Guide de l'utilisateur

Elastic Load Balancing

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Elastic Load Balancing: Guide de l’utilisateur

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Qu'est-ce qu'Elastic Load Balancing ? ... 1
Avantages offerts par l'équilibreur de charge ... 1
Caractéristiques d'Elastic Load Balancing ... 1
Accès à Elastic Load Balancing ... 2
Services connexes ... 2
Tarification ... 4
Fonctionnement d'Elastic Load Balancing ... 5
Zones de disponibilité et nœuds d'équilibreurs de charge ... 5
Equilibrage de charge entre zones ... 6
Changement de zone ... 9
Routage des demandes ... 9
Algorithme de routage ... 10
Connexions HTTP ... 11
En-têtes HTTP ... 12
Limites des en-têtes HTTP ... 13
Schéma d'un équilibreur de charge ... 13
Types d'adresses IP ... 14
MTU réseau ... 16
Premiers pas ... 17
Création d'un Application Load Balancer ... 17
Créer un Network Load Balancer ... 17
Création d'un Gateway Load Balancer ... 18
Sécurité ... 19
Protection des données ... 20
Chiffrement au repos ... 21
Chiffrement en transit ... 21
Gestion des identités et des accès ... 22
Public ciblé ... 22
Authentification par des identités ... 23
Gestion des accès à l'aide de politiques ... 27
Comment Elastic Load Balancing fonctionne avec IAM ... 30
Autorisations de l'API de balisage des ressources ... 43
Rôle lié à un service ... 45
AWS politiques gérées ... 46

Validation de conformité 49
Résilience 50
Sécurité de l'infrastructure 51
Isolement de réseau 52
Contrôle du trafic réseau 52
AWS PrivateLink 53
Création d'un point de terminaison d'interface pour Elastic Load Balancing 54
Création d'une politique de point de terminaison d'un VPC pour Elastic Load Balancing 54
Limitation des demandes d'API 56
Comment l'étranglement est appliqué 56
Limitation du débit de demande 57
Demandez la taille des seaux de jetons et les taux de recharge 57
Surveillance des demandes d'API 61
Rapports de facturation et d'utilisation 62
Application Load Balancers 62
Network Load Balancers 63
Gateway Load Balancers 63
Équilibreurs de charge classiques 63
Journalisation des appels d'API 65
Événements de gestion d'Elastic Load Balancing dans CloudTrail 66
Exemples d'événements Elastic Load Balancing 67
Migration de votre Classic Load Balancer 72
Les avantages de la migration 72
Assistant de migration 73
Migration de l'utilitaire de copie 75
Migration manuelle 75
Empêcher les utilisateurs de créer des équilibreurs de charge classiques 78
..... lxxx

Qu’est-ce qu’Elastic Load Balancing ?

Elastic Load Balancing distribue automatiquement votre trafic entrant sur plusieurs cibles, telles que EC2 les instances, les conteneurs et les 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 plusieurs types d'équilibreurs de charge. Vous pouvez sélectionner le type d'équilibreur de charge qui correspond le mieux à vos besoins. Pour plus d'informations, consultez la section .

Pour plus d'informations sur les équilibreurs de charge de la génération actuelle, 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

Les Classic Load Balancers sont la précédente génération d'équilibreurs de charge d'Elastic Load Balancing. Nous vous recommandons de migrer vers un équilibreur de charge de génération actuelle. Pour plus d'informations, consultez Migrer votre Classic Load Balancer.

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.
- AWS Interface de ligne de commande (AWS CLI) : fournit des commandes pour un large éventail de AWS services, notamment Elastic Load Balancing. AWS CLI Il est pris en charge sur Windows, macOS et Linux. Pour de plus amples informations, veuillez consulter AWS Command Line Interface.
- AWS SDKs— Fournissez des informations spécifiques à la langue APIs et prenez en charge de nombreux détails de connexion, tels que le calcul des signatures, la gestion des nouvelles tentatives de demande et la gestion des erreurs. Pour de plus amples informations, veuillez consulter AWS SDKs.
- 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 :
  - Équilibreurs de charge d'application, équilibreurs de charge réseau et équilibreurs de charge de passerelle — version API 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 EC2 instances. Pour plus d'informations, consultez le guide de EC2 l'utilisateur Amazon.

- 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 en fonction de l'évolution de la demande sur vos instances. 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 d'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 — Vous permet de surveiller votre équilibreur de charge et de prendre les mesures nécessaires. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.
- Amazon ECS — Vous permet d'exécuter, d'arrêter et de gérer des conteneurs Docker sur un cluster d' EC2 instances. 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 AWS régions. Pour plus d'informations, consultez le Manuel 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, cela se `www.example.com` traduirait par l'adresse `192.0.2.1` IP numérique. AWS affecte URLs 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 votre Application Load Balancer pour autoriser ou bloquer les demandes en fonction des règles d'une liste de contrôle d'accès Web (ACL Web). Pour plus d'informations, consultez le Manuel 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 en provenance des clients et achemine les demandes vers ses cibles enregistrées (telles que EC2 les instances) 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.

Table des matières

- Zones de disponibilité et nœuds d'équilibreurs de charge
- Routage des demandes
- Schéma d'un équilibreur de charge
- Types d'adresses IP
- MTU réseau pour votre 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.

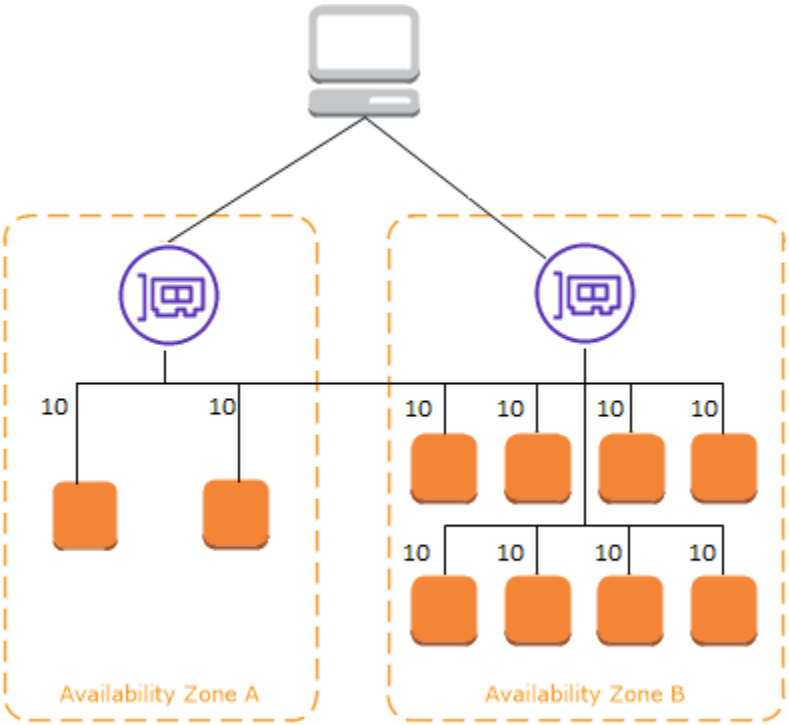
Une fois qu'une zone de disponibilité est désactivée, les cibles de cette zone de disponibilité restent enregistrées auprès de l'équilibreur de charge. Cependant, même si elles restent enregistrées, l'équilibreur de charge ne leur achemine plus de trafic.

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.

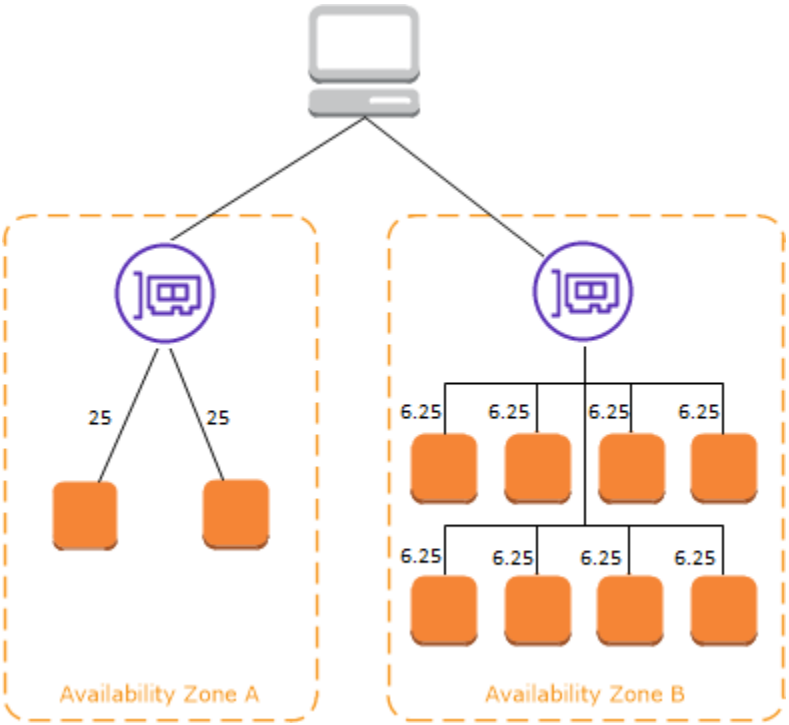
Si l'équilibrage de charge entre zones est activé, chacune des 10 cibles reçoit 10 % du trafic. En effet, chaque nœud d'équilibreur de charge peut acheminer ses 50 % du trafic client vers l'ensemble des 10 cibles.



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. Pour plus d'informations, consultez la section Équilibrage de charge entre zones dans le Guide de l'utilisateur pour les équilibreurs de charge réseau.

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 d'Amazon Application Recovery Controller (ARC) (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. L'ARC crée le décalage 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, consultez Comment fonctionne un changement de zone : bilans de santé et adresses IP zonales dans le manuel du développeur Amazon Application Recovery Controller (ARC).

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

- Le décalage de zone est pris en charge lorsque vous utilisez un Network Load Balancer avec l'équilibrage de charge entre zones activé ou désactivé.
- 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.

Pour plus de conseils et d'informations, consultez les meilleures pratiques pour les changements de zone dans ARC dans le manuel du développeur Amazon Application Recovery Controller (ARC).

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 Gateway Load Balancers, le nœud d'équilibrage de charge qui reçoit la connexion utilise un algorithme de hachage de flux à 5 tuples pour sélectionner un dispositif cible. Une fois qu'un flux est établi, tous les paquets du même flux sont systématiquement acheminés vers le même dispositif cible. L'équilibreur de charge et les appareils cibles échangent du trafic à l'aide du protocole GENEVE sur le port 6081.

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.

Types d'adresses IP

Le type d'adresse IP que vous spécifiez pour votre équilibreur de charge détermine la manière dont les clients peuvent communiquer avec l'équilibreur de charge.

- IPv4 uniquement — Les clients communiquent en utilisant des IPv4 adresses publiques et privées. Les sous-réseaux que vous sélectionnez pour votre équilibreur de charge doivent comporter des plages d' IPv4 adresses.
- Dualstack — Les clients communiquent en utilisant des adresses et des adresses publiques IPv4 et IPv6 privées. Les sous-réseaux que vous sélectionnez pour votre équilibreur de charge doivent comporter des plages IPv4 d' IPv6 adresses.
- Dualstack sans public IPv4 — Les clients communiquent en utilisant des adresses publiques et privées et IPv6 des adresses privées IPv4 . Les sous-réseaux que vous sélectionnez pour votre équilibreur de charge doivent comporter des plages IPv4 d' IPv6 adresses. Cette option n'est pas prise en charge avec le schéma d'`internal`équilibrage de charge.

Le tableau suivant décrit les types d'adresses IP pris en charge pour chaque type d'équilibreur de charge.

Nouveau type d'équilibreur de charge	IPv4 uniquement	Double pile	Dualstack sans public IPv4
Application Load Balancer	Oui	Oui	Oui
Network Load Balancer	Oui	Oui	Non
Passerelle équilibreur de charge	Oui	Oui	Non

Nouveau type d'équilibreur de charge	IPv4 uniquement	Double pile	Dualstack sans public IPv4
Classic Load Balancer	Oui	Non	Non

Le type d'adresse IP que vous spécifiez pour votre groupe cible détermine la manière dont l'équilibreur de charge peut communiquer avec les cibles.

- IPv4 uniquement — L'équilibreur de charge communique à l'aide d' IPv4 adresses privées. Vous devez enregistrer les cibles avec IPv4 des adresses appartenant à un groupe IPv4 cible.
- IPv6 uniquement — L'équilibreur de charge communique à l'aide d' IPv6 adresses. Vous devez enregistrer les cibles avec IPv6 des adresses appartenant à un groupe IPv6 cible. Le groupe cible doit être utilisé avec un équilibreur de charge à double pile.

Le tableau suivant décrit les types d'adresses IP pris en charge pour chaque protocole de groupe cible.

Protocole du groupe cible	IPv4 uniquement	IPv6 uniquement	
HTTP et HTTPS	Oui	Oui	
TCP	Oui	Oui	
TLS	Oui	Oui	
UDP et TCP_UDP	Oui	Oui	
GENEVE	-	-	

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 plus d'informations sur Path MTU Discovery et sur l'activation des trames jumbo, consultez Path MTU Discovery dans le guide de l'utilisateur Amazon EC2 .

Prise en main d'Elastic Load Balancing

Elastic Load Balancing prend en charge plusieurs types d'équilibreurs de charge. Vous pouvez sélectionner le type d'équilibreur de charge qui correspond le mieux à vos besoins. Pour plus d'informations, consultez la section .

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
- Créer un Network Load Balancer
- Création d'un Gateway Load Balancer

Création d'un Application Load Balancer

Pour créer un équilibreur de charge d'application à l'aide de AWS Management Console, consultez la section Getting started with Application Load Balancers dans le guide de l'utilisateur pour les équilibreurs de charge d'application.

Pour créer un équilibreur de charge d'application à l'aide du AWS CLI, reportez-vous à la section Créer un équilibreur de charge d'application à l'aide AWS CLI du guide de l'utilisateur pour les équilibreurs de charge d'application.

Créer un Network Load Balancer

Pour créer un Network Load Balancer à l'aide de AWS Management Console, voir Getting started with Network Load Balancers dans le Guide de l'utilisateur des Network Load Balancers.

Pour créer un Network Load Balancer à l'aide du AWS CLI, reportez-vous à la section Create a Network Load Balancer using the in AWS CLIthe User Guide for Network Load Balancers.

Création d'un Gateway Load Balancer

Pour créer un Gateway Load Balancer à l'aide de AWS Management Console, consultez Getting started with Gateway Load Balancers dans le Guide de l'utilisateur des Gateway Load Balancers.

Pour créer un Gateway Load Balancer à l'aide du AWS CLI, consultez Getting started with Gateway Load Balancers using the AWS CLI in the User Guide for Gateway Load Balancers.

La sécurité dans Elastic Load Balancing

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

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

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le AWS cadre des programmes de de). Pour en savoir plus sur les programmes de conformité qui s'appliquent à Elastic Load Balancing, consultez la section AWS services concernés par programme de conformité et .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service 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 apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à 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'appliances répertoriés dans la liste des partenaires Elastic Load Balancing ont intégré et qualifié leur logiciel d'appliance avec AWS. Vous pouvez accorder une plus grande confiance aux logiciels d'appareils fournis par les prestataires figurant dans cette liste. Toutefois, AWS cela ne garantit pas la sécurité ou la fiabilité des logiciels de ces fournisseurs.

Table des matières

- Protection des données dans Elastic Load Balancing

- 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 plus d'informations 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. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- 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 140-3 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez Norme FIPS (Federal Information Processing Standard) 140-3.

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 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 SDKs. Toutes les données que vous entrez 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 effectue le chiffrement et le déchiffrement du trafic, au lieu de demander à chaque EC2 instance de gérer le travail de terminaison du protocole 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 outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. 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 outil que vous pouvez utiliser sans frais supplémentaires.

Table des matières

- Public ciblé
- Authentification par des identités
- Gestion des accès à l'aide de politiques
- Comment Elastic Load Balancing fonctionne avec IAM
- Autorisations d'API Elastic Load Balancing pour baliser les ressources lors de la création
- Rôle lié à un service Elastic Load Balancing
- AWS politiques gérées pour Elastic Load Balancing

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez 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 est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification 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 l'aide de la fédération, vous assumez indirectement un rôle.

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

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez AWS Signature Version 4 pour les demandes d'API 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, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour plus d'informations, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Authentification multifactorielle AWS dans IAM dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas

utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. 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 au sein de vous Compte AWS qui possède des 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 telles que des mots de passe et des 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 d'effectuer une rotation des 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 nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les 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 plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Pour assumer temporairement un rôle IAM dans le AWS Management Console, vous pouvez passer d'un rôle d'utilisateur à un rôle IAM (console). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Méthodes pour endosser un rôle 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, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les

ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités 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, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes 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.
  - Rôle de 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 un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

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

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 appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

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 Définition d'autorisations IAM personnalisées avec des politiques gérées par le client 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 associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées 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. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

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

Listes de contrôle d'accès (ACLs)

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

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la présentation de la liste 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 courants. 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 fonctionnalité 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 en résultant 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 annule 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 (SCPs) : SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de contrôle des ressources (RCPs) : RCPs politiques JSON que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, consultez la section Resource control policies (RCPs) dans le guide de AWS Organizations l'utilisateur.
- 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 séance en résultant 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 annule l'autorisation. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment 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
ACLs	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 l'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 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 Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. 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 les ressources : non

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

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal intercompte à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (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 Accès intercompte aux ressources dans IAM 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 AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API 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 politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions Elastic Load Balancing, consultez les sections Actions définies par Elastic Load Balancing V2 et Actions définies par Elastic Load Balancing V1 dans le Service Authorization Reference.

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

Ressources de stratégie pour Elastic Load Balancing

Prend en charge les ressources de politique : oui

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

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. 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-les ARNs par des virgules.

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

Pour consulter la liste des types de ressources Elastic Load Balancing et de leurs caractéristiques ARNs, consultez la section Ressources définies par Elastic Load Balancing V2 et Ressources définies par Elastic Load Balancing V1 dans le Service Authorization Reference. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez les sections Actions définies par Elastic Load Balancing V2 et Actions définies par Elastic Load Balancing V1.

Clés de condition de stratégie pour Elastic Load Balancing

Prend en charge les clés de condition de politique spécifiques au service : oui

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

L'élément `Condition` (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 `OR` opération 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 au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition d'Elastic Load Balancing, voir Clés de condition pour Elastic Load Balancing V2 et clés de condition pour Elastic Load Balancing V1 dans le Service Authorization Reference. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez les sections Actions définies par Elastic Load Balancing V2 et Actions définies par Elastic Load Balancing V1.

Clés de condition

- Clé de condition elasticloadbalancing:ListenerProtocol
- Clé de condition elasticloadbalancing:SecurityPolicy
- Clé de condition elasticloadbalancing:Scheme
- Clé de condition elasticloadbalancing:SecurityGroup
- Clé de condition elasticloadbalancing:Subnet
- Clé de condition elasticloadbalancing:ResourceTag

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

L'exemple de politique suivant oblige les utilisateurs à sélectionner le protocole HTTPS pour les écouteurs de leurs équilibreurs de charge d'application et le protocole TLS pour les écouteurs de leurs équilibreurs de charge réseau.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateListener",
            "elasticloadbalancing:ModifyListener"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals":{
                "elasticloadbalancing:ListenerProtocol": [
                    "HTTPS",
                    "TLS"
                ]
            },
        }
    }
}
```

Avec un Classic Load Balancer, vous pouvez spécifier plusieurs écouteurs en un seul appel. Par conséquent, votre politique doit utiliser une clé contextuelle à valeurs multiples, comme illustré dans l'exemple suivant.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "elasticloadbalancing:CreateLoadBalancer",
                "elasticloadbalancing:CreateLoadBalancerListeners"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "elasticloadbalancing:ListenerProtocol": [
                        "TCP",
                        "HTTP",
                        "HTTPS"
                    ]
                }
            }
        }
    ]
}
```

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

L'exemple de politique suivant oblige les utilisateurs à sélectionner l'une des politiques de sécurité spécifiées pour leurs équilibreurs de charge d'application et leurs équilibreurs de charge réseau.

```
{
    "Version": "2012-10-17",
    "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. La politique est disponible pour les équilibreurs de charge d'application, les équilibreurs de charge réseau et les équilibreurs de charge classiques. 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`

L'exemple de politique suivant oblige les utilisateurs à sélectionner le schéma spécifié pour leurs équilibreurs de charge.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action":"elasticloadbalancing:CreateLoadBalancer",
        "Resource": "*",
        "Condition": {
            "StringEquals":{
                "elasticloadbalancing:Scheme": "internal"
            },
        }
    }
}
```

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

> **Important**
>
> Elastic Load Balancing accepte toutes les capitalisations du groupe de sécurité. IDs 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. La politique est disponible pour les équilibreurs de charge d'application, les équilibreurs de charge réseau et les équilibreurs de charge classiques. 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`

L'exemple de politique suivant oblige les utilisateurs à sélectionner l'un des groupes de sécurité spécifiés pour leurs équilibreurs de charge.

```
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateLoadBalancer",
            "elasticloadbalancing:SetSecurityGroup"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEqualsIgnoreCase":{
                "elasticloadbalancing:SecurityGroup": [
                    "sg-51530134",
                    "sg-51530144",
                    "sg-51530139"
                ]
            },
        }
    }
}
```

Clé de condition elasticloadbalancing:Subnet

> **Important**
>
> Elastic Load Balancing accepte toutes les capitalisations du sous-réseau. IDs 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. 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. 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`

L'exemple de politique suivant oblige les utilisateurs à sélectionner l'un des sous-réseaux spécifiés pour leurs équilibreurs de charge.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": [
            "elasticloadbalancing:CreateLoadBalancer",
            "elasticloadbalancing:SetSubnets"
        ],
        "Resource": "*",
        "Condition": {
            "ForAnyValue:StringEqualsIgnoreCase":{
```

```
                "elasticloadbalancing:Subnet": [
                    "subnet-01234567890abcdef",
                    "subnet-01234567890abcdeg "
                ]
            },
        }
    }
}
```

Clé de condition elasticloadbalancing:ResourceTag

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

ACLs dans Elastic Load Balancing

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs 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

Prise en charge d'ABAC (balises 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 balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. 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 étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`.

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

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

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

Prend en charge les informations d'identification temporaires : oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, 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 Passage d'un rôle utilisateur à un rôle IAM (console) dans le Guide de l'utilisateur IAM.

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

Autorisations de principal entre services pour Elastic Load Balancing

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

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal

appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes 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 rôles de service : Non

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

Rôles liés à un service pour Elastic Load Balancing

Prend en charge les rôles liés aux services : Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au 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 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).

```
{
  "Version": "2012-10-17",
  "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).

```
{
  "Version": "2012-10-17",
  "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 la section 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 AWSServiceRoleForElasticLoadBalancing pour appeler d'autres AWS services en votre nom.

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

La politique d'autorisation des rôles estAWSElasticLoadBalancingServiceRolePolicy. Pour voir les autorisations de cette stratégie, consultez AWSElasticLoadBalancingServiceRolePolicy dans le AWS Guide de référence des stratégies gérées par.

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 de plus amples informations, veuillez consulter Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Modification du rôle lié à un service

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

Supprimer le rôle lié à un service

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

Vous ne pouvez supprimer ce rôle lié à un service qu'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 plus d'informations, voir Supprimer un rôle lié à un service dans le Guide de l'utilisateur IAM.

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

AWS politiques gérées pour Elastic Load Balancing

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation

courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSElasticLoadBalancingClassicServiceRolePolicy

Cette politique inclut toutes les autorisations requises par Elastic Load Balancing (Classic Load Balancer) pour appeler d'autres AWS services 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 voir les autorisations de cette stratégie, consultez AWSElasticLoadBalancingClassicServiceRolePolicy dans le AWS Guide de référence des stratégies gérées par.

AWS politique 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 voir les autorisations de cette stratégie, consultez AWSElasticLoadBalancingServiceRolePolicy dans le AWS Guide de référence des stratégies gérées par.

AWS politique gérée : ElasticLoadBalancingFullAccess

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

Pour voir les autorisations de cette stratégie, consultez ElasticLoadBalancingFullAccess dans le AWS Guide de référence des stratégies gérées par.

AWS politique gérée : ElasticLoadBalancingReadOnly

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

Pour voir les autorisations de cette stratégie, consultez ElasticLoadBalancingReadOnly dans le AWS Guide de référence des stratégies gérées par.

Elastic Load Balancing met à jour les politiques AWS gérées

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

Modification	Description	Date
AWSElasticLoadBalancingServiceRolePolicy : mise à jour d'une stratégie existante	Ajout de l'`ec2:AllocateIpamPoolCidr` action permettant d'accorder des autorisations pour allouer des blocs CIDR à partir de pools IPAM.	17 février 2025
ElasticLoadBalancingFullAccess : mise à jour d'une stratégie existante	Ajout des `arc-zonal-shift:*` actions permettant d'accorder les autorisations requises pour le changement de zone.	28 novembre 2023
ElasticLoadBalancingReadOnly : mise à jour d'une stratégie existante	Les actions suivantes ont été ajoutées pour accorder les autorisations requises pour le changement de zone :`arc-zonal-shift:GetManagedResource` , `arc-zonal-shift:ListManagedResources` et`arc-zonal-shift:ListZonalShifts` .	28 novembre 2023

Modification	Description	Date
AWSElasticLoadBalancingServiceRolePolicy : mise à jour d'une stratégie existante	Ajout de l'`ec2:DescribeVpcPeeringConnections` action permettant d'accorder les autorisations requises pour les connexions de peering.	11 octobre 2021
ElasticLoadBalancingFullAccess : mise à jour d'une stratégie existante	Ajout de l'`ec2:DescribeVpcPeeringConnections` action permettant d'accorder les autorisations requises pour les connexions de peering.	11 octobre 2021
ElasticLoadBalancingFullAccess : nouvelle politique	Fournit un accès complet à Elastic Load Balancing et aux services dépendants.	20 septembre 2018
ElasticLoadBalancingReadOnly : nouvelle politique	Fournit un accès en lecture seule à Elastic Load Balancing et aux services dépendants.	20 septembre 2018
Elastic Load Balancing a commencé à suivre les modifications	Elastic Load Balancing a commencé à suivre les modifications apportées AWS à ses politiques gérées.	20 septembre 2018

Validation de la conformité pour Elastic Load Balancing

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Conformité et gouvernance de la sécurité : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- Référence des services éligibles HIPAA : liste les services éligibles HIPAA. Tous ne Services AWS sont pas éligibles à la loi HIPAA.
- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides 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 des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne 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.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans Elastic Load Balancing

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. 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 AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Outre l'infrastructure AWS globale, Elastic Load Balancing fournit les fonctionnalités suivantes pour renforcer la résilience de vos données :

- Distribue le trafic entrant sur plusieurs instances dans une ou plusieurs zones de disponibilité.
- Vous pouvez les utiliser AWS Global Accelerator avec vos équilibreurs de charge d'application pour répartir le trafic entrant entre plusieurs équilibreurs de charge dans une ou plusieurs AWS régions. Pour plus d'informations, consultez le Manuel du développeur AWS Global Accelerator.
- Amazon ECS vous permet d'exécuter, d'arrêter et de gérer des conteneurs Docker sur un cluster d' EC2 instances. 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 AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des 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 cloud privé virtuel (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 EC2 des instances 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 de plus amples informations, veuillez consulter 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 vos EC2 instances Amazon afin d'accepter 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).

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

Limite

AWS PrivateLink ne prend pas en charge les équilibreurs de charge réseau dotés de 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 plus d'informations, consultez Création d'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 .

Limitation des demandes pour l'API Elastic Load Balancing

Elastic Load Balancing limite ses demandes d'API pour chaque AWS compte par région. Nous faisons cela pour améliorer les performances et la disponibilité du service. Throttling garantit que les demandes adressées à l'API Elastic Load Balancing ne dépassent pas les limites de demandes d'API maximales autorisées. Les demandes d'API sont soumises aux limites de demandes, que vous les appeliez ou qu'elles soient appelées en votre nom (par exemple, par l'application AWS Management Console ou une application tierce).

Si vous dépassez une limite de limitation de l'API Elastic Load Balancing, vous obtenez le code `ThrottlingException` d'erreur et un message d'`Rate exceeded`erreur.

Nous vous recommandons de vous préparer à gérer l'étranglement avec élégance. Pour plus d'informations, consultez les sections Expiration, nouvelles tentatives et interruption avec gigue. Si vous êtes confronté à un niveau élevé de régulation, vous pouvez nous contacter AWS Support pour vous aider à évaluer votre utilisation des API et les solutions potentielles. Chaque cas est évalué individuellement. Support peut augmenter vos limites dans les limites de sécurité du système, afin de maintenir une haute disponibilité et des performances prévisibles.

Comment l'étranglement est appliqué

Elastic Load Balancing utilise l'algorithme Token Bucket pour implémenter la régulation des API. Avec cet algorithme, votre compte dispose d'un compartiment contenant un nombre spécifique de jetons. Le nombre de jetons dans le compartiment représente votre limite de limitation à chaque seconde.

Elastic Load Balancing propose deux ensembles d'actions d'API. La version 2 de l'API ELB prend en charge les types d'équilibreurs de charge suivants : équilibreurs de charge d'application, équilibreurs de charge réseau et équilibreurs de charge de passerelle. La version 1 de l'API ELB prend en charge les équilibreurs de charge classiques. Chaque version de l'API ELB possède ses propres buckets et jetons.

Les services qui appellent l'API Elastic Load Balancing en votre nom, tels qu'Amazon EC2, Amazon ECS, Amazon EC2 Auto Scaling, et qui AWS CloudFormation disposent de leurs propres buckets au niveau du compte. Ces services ne consomment pas de jetons provenant de vos buckets.

Limitation du débit de demande

Avec la limitation du taux de demandes, le nombre de demandes d'API que vous effectuez est limité. Chaque requête que vous effectuez supprime un jeton du compartiment. Par exemple, la taille du bucket de jetons pour les actions d'API non mutantes est de 40 jetons. Vous pouvez effectuer jusqu'à 40 `Describe*` demandes en une seconde. Si vous dépassez 40 `Describe*` demandes en une seconde, vous êtes limité et les demandes restantes échouent au cours de cette seconde.

Les seaux se rechargent automatiquement à un débit défini. Si un compartiment est inférieur à sa capacité maximale, un nombre défini de jetons est ajouté chaque seconde jusqu'à ce que le compartiment atteigne sa capacité maximale. Si un seau est plein lorsque les jetons de recharge arrivent, ils sont jetés. Un bucket ne peut pas contenir plus de jetons que son maximum. Par exemple, la taille du bucket pour les actions d'API non mutantes est de 40 jetons et le taux de recharge est de 10 jetons par seconde. Si vous faites 40 `DescribeLoadBalancers` demandes en une seconde, le bucket est réduit à zéro (0) jeton. Nous ajoutons 10 jetons de recharge au seau chaque seconde, jusqu'à ce qu'il atteigne sa capacité maximale de 40 jetons. Cela signifie qu'il faut 4 secondes pour qu'un compartiment vide atteigne sa capacité maximale, si aucune demande n'est faite pendant cette période.

Il n'est pas nécessaire d'attendre qu'un bucket soit complètement plein pour pouvoir effectuer des demandes d'API. Vous pouvez utiliser des jetons lorsqu'ils sont ajoutés à un bucket. Si vous utilisez immédiatement les jetons de recharge, le seau n'atteint pas sa capacité maximale.

Il existe une limite de limitation au niveau du compte qui est partagée entre toutes les actions de l'API Elastic Load Balancing. La capacité du bucket au niveau du compte est de 40 jetons et le taux de recharge est de 10 jetons de demande par seconde.

Demandez la taille des seaux de jetons et les taux de recharge

Pour limiter le taux de demandes, les actions de l'API sont regroupées en catégories. Chaque catégorie a ses propres limites.

Catégories

- Actions de mutation : actions d'API qui créent, modifient ou suppriment des ressources. Cette catégorie inclut généralement toutes les actions d'API qui ne sont pas considérées comme des actions non mutantes. La limite de régulation de ces actions est inférieure à celle des actions d'API non mutantes.

- Actions non mutantes : actions d'API qui récupèrent des données sur les ressources. Ces actions d'API présentent généralement les limites de limitation d'API les plus élevées.
- Actions gourmandes en ressources : actions d'API dont l'exécution prend le plus de temps et consomme le plus de ressources. Ces actions ont une limite d'étranglement encore plus faible que les actions mutantes. Ces actions sont limitées séparément des autres actions de mutation.
- Actions d'enregistrement : actions d'API qui enregistrent ou désenregistrent des cibles. Ces actions d'API sont limitées séparément des autres actions de mutation.
- Actions non classées : ces actions d'API reçoivent leur propre taille de bucket de jetons et leur propre taux de recharge, même si elles appartiennent à l'une des autres catégories.

Le tableau suivant indique la capacité et les taux de recharge par défaut pour les compartiments de jetons de demande classés par catégories.

Catégorie	ELBv2 actions	ELBv1 actions	Capacité du godet	Taux de recharge (par seconde)
Nécessite beaucoup de ressources	`CreateLoadBalancer`, `SetSubnets`	`CreateLoadBalancer`, `AttachLoadBalancerToSubnets`, `DetachLoadBalancerFromSubnets`, `EnableAvailabilityZonesForLoadBalancer`, `DisableAvailabilityZonesForLoadBalancer`	10	0,2 †
Inscription	`RegisterTargets`, `DeregisterTargets`	`RegisterInstancesWithLoadBalancer`, `DeregisterInstancesFromLoadBalancer`	20	4

Catégorie	ELBv2 actions	ELBv1 actions	Capacité du godet	Taux de recharge (par seconde)
Non mutant	`DescribeAccountLimits`, `DescribeListenerCertificates`, `DescribeListeners`, `DescribeLoadBalancerAttributes`, `DescribeLoadBalancers`, `DescribeRules`, `DescribeSSLPolicies`, `DescribeTags`, `DescribeTargetGroupAttributes`, `DescribeTargetGroups`, `DescribeTargetHealth`	`Describe*`	40	10

Catégorie	ELBv2 actions	ELBv1 actions	Capacité du godet	Taux de recharge (par seconde)
Mutant	`AddListenerCertificates`, `AddTags`, `CreateListener`, `CreateRule`, `CreateTargetGroup`, `DeleteListener`, `DeleteLoadBalancer`, `DeleteRule`, `DeleteTargetGroup`, `ModifyListener`, `ModifyLoadBalancerAttributes`, `ModifyRule`, `ModifyTargetGroup`, `ModifyTargetGroupAttributes`, `RemoveListenerCertificates`, `RemoveTags`, `SetIpAddressType`, `SetRulePriorities`, `SetSecurityGroups`	`AddTags`, `ApplySecurityGroupsToLoadBalancer`, `ConfigureHealthCheck`, `CreateAppCookieStickinessPolicy`, `CreateLbCookieStickinessPolicy`, `CreateLoadBalancerListener`, `CreateLoadBalancerPolicy`, `Delete*`, `ModifyLoadBalancerAttributes`, `RemoveTags`, `SetLoadBalancer*`	20	3

Le tableau suivant indique la capacité et les taux de recharge par défaut pour les compartiments de jetons de demande non classés pour. ELBv2

ELBv2 actions	Capacité du godet	Taux de recharge (par seconde)
`CreateTrustStore`	10	0,2 †
`AddTrustStoreRevocations`, `DeleteSharedTrustStoreAssoc`	10	0,2 †

ELBv2 actions	Capacité du godet	Taux de recharge (par seconde)
`iation` , `DeleteTrustStore` , `ModifyTrustStore` , `RemoveTrustStoreRevocations`		
`GetTrustStoreCaCertificatesBundle` , `GetTrustStoreRevocationContent`	20	4
`DescribeTrustStoreAssociations` , `DescribeTrustStoreRevocations` , `DescribeTrustStores`	40	10

† Les taux de recharge fractionnés nécessitent plusieurs secondes pour générer un jeton complet.

Surveillance des demandes d'API

Vous pouvez l'utiliser AWS CloudTrail pour surveiller vos demandes d'API Elastic Load Balancing. Pour de plus amples informations, veuillez consulter Consignez les appels d'API pour Elastic Load Balancing en utilisant AWS CloudTrail.

Comprendre les codes relatifs à Elastic Load Balancing dans les rapports de facturation et d'utilisation

Lorsque vous utilisez Elastic Load Balancing, nous incluons les codes associés dans vos rapports AWS de facturation et d'utilisation. L'examen de ces codes vous aide à comprendre les coûts et les habitudes d'utilisation de votre équilibreur de charge. Le suivi et la gestion de vos dépenses sont essentiels pour optimiser vos coûts.

Pour plus d'informations, veuillez consultez Tarification Elastic Load Balancing.

Les tableaux suivants décrivent les codes d'Elastic Load Balancing qui apparaissent dans vos rapports de facturation et d'utilisation. Les unités sont des heures ou des unités de capacité de l'équilibreur de charge (LCU). Chaque type d'équilibreur de charge possède une définition spécifique du LCU. Pour plus d'informations sur chaque type LCUs d'équilibreur de charge, consultez la section Tarification d'Elastic Load Balancing. Pour obtenir la liste des codes régionaux utilisés dans les rapports de facturation et d'utilisation, consultez AWS la section Codes de facturation régionaux.

Application Load Balancers

Code	Description	Unités
`region-LoadBalancerUsage`	La durée de fonctionnement.	Heures
`region-LCUUsage`	Le d' LCUs occasion.	LCU
`region-IdleProvisionedLBCapacity`	Le LCUs réservé mais non utilisé.	LCU
`region-TS-LoadBalancerUsage`	Durée pendant laquelle un trust store est utilisé par Mutual TLS.	Heures
`region-Outposts-LoadBalancerUsage`	La durée de fonctionnement sur Outposts.	Heures

Code	Description	Unités
region-Outposts-LCUUsage	Ils LCUs sont utilisés sur Outposts.	LCU
region-ReservedLCUUsage	Le LCUs réservé.	LCU

Network Load Balancers

Code	Description	Unités
region-LoadBalancerUsage	La durée de fonctionnement.	Heures
region-LCUUsage	Le d' LCUs occasion.	LCU

Gateway Load Balancers

Code	Description	Unités
region-LoadBalancerUsage	La durée de fonctionnement.	Heures
region-LCUUsage	Le d' LCUs occasion.	LCU

Équilibreurs de charge classiques

Code	Description	Unités
region-LoadBalancerUsage	La durée de fonctionnement.	Heures

Code	Description	Unités
region-DataProcessing-Bytes	Les données traitées.	Go
region-IdleProvisionedLBCapacity	Le LCUs réservé mais non utilisé.	LCU

Consignez les appels d'API pour Elastic Load Balancing en utilisant AWS CloudTrail

Elastic Load Balancing est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service. CloudTrail capture les appels d'API pour Elastic Load Balancing sous forme d'événements. Les appels capturés incluent des appels provenant des appels de code AWS Management Console et destinés aux opérations de l'API Elastic Load Balancing. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à Elastic Load Balancing, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires.

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

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur root.
- Si la demande a été faite au nom d'un utilisateur du centre d'identité IAM.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

CloudTrail est actif dans votre compte Compte AWS lorsque vous créez le compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'historique des CloudTrail événements fournit un enregistrement consultable, consultable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés dans un. Région AWS Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur. La consultation de CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou CloudTrailLake.

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du AWS Management Console sont multirégionaux. Vous ne pouvez

créer un journal de suivi en une ou plusieurs régions à l'aide de l' AWS CLI. Il est recommandé de créer un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS de votre compte. Si vous créez un journal de suivi pour une seule région, il convient de n'afficher que les événements enregistrés dans le journal de suivi pour une seule région Région AWS. Pour plus d'informations sur les journaux de suivi, consultez Créez un journal de suivi dans vos Compte AWS et Création d'un journal de suivi pour une organisation dans le AWS CloudTrail Guide de l'utilisateur.

Vous pouvez envoyer une copie de vos événements de gestion en cours dans votre compartiment Amazon S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

CloudTrail Stockages de données sur les événements du lac

CloudTrail Lake vous permet d'exécuter des requêtes SQL sur vos événements. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement. Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous sélectionnez en appliquant des sélecteurs d'événements avancés. Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section Travailler avec AWS CloudTrail Lake dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail Les stockages et requêtes de données sur les événements de Lake entraînent des coûts. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Événements de gestion d'Elastic Load Balancing dans CloudTrail

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

Elastic Load Balancing enregistre les opérations du plan de contrôle en tant qu'événements de gestion. Pour obtenir la liste des opérations du plan de contrôle, consultez les rubriques suivantes :

- Équilibreurs de charge d'application — API Elastic Load Balancing, version de référence 2015-12-01
- Équilibreurs de charge réseau — API Elastic Load Balancing, version de référence 2015-12-01
- Équilibreurs de charge Gateway — Version de référence de l'API Elastic Load Balancing 2015-12-01
- Equilibreurs de charge classiques — Version de référence de l'API Elastic Load Balancing 2012-06-01

Exemples d'événements Elastic Load Balancing

Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération d'API demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Les événements n'apparaissent donc pas dans un ordre spécifique.

Les exemples suivants montrent les CloudTrail événements d'un utilisateur qui a créé un équilibreur de charge puis l'a supprimé à l'aide du AWS CLI. Vous pouvez identifier l'interface de ligne de commande à l'aide des éléments `userAgent`. Vous pouvez identifier les appels d'API demandés à l'aide des éléments `eventName`. Il est possible de trouver des informations sur l'utilisateur (`Alice`) dans l'élément `userIdentity`.

Example Exemple 1 : CreateLoadBalancer depuis l' ELBv2 API

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "CreateLoadBalancer",
```

```
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "subnets": ["subnet-8360a9e7","subnet-b7d581c0"],
        "securityGroups": ["sg-5943793c"],
        "name": "my-load-balancer",
        "scheme": "internet-facing"
    },
    "responseElements": {
        "loadBalancers":[{
            "type": "application",
            "loadBalancerName": "my-load-balancer",
            "vpcId": "vpc-3ac0fb5f",
            "securityGroups": ["sg-5943793c"],
            "state": {"code":"provisioning"},
            "availabilityZones": [
               {"subnetId":"subnet-8360a9e7","zoneName":"us-west-2a"},
               {"subnetId":"subnet-b7d581c0","zoneName":"us-west-2b"}
            ],
            "dNSName": "my-load-balancer-1836718677.us-west-2.elb.amazonaws.com",
            "canonicalHostedZoneId": "Z2P70J7HTTTPLU",
            "createdTime": "Apr 11, 2016 5:23:50 PM",
            "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/ffcddace1759e1d0",
            "scheme": "internet-facing"
        }]
    },
    "requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
    "eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```

Example Exemple 2 : DeleteLoadBalancer depuis l' ELBv2 API

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
```

```
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "DeleteLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "loadBalancerArn": "arn:aws:elasticloadbalancing:us-
west-2:123456789012:loadbalancer/app/my-load-balancer/ffcddace1759e1d0"
    },
    "responseElements": null,
    "requestID": "349598b3-000e-11e6-a82b-298133eEXAMPLE",
    "eventID": "75e81c95-4012-421f-a0cf-babdaEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-12-01",
    "recipientAccountId": "123456789012"
}
```

Example Exemple 3 : CreateLoadBalancer depuis l'API ELB

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJDPLRKLG7UEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-01T15:31:48Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "CreateLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "subnets": ["subnet-12345678","subnet-76543210"],
        "loadBalancerName": "my-load-balancer",
```

```
        "listeners": [{
           "protocol": "HTTP",
           "loadBalancerPort": 80,
           "instanceProtocol": "HTTP",
           "instancePort": 80
        }]
    },
    "responseElements": {
        "dNSName": "my-loadbalancer-1234567890.elb.amazonaws.com"
    },
    "requestID": "b9960276-b9b2-11e3-8a13-f1ef1EXAMPLE",
    "eventID": "6f4ab5bd-2daa-4d00-be14-d92efEXAMPLE",
    "eventType": "AwsApiCall",
    "apiVersion": "2012-06-01",
    "recipientAccountId": "123456789012"
}
```

Example Exemple 4 : DeleteLoadBalancer depuis l'API ELB

```
{
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJDPLRKLG7UEXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2016-04-08T12:39:25Z",
    "eventSource": "elasticloadbalancing.amazonaws.com",
    "eventName": "DeleteLoadBalancer",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "aws-cli/1.10.10 Python/2.7.9 Windows/7 botocore/1.4.1",
    "requestParameters": {
        "loadBalancerName": "my-load-balancer"
    },
    "responseElements": null,
    "requestID": "f0f17bb6-b9ba-11e3-9b20-999fdEXAMPLE",
    "eventID": "4f99f0e8-5cf8-4c30-b6da-3b69fEXAMPLE"
    "eventType": "AwsApiCall",
    "apiVersion": "2012-06-01",
```

```
    "recipientAccountId": "123456789012"
}
```

Pour plus d'informations sur le contenu des CloudTrail enregistrements, voir le contenu des CloudTrail enregistrements dans le Guide de AWS CloudTrail l'utilisateur.

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 plus d'informations sur les différentes fonctionnalités de chaque type d'équilibreur de charge, consultez la section Fonctionnalités d'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 vous aider à 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 à une autre et routage des demandes vers plusieurs applications sur une seule EC2 instance.
- 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 EC2 instance.
- 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, G1 CS1, G2,, M1 HI1 HS1, 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 EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sous Load Balancing (Équilibrage de charge), choisissez Load Balancers (Équilibreurs de charge).
3. Sélectionnez 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 de plus amples informations, veuillez consulter 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 EC2 instances 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.

Empêcher les utilisateurs de créer des équilibreurs de charge classiques

Vous pouvez créer une politique IAM qui empêche les utilisateurs de créer des équilibreurs de charge classiques dans votre compte.

Elastic Load Balancing V2 et Elastic Load Balancing V1 APIs fournissent tous deux une action d'`CreateLoadBalancer`API. Lorsque vous créez un Classic Load Balancer, vous utilisez l'action API V1, qui crée à la fois l'équilibreur de charge et les écouteurs. Lorsque vous créez un Application Load Balancer, un Network Load Balancer ou un Gateway Load Balancer, vous utilisez l'action API V2, qui crée uniquement l'équilibreur de charge. L'API V2 fournit une `CreateListener` action que vous utilisez pour créer des écouteurs pour un équilibreur de charge après sa création.

La politique suivante refuse aux utilisateurs l'autorisation de créer un équilibreur de charge si le protocole d'écoute est spécifié. Étant donné que vous devez configurer au moins un écouteur lorsque vous créez un Classic Load Balancer, cette politique empêche les utilisateurs de créer des Classic Load Balancer. Cela n'empêche pas les utilisateurs de créer d'autres types d'équilibreurs de charge, car des actions d'API distinctes permettent de créer ces équilibreurs de charge et leurs écouteurs.

```
{
    "Version": "2012-10-17",
    "Effect": "Deny",
    "Action": "elasticloadbalancing:CreateLoadBalancer",
    "Resource": [
        "arn:aws:elasticloadbalancing:*:*:loadbalancer/*"
    ],
    "Condition": {
        "Null": {
            "elasticloadbalancing:ListenerProtocol": false
        }
    }
}
```

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.