaine `*.amazonaws.com`.

Résoudre les problèmes liés à un Classic Load Balancer : enregistrement d'instance

Lorsque vous enregistrez une instance auprès de votre équilibreur de charge, plusieurs étapes doivent être suivies avant que l'équilibreur de charge puisse commencer à envoyer des demandes à votre instance.

Voici les problèmes que votre équilibreur de charge peut rencontrer lors de l'enregistrement de vos instances EC2, les causes potentielles et les étapes que vous pouvez suivre pour résoudre les problèmes.

Problèmes

- L'enregistrement d'une instance EC2 prend trop de temps
- Impossible d'enregistrer une instance lancée à partir d'une AMI payante

L'enregistrement d'une instance EC2 prend trop de temps

Problème : il faut plus de temps que prévu pour que les instances EC2 enregistrées soient à l'état `InService`.

Cause : votre instance peut ne pas avoir réussi la vérification de l'état. Une fois les étapes initiales de l'enregistrement d'instance achevées (cela peut prendre jusqu'à environ 30 secondes), l'équilibreur de charge commence à envoyer des demandes de vérification de l'état. Votre instance n'est pas à l'état `InService` tant que qu'une vérification de l'état n'a pas réussi.

Solution : consultez La connexion aux instances a expiré.

Impossible d'enregistrer une instance lancée à partir d'une AMI payante

Problème : Elastic Load Balancing n'enregistre pas une instance lancée à l'aide d'une AMI payante.

Cause : Vos instances ont peut-être été lancées à l'aide d'une AMI payante d'Amazon DevPay.

Solution : Elastic Load Balancing ne prend pas en charge l'enregistrement d'instances lancées à l'aide d'AMI payantes d'Amazon DevPay. Notez que vous pouvez utiliser des AMI payantes depuis AWS Marketplace. Si vous utilisez déjà une AMI payante AWS Marketplace et que vous ne parvenez pas à enregistrer une instance lancée à partir de cette AMI payante, adressez-vous au AWS Support Centre pour obtenir de l'aide.

Quotas liés à votre Classic Load Balancer

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.

Pour afficher les quotas pour vos Classic Load Balancers ouvrez la console Service Quotas. Dans le volet 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.

Les quotas de votre compte AWS concernant les Classic Load Balancers sont les suivants :

Nom	Par défaut	Ajustable
Classic Load Balancer par région	20	Oui
Écouteurs par Classic Load Balancer	100	Oui
Instances enregistrées par Classic Load Balancer	1 000	Oui

Historique des documents pour les équilibreurs de charge classiques

Le tableau suivant décrit les versions des Classic Load Balancers.

Modification	Description	Date
Mode d'atténuation de désynchronisation	Ajout de la prise en charge du mode d'atténuation de désynchronisation. Pour plus d'informations, consultez Configurer le mode d'atténuation de la désynchronisation pour votre Classic Load Balancer.	17 août 2020
Équilibreurs de charge classiques	Avec le lancement des Application Load Balancers et des dispositifs d'équilibrage de charge de réseau, les équilibreurs de charge créés avec l'API 2016-06-01 sont maintenant appelés Classic Load Balancers. Pour plus d'informations sur les différences entre ces types d'équilibreurs de charge, consultez la section Fonctionnalités d'Elastic Load Balancing.	11 août 2016
Support pour AWS Certificate Manager (ACM)	Vous pouvez demander un certificat SSL/TLS auprès d'ACM et le déployer sur votre équilibreur de charge. Pour plus d'informations, consultez la section Certificats SSL/TLS	21 janvier 2016

	pour les équilibreurs de charge classiques.	
Support pour des ports supplémentaires	Les équilibreurs de charge dans un VPC peuvent écouter sur n'importe quel port compris dans la plage 1-65535. Pour plus d'informations, consultez Listeners for your Classic Load Balancer.	15 septembre 2015
Champs supplémentaires pour les entrées du journal d'accès	Ajout des champs `user_agent` , `ssl_cipher` et `ssl_protocol` . Pour plus d'informations, consultez la section Fichiers journaux d'accès.	18 mai 2015
Support pour le balisage de votre équilibreur de charge	À partir de cette version, la CLI Elastic Load Balancing (ELB CLI) a été remplacée par AWS Command Line Interface (AWS CLI), un outil unifié permettant de gérer plusieurs AWS services. Les nouvelles fonctions publiées après la CLI ELB version 1.0.35.0 (datée du 24/07/14) seront incluses uniquement dans l'interface AWS CLI . Si vous utilisez actuellement la CLI ELB, nous vous recommandons de commencer à plutôt utiliser l'interface AWS CLI . Pour plus d'informations, consultez le Guide de l'utilisateur AWS Command Line Interface .	11 août 2014

Délai d'inactivité de la connexion	Vous pouvez configurer le délai d'inactivité des connexions pour votre équilibreur de charge.	24 juillet 2014
Support pour accorder aux utilisateurs et aux groupes l'accès à des équilibreurs de charge ou à des actions d'API spécifiques	Vous pouvez créer une stratégie pour accorder à des utilisateurs et groupes l'accès à des équilibreurs de charge ou à des actions d'API spécifiques.	12 mai 2014
Support pour AWS CloudTrail	Vous pouvez l'utiliser CloudTrail pour capturer les appels d'API effectués par vous ou en votre nom Compte AWS à l'aide de l'API ELB, de la CLI ELB ou du. AWS Management Console AWS CLI Pour plus d'informations, consultez la section Logging des appels d'API pour votre Classic Load Balancer à l'aide de. AWS CloudTrail	4 avril 2014

Drainage des connexions	Ajout d'informations sur le drainage de la connexion. Avec cette prise en charge, vous pouvez permettre à votre équilibreur de charge d'arrêter d'envoyer de nouvelles demandes à l'instance enregistrée lorsque l'enregis trement de l'instance est en cours d'annulation ou lorsque l'instance devient défectueu se, tout en maintenant les connexions existantes ouvertes. Pour plus d'informa tions, consultez Configurer le drainage des connexions pour votre Classic Load Balancer.	20 mars 2014
Journaux d'accès	Vous pouvez activer votre équilibreur de charge pour capturer des informations détaillées sur les demandes envoyées à votre équilibreur de charge et les stocker dans un compartiment Amazon S3. Pour plus d'informa tions, consultez les journaux d'accès de votre Classic Load Balancer.	6 mars 2014

Support pour TLSv1.1-1.2	Ajout d'informations sur la prise en charge du protocole TLSv1.1-1. 2 pour les équilibreurs de charge configurés avec des écouteurs HTTPS/SSL. Avec cette prise en charge, Elastic Load Balancing met également à jour les configurations de négociation SSL prédéfinies. Pour plus d'informations sur les configurations de négociation SSL prédéfinies mises à jour, voir Configurations de négociation SSL pour les équilibreurs de charge classiques. Pour plus d'informations sur la mise à jour de votre configuration de négociation SSL actuelle, consultez Mettre à jour la configuration de négociation SSL de votre Classic Load Balancer.	19 février 2014
Equilibrage de charge entre zones	Ajout d'informations sur l'activation de l'équilibrage de charge entre zones pour votre équilibreur de charge. Pour plus d'informations, consultez Configurer l'équilibrage de charge entre zones pour votre Classic Load Balancer.	6 novembre 2013

CloudWatch Métriques supplémentaires	Ajout d'informations sur les métriques Cloudwatch supplémentaires présentées par Elastic Load Balancing. Pour plus d'informations, consultez CloudWatch les statistiques de votre Classic Load Balancer.	28 octobre 2013
Support pour le protocole proxy	Ajout d'informations sur la prise en charge du protocole proxy pour les équilibreurs de charge configurés pour les connexions TCP/SSL. Pour plus d'informations, consultez la section En-tête du protocole proxy.	30 juillet 2013
Support pour le basculement du DNS	Ajout d'informations sur la configuration du basculement DNS sur Amazon Route 53 pour les équilibreurs de charge. Pour plus d'informations, consultez Utiliser le basculement DNS d'Amazon Route 53 pour votre équilibreur de charge.	3 juin 2013
Support de console pour l'affichage CloudWatch des métriques et la création d'alarmes	Ajout d'informations sur l'affichage CloudWatch des métriques et la création d'alarmes pour un équilibreur de charge spécifique à l'aide de la console. Pour plus d'informations, consultez CloudWatch les statistiques de votre Classic Load Balancer.	28 mars 2013

Support pour l'enregistrement des instances EC2 dans un VPC par défaut	Ajout de la prise en charge pour les instances EC2 lancées dans un VPC par défaut.	11 mars 2013
Équilibreurs de charge internes	Avec cette version, un équilibreur de charge dans un Virtual Private Cloud (VPC) peut être créé en interne ou pour être accessible sur Internet. Un équilibreur de charge interne possède un nom DNS publiquement résolu qui est converti en adresses IP privées. Un équilibreur de charge accessible sur Internet possède un nom DNS publiquement résolu qui est converti en adresses IP publiques. Pour plus d'informations, voir Création d'un Classic Load Balancer interne.	10 juin 2012
Support de console pour la gestion des écouteurs, des paramètres de chiffrement et des certificats SSL	Pour plus d'informations, consultez Configurer un écouteur HTTPS pour votre Classic Load Balancer et Remplacer le certificat SSL pour votre Classic Load Balancer.	18 mai 2012
Support pour Elastic Load Balancing dans Amazon VPC	Ajout de la prise en charge de la création d'un équilibreur de charge dans un Virtual Private Cloud (VPC).	21 novembre 2011

Amazon CloudWatch	Vous pouvez surveiller votre équilibreur de charge à l'aide CloudWatch de. Pour plus d'informations, consultez CloudWatch les statistiques de votre Classic Load Balancer.	17 octobre 2011
Fonctionnalités de sécurité supplémentaires	Vous pouvez configurer des chiffrements SSL, l'authent ification de connexion SSL principale et l'authentification de serveur principal. Pour plus d'informations, consultez Create a Classic Load Balancer avec un écouteur HTTPS.	30 août 2011
Nom de domaine Zone Apex	Pour plus d'informations, consultez Configurer un nom de domaine personnalisé pour votre Classic Load Balancer.	24 mai 2011

Support pour les en-têtes X-Forwarded-Proto et X-Forwarded-Port	L'en-tête X-Forwarded-Proto indique le protocole de la demande d'origine, et l'en-tête X-Forwarded-Port indique le port de la demande d'origine. L'ajout de ces en-têtes à des demandes permet aux clients de déterminer si une demande entrante vers leur équilibreur de charge est chiffrée et d'identifier le port spécifique de l'équilibreur de charge sur lequel la demande a été reçue. Pour plus d'informations, consultez les rubriques En-têtes HTTP et équilibreurs de charge classiques.	27 octobre 2010
Support pour HTTPS	Avec cette version, vous pouvez utiliser le protocole SSL/TLS pour chiffrer le trafic et transférer le traitement SSL de l'instance d'application à l'équilibreur de charge. Cette fonction assure également la gestion centralisée des certificats de serveur SSL sur l'équilibreur de charge, plutôt que de gérer les certificats sur les différentes instances d'application.	14 octobre 2010
Support pour AWS Identity and Access Management (IAM)	Ajout du support d'IAM.	2 septembre 2010

Sessions permanentes	Pour plus d'informations, consultez Configurer des sessions persistantes pour votre Classic Load Balancer.	7 avril 2010
AWS SDK for Java	Ajout de la prise en charge du Kit SDK pour Java.	22 mars 2010
AWS SDK for .NET	Ajout du support pour AWS SDK for .NET.	11 novembre 2009
Nouveau service	Version bêta publique initiale d'Elastic Load Balancing.	18 mai 2009

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.