aws

Guide de l’utilisateur

Elastic Load Balancing

Elastic Load Balancing: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'Elastic Load Balancing ?

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 fait évoluer la capacité de votre équilibreur de charge automatiquement en fonction de l'évolution du trafic entrant.

Avantages offerts par l'équilibreur de charge

Un équilibreur de charge répartit les charges de travail sur plusieurs ressources de calcul, telles que des serveurs virtuels. L'utilisation d'un équilibreur de charge augmente la disponibilité et la tolérance aux pannes de vos applications.

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

Vous pouvez configurer des vérifications de l'état, qui surveillent l'état de santé des ressources de calcul afin que l'équilibreur de charge envoie les demandes uniquement aux ressources saines. Vous pouvez également charger votre équilibreur de charge du travail de chiffrement et de déchiffrement afin que vos ressources de calcul se concentrent sur leur propre travail.

Caractéristiques d'Elastic Load Balancing

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. Pour plus d'informations, consultezComparaisons de produits.

Pour plus d'informations sur l'utilisation de chaque équilibreur de charge, consultez la documentation suivante :

- Guide de l'utilisateur des équilibreurs de charge d'application
- Guide de l'utilisateur des Network Load Balancers
- Guide de l'utilisateur pour les Gateway Load Balancers
- Guide de l'utilisateur des équilibreurs de charge classiques

Accès à Elastic Load Balancing

Vous pouvez créer vos équilibreurs de charge, y accéder et les gérer à l'aide des interfaces suivantes :

- AWS Management Console – Fournit une interface web que vous pouvez utiliser pour accéder à Elastic Load Balancing.
- Interface de ligne de commande AWS (AWS CLI) – Propose des commandes pour une large gamme de services AWS, notamment Elastic Load Balancing. La AWS CLI est prise en charge sur Windows, macOS et Linux. Pour de plus amples informations, veuillez consulter AWS Command Line Interface.
- Kits SDK AWS : fournissent des API propres au langage et se chargent de nombreux détails de connexion, tels que le calcul des signatures, la gestion des nouvelles tentatives de demande et la gestion des erreurs. Pour plus d'informations, consultez Kits SDK AWS.
- API de requête : Fournit des actions d'API de bas niveau appelées à l'aide de demandes HTTPS. L'utilisation de l'API de requête est le moyen le plus direct d'accéder à un Elastic Load Balancing. Toutefois, l'utilisation de l'API de requête nécessite que votre application gère les détails de bas niveau, tels que la génération du hachage pour signer la demande et la gestion des erreurs. Pour plus d'informations, consultez les ressources suivantes :
  - Application Load Balancer et Network Load Balancer – API version 2015-12-01
  - Classic Load Balancers – API version 2012-06-01

Services connexes

Elastic Load Balancing fonctionne avec les services suivants pour améliorer la disponibilité et la capacité de mise à l'échelle de vos applications.

- Amazon EC2 – Serveurs virtuels qui exécutent vos applications dans le cloud. Vous pouvez configurer votre équilibreur de charge pour acheminer le trafic vers vos instances EC2. Pour plus d'informations, consultez le Guide de l'utilisateur Amazon EC2 pour les instances Linux ou le Guide de l'utilisateur Amazon EC2 pour les instances Windows.
- Amazon EC2 Auto Scaling – Garantit que vous exécutez le nombre d'instances souhaité, même en cas de défaillance d'une instance. Amazon EC2 Auto Scaling vous permet également d'augmenter ou de diminuer automatiquement le nombre d'instances à mesure que la demande sur vos instances change. Si vous activez Auto Scaling avec Elastic Load Balancing, les instances lancées par Auto Scaling sont automatiquement enregistrées auprès de l'équilibreur de charge. De même,

l'enregistrement des instances qui sont terminées par Auto Scaling est automatiquement annulé auprès de l'équilibreur de charge. Pour plus d'informations, consultez le Guide de l'utilisateur Amazon EC2 Auto Scaling.

- AWS Certificate Manager – Lorsque vous créez un écouteur HTTPS, vous pouvez spécifier les certificats fournis par ACM. L'équilibreur de charge utilise les certificats pour mettre fin aux connexions et déchiffrer les demandes de clients.
- Amazon CloudWatch – Permet de surveiller votre équilibreur de charge et de prendre les mesures nécessaires. Pour plus d'informations, consultez le Guide de l'utilisateur Amazon CloudWatch.
- Amazon ECS – Vous permet d'exécuter, d'arrêter et de gérer des conteneurs Docker sur un cluster d'instances EC2. Vous pouvez configurer votre équilibreur de charge pour acheminer le trafic vers vos conteneurs. Pour plus d'informations, consultez le Guide du développeur Amazon Elastic Container Service.
- AWS Global Accelerator – Améliore la disponibilité et les performances de votre application. Utilisez un accélérateur pour répartir le trafic entre plusieurs équilibreurs de charge dans une ou plusieurs régions AWS. Pour plus d'informations, consultez le Guide du développeur AWS Global Accelerator.
- Route 53 – Constitue un moyen extrêmement fiable et rentable d'acheminer les visiteurs vers des sites web en traduisant les noms de domaines en adresses IP numériques que les ordinateurs utilisent pour se connecter les uns aux autres. Par exemple, il traduira `www.example.com` en adresse IP numérique `192.0.2.1`. AWS attribue des URL à vos ressources, telles que les équilibreurs de charge. Vous pourrez néanmoins vouloir une URL qui soit simple à mémoriser par les utilisateurs. Par exemple, vous pouvez mapper votre nom de domaine à un équilibreur de charge. Pour plus d'informations, consultez le Guide du développeur Amazon Route 53.
- AWS WAF – Vous pouvez utiliser AWS WAF avec votre Application Load Balancer pour autoriser ou bloquer des demandes en fonction des règles d'une liste de contrôle d'accès web (ACL web). Pour plus d'informations, consultez le Guide du développeur AWS WAF.

Tarification

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

Fonctionnement d'Elastic Load Balancing

Un équilibreur de charge accepte le trafic entrant issu des clients et achemine les demandes à ses cibles enregistrées (des instances EC2 par exemple) dans une ou plusieurs zones de disponibilité. L'équilibreur de charge surveille également l'état des cibles enregistrées et veille à ne rediriger le trafic que vers des cibles saines. Lorsque l'équilibreur de charge détecte une cible qui n'est pas saine, il arrête le routage du trafic vers cette cible. Il le reprend lorsqu'il détecte que la cible est de nouveau saine.

Vous configurez votre équilibreur de charge pour qu'il accepte le trafic entrant en spécifiant un ou plusieurs écouteurs. Un écouteur est un processus qui vérifie les demandes de connexion. Il est configuré avec un protocole et un numéro de port pour les connexions entre les clients et l'équilibreur de charge. De même, il est configuré avec un protocole et un numéro de port pour les connexions entre l'équilibreur de charge et les cibles.

Elastic Load Balancing prend en charge les types d'équilibreurs de charge suivants :

- Application Load Balancers
- Network Load Balancers
- Gateway Load Balancers
- Équilibreurs de charge classiques

Il existe une différence clé dans la configuration des équilibreurs de charge. Avec Aplication Load Balancers, Network Load Balancers et Gateway Load Balancers, vous enregistrez des cibles dans des groupes cibles, et vous acheminez le trafic vers les groupes cibles. Avec les Classic Load Balancers, vous enregistrez les instances auprès de l'équilibreur de charge.

Zones de disponibilité et nœuds d'équilibreurs de charge

Lorsque vous activez une zone de disponibilité pour votre équilibreur de charge, Elastic Load Balancing crée un nœud d'équilibreur de charge dans la zone de disponibilité. Si vous enregistrez des cibles dans une zone de disponibilité mais que vous n'activez pas la zone de disponibilité, ces cibles enregistrées ne reçoivent pas le trafic. Votre équilibreur de charge est plus efficace si vous vous assurez que chaque zone de disponibilité activée contient au moins une cible enregistrée.

Nous recommandons d'activer plusieurs zones de disponibilité pour tous les équilibreurs de charge. Cependant, avec un Application Load Balancer, vous devez activer au moins deux zones de

disponibilité. Cette configuration permet de s'assurer que l'équilibreur de charge peut continuer à acheminer le trafic. Si une zone de disponibilité devient indisponible ou ne contient pas de cible saine, l'équilibreur de charge peut acheminer le trafic vers les cibles saines d'une autre zone de disponibilité.

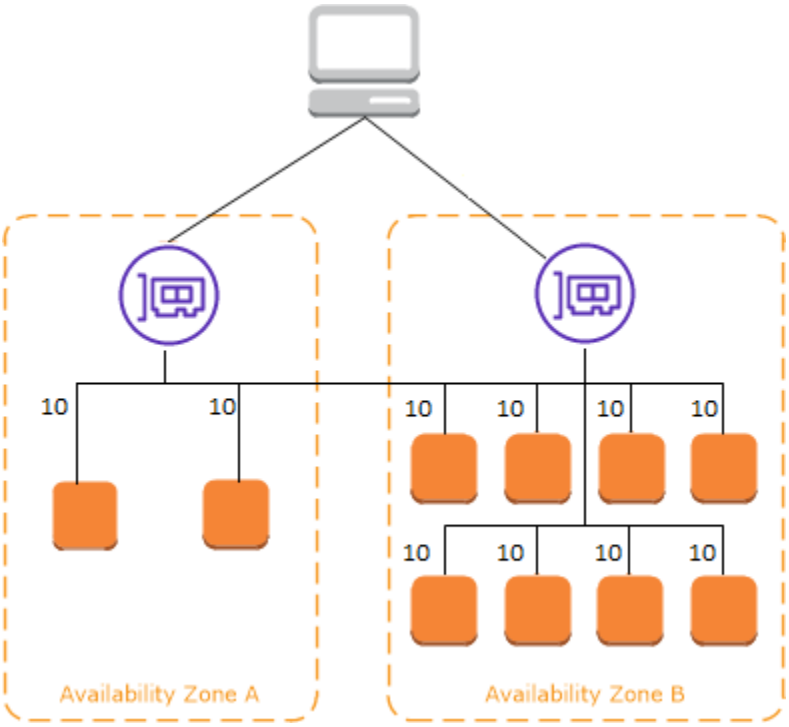
Une fois qu'une zone de disponibilité est désactivée, les cibles de cette zone de disponibilité restent enregistrées auprès de l'équilibreur de charge. Cependant, même si elles restent enregistrées, l'équilibreur de charge ne leur achemine plus de trafic.

Equilibrage de charge entre zones

Les nœuds de votre équilibreur de charge distribuent les requêtes des clients à des cibles enregistrées. Lorsque l'équilibrage de charge entre zones est activé, chaque nœud d'équilibreur de charge distribue le trafic entre les cibles enregistrées dans toutes les zones de disponibilité activées. Lorsque l'équilibrage de charge entre zones est désactivé, chaque nœud d'équilibreur de charge distribue le trafic entre les cibles enregistrées dans sa zone de disponibilité uniquement.

Les diagrammes suivants illustrent l'effet de la répartition de charge entre zones avec le routage en tourniquet comme algorithme de routage par défaut. Il existe deux zones de disponibilité activées, avec deux cibles dans la zone de disponibilité A et huit cibles dans la zone de disponibilité B. Les clients envoient des demandes, et Amazon Route 53 répond à chaque demande avec l'adresse IP de l'un des nœuds de l'équilibreur de charge. Sur la base de l'algorithme de routage circulaire, le trafic est distribué de telle sorte que chaque nœud d'équilibreur de charge reçoit 50 % du trafic des clients. Chaque nœud d'équilibreur de charge distribue son partage du trafic entre cibles enregistrées dans son champ.

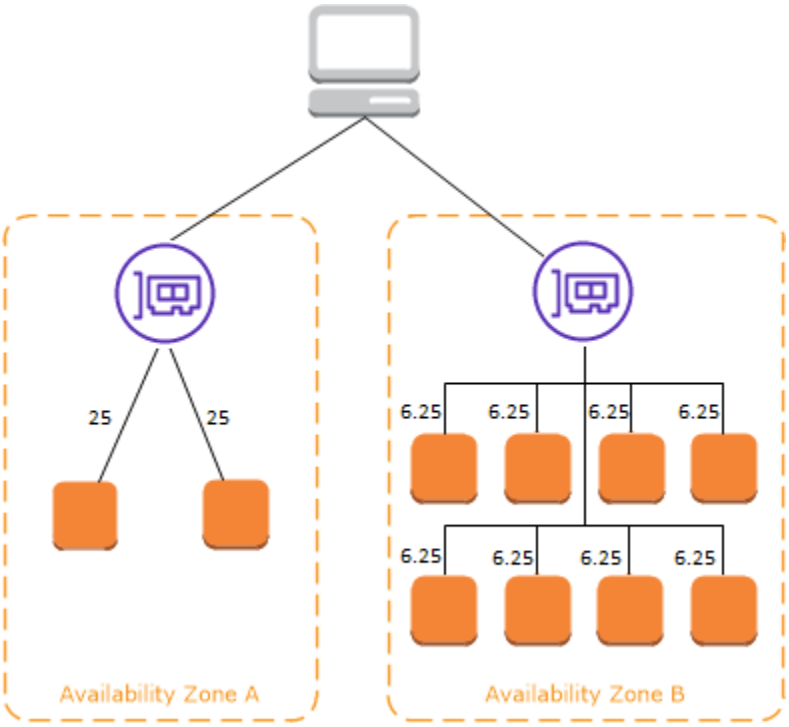
Si l'équilibrage de charge entre zones est activé, chacune des 10 cibles reçoit 10 % du trafic. En effet, chaque nœud d'équilibreur de charge peut acheminer ses 50 % du trafic client vers l'ensemble des 10 cibles.



Si l'équilibrage de charge entre zones est désactivé :

- Chacune des deux cibles de la zone de disponibilité A reçoit 25 % du trafic.
- Chacune des huit cibles de la zone de disponibilité B reçoit 6,25 % du trafic.

En effet, chaque nœud d'équilibreur de charge peut acheminer ses 50 % du trafic client uniquement vers les cibles dans sa zone de disponibilité.



Avec les Application Load Balancers, la répartition de charge entre zones est toujours activé au niveau de l'équilibreur de charge. Au niveau du groupe cible, la répartition de charge entre zones peut être désactivé. Pour plus d'informations, consultez Désactiver la répartition de charge entre zones dans le Guide de l'utilisateur pour Application Load Balancers.

Avec les Network Load Balancers et les Gateway Load Balancers, la répartition de charge entre zones est désactivée par défaut. Après avoir créé un équilibreur de charge, vous pouvez activer ou désactiver la répartition de charge entre zones à tout moment.

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. Pour plus d'informations, consultez Activer la répartition de charge entre zones dans le Guide de l'utilisateur pour Classic Load Balancers.

Changement de zone

Le changement de zone est une fonctionnalité du Contrôleur de récupération d'application Amazon Route 53 (Route 53 ARC). Avec le changement de zone, vous pouvez déplacer une ressource

d'équilibreur de charge hors d'une zone de disponibilité altérée en une seule action. De cette façon, vous pouvez continuer à opérer depuis d'autres zones de disponibilité saines dans une Région AWS.

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

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

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

- La répartition de charge entre zones n'est pas prise en charge avec les changements de zone. Vous devez désactiver la répartition de charge entre zones pour utiliser cette fonctionnalité.
- Le changement de zone n'est pas pris en charge lorsque vous utilisez un Application Load Balancer comme point de terminaison d'accélérateur dans AWS Global Accelerator.
- Vous pouvez démarrer un changement de zone pour un équilibreur de charge spécifique uniquement pour une zone de disponibilité unique. Vous ne pouvez pas commencer un changement de zone pour plusieurs zones de disponibilité.
- AWS supprime de manière proactive les adresses IP des équilibreurs de charge zonaux du DNS lorsque plusieurs problèmes d'infrastructure ont un impact sur les services. Vérifiez toujours la capacité actuelle de la zone de disponibilité avant de commencer un changement de zone. Si la répartition de charge entre zones de vos équilibreurs de charge est désactivée et que vous utilisez un changement de zone pour supprimer une adresse IP d'équilibreur de charge zonal, la zone de disponibilité affectée par le changement de zone perd également sa capacité cible.
- Lorsqu'un Application Load Balancer est la cible d'un Network Load Balancer, commencez toujours le changement de zone à partir du Network Load Balancer. Si vous commencez un changement de zone à partir de l'Application Load Balancer, le Network Load Balancer ne reconnaît pas le changement et continue à envoyer du trafic vers l'Application Load Balancer.

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

Routage des demandes

Avant qu'un client envoie une demande à votre équilibreur de charge, il résout le nom de domaine de l'équilibreur de charge à l'aide d'un serveur de système de noms de domaine (DNS). Etant donné que vos équilibreurs de charge se trouvent dans le domaine `amazonaws.com`, l'entrée DNS est contrôlée par Amazon. Les serveurs DNS d'Amazon retournent une ou plusieurs adresses IP au client. Il s'agit des adresses IP des nœuds de votre équilibreur de charge. Avec les Network Load Balancers, Elastic Load Balancing crée une interface réseau pour chaque zone de disponibilité que vous activez et l'utilise pour obtenir une adresse IP statique. Si vous le souhaitez, vous pouvez associer une adresse IP Elastic à chaque interface réseau lorsque vous créez le Network Load Balancer.

Alors que le trafic vers votre application évolue dans le temps, Elastic Load Balancing met à l'échelle votre équilibreur de charge et met à jour l'entrée DNS. L'entrée DNS indique également le time-to-live (TTL) de 60 secondes. Ainsi, les adresses IP peuvent être remappées rapidement en cas d'évolution du trafic.

Le client détermine les adresses IP à utiliser pour envoyer des demandes à l'équilibreur de charge. Le nœud d'équilibreur de charge qui reçoit la demande sélectionne une cible enregistrée saine et envoie la demande à la cible à l'aide de son adresse IP privée.

Pour de plus amples informations, consultez Acheminement du trafic vers un équilibreur de charge ELB dans le Guide du développeur Amazon Route 53.

Algorithme de routage

Avec les Application Load Balancers, le nœud de l'équilibreur de charge qui reçoit la demande procède comme suit :

1. Évalue les règles de l'écouteur par ordre de priorité pour déterminer la règle à appliquer.
2. Sélectionne une cible dans le groupe cible pour l'action de règle, à l'aide de l'algorithme de routage configuré pour le groupe cible. L'algorithme de routage par défaut est l'algorithme de routage en tourniquet. Le routage est effectué indépendamment pour chaque groupe cible, même si une cible est enregistrée avec plusieurs groupes cible.

Avec les Network Load Balancers, le nœud de l'équilibreur de charge qui reçoit la connexion procède comme suit :

1. Sélectionne une cible dans le groupe cible pour la règle par défaut à l'aide d'un algorithme de hachage de flux. Il base l'algorithme sur :
   - le protocole
   - l'adresse IP et le port source
   - l'adresse IP et le port de destination
   - le numéro de séquence TCP
2. Achemine chaque connexion TCP est acheminée vers une seule cible pendant la durée de vie de la connexion. Les connexions TCP d'un client ont des ports source et des numéros de séquence différents, et peuvent être acheminées vers des cibles différentes.

Avec les Classic Load Balancers, le nœud de l'équilibreur de charge qui reçoit la demande sélectionne une instance enregistrée comme suit :

- Il utilise l'algorithme de routage en tourniquet pour les écouteurs TCP
- Il utilise l'algorithme de routage des demandes en attente les moins prioritaires pour les écouteurs HTTP et HTTPS

Connexions HTTP

Classic Load Balancers utilisent des connexions pré-ouvertes, mais pas les Application Load Balancers. Classic Load Balancers et Application Load Balancers utilisent le multiplexage des connexions. Cela signifie que les demandes de plusieurs clients sur plusieurs connexions front-end peuvent être acheminées vers une cible donnée via une seule connexion backend. Le multiplexage des connexions améliore la latence et réduit la charge sur vos applications. Pour empêcher le multiplexage des connexions, désactivez les en-têtes HTTP `keep-alive` en définissant l'en-tête `Connection: close` dans vos réponses HTTP.

Application Load Balancers et Classic Load Balancers prennent en charge le protocole HTTP en pipeline sur les connexions fronend. Ils ne pas prennent en charge le protocole HTTP en pipeline sur les connexions backend.

Les équilibreurs de charge d'application prennent en charge les méthodes de requête HTTP suivantes : GET, HEAD, POST, PUT, DELETE, OPTIONS et PATCH.

Application Load Balancers prennent en charge les protocoles suivants pour les connexions front-end : HTTP/0.9, HTTP/1.0, HTTP/1.1 et HTTP/2. Vous pouvez utiliser HTTP/2 uniquement avec les écouteurs HTTPS, et vous pouvez envoyer jusqu'à 128 demandes en parallèle à partir d'une connexion HTTP/2. Les équilibreurs de charge des applications prennent également en charge les mises à niveau de connexion du protocole HTTP vers WebSockets. Toutefois, en cas de mise à niveau de la connexion, les règles de routage et les AWS WAF intégrations de l'écouteur Application Load Balancer ne s'appliquent plus.

Application Load Balancers utilisent HTTP/1.1 sur les connexions principales (équilibreur de charge vers la cible enregistrée) par défaut. Cependant, vous pouvez utiliser la version du protocole pour envoyer la demande aux cibles via HTTP/2 ou gRPC. Pour plus d'informations, consultez Versions de protocole. L'en-tête `keep-alive` est pris en charge par défaut sur les connexions backend. Pour les demandes HTTP/1.0 des clients qui n'ont pas un en-tête d'hôte, l'équilibreur de charge génère un en-tête d'hôte pour les demandes HTTP/1.1 envoyées sur les connexions backend. L'en-tête d'hôte contient le nom DNS de l'équilibreur de charge.

Classic Load Balancers prennent en charge les protocoles suivants pour les connexions front-end (client vers équilibreur de charge) : HTTP/0.9, HTTP/1.0 et HTTP/1.1. Ils utilisent le protocole HTTP/1.1 sur les connexions backend (équilibreur de charge vers cible enregistrée). L'en-tête `keep-alive` est pris en charge par défaut sur les connexions backend. Pour les demandes HTTP/1.0 des clients qui n'ont pas un en-tête d'hôte, l'équilibreur de charge génère un en-tête d'hôte pour les demandes HTTP/1.1 envoyées sur les connexions backend. L'en-tête d'hôte contient l'adresse IP du nœud de l'équilibreur de charge.

En-têtes HTTP

Application Load Balancers et Classic Load Balancers ajoutent automatiquement les en-têtes X-Forwarded-For, X-Forwarded-Proto et X-Forwarded-Port à la demande.

Application Load Balancers convertissent les noms d'hôtes contenus dans les en-têtes d'hôtes HTTP en minuscules avant de les envoyer aux cibles.

Pour les connexions front-end qui utilisent HTTP/2, les noms d'en-tête sont en minuscules. Avant que la demande soit envoyée à la cible à l'aide de HTTP/1.1, les noms d'en-tête suivants sont convertis en casse mixte : X-Forwarded-For, X-Forwarded-Proto, X-Forwarded-Port, Host, X-Amzn-Trace-Id, Upgrade et Connection. Tous les autres noms d'en-tête sont en minuscules.

Les Application Load Balancers et les Classic Load Balancers prennent en compte l'en-tête de connexion de la demande client entrante après avoir redirigé la réponse vers le client.

Lorsque Application Load Balancers et Classic Load Balancers utilisant HTTP/1.1 reçoivent un en-tête Expect: 100-Continue, ils répondent immédiatement par HTTP/1.1 100 Continue sans tester la longueur de l'en-tête du contenu. L'en-tête de demande Expect: 100-Continue n'est pas transmis à ses cibles.

Lors de l'utilisation de HTTP/2, Application Load Balancers ne prennent pas en charge l'en-tête Expect: 100-Continue provenant des demandes des clients. Application Load Balancer ne répondra pas avec HTTP/2 100 Continue ou ne transmettra pas cet en-tête à ses cibles.

Limites des en-têtes HTTP

Les limites de taille des Application Load Balancers qui suivent sont des limites strictes qui ne peuvent pas être modifiées :

- Ligne de demande : 16 K
- En-tête simple : 16 K
- En-tête de réponse entier : 32 K
- En-tête de demande entier : 64 K

Schéma d'un équilibreur de charge

Lorsque vous créez un équilibreur de charge, 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.

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.

Les équilibreurs de charge internes et accessibles sur Internet acheminent les demandes vers vos cibles à l'aide d'adresses IP privées. Par conséquent, vos cibles n'ont pas besoin d'adresses IP publiques pour recevoir des demandes d'un équilibreur de charge interne ou accessible sur Internet.

Si votre application comporte plusieurs niveaux, vous pouvez concevoir une architecture qui utilise à la fois des équilibreurs de charge internes et accessibles sur Internet. Par exemple, c'est le cas si votre application utilise des serveurs web qui doivent être connectés à Internet et des serveurs de base de données qui ne sont connectés qu'aux serveurs web. 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 d'application auprès de celui-ci. Les serveurs web reçoivent les demandes de l'équilibreur de charge accessible sur Internet et les envoient pour les serveurs d'application à l'équilibreur de charge interne. Les serveurs d'application reçoivent les demandes de l'équilibreur de charge interne.

MTU réseau pour votre équilibreur de charge

L'unité de transmission maximale (MTU) détermine la taille, en octets, du paquet le plus volumineux susceptible d'être envoyé via le réseau. Plus la MTU d'une connexion est élevée, plus la quantité de données pouvant être transmises dans un seul paquet est importante. Les trames Ethernet se composent du paquet, ou des données réelles que vous envoyez, et des informations de surcharge du réseau qui l'entourent. Le trafic envoyé via une passerelle Internet a une MTU de 1 500. Cela signifie que si un paquet est supérieur à 1 500 octets, il est fragmenté pour être envoyé en utilisant plusieurs trames, ou il est supprimé si `Don't Fragment` est défini dans l'en-tête IP.

La taille de la MTU sur les nœuds d'équilibreur de charge n'est pas configurable. Les trames jumbo (MTU de 9001) sont utilisées en standard sur tous les nœuds d'équilibreur de charge pour Application Load Balancers, Network Load Balancers et Classic Load Balancers. Gateway Load Balancers prennent en charge une MTU de 8 500. Pour plus d'informations, consultez Unité de transmission maximale (MTU) dans le Guide de l'utilisateur pour Gateway Load Balancers.

La MTU du chemin correspond à la taille maximum du paquet prise en charge sur le chemin entre l'hôte de départ et l'hôte de destination. La détection de la MTU du chemin (PMTUD) permet de déterminer la MTU du chemin entre deux appareils. La détection de la MTU du chemin est particulièrement importante si le client ou la cible ne prend pas en charge les trames jumbo.

Lorsqu'un hôte envoie un paquet dont la taille est supérieure au MTU de l'hôte destinataire ou au MTU d'un périphérique situé sur le chemin, l'hôte ou le périphérique destinataire abandonne le paquet et renvoie le message ICMP suivant : `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set (Type 3, Code 4)`. Cela indique à l'hôte émetteur de diviser la charge utile en plusieurs paquets plus petits et de les retransmettre.

Si des paquets supérieurs à la taille de MTU de l'interface client ou cible continuent d'être supprimés, il est probable que la détection de la MTU du chemin (PMTUD) ne fonctionne pas. Pour éviter cela, assurez-vous que la détection de la MTU du chemin fonctionne de bout en bout et que vous avez activé les trames jumbo sur vos clients et cibles. Pour de plus amples informations sur la détection de la MTU du chemin et sur l'activation de trames jumbo, veuillez consulter Détection de la MTU du chemin dans le Guide de l'utilisateur Amazon EC2.

Prise en main d'Elastic Load Balancing

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. Pour plus d'informations, consultezComparaisons de produits.

Des démonstrations de configurations courantes d'équilibreur de charge sont disponibles sur la page Démonstrations Elastic Load Balancing (français non garanti).

Si vous possédez un Classic Load Balancer, vous pouvez migrer vers un Application Load Balancer ou un Network Load Balancer. Pour de plus amples informations, veuillez consulter Migration de votre Classic Load Balancer.

Table des matières

Création d'un Application Load Balancer

Pour créer un Application Load Balancer à l'aide de la AWS Management Console, consultez Prise en main d'Application Load Balancers dans le Guide de l'utilisateur pour Application Load Balancers.

Pour créer un Application Load Balancer à l'aide de l'AWS CLI, consultez Créer un Application Load Balancer à l'aide de l'AWS CLI dans le Guide de l'utilisateur pour Application Load Balancers.

Créer un Network Load Balancer

Pour créer un Network Load Balancer à l'aide de la AWS Management Console, consultez Prise en main de Network Load Balancers dans le Guide de l'utilisateur pour Network Load Balancers.

Pour créer un Network Load Balancer à l'aide de l'AWS CLI, consultez Création d'un Network Load Balancer à l'aide de l'AWS CLI dans le Guide de l'utilisateur pour Network Load Balancers.

Créer un Gateway Load Balancer

Pour créer un Gateway Load Balancer à l'aide de la AWS Management Console, consultez Prise en main de Gateway Load Balancers dans le Guide de l'utilisateur pour Gateway Load Balancers.

Pour créer un Gateway Load Balancer à l'aide de l'AWS CLI, consultez Prise en main de Gateway Load Balancers en utilisant l'AWS CLI dans le Guide de l'utilisateur pour Gateway Load Balancers.

Création d'un un Classic Load Balancer

Pour créer un Classic Load Balancer à l'aide de l'AWS Management Console, consultez Créer un Classic Load Balancer dans le Guide de l'utilisateur pour Classic Load Balancers.

La sécurité dans Elastic Load Balancing

Chez AWS, la sécurité dans le cloud est notre priorité numéro 1. En tant que client AWS, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses en termes de sécurité.

La sécurité est une responsabilité partagée entre AWS et vous-même. Le modèle de responsabilité partagéede décrit ceci comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est responsable de la protection de l'infrastructure qui exécute des services AWS dans le cloud AWS. AWS vous fournit également les services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de conformité AWS. Pour découvrir les programmes de conformité qui s'appliquent à Elastic Load Balancing, consultez Services AWS concernés par le programme de conformité.
- Sécurité dans le cloud : votre responsabilité est déterminée par le AWSservice que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise, ainsi que la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Elastic Load Balancing. Elle vous montre comment configurer Elastic Load Balancing pour atteindre vos objectifs en matière de sécurité et de conformité. Vous pouvez également apprendre à utiliser d'autres services AWS qui vous aident à contrôler et sécuriser vos ressources Elastic Load Balancing.

Avec un Gateway Load Balancer, vous êtes responsable du choix et de la qualification des logiciels proposés par les fournisseurs d'appareils. Vous devez faire confiance au logiciel de l'appliance pour inspecter ou modifier le trafic provenant de l'équilibreur de charge, qui agit au niveau de la couche 3 du modèle OSI (Open Systems Interconnection), la couche réseau. Les fournisseurs d'appareils répertoriés dans la liste des partenaires Elastic Load Balancing ont intégré et qualifié leur logiciel d'appareil avec AWS. Vous pouvez accorder une plus grande confiance aux logiciels d'appareils fournis par les prestataires figurant dans cette liste. Toutefois, AWS ne garantit pas la sécurité ou la fiabilité des logiciels de ces fournisseurs.

Table des matières

- Gestion des identités et des accès pour Elastic Load Balancing
- Validation de la conformité pour Elastic Load Balancing
- Résilience dans Elastic Load Balancing
- Sécurité de l'infrastructure dans Elastic Load Balancing
- Accès à Elastic Load Balancing à l'aide d'un point de terminaison d'interface (AWS PrivateLink)

Protection des données dans Elastic Load Balancing

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans Elastic Load Balancing. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard)

disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l’information fédérale).

Nous vous recommandons fortement de ne jamais placer d’informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Elastic Load Balancing ou une autre solution Services AWS à l'aide de la console AWS CLI, de l'API ou AWS des SDK. Toutes les données que vous saisissez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d’informations d’identification dans l’adresse URL permettant de valider votre demande adressée à ce serveur.

Chiffrement au repos

Si vous activez le chiffrement côté serveur avec des clés de chiffrement gérées par Amazon S3 (SSE-S3) pour votre compartiment S3 destiné aux journaux d'accès à Elastic Load Balancing, Elastic Load Balancing chiffre automatiquement chaque fichier de journal d'accès avant qu'il ne soit stocké dans votre compartiment S3. Elastic Load Balancing déchiffre également les fichiers journaux d'accès lorsque vous y accédez. 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.

Chiffrement en transit

Elastic Load Balancing simplifie le processus de création d'applications Web sécurisées en arrêtant le trafic HTTPS et TLS à partir des clients au niveau de l'équilibreur de charge. L'équilibreur de charge procède au chiffrement et au déchiffrement du trafic, au lieu d'exiger que chaque instance EC2 gère le travail pour l’arrêt TLS. Lorsque vous configurez un écouteur sécurisé, vous spécifiez les suites de chiffrement et les versions de protocole prises en charge par votre application, ainsi qu'un certificat de serveur à installer sur votre équilibreur de charge. Vous pouvez utiliser AWS Certificate Manager (ACM) ou AWS Identity and Access Management (IAM) pour gérer vos certificats de serveur. Les Application Load Balancer prennent en charge les écouteurs HTTPS. Les Network Load Balancers prennent en charge les écouteurs TLS. Classic Load Balancers prennent en charge les écouteurs HTTPS et TLS.

Gestion des identités et des accès pour Elastic Load Balancing

AWS Identity and Access Management (IAM) est un Service AWS qui aide un administrateur à contrôler en toute sécurité l'accès aux ressources AWS. Des administrateurs IAM contrôlent les personnes qui s'authentifient (sont connectées) et sont autorisées (disposent d'autorisations) à utiliser des ressources Elastic Load Balancing. IAM est un Service AWS que vous pouvez utiliser sans frais supplémentaires.

Table des matières

Public ciblé

Votre utilisation d'AWS Identity and Access Management (IAM) diffère selon la tâche que vous accomplissez dans Elastic Load Balancing.

Utilisateur du service – Si vous utilisez le service Elastic Load Balancing pour accomplir votre tâche, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Plus vous utiliserez de fonctionnalités Elastic Load Balancing pour effectuer votre travail, plus vous pourriez avoir besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur.

Administrateur du service – Si vous êtes responsable des ressources Elastic Load Balancing dans votre entreprise, vous bénéficiez probablement d'un accès total à Elastic Load Balancing. Votre responsabilité est de déterminer les fonctionnalités Elastic Load Balancing ainsi que les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM.

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaiterez peut-être en savoir plus sur la façon d'écrire des stratégies pour gérer l'accès à Elastic Load Balancing.

Authentification par des identités

L'authentification correspond au processus par lequel vous vous connectez à AWS avec vos informations d'identification. Vous devez vous authentifier (être connecté à AWS) en tant qu'Utilisateur racine d'un compte AWS, en tant qu'utilisateur IAM ou en endossant un rôle IAM.

Vous pouvez vous connecter à AWS en tant qu'identité fédérée à l'aide des informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification de connexion unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS en utilisant la fédération, vous endossez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter à la AWS Management Console ou au portail d'accès AWS. Pour plus d'informations sur la connexion à AWS, consultez Connexion à votre Compte AWSdans le Guide de l'utilisateurConnexion à AWS.

Si vous accédez à AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes en utilisant vos informations d'identification. Si vous n'utilisez pas les outils AWS, vous devez signer les requêtes vous-même. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez Signature des demandes d'API AWS dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, AWS vous recommande d'utiliser l'authentification multifactorielle (MFA) pour améliorer la sécurité de votre compte. Pour en savoir plus, veuillez consulter Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Utilisateur root Compte AWS

Lorsque vous créez un Compte AWS, vous commencez avec une seule identité de connexion disposant d'un accès complet à tous les Services AWS et ressources du compte. Cette identité est appelée utilisateur root du Compte AWS. Vous pouvez y accéder en vous connectant à l'aide

de l'adresse électronique et du mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur root pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur root et utilisez-les pour effectuer les tâches que seul l'utilisateur root peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

Demandez aux utilisateurs humains, et notamment aux utilisateurs qui nécessitent un accès administrateur, d'appliquer la bonne pratique consistant à utiliser une fédération avec fournisseur d'identité pour accéder à Services AWS en utilisant des informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, un fournisseur d'identité Web, l'AWS Directory Service, l'annuaire Identity Center ou tout utilisateur qui accède à Services AWS en utilisant des informations d'identification fournies via une source d'identité. Quand des identités fédérées accèdent à Comptes AWS, elles endossent des rôles, ces derniers fournissant des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous connecter et vous synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité pour une utilisation sur l'ensemble de vos applications et de vos Comptes AWS. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center.

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité dans votre Compte AWS qui dispose d'autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations

pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une entité au sein de votre Compte AWS qui dispose d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez temporairement endosser un rôle IAM dans la AWS Management Console en changeant de rôle. Vous pouvez obtenir un rôle en appelant une opération d'API AWS CLI ou AWS à l'aide d'une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center.
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, certains Services AWS vous permettent d'attacher une politique directement à une ressource (au lieu d'utiliser un rôle en tant que proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les

ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

- Accès interservices : certains Services AWS utilisent des fonctions dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, une fonction du service ou un rôle lié au service.
  - Forward access sessions (FAS) – Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions dans AWS, vous êtes considéré comme un principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche une autre action dans un autre service. FAS utilise les autorisations du principal appelant Service AWS, combinées à la demande Service AWS pour effectuer des demandes aux services en aval. Les demandes de FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Fonction du service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié au service – Un rôle lié au service est un type de fonction du service lié à un Service AWS. Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre Compte AWS et sont détenus par le service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications s'exécutant sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer des informations d'identification temporaires pour les applications s'exécutant sur une instance EC2 et effectuant des demandes d'API AWS CLI ou AWS. Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un rôle AWS à une instance EC2 et le rendre disponible à toutes les applications associées, vous pouvez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez les accès dans AWS en créant des politiques et en les attachant à des identités AWS ou à des ressources. Une politique est un objet dans AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit les autorisations de ces dernières. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur racine ou séance de rôle) envoie une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées dans AWS en tant que documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Présentation des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur avec cette politique peut obtenir des informations utilisateur à partir de la AWS Management Console, de la AWS CLI ou de l'API AWS.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez attacher à plusieurs

utilisateurs, groupes et rôles dans votre Compte AWS. Les politiques gérées incluent les politiques gérées par AWS et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou des Services AWS.

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques gérées AWS depuis IAM dans une politique basée sur une ressource.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3, AWS WAF et Amazon VPC sont des exemples de services prenant en charge les ACL. Pour en savoir plus sur les listes de contrôle d'accès, consultez Présentation des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courantes. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonction avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder

à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations qui en résultent représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) - les SCP sont des politiques JSON qui spécifient le nombre maximal d'autorisations pour une organisation ou une unité d'organisation (OU) dans AWS Organizations. AWS Organizations est un service qui vous permet de regrouper et de gérer de façon centralisée plusieurs Comptes AWS détenus par votre entreprise. Si vous activez toutes les fonctions d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. La SCP limite les autorisations pour les entités dans les comptes membres, y compris dans chaque Utilisateur racine d'un compte AWS. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations.
- politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de la séance obtenue sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations, consultez Politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations obtenues sont plus compliquées à comprendre. Pour découvrir la façon dont AWS détermine s'il convient d'autoriser une demande en présence de plusieurs types de politiques, veuillez consulter Logique d'évaluation de politiques dans le Guide de l'utilisateur IAM.

Comment Elastic Load Balancing fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Elastic Load Balancing, découvrez les fonctionnalités IAM disponibles pour une utilisation avec Elastic Load Balancing.

Fonctionnalités IAM que vous pouvez utiliser avec Elastic Load Balancing

Fonctionnalité IAM	Prise en charge d'Elastic Load Balancing
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Politiques basées sur l'identité pour Elastic Load Balancing

Prend en charge les politiques basées sur une identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un Groupes d'utilisateurs IAM ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur une ressource dans Elastic Load Balancing

Prend en charge les politiques basées sur une ressource	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment Amazon S3. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou des Services AWS.

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Quand le principal et la ressource se trouvent dans des Comptes AWS différents, un administrateur IAM dans le compte approuvé doit également accorder à l'entité principal (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez Différence entre les rôles IAM et les politiques basées sur une ressource dans le Guide de l'utilisateur IAM.

Actions de stratégie pour Elastic Load Balancing

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de politique possèdent généralement le même nom que l'opération d'API AWS associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour voir une liste des actions d'Elastic Load Balancing, consultez Actions définies par Elastic Load Balancing dans la Référence de l'autorisation des services.

Les actions de politique dans Elastic Load Balancing utilisent le préfixe suivant avant l'action :

```
elasticloadbalancing
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
    "elasticloadbalancing:action1",
    "elasticloadbalancing:action2"
]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante :

```
"Action": "elasticloadbalancing:Describe*"
```

Pour obtenir la liste complète des actions d'API pour Elastic Load Balancing, consultez la documentation suivante :

- Application Load Balancers, Network Load Balancers et Gateway Load Balancers – Référence d'API version 2015-12-01

- Classic Load Balancers – Référence d'API version 2012-06-01

Pour plus d'informations sur les autorisations requises par chaque action Elastic Load Balancing, consultez Autorisations d'API Elastic Load Balancing.

Ressources de stratégie pour Elastic Load Balancing

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets pour lesquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Certaines actions d'API Elastic Load Balancing prennent en charge plusieurs ressources. Pour spécifier plusieurs ressources dans une seule instruction, séparez leurs ARN par des virgules.

```
"Resource": [
    "resource1",
    "resource2"
]
```

Pour afficher la liste des types de ressources Elastic Load Balancing et leurs ARN, consultez Ressources définies par Elastic Load Balancing dans la Référence de l'autorisation de service. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Elastic Load Balancing.

Clés de condition de stratégie pour Elastic Load Balancing

Prise en charge des clés de condition de stratégie spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques JSON AWS pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une opération `OR` logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques à un service. Pour afficher toutes les clés de condition globales AWS, consultez Clés de contexte de condition globale AWS dans le Guide de l'utilisateur IAM.

Pour afficher la liste des clés de condition Elastic Load Balancing, consultez Clés de condition pour Elastic Load Balancing dans la Référence de l'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Elastic Load Balancing.

Clé de condition **`elasticloadbalancing:ResourceTag`**

La clé de condition `elasticloadbalancing:ResourceTag/`*`key`* est spécifique à Elastic Load Balancing. Les actions suivantes prennent en charge cette clé de condition :

Version de l'API 2015-12-01

- AddTags
- CreateListener
- CreateLoadBalancer
- DeleteLoadBalancer
- DeleteTargetGroup
- DeregisterTargets
- ModifyLoadBalancerAttributes
- ModifyTargetGroup
- ModifyTargetGroupAttributes
- RegisterTargets
- RemoveTags
- SetIpAddressType
- SetSecurityGroups
- SetSubnets

Version de l'API 2012-06-01

- AddTags
- ApplySecurityGroupsToLoadBalancer
- AttachLoadBalancersToSubnets
- ConfigureHealthCheck
- CreateAppCookieStickinessPolicy
- CreateLBCookieStickinessPolicy
- CreateLoadBalancer
- CreateLoadBalancerListeners
- CreateLoadBalancerPolicy
- DeleteLoadBalancer
- DeleteLoadBalancerListeners

- DeleteLoadBalancerPolicy
- DeregisterInstancesFromLoadBalancer
- DetachLoadBalancersFromSubnets
- DisableAvailabilityZonesForLoadBalancer
- EnableAvailabilityZonesForLoadBalancer
- ModifyLoadBalancerAttributes
- RegisterInstancesWithLoadBalancer
- RemoveTags
- SetLoadBalancerListenerSSLCertificate
- SetLoadBalancerPoliciesForBackendServer
- SetLoadBalancerPoliciesOfListener

Clé de condition **elasticloadbalancing:ListenerProtocol**

La clé de elasticloadbalancing:ListenerProtocol condition peut être utilisée pour les conditions qui définissent les types d'écouteurs pouvant être créés et utilisés. Les actions suivantes prennent en charge cette clé de condition :

Version de l'API 2015-12-01

- CreateListener
- ModifyListener

Version de l'API 2012-06-01

- CreateLoadBalancer
- CreateLoadBalancerListeners

La politique est disponible pour les équilibreurs de charge d'application, les équilibreurs de charge réseau et les équilibreurs de charge classiques. Voici un exemple de politique qui permet aux utilisateurs de sélectionner uniquement l'un des protocoles spécifiés pour leur écouteur.

Protocoles pris en charge :

- HTTPS

- HTTP
- TCP
- SSL
- TLS
- UDP
- TCP_UDP

```
"Version": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateListener",
            "elasticloadbalancing:ModifyListener"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals":{
                    "elasticloadbalancing:ListenerProtocol": [
                    "HTTPS",
                    "TLS"
                    ]
            },
        }
```

Clé de condition **`elasticloadbalancing:SecurityPolicy`**

La clé de `elasticloadbalancing:SecurityPolicy` condition peut être utilisée pour les conditions qui définissent et appliquent des politiques de sécurité spécifiques sur les équilibreurs de charge. Les actions suivantes prennent en charge cette clé de condition :

Version de l'API 2015-12-01

- `CreateListener`
- `ModifyListener`

Version de l'API 2012-06-01

- `CreateLoadBalancerPolicy`
- `SetLoadBalancerPoliciesOfListener`

La politique est disponible pour les équilibreurs de charge d'application, les équilibreurs de charge réseau et les équilibreurs de charge classiques. Voici un exemple de politique qui permet aux utilisateurs de sélectionner uniquement l'une des politiques de sécurité spécifiées pour leur équilibreur de charge.

```
"Resource": [
"Version": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateListener",
            "elasticloadbalancing:ModifyListener"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEquals":{
                "elasticloadbalancing:SecurityPolicy": [
                    "ELBSecurityPolicy-TLS13-1-2-2021-06",
                    "ELBSecurityPolicy-TLS13-1-2-Res-2021-06",
                    "ELBSEcurityPolicy-TLS13-1-1-2021-06"
                ]
            },
        }
]
```

Clé de condition **`elasticloadbalancing:Scheme`**

La clé de `elasticloadbalancing:Scheme` condition peut être utilisée pour les conditions qui définissent le schéma pouvant être sélectionné lors de la création de l'équilibreur de charge. Les actions suivantes prennent en charge cette clé de condition :

Version de l'API 2015-12-01

- `CreateLoadBalancer`

Version de l'API 2012-06-01

- `CreateLoadBalancer`

La politique est disponible pour les équilibreurs de charge d'application, les équilibreurs de charge réseau et les équilibreurs de charge classiques. Voici un exemple de politique qui permet uniquement aux utilisateurs de sélectionner l'un des schémas spécifiés pour leur équilibreur de charge.

```
"Version": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action":"elasticloadbalancing:CreateLoadBalancer",
        "Resource": "*",
        "Condition": {
            "StringEquals":{
                "elasticloadbalancing:Scheme": "internal"
            },
        }
```

Clé de condition **`elasticloadbalancing:Subnet`**

> **Important**
>
> Elastic Load Balancing accepte toutes les capitalisations des identifiants de sous-réseau. Veillez toutefois à utiliser les opérateurs de condition appropriés, qui ne tiennent pas compte des majuscules et des minuscules, par exemple`StringEqualsIgnoreCase`.

La clé de `elasticloadbalancing:Subnet` condition peut être utilisée pour les conditions qui définissent les sous-réseaux qui peuvent être créés et attachés aux équilibreurs de charge. Les actions suivantes prennent en charge cette clé de condition :

Version de l'API 2015-12-01

- `CreateLoadBalancer`
- `SetSubnets`

Version de l'API 2012-06-01

- `CreateLoadBalancer`
- `AttachLoadBalancerToSubnets`

La politique est disponible pour les équilibreurs de charge d'application, les équilibreurs de charge réseau, les équilibreurs de charge de passerelle et les équilibreurs de charge classiques. Voici un

exemple de politique qui permet aux utilisateurs de sélectionner uniquement l'un des sous-réseaux spécifiés pour leur équilibreur de charge.

```
"Version": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateLoadBalancer",
            "elasticloadbalancing:SetSubnets"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEqualsIgnoreCase":{
                "elasticloadbalancing:Subnet": [
                    "subnet-01234567890abcdef",
                    "subnet-01234567890abcdeg "
                ]
            },
        }
```

Clé de condition **`elasticloadbalancing:SecurityGroup`**

> **Important**
>
> Elastic Load Balancing accepte toutes les majuscules des identifiants. SecurityGroup Veillez toutefois à utiliser les opérateurs de condition appropriés, qui ne tiennent pas compte des majuscules et des minuscules, par exemple`StringEqualsIgnoreCase`.

La clé de `elasticloadbalancing:SecurityGroup` condition peut être utilisée pour les conditions qui définissent les groupes de sécurité pouvant être appliqués aux équilibreurs de charge. Les actions suivantes prennent en charge cette clé de condition :

Version de l'API 2015-12-01

- `CreateLoadBalancer`
- `SetSecurityGroups`

Version de l'API 2012-06-01

- `CreateLoadBalancer`

- `ApplySecurityGroupsToLoadBalancer`

La politique est disponible pour les équilibreurs de charge d'application, les équilibreurs de charge réseau et les équilibreurs de charge classiques. Voici un exemple de politique qui permet aux utilisateurs de sélectionner uniquement l'un des groupes de sécurité spécifiés pour leur équilibreur de charge.

```
"Version": "2015-12-01",
    "Statement": {"Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateLoadBalancer",
            "elasticloadbalancing:SetSecurityGroup"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEqualsIgnoreCase":{
                "elasticloadbalancing:SecurityGroup": [
                    "sg-51530134",
                    "sg-51530144",
                    "sg-51530139"
                ]
            },
        }
```

Les ACL dans Elastic Load Balancing

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec Elastic Load Balancing

Prend en charge ABAC (étiquettes dans les politiques)	Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés étiquettes. Vous pouvez attacher des étiquettes à des entités IAM (utilisateurs ou rôles), ainsi qu'à de nombreuses ressources AWS. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des balises, vous devez fournir les informations de balise dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec Elastic Load Balancing

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas quand vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, notamment sur les Services AWS qui fonctionnent avec des informations d'identification temporaires, consultez Services AWS qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.

Vous utilisez des informations d'identification temporaires quand vous vous connectez à la AWS Management Console en utilisant toute méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS en utilisant le lien d'authentification unique (SSO) de votre société, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous

connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide d'AWS CLI ou de l'API AWS. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour accéder à AWS. AWS recommande de générer des informations d'identification temporaires de façon dynamique au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations de principal entre services pour Elastic Load Balancing

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous vous servez d'un utilisateur IAM ou d'un rôle IAM pour accomplir des actions dans AWS, vous êtes considéré comme un principal. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui déclenche une autre action dans un autre service. FAS utilise les autorisations du principal appelant Service AWS, combinées à la demande Service AWS pour effectuer des demandes aux services en aval. Les demandes de FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour Elastic Load Balancing

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

Rôles liés à un service pour Elastic Load Balancing

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de fonction du service lié à un Service AWS. Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre Compte AWS et sont détenus par le service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service Elastic Load Balancing, consultez Rôle lié à un service Elastic Load Balancing.

Autorisations d'API Elastic Load Balancing

Vous devez autoriser les utilisateurs à appeler les actions d'API Elastic Load Balancing dont ils ont besoin. En outre, pour certaines actions Elastic Load Balancing, vous devez autoriser les utilisateurs à appeler des actions spécifiques à partir de l'API Amazon EC2.

Autorisations requises pour l'API 2015-12-01

Lorsque vous appelez les actions suivantes à partir de l'API 2015-12-01, vous devez autoriser les utilisateurs à appeler les actions spécifiées.

`CreateLoadBalancer`

- `elasticloadbalancing:CreateLoadBalancer`
- `ec2:DescribeAccountAttributes`
- `ec2:DescribeAddresses`
- `ec2:DescribeInternetGateways`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `iam:CreateServiceLinkedRole`

`CreateTargetGroup`

- `elasticloadbalancing:CreateTargetGroup`
- `ec2:DescribeInternetGateways`
- `ec2:DescribeVpcs`

`RegisterTargets`

- `elasticloadbalancing:RegisterTargets`

- ec2:DescribeInstances
- ec2:DescribeInternetGateways
- ec2:DescribeSubnets
- ec2:DescribeVpcs

SetIpAddressType

- elasticloadbalancing:SetIpAddressType
- ec2:DescribeSubnets

SetSubnets

- elasticloadbalancing:SetSubnets
- ec2:DescribeSubnets

Autorisations requises pour l'API 2012-06-01

Lorsque vous appelez les actions suivantes à partir de l'API 2012-06-01, vous devez autoriser les utilisateurs à appeler les actions spécifiées.

ApplySecurityGroupsToLoadBalancer

- elasticloadbalancing:ApplySecurityGroupsToLoadBalancer
- ec2:DescribeAccountAttributes
- ec2:DescribeSecurityGroups

AttachLoadBalancerToSubnets

- elasticloadbalancing:AttachLoadBalancerToSubnets
- ec2:DescribeSubnets

CreateLoadBalancer

- elasticloadbalancing:CreateLoadBalancer
- ec2:CreateSecurityGroup
- ec2:DescribeAccountAttributes
- ec2:DescribeInternetGateways
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcs

- iam:CreateServiceLinkedRole

DeregisterInstancesFromLoadBalancer

- elasticloadbalancing:DeregisterInstancesFromLoadBalancer
- ec2:DescribeClassicLinkInstances
- ec2:DescribeInstances

DescribeInstanceHealth

- elasticloadbalancing:DescribeInstanceHealth
- ec2:DescribeClassicLinkInstances
- ec2:DescribeInstances

DescribeLoadBalancers

- elasticloadbalancing:DescribeLoadBalancers
- ec2:DescribeSecurityGroups

DisableAvailabilityZonesForLoadBalancer

- elasticloadbalancing:DisableAvailabilityZonesForLoadBalancer
- ec2:DescribeAccountAttributes
- ec2:DescribeInternetGateways
- ec2:DescribeVpcs

EnableAvailabilityZonesForLoadBalancer

- elasticloadbalancing:EnableAvailabilityZonesForLoadBalancer
- ec2:DescribeAccountAttributes
- ec2:DescribeInternetGateways
- ec2:DescribeSubnets
- ec2:DescribeVpcs

RegisterInstancesWithLoadBalancer

- elasticloadbalancing:RegisterInstancesWithLoadBalancer
- ec2:DescribeAccountAttributes
- ec2:DescribeClassicLinkInstances
- ec2:DescribeInstances
- ec2:DescribeVpcClassicLink

Autorisations d'API Elastic Load Balancing pour baliser les ressources lors de la création

Pour que les utilisateurs puissent baliser les ressources lors de leur création, ils doivent disposer d'autorisations pour utiliser l'action qui crée la ressource, comme `elasticloadbalancing:CreateLoadBalancer` ou `elasticloadbalancing:CreateTargetGroup`. Si des balises sont spécifiées dans l'action de création de ressources, une autorisation supplémentaire est requise sur l'action `elasticloadbalancing:AddTags` pour vérifier si les utilisateurs disposent des autorisations nécessaires pour appliquer des balises aux ressources en cours de création. Par conséquent, les utilisateurs doivent également avoir des autorisations explicites d'utiliser l'action `elasticloadbalancing:AddTags`.

Dans la définition de politique IAM de l'action `elasticloadbalancing:AddTags`, vous pouvez utiliser l'élément `Condition` avec la clé de condition `elasticloadbalancing:CreateAction` pour accorder des autorisations de balisage à l'action qui crée la ressource.

L'exemple suivant illustre une stratégie qui permet aux utilisateurs de créer des groupes cibles et de leur appliquer des balises lors de la création. Les utilisateurs ne sont pas autorisés à attribuer des balises aux ressources existantes (ils ne peuvent pas appeler l'action `elasticloadbalancing:AddTags` directement).

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "elasticloadbalancing:CreateTargetGroup"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "elasticloadbalancing:AddTags"
      ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
```

```
            "elasticloadbalancing:CreateAction" : "CreateTargetGroup"
         }
      }
   }
  ]
}
```

De même, la stratégie suivante permet aux utilisateurs de créer un équilibreurs de charge et appliquer des balises lors de la création. Les utilisateurs ne sont pas autorisés à attribuer des balises aux ressources existantes (ils ne peuvent pas appeler l'action `elasticloadbalancing:AddTags` directement).

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "elasticloadbalancing:CreateLoadBalancer"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "elasticloadbalancing:AddTags"
      ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "elasticloadbalancing:CreateAction" : "CreateLoadBalancer"
         }
      }
    }
  ]
}
```

L'action `elasticloadbalancing:AddTags` est uniquement évaluée si les balises sont appliquées pendant l'action de création de ressources. Par conséquent, un utilisateur qui est autorisé à créer une ressource (en supposant qu'il n'existe aucune condition de balisage) n'a pas besoin des autorisations

d'utiliser l'action `elasticloadbalancing:AddTags` si aucune balise n'est spécifié dans la demande. Toutefois, si l'utilisateur essaie de créer une ressource avec des balises, la demande échoue s'il n'a pas les autorisations d'utiliser l'action `elasticloadbalancing:AddTags`.

Rôle lié à un service Elastic Load Balancing

Elastic Load Balancing utilise un rôle lié à un service pour les autorisations dont il a besoin pour appeler d'autres services AWS en votre nom. Pour plus d'informations, consultez Utilisation des rôles liés à un service dans le Guide de l'utilisateur IAM.

Autorisations accordées par le rôle lié à un service

Elastic Load Balancing utilise le rôle lié au service nommé AWSServiceRoleForElasticLoadBalancingpour effectuer les actions suivantes en votre nom :

- `ec2:AssignIpv6Addresses`
- `ec2:AssignPrivateIpAddresses`
- `ec2:AssociateAddress`
- `ec2:AttachNetworkInterface`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateNetworkInterface`
- `ec2:CreateSecurityGroup`
- `ec2:DeleteNetworkInterface`
- `ec2:DescribeAccountAttributes`
- `ec2:DescribeAddresses`
- `ec2:DescribeClassicLinkInstances`
- `ec2:DescribeCoipPools`
- `ec2:DescribeInstances`
- `ec2:DescribeInternetGateways`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcClassicLink`
- `ec2:DescribeVpcPeeringConnections`

- `ec2:DescribeVpcs`
- `ec2:DetachNetworkInterface`
- `ec2:DisassociateAddress`
- `ec2:GetCoipPoolUsage`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:ReleaseAddress`
- `ec2:UnassignIpv6Addresses`
- `logs:CreateLogDelivery`
- `logs:DeleteLogDelivery`
- `logs:GetLogDelivery`
- `logs:ListLogDeliveries`
- `logs:UpdateLogDelivery`
- `outposts:GetOutpostInstanceTypes`

AWSServiceRoleForElasticLoadBalancingfait confiance au `elasticloadbalancing.amazonaws.com` service pour assumer le rôle.

Création du rôle lié à un service

Vous n'avez pas besoin de créer manuellement le rôle lié à un service AWSServiceRoleForElasticLoadBalancing. Elastic Load Balancing crée ce rôle pour vous lorsque vous créez un équilibreur de charge ou un groupe cible.

Pour qu'Elastic Load Balancing crée un rôle lié à un service à votre place, vous devez avoir les autorisations requises. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Si vous avez créé un équilibreur de charge avant le 11 janvier 2018, Elastic Load Balancing l'a créé AWSServiceRoleForElasticLoadBalancingdans votre AWS compte. Pour plus d'informations, veuillez consulter Un nouveau rôle est apparu dans mon compte AWS dans le IAM Guide de l'utilisateur.

Modifier le rôle lié à un service

Vous pouvez modifier la description de l'AWSServiceRoleForElasticLoadBalancingutilisation d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Suppression du rôle lié à un service

Si vous n'avez plus besoin d'utiliser Elastic Load Balancing, nous vous recommandons de le supprimer AWSServiceRoleForElasticLoadBalancing.

Vous pouvez supprimer ce rôle lié à un service après avoir supprimé tous les équilibreurs de charge de votre compte AWS. Ainsi, vous ne pouvez pas involontairement supprimer l'autorisation d'accéder à vos équilibreurs de charge. Pour plus d'informations, consultez Supprimer un Application Load Balancer, Supprimer un Network Load Balancer et Supprimer un Classic Load Balancer.

Vous pouvez utiliser la console IAM, l'IAM CLI ou l'IAM API pour supprimer les rôles liés aux services. Pour de plus amples informations, veuillez consulter Suppression d'un rôle lié à un service dans le IAM Guide de l'utilisateur.

Après la suppression AWSServiceRoleForElasticLoadBalancing, Elastic Load Balancing crée à nouveau le rôle si vous créez un équilibreur de charge.

Politiques gérées par AWS pour Elastic Load Balancing

Pour ajouter des autorisations à des utilisateurs, des groupes et des rôles, il est plus facile d'utiliser des politiques gérées par AWS que d'écrire des politiques vous-même. Il faut du temps et de l'expertise pour créer des politiques gérées par le client IAM qui ne fournissent à votre équipe que les autorisations dont elle a besoin. Pour démarrer rapidement, vous pouvez utiliser nos politiques gérées par AWS. Ces politiques couvrent des cas d'utilisation courants et sont disponibles dans votre Compte AWS. Pour plus d'informations sur les politiques gérées par AWS, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

Les services AWS assurent la maintenance et la mise à jour des politiques gérées AWS. Vous ne pouvez pas modifier les autorisations définies dans les politiques gérées par AWS. Les services peuvent ajouter des autorisations supplémentaires à une politique gérée par AWS pour prendre en charge de nouvelles fonctionnalités. Ce type de mise à jour affecte toutes les identités (utilisateurs, groupes et rôles) auxquelles la politique est attachée. Les services sont très susceptibles de mettre à jour une politique gérée par AWS quand une nouvelle fonctionnalité est lancée ou quand de nouvelles opérations sont disponibles. Les services ne supprimant pas les autorisations d'une politique gérée par AWS, les mises à jour de politique n'interrompent vos autorisations existantes.

En outre, AWS prend en charge des politiques gérées pour des activités professionnelles couvrant plusieurs services. Par exemple, la politique ReadOnlyAccess gérée par AWS donne accès en lecture seule à l'ensemble des services et des ressources AWS. Quand un service lance une

nouvelle fonctionnalité, AWS ajoute des autorisations en lecture seule pour les nouvelles opérations et ressources. Pour obtenir une liste des politiques de fonctions et leur description, consultez Politiques gérées par AWS pour les fonctions de tâche dans le Guide de l'utilisateur IAM.

AWSpolitique gérée : AWSElasticLoadBalancingClassicServiceRolePolicy

Cette politique inclut toutes les autorisations dont Elastic Load Balancing (Classic Load Balancer) a besoin pour appeler d'autres services AWS en votre nom. Les rôles liés à un service sont prédéfinis. Avec des rôles prédéfinis, vous n'avez pas besoin d'ajouter manuellement les autorisations requises pour qu'Elastic Load Balancing effectue des actions en votre nom. Vous ne pouvez pas joindre, détacher, modifier ou supprimer cette politique.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSElasticLoadBalancingClassicServiceRolePolicyà la référence des politiques AWS gérées.

Stratégie AWS gérée : AWSElasticLoadBalancingServiceRolePolicy

Cette politique inclut toutes les autorisations dont Elastic Load Balancing a besoin pour appeler d'autres services AWS en votre nom. Les rôles liés à un service sont prédéfinis. Avec des rôles prédéfinis, vous n'avez pas besoin d'ajouter manuellement les autorisations requises pour qu'Elastic Load Balancing effectue des actions en votre nom. Vous ne pouvez pas joindre, détacher, modifier ou supprimer cette politique.

Pour consulter les autorisations associées à cette politique, reportez-vous AWSElasticLoadBalancingServiceRolePolicyà la référence des politiques AWS gérées.

Stratégie AWS gérée : ElasticLoadBalancingFullAccess

Cette politique donne un accès complet au service Elastic Load Balancing et un accès limité aux autres services via la console de gestion AWS.

Pour consulter les autorisations associées à cette politique, reportez-vous ElasticLoadBalancingFullAccessà la référence des politiques AWS gérées.

Stratégie AWS gérée : ElasticLoadBalancingReadOnly

Cette politique fournit un accès en lecture seule à Elastic Load Balancing et aux services dépendants.

Pour consulter les autorisations associées à cette politique, reportez-vous ElasticLoadBalancingReadOnlyà la référence des politiques AWS gérées.

Les mises à jour apportées par Elastic Load Balancing aux politiques gérées par AWS

Consultez les détails des mises à jour des stratégies gérées AWS pour Elastic Load Balancing depuis que ce service a commencé à suivre ces modifications.

Modification	Description	Date
Stratégie AWS gérée : ElasticLoadBalancingFullAccess – Mettre à jour vers une politique existante.	Elastic Load Balancing a ajouté une nouvelle action permettant d'autoriser l'utilisation du changement de zone. Cette action a été ajoutée à la stratégie d'accès complet d'Elastic Load Balancing. Il est associé aux opérations de l'API `arc-zonal-shift:*` .	28 novembre 2022
Stratégie AWS gérée : ElasticLoadBalancingReadOnly – Mettre à jour vers une politique existante.	Elastic Load Balancing a ajouté une nouvelle action permettant d'autoriser l'utilisation du changement de zone. Cette action a été ajoutée à la politique de lecture seule d'Elastic Load Balancing. Il est associé aux opérations de l'API `arc-zonal-shift:GetManagedResource` , `arc-zonal-shift:ListManagedResources` et `arc-zonal-shift:ListZonalShifts` .	28 novembre 2022
Stratégie AWS gérée : AWSElasticLoadBalancingServiceRolePolicy – Mettre à jour vers une politique existante.	Elastic Load Balancing a ajouté une nouvelle action permettant d'autoriser l'utilisation de connexions d'appairage. Cette action a été ajoutée à la politique des rôles liés à un service, pour le plan de contrôle Elastic Load Balancing. Il est associé à l'opération de l'API `ec2:DescribeVpcPeeringConnections` .	11 octobre 2021
Stratégie AWS gérée : ElasticLoadBalancingFullAccess – Mettre à jour vers une politique existante.	Elastic Load Balancing a ajouté une nouvelle action permettant d'autoriser l'utilisation de connexions d'appairage. Cette action a été ajoutée à la stratégie d'accès complet d'Elastic Load Balancing. Il est associé à l'opération de	11 octobre 2021

Modification	Description	Date
	l'API `ec2:DescribeVpcPeeringConnections` .	
AWSpolitique gérée : AWSElasticLoadBalancingClassicServiceRolePolicy – Mettre à jour vers une politique existante.	Elastic Load Balancing a ajouté une politique de rôle liée à un service (pour le plan de contrôle) pour le Classic Load Balancer. Cette mise à jour concerne la version 2 (par défaut).	7 octobre 2019
Stratégie AWS gérée : ElasticLoadBalancingReadOnly	Fournit un accès en lecture seule à Elastic Load Balancing et aux services dépendants. Il s'agit de la version 1 (par défaut).	20 septembre 2018
Elastic Load Balancing a commencé à suivre les modifications	Elastic Load Balancing a commencé à suivre les modifications pour ses politiques gérées par AWS.	23 juillet 2021

Validation de la conformité pour Elastic Load Balancing

Pour savoir si un Service AWS fait partie du champ d'application de programmes de conformité spécifiques, consultez Services AWS dans le champ d'application par programme de conformité et choisissez le programme de conformité qui vous intéresse. Pour obtenir des renseignements généraux, consultez Programmes de conformité AWS.

Vous pouvez télécharger les rapports d'audit externes avec AWS Artifact. Pour plus d'informations, consultez Téléchargement des rapports dans AWS Artifact.

Votre responsabilité de conformité lors de l'utilisation de Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise, ainsi que par la législation et la réglementation applicables. AWS fournit les ressources suivantes pour faciliter le respect de la conformité :

- Guides Quick Start de la sécurité et de la conformité : ces guides de déploiement traitent de considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de référence dans AWS centrés sur la sécurité et la conformité.

- Architecture pour la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent utiliser AWS pour créer des applications éligibles à la loi HIPAA.

  > **Note**
  >
  > Tous les Services AWS ne sont pas éligibles à HIPAA. Pour plus d'informations, consultez HIPAA Eligible Services Reference.

- Ressources de conformité AWS : cet ensemble de manuels et de guides peut s'appliquer à votre secteur d'activité et à votre emplacement.
- AWSGuides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide de règles dans le Guide du développeur AWS Config : le service AWS Config évalue dans quelle mesure vos configurations de ressources sont conformes aux pratiques internes, aux directives sectorielles et aux réglementations.
- AWS Security Hub : ce Service AWS fournit une vue complète de votre état de sécurité dans AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- AWS Audit Manager : ce service Service AWS vous aide à auditer en continu votre utilisation d'AWS pour simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans Elastic Load Balancing

L'infrastructure mondiale d'AWS repose sur les régions et les zones de disponibilité AWS. Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, reliées par un réseau à latence faible, à débit élevé et à forte redondance. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage

disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les régions et les zones de disponibilité AWS, consultez AWS Infrastructure mondiale.

Outre l'infrastructure mondiale AWS, Elastic Load Balancing propose les fonctionnalités suivantes pour la prise en charge de la résilience des données :

- Distribue le trafic entrant sur plusieurs instances dans une ou plusieurs zones de disponibilité.
- Vous pouvez utiliser AWS Global Accelerator avec vos Application Load Balancers pour distribuer le trafic entrant sur plusieurs équilibreurs de charge dans une ou plusieurs régions AWS. Pour plus d'informations, consultez le Guide du développeur AWS Global Accelerator.
- Amazon ECS vous permet d'exécuter, d'arrêter et de gérer des conteneurs Docker sur un cluster d'instances EC2. Vous pouvez configurer votre service Amazon ECS pour qu'il utilise un équilibreur de charge afin de distribuer le trafic entrant entre les services d'un cluster. Pour plus d'informations, consultez le Guide du développeur Amazon Elastic Container Service.

Sécurité de l'infrastructure dans Elastic Load Balancing

En tant que service géré, Elastic Load Balancing est protégé par la sécurité du réseau mondial AWS. Pour plus d'informations sur les services de sécurité AWS et la manière dont AWS protège l'infrastructure, consultez la section Sécurité du cloud AWS. Pour concevoir votre environnement AWS en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le Security Pillar AWS Well-Architected Framework (Pilier de sécurité de l'infrastructure Well-Architected Framework).

Vous utilisez les appels d'API AWS publiés pour accéder à Elastic Load Balancing via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service

(AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Isolement de réseau

Un Virtual Private Cloud (VPC) est un réseau virtuel situé dans votre propre zone logiquement isolée dans le cloud AWS. Un sous-réseau est une plage d'adresses IP dans un VPC. Lorsque vous créez un équilibreur de charge, vous pouvez spécifier un ou plusieurs sous-réseaux pour les nœuds d'équilibreur de charge. Vous pouvez déployer des instances EC2 dans les sous-réseaux de votre VPC et les enregistrer auprès de votre équilibreur de charge. Pour plus d'informations sur les VPC et les sous-réseaux, consultez le Guide de l'utilisateur Amazon VPC.

Lorsque vous créez un équilibreur de charge dans un VPC, il peut être connecté à Internet ou interne. Un équilibreur de charge interne peut acheminer uniquement des demandes provenant de clients ayant un accès au VPC de l'équilibreur de charge.

Votre équilibreur de charge envoie des demandes à ses cibles enregistrées en utilisant des adresses IP privées. Par conséquent, vos cibles n'ont pas besoin d'adresses IP publiques pour recevoir des demandes de la part d'un équilibreur de charge.

Pour appeler l'API Elastic Load Balancing depuis votre VPC à l'aide d'adresses IP privées, utilisez AWS PrivateLink. Pour plus d'informations, consultez Accès à Elastic Load Balancing à l'aide d'un point de terminaison d'interface (AWS PrivateLink).

Contrôle du trafic réseau

Tenez compte des options suivantes pour sécuriser le trafic réseau lorsque vous utilisez un équilibreur de charge :

- Utilisez des écouteurs sécurisés pour prendre en charge les communications chiffrées entre les clients et vos équilibreurs de charge. Les Application Load Balancer prennent en charge les écouteurs HTTPS. Les Network Load Balancers prennent en charge les écouteurs TLS. Classic Load Balancers prennent en charge les écouteurs HTTPS et TLS. Vous pouvez choisir parmi les stratégies de sécurité prédéfinies de sorte que votre équilibreur de charge spécifie les suites de chiffrement et les versions de protocole prises en charge par votre application. Vous pouvez utiliser AWS Certificate Manager (ACM) ou AWS Identity and Access Management (IAM) pour gérer les certificats de serveur installés sur votre équilibreur de charge. Vous pouvez utiliser le protocole SNI (Server Name Indication) pour desservir plusieurs sites Web sécurisés à l'aide d'un seul écouteur

sécurisé. SNI est automatiquement activé pour votre équilibreur de charge lorsque vous associez plusieurs certificats de serveur à un écouteur sécurisé.

- Configurez les groupes de sécurité pour vos Application Load Balancers et Classic Load Balancers de manière à accepter le trafic provenant uniquement de clients spécifiques. Ces groupes de sécurité doivent autoriser le trafic entrant en provenance des clients sur les ports d'écoute et le trafic sortant vers les clients.
- Configurez les groupes de sécurité pour que vos instances Amazon EC2 acceptent uniquement le trafic provenant de l'équilibreur de charge. Ces groupes de sécurité doivent autoriser le trafic entrant à partir de l'équilibreur de charge sur les ports d'écoute et les ports de vérification de l'état.
- Configurez votre Application Load Balancer pour authentifier en toute sécurité les utilisateurs via un fournisseur d'identité ou à l'aide d'identités d'entreprise. Pour plus d'informations, consultez Authentification des utilisateurs à l'aide d'un Application Load Balancer.
- Utilisez AWS WAF avec vos Application Load Balancers pour autoriser ou bloquer des demandes en fonction des règles d'une liste de contrôle d'accès web (ACL web).

Accés à Elastic Load Balancing à l'aide d'un point de terminaison d'interface (AWS PrivateLink)

Vous pouvez établir une connexion privée entre votre cloud privé virtuel (VPC) et l'API Elastic Load Balancing en créant un point de terminaison d'un VPC d'interface. Vous pouvez utiliser cette connexion pour appeler l'API Elastic Load Balancing à partir de votre VPC sans avoir à associer une passerelle Internet, une instance NAT ou une connexion VPN à votre VPC. Le point de terminaison fournit une connectivité fiable et évolutive à l'API Elastic Load Balancing, versions 2015-12-01 et 2012-06-01, que vous utilisez pour créer et gérer vos équilibreurs de charge.

Les points de terminaison d'un VPC d'interface sont alimentés par AWS PrivateLink, une fonctionnalité qui permet la communication entre vos applications et Services AWS à l'aide d'adresses IP privées. Pour de plus amples informations, veuillez consulter AWS PrivateLink.

Limite

AWS PrivateLink ne prend pas en charge Network Load Balancers avec plus de 50 écouteurs.

Création d'un point de terminaison d'interface pour Elastic Load Balancing

Création d'un point de terminaison pour Elastic Load Balancing à l'aide du nom de service suivant :

```
com.amazonaws.region.elasticloadbalancing
```

Pour de plus amples informations, veuillez consulter Créer un point de terminaison d'interface dans le Guide AWS PrivateLink.

Création d'une politique de point de terminaison d'un VPC pour Elastic Load Balancing

Vous pouvez attacher une stratégie à votre point de terminaison d'un VPC pour contrôler l'accès à l'API Elastic Load Balancing. La politique spécifie :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- La ressource sur laquelle les actions peuvent être effectuées.

L'exemple suivant montre une stratégie de point de terminaison VPC qui refuse à tout le monde l'autorisation de créer un équilibreur de charge via le point de terminaison. L'exemple de politique accorde également à tout le monde l'autorisation d'effectuer toutes les autres actions.

```
{
   "Statement": [
        {
            "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*"
        },
        {
            "Action": "elasticloadbalancing:CreateLoadBalancer",
            "Effect": "Deny",
            "Resource": "*",
            "Principal": "*"
        }
    ]
}
```

Pour plus d'informations, consultez Contrôle de l'accès aux services à l'aide de politiques de point de terminaison dans le Guide AWS PrivateLink.

Migration de votre Classic Load Balancer

Elastic Load Balancing prend en charge les types d'équilibreurs de charge suivants : Application Load Balancers, Network Load Balancers, Gateway Load Balancers et Classic Load Balancers. Pour en savoir plus sur les différentes fonctionnalités de chaque type d'équilibreur de charge, consultez Comparaison des produits Elastic Load Balancing.

Vous pouvez également choisir de migrer un Classic Load Balancer existant dans un VPC vers un Application Load Balancer ou un Network Load Balancer.

Avantages de la migration depuis un Classic Load Balancer

Chaque type d'équilibreur de charge possède ses propres caractéristiques, fonctions et configurations uniques. Passez en revue les avantages de chaque équilibreur de charge pour choisir celui qui vous convient le mieux.

Application Load Balancer

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

Support pour :

- Conditions de chemin, conditions d'hôte et conditions d'en-tête HTTP.
- Redirection des demandes d'une URL vers une autre et routage des demandes vers plusieurs applications sur une seule instance EC2.
- Renvoyer des réponses HTTP personnalisées.
- Enregistrement des cibles par adresse IP et enregistrement des fonctions Lambda en tant que cibles. Y compris des cibles extérieures au VPC pour l'équilibreur de charge.
- Authentification des utilisateurs par le biais d'identités professionnelles ou sociales.
- Applications conteneurisées Amazon Elastic Container Service (Amazon ECS).
- Surveillance indépendante de l'état de santé de chaque service.

Les journaux d'accès contiennent des informations supplémentaires et sont stockés dans un format compressé.

Amélioration globale des performances de l'équilibreur de charge.

Network Load Balancer

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

Support pour :

- Adresses IP statiques, qui permettent d'attribuer une adresse IP élastique par sous-réseau activé pour l'équilibreur de charge.
- Enregistrement des cibles par adresse IP, y compris des cibles situées en dehors du VPC pour l'équilibreur de charge.
- Acheminement des demandes vers plusieurs applications sur une seule instance EC2.
- Applications conteneurisées Amazon Elastic Container Service (Amazon ECS).
- Surveillance indépendante de l'état de santé de chaque service.

Possibilité de traiter des charges de travail volatiles et de passer à des millions de requêtes par seconde.

Migrer en utilisant l'assistant de migration

L'assistant de migration utilise la configuration de votre Classic Load Balancer pour créer un Application Load Balancer ou un Network Load Balancer équivalent. Elle réduit le temps et les efforts nécessaires à la migration d'un Classic Load Balancer par rapport aux autres méthodes.

> **Note**
>
> L'assistant crée un nouvel équilibreur de charge. L'assistant ne convertit pas le Classic Load Balancer existant en Application Load Balancer ou Network Load Balancer. Vous devez rediriger manuellement le trafic vers le nouvel équilibreur de charge.

Limites

- Le nom du nouvel équilibreur de charge ne peut pas être identique à celui d'un équilibreur de charge existant du même type, dans la même région.

- Si le Classic Load Balancer possède des balises contenant le `aws:` préfixe dans leur clé, ces balises ne sont pas migrées.

Lors de la migration vers un Application Load Balancer

- Si le Classic Load Balancer ne possède qu'un seul sous-réseau, vous devez en spécifier un deuxième.
- Si le Classic Load Balancer possède des écouteurs HTTP/HTTPS qui utilisent des contrôles de santé TCP, le protocole de contrôle de santé est mis à jour vers HTTP et le chemin est défini sur «/».
- Si le Classic Load Balancer possède des écouteurs HTTPS utilisant une politique de sécurité personnalisée ou non prise en charge, l'assistant de migration utilise la politique de sécurité par défaut pour le nouveau type d'équilibreur de charge.

Lors de la migration vers un Network Load Balancer

- Les types d'instances suivants ne seront pas enregistrés auprès du nouveau groupe cible : C1, CC1, CC2, CG1, CG2, CR1, CS1, G1, G2, HI1, HS1, M1, M2, M3, T1
- Certains paramètres de contrôle de santé de votre Classic Load Balancer peuvent ne pas être transférables au nouveau groupe cible. Ces cas seront indiqués sous forme de modification dans la section récapitulative de l'assistant de migration.
- Si le Classic Load Balancer possède des écouteurs SSL, l'assistant de migration crée un écouteur TLS en utilisant le certificat et la politique de sécurité de l'écouteur SSL.

Processus de l'assistant de migration

Pour migrer un Classic Load Balancer à l'aide de l'assistant de migration

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 Classic Load Balancer que vous souhaitez migrer.
4. Dans la section Détails des équilibreurs de charge, choisissez Lancer l'assistant de migration.
5. Choisissez Migrate to Application Load Balancer ou Migrate to Network Load Balancer pour ouvrir l'assistant de migration.

6. Sous Nom du nouvel équilibreur de charge, dans Nom de l'équilibreur de charge, entrez le nom de votre nouvel équilibreur de charge.
7. Sous Nommer le nouveau groupe cible et passer en revue les cibles, dans Nom du groupe cible, saisissez le nom de votre nouveau groupe cible.
8. (Facultatif) Sous Cibles, vous pouvez consulter les instances cibles qui seront enregistrées auprès du nouveau groupe cible.
9. (Facultatif) Sous Vérifier les balises, vous pouvez consulter les balises qui seront appliquées à votre nouvel équilibreur de charge
10. Sous Résumé pour Application Load Balancer ou Résumé pour Network Load Balancer, passez en revue et vérifiez les options de configuration attribuées par l'assistant de migration.
11. Une fois que vous êtes satisfait du résumé de la configuration, choisissez Create Application Load Balancer ou Create Network Load Balancer pour démarrer la migration.

Migrer à l'aide de l'utilitaire de copie de l'équilibreur de charge

Les utilitaires de copie de l'équilibreur de charge sont disponibles dans le référentiel Elastic Load Balancing Tools, sur la AWS GitHub page.

Ressources

- Outils Elastic Load Balancing
- Utilitaire de copie Classic Load Balancer vers Application Load Balancer
- Utilitaire de copie Classic Load Balancer vers Network Load Balancer

Migrez votre équilibreur de charge manuellement

Les informations suivantes fournissent des instructions générales pour créer manuellement un nouvel Application Load Balancer ou un Network Load Balancer basé sur un Classic Load Balancer existant dans un VPC. Vous pouvez effectuer la migration à l'aide du AWS Management Console AWS CLI, du ou d'un AWS SDK. Pour plus d'informations, consultez Prise en main d'Elastic Load Balancing.

Une fois que vous avez terminé le processus de migration, vous pouvez tirer parti des fonctions de votre nouvel équilibreur de charge.

Processus de migration manuel

Étape 1 : Créer un équilibreur de charge

Créez un équilibreur de charge avec une configuration équivalente au Classic Load Balancer à migrer.

1. Créez un équilibreur de charge, avec la même méthode (accessible sur Internet ou interne), les mêmes sous-réseaux et groupes de sécurité que le Classic Load Balancer.
2. Créez un seul groupe cible pour votre équilibreur de charge, avec les mêmes paramètres de surveillance de l'état dont vous disposez pour votre Classic Load Balancer.
3. Effectuez l'une des actions suivantes :
   - Si votre Classic Load Balancer est attaché à un groupe Auto Scaling, attachez votre groupe cible au groupe Auto Scaling. Cette action enregistre également les instances Auto Scaling auprès du groupe cible.
   - Enregistrez vos instances EC2 auprès de votre groupe cible.
4. Créez un ou plusieurs écouteurs, chacun avec une règle par défaut qui transfère les demandes vers le groupe cible. Si vous créez un écouteur HTTPS, vous pouvez spécifier le même certificat que celui que vous avez spécifié pour votre Classic Load Balancer. Nous vous recommandons d'utiliser la stratégie de sécurité par défaut.
5. Si votre Classic Load Balancer a des balises, passez-les en revue et ajoutez les balises appropriées pour à nouvel équilibreur de charge.

Étape 2 : Rediriger progressivement du trafic vers votre nouvel équilibreur de charge

Une fois que vos instances sont enregistrées auprès de votre nouvel équilibreur de charge, vous pouvez commencer le processus de redirection du trafic de l'ancien équilibreur de charge vers le nouveau. Cela vous permet de tester votre nouvel équilibreur de charge tout en minimisant les risques liés à la disponibilité de votre application.

Pour rediriger progressivement le trafic vers votre nouvel équilibreur de charge

1. Collez le nom DNS de votre nouvel équilibreur de charge dans le champ d'adresse d'un navigateur web connecté à Internet. Si tout fonctionne, le navigateur affiche la page par défaut de votre application.
2. Créez un enregistrement DNS qui associe votre nom de domaine à votre nouvel équilibreur de charge. Si votre service DNS prend en charge la répartition de charge, spécifiez un poids

de 1 dans le nouvel enregistrement DNS et un poids de 9 dans l'enregistrement DNS existant pour votre ancien équilibreur de charge. Cela permet de diriger 10 % du trafic vers le nouvel équilibreur de charge et 90 % du trafic vers l'ancien équilibreur de charge.

3. Surveillez votre nouvel équilibreur de charge pour vérifier qu'il reçoit le trafic et qu'il achemine les demandes vers vos instances.

> **Important**
>
> Le time-to-live (TTL) dans l'enregistrement DNS est de 60 secondes. Cela signifie que tout serveur DNS qui résout votre nom de domaine conserve les informations de l'enregistrement dans son cache pendant 60 secondes, tandis que les modifications se propagent. Par conséquent, ces serveurs DNS peuvent encore acheminer le trafic vers votre ancien équilibreur de charge jusqu'à 60 secondes après la fin de l'étape précédente. Lors de la propagation, le trafic peut être dirigé vers n'importe quel équilibreur de charge.

4. Continuez à mettre à jour le poids de vos enregistrements DNS jusqu'à ce que l'ensemble du trafic soit dirigé vers votre nouvel équilibreur de charge. Lorsque vous avez terminé, vous pouvez supprimer l'enregistrement DNS de votre ancien équilibreur de charge.

Étape 3 : mettre à jour les politiques, les scripts et le code

Si vous avez migré votre Classic Load Balancer vers un Application Load Balancer ou un Network Load Balancer, veillez à effectuer les opérations suivantes :

- Mettez à jour les politiques IAM qui utilisent la version d'API 2012-06-01 pour utiliser la version 2015-12-01.
- Mettez à jour les processus qui utilisent CloudWatch les métriques de l'espace de `AWS/ELB` noms pour utiliser les métriques de l'espace de `AWS/NetworkELB` noms `AWS/ApplicationELB` or.
- Mettez à jour les scripts qui utilisent aws elb AWS CLI des commandes pour utiliser aws elbv2 AWS CLI des commandes.
- Mettez à jour les AWS CloudFormation modèles qui utilisent la `AWS::ElasticLoadBalancing::LoadBalancer` ressource pour utiliser les `AWS::ElasticLoadBalancingV2` ressources.
- Mettez à jour le code qui utilise la version d'API Elastic Load Balancing 2012-06-01 pour utiliser la version 2015-12-01.

Ressources

- elbv2 dans la Référence de commande de l'AWS CLI
- Référence d'API Elastic Load Balancing (version 2015-12-01)
- Gestion des identités et des accès pour Elastic Load Balancing
- Métriques Application Load Balancer dans le Guide de l'utilisateur pour Application Load Balancers
- Métriques Network Load Balancer dans le Guide de l'utilisateur pour Network Load Balancers
- AWS::ElasticLoadBalancingV2::LoadBalancer dans le guide de l'utilisateur AWS CloudFormation

Étape 4 : supprimer l'ancien équilibreur de charge

Vous pouvez supprimer l'ancien Classic Load Balancer une fois que :

- Vous avez redirigé tout le trafic de l'ancien équilibreur de charge vers le nouveau.
- Toutes les demandes existantes qui ont été acheminées vers l'ancien équilibreur de charge ont abouti.

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.