aws

Network Load Balancers

Elastic Load Balancing

Elastic Load Balancing: Network Load Balancers

Table of Contents

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

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 met à l'échelle votre équilibreur de charge à mesure que votre trafic entrant change au fil du temps. Il est capable de s'adapter automatiquement à la plupart des applications.

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

Composants du Network Load Balancer

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

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

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

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

- Équilibreurs de charge

- Écouteurs
- Groupes cibles

Présentation du Network Load Balancer

Un Network Load Balancer fonctionne à la quatrième couche du modèle Open Systems Interconnection (OSI). Il est capable de traiter des millions de requêtes par seconde. Une fois que l'équilibreur de charge reçoit une demande d'un client, il sélectionne une cible dans le groupe cible pour la règle par défaut. Il tente d'envoyer la demande à la cible sélectionnée en utilisant le protocole et le port que vous avez spécifiés.

Lorsque vous activez une zone de disponibilité pour l'équilibreur de charge, Elastic Load Balancing crée un nœud d'équilibreur de charge dans la zone de disponibilité. Par défaut, chaque nœud d'équilibreur de charge répartit le trafic parmi les cibles enregistrées dans sa zone de disponibilité uniquement. Si vous activez l'équilibrage de charge entre zones permet, chaque nœud d'équilibreur de charge répartit le trafic entre les cibles enregistrées dans toutes les zones de disponibilité activées. Pour de plus amples informations, veuillez consulter Mettez à jour les zones de disponibilité de votre Network Load Balancer.

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

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

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

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

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

Lorsque vous créez un groupe cible, vous spécifiez son type de cible, qui détermine la façon dont vous enregistrez les cibles. Par exemple, vous pouvez enregistrer une instance IDs, des adresses IP ou un Application Load Balancer. Le type de cible détermine également si les adresses IP client sont préservées. Pour de plus amples informations, veuillez consulter the section called “Préservation de l’IP du client”.

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

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

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

Avantages de la migration depuis un Classic Load Balancer

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

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

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

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

Premiers pas

Pour créer un Network Load Balancer à l'aide du AWS Management Console, ou AWS CLI AWS CloudFormation, voir. Création d'un Network Load Balancer

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

Tarification

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

Network Load Balancers

Un Network Load Balancer est le point de contact unique pour les clients. Les clients envoient des demandes au Network Load Balancer, qui les envoie à des cibles, EC2 telles que des instances, dans une ou plusieurs zones de disponibilité.

Pour configurer votre Network Load Balancer, vous créez des groupes cibles, puis vous enregistrez des cibles auprès de vos groupes cibles. Votre Network Load Balancer est plus efficace si vous vous assurez que chaque zone de disponibilité activée possède au moins une cible enregistrée. Vous créez également des écouteurs pour rechercher les demandes de connexion des clients et pour acheminer les demandes des clients vers les cibles dans vos groupes cibles.

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

Table des matières

États d'un équilibreur de charge

Un Network Load Balancer peut se trouver dans l'un des états suivants :

`provisioning`

Le Network Load Balancer est en cours de configuration.

`active`

Le Network Load Balancer est entièrement configuré et prêt à acheminer le trafic.

`failed`

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

Type d’adresse IP

Vous pouvez définir les types d'adresses IP que les clients peuvent utiliser avec votre Network Load Balancer.

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

`ipv4`

Les clients doivent se connecter à l'aide d' IPv4 adresses (par exemple, 192.0.2.1).

`dualstack`

Les clients peuvent se connecter au Network Load Balancer en utilisant à la fois des IPv4 adresses (par exemple, 192.0.2.1) et des IPv6 adresses (par exemple, 2001:0 db 8:85 a 3:0:0:8 a2e : 0370:7334).

Considérations

- Le Network Load Balancer communique avec les cibles en fonction du type d'adresse IP du groupe cible.
- Pour prendre en charge la préservation de l'adresse IP source pour IPv6 les écouteurs UDP, assurez-vous que le préfixe Enable pour le NAT IPv6 source est activé.
- Lorsque vous activez le mode dualstack pour le Network Load Balancer, Elastic Load Balancing fournit un enregistrement DNS AAAA pour le Network Load Balancer. Les clients qui

communiquent avec le Network Load Balancer à l'aide d' IPv4 adresses résolvent l'enregistrement DNS A. Les clients qui communiquent avec le Network Load Balancer à l'aide d' IPv6 adresses résolvent l'enregistrement DNS AAAA.

- L'accès à votre Network Load Balancer interne à double pile via la passerelle Internet est bloqué afin d'empêcher tout accès involontaire à Internet. Toutefois, cela n'empêche pas d'autres accès à Internet (par exemple, via le peering, Transit Gateway ou Site-to-Site VPN). AWS Direct Connect

Pour de plus amples informations, veuillez consulter Mettez à jour les types d'adresses IP de votre Network Load Balancer.

Délai d'inactivité des connexions

Pour chaque demande TCP effectuée par un client via un Network Load Balancer, l'état de cette connexion est suivi. Si aucune donnée n'est envoyée via la connexion par le client ou par la cible pendant une durée supérieure au délai d'inactivité, la connexion n'est plus suivie. Si un client ou une cible envoie des données après l'expiration du délai d'inactivité, le client reçoit un paquet TCP RST indiquant que la connexion n'est plus valide.

La valeur du délai d'inactivité par défaut pour les flux TCP est de 350 secondes, mais elle peut être mise à jour à n'importe quelle valeur comprise entre 60 et 6 000 secondes. Les clients ou les cibles peuvent utiliser des paquets TCP keepalive pour relancer le délai d'inactivité. Les paquets keepalive envoyés pour maintenir les connexions TLS ne peuvent pas contenir de données ou de charge utile.

Le délai d'inactivité de la connexion pour les écouteurs TLS est de 350 secondes et ne peut pas être modifié. Lorsqu'un écouteur TLS reçoit un paquet TCP keepalive d'un client ou d'une cible, l'équilibreur de charge génère des paquets TCP keepalive et les envoie aux connexions frontend et backend toutes les 20 secondes. Vous ne pouvez pas modifier ce comportement.

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

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

Pour de plus amples informations, veuillez consulter Mettre à jour le délai d'inactivité.

Attributs de l'équilibreur de charge

Vous pouvez configurer votre Network Load Balancer en modifiant ses attributs. Pour de plus amples informations, veuillez consulter Modifier les attributs de l'équilibreur de charge.

Les attributs de l'équilibreur de charge pour les équilibreurs de charge réseau sont les suivants :

`access_logs.s3.enabled`

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

`access_logs.s3.bucket`

Le nom du compartiment Amazon S3 pour les journaux d'accès. Cet attribut est obligatoire si les journaux d'accès sont activés. Pour de plus amples informations, veuillez consulter Conditions requises pour le compartiment.

`access_logs.s3.prefix`

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

`deletion_protection.enabled`

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

`ipv6.deny_all_igw_traffic`

Bloque l'accès de la passerelle Internet (IGW) au Network Load Balancer, empêchant ainsi tout accès involontaire à votre Network Load Balancer interne via une passerelle Internet. Il est configuré `false` pour les équilibreurs de charge réseau connectés à Internet et `true` pour les équilibreurs de charge réseau internes. Cet attribut n'empêche pas l'accès à Internet hors IGW (par exemple, via le peering, AWS Direct Connect Transit Gateway ou). Site-to-Site VPN

`load_balancing.cross_zone.enabled`

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

`dns_record.client_routing_policy`

Indique comment le trafic est réparti entre les zones de disponibilité des équilibreurs de charge réseau. Les valeurs possibles sont `availability_zone_affinity` avec 100 %

d'affinité zonale, `partial_availability_zone_affinity` avec 85 % d'affinité zonale et `any_availability_zone` avec 0 % d'affinité zonale.

`secondary_ips.auto_assigned.per_subnet`

Le nombre d'adresses IP secondaires à configurer. À utiliser pour résoudre les erreurs d'allocation de ports si vous ne pouvez pas ajouter de cibles. La plage valide est comprise entre 0 et 7. La valeur par défaut est 0. Une fois cette valeur définie, vous ne pouvez pas la diminuer.

`zonal_shift.config.enabled`

Indique si le décalage de zone est activé. L'argument par défaut est `false`.

Equilibrage de charge entre zones

Par défaut, chaque nœud Network Load Balancer distribue le trafic entre les cibles enregistrées dans sa zone de disponibilité uniquement. Si vous activez l'équilibrage de charge entre zones, chaque nœud Network Load Balancer distribue le trafic entre les cibles enregistrées dans toutes les zones de disponibilité activées. Vous pouvez également activer l'équilibrage de charge entre zones au niveau du groupe cible. Pour plus d'informations, veuillez consulter the section called "Équilibrage de charge entre zones" et Équilibrage de charge entre zones (langue française non garantie) dans le Guide de l'utilisateur Elastic Load Balancing.

Nom du DNS

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

Si vous préférez utiliser un nom DNS plus facile à mémoriser, vous pouvez créer un nom de domaine personnalisé et l'associer au nom DNS de votre Network Load Balancer. Lorsqu'un client fait une demande à l'aide de ce nom de domaine personnalisé, le serveur DNS la résout avec le nom DNS de votre Network Load Balancer.

Tout d'abord, enregistrez un nom de domaine auprès d'un bureau d'enregistrement de noms de domaine accrédité. Utilisez ensuite votre service DNS, tel que votre bureau d'enregistrement de domaines, pour créer un enregistrement DNS afin d'acheminer les demandes vers votre Network Load Balancer. Pour plus d'informations, consultez la documentation de votre service DNS. Par exemple, si vous utilisez Amazon Route 53 comme service DNS, vous créez un enregistrement d'alias qui pointe vers votre Network Load Balancer. Pour de plus amples informations, consultez

Acheminement du trafic vers un équilibreur de charge ELB dans le Guide du développeur Amazon Route 53.

Le Network Load Balancer possède une adresse IP par zone de disponibilité activée. Il s'agit des adresses IP des nœuds Network Load Balancer. Le nom DNS du Network Load Balancer correspond à ces adresses. Supposons, par exemple, que le nom de domaine personnalisé de votre Network Load Balancer soit. `example.networkloadbalancer.com` Utilisez la nslookup commande dig ou suivante pour déterminer les adresses IP des nœuds Network Load Balancer.

Linux ou Mac

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

Windows

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

Le Network Load Balancer possède des enregistrements DNS pour ses nœuds. Vous pouvez utiliser des noms DNS avec la syntaxe suivante pour déterminer les adresses IP des nœuds Network Load Balancer :. *az name*- *id* .elb. *region*.amazonaws.com.

Linux ou Mac

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

Windows

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

Santé zonale de l'équilibreur de charge

Les équilibreurs de charge réseau possèdent des enregistrements DNS zonaux et des adresses IP dans Route 53 pour chaque zone de disponibilité activée. Lorsqu'un Network Load Balancer échoue à un contrôle de santé zonal pour une zone de disponibilité particulière, son enregistrement DNS est supprimé de Route 53. L'état de santé des zones de l'équilibreur de charge est surveillé à l'aide de la CloudWatch métrique Amazon`ZonalHealthStatus`, ce qui vous permet de mieux comprendre les événements à l'origine d'une défaillance afin de mettre en œuvre des mesures préventives afin de garantir une disponibilité optimale des applications. Pour plus d'informations, voir,Métriques des Network Load Balancers.

Les équilibreurs de charge réseau peuvent échouer aux contrôles de santé zonaux pour de multiples raisons, ce qui les rend insalubres. Vous trouverez ci-dessous les causes les plus fréquentes d'un mauvais fonctionnement des équilibreurs de charge réseau dû à l'échec des contrôles de santé zonaux.

Vérifiez les causes possibles suivantes :

- Il n'existe aucune cible saine pour l'équilibreur de charge
- Le nombre de cibles saines est inférieur au minimum configuré
- Un changement de zone ou un changement automatique de zone est en cours
- Le trafic est automatiquement transféré vers les zones saines en raison de problèmes détectés

Création d'un Network Load Balancer

Un Network Load Balancer prend les demandes des clients et les distribue entre les cibles d'un groupe cible, telles que EC2 les instances. Pour de plus amples informations, veuillez consulter the section called “Présentation du Network Load Balancer”.

Tâches

Prérequis

- Déterminez les zones de disponibilité et les types d'adresses IP que votre application prendra en charge. Configurez votre VPC d'équilibrage de charge avec des sous-réseaux dans chacune de ces zones de disponibilité. Si l'application prend en charge à la fois le IPv6 trafic IPv4 et le trafic, assurez-vous que les sous-réseaux possèdent les deux IPv4 et IPv6 CIDRs. Déployez au moins une cible dans chaque zone de disponibilité.
- Assurez-vous que les groupes de sécurité pour les instances cibles autorisent le trafic sur le port d'écoute à partir des adresses IP des clients (si les cibles sont spécifiées par l'ID d'instance) ou des nœuds d'équilibrage de charge (si les cibles sont spécifiées par adresse IP). Pour de plus amples informations, veuillez consulter the section called “Groupes de sécurité cibles”.

- Assurez-vous que les groupes de sécurité des instances cibles autorisent le trafic provenant de l'équilibreur de charge sur le port de vérification de l'état à l'aide du protocole de vérification de l'état.
- Si vous prévoyez de fournir des adresses IP statiques à votre équilibreur de charge, assurez-vous que chaque adresse IP élastique provient du pool d' IPv4adresses d'Amazon et qu'elle possède le même groupe de bordure réseau que l'équilibreur de charge.

Créer l'équilibreur de charge

Dans le cadre de la création d'un Network Load Balancer, vous allez créer l'équilibreur de charge, au moins un écouteur et au moins un groupe cible. Votre équilibreur de charge est prêt à traiter les demandes des clients lorsqu'il existe au moins une cible enregistrée saine dans chacune des zones de disponibilité activées.

Console

Pour créer un Network Load Balancer

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

    a. Dans le champ Nom de l'équilibreur de charge, entrez le nom de votre Network Load Balancer. Le nom doit être unique au sein de votre ensemble d'équilibreurs de charge dans la région. Le nom doit avoir un maximum de 32 caractères et ne peut contenir que des caractères alphanumériques et des traits d'union. Il ne peut pas commencer ou se terminer par un trait d'union, ou par `internal-`.

    b. Pour Scheme (Méthode), choisissez Internet-facing (Accessible sur Internet) ou Internal (Interne). Un Network Load Balancer connecté à Internet achemine les demandes des clients vers des cibles via Internet. Un Network Load Balancer interne achemine les demandes vers des cibles à l'aide d'adresses IP privées.

    c. Pour le type d'adresse IP de l'équilibreur de charge, indiquez IPv4si vos clients utilisent des IPv4 adresses pour communiquer avec le Network Load Balancer ou Dualstack s'ils utilisent IPv4 les deux IPv6 adresses pour communiquer avec le Network Load Balancer.

6. Mappage du réseau

   a. Pour le VPC, sélectionnez le VPC que vous avez préparé pour votre équilibreur de charge. Dans le cas d'un équilibreur de charge connecté à Internet, seule VPCs une passerelle Internet est disponible pour la sélection.

   b. Avec un équilibreur de charge à double pile, vous ne pouvez pas ajouter d'écouteur UDP à moins que le préfixe Enable pour le NAT source soit activé (IPv6 préfixes NAT source par sous-réseau).

   c. Pour les zones de disponibilité et les sous-réseaux, sélectionnez au moins une zone de disponibilité, puis un sous-réseau par zone. Notez que les sous-réseaux partagés avec vous peuvent être sélectionnés.

      Si vous sélectionnez plusieurs zones de disponibilité et que vous vous assurez d'avoir enregistré des cibles dans chaque zone sélectionnée, cela augmente la tolérance aux pannes de votre application.

   d. Avec un équilibreur de charge connecté à Internet, vous pouvez sélectionner une adresse IP élastique pour chaque zone de disponibilité. Ceci fournit des adresses IP statiques à votre équilibreur de charge.

      Avec un équilibreur de charge interne, vous pouvez saisir une IPv4 adresse privée à partir de la plage d'adresses de chaque sous-réseau ou en AWS sélectionner une pour vous.

      Avec un équilibreur de charge à double pile, vous pouvez saisir une IPv6 adresse à partir de la plage d'adresses de chaque sous-réseau ou en AWS sélectionner une pour vous.

      Pour un équilibreur de charge dont le NAT source est activé, vous pouvez entrer un IPv6 préfixe personnalisé ou laisser le soin d'en AWS sélectionner un pour vous.

7. Groupes de sécurité

   Nous présélectionnons le groupe de sécurité par défaut pour le VPC d'équilibrage de charge. Vous pouvez sélectionner des groupes de sécurité supplémentaires selon vos besoins. Si aucun groupe de sécurité ne répond à vos besoins, choisissez Créer un nouveau groupe de sécurité pour en créer un maintenant. Pour plus d'informations, veuillez consulter Création d'un groupe de sécurité dans le Guide de l'utilisateur Amazon VPC.

> **Warning**
>
> Si vous n'associez aucun groupe de sécurité à votre Network Load Balancer pour le moment, vous ne pourrez pas les associer ultérieurement.

8. Écouteurs et routage

   a. La valeur par défaut est un écouteur qui accepte le trafic TCP sur le port 80. Vous pouvez conserver les paramètres de l'écouteur par défaut ou modifier Protocole et Port selon vos besoins.

   b. Pour Action par défaut, sélectionnez un groupe cible pour transférer le trafic. Si aucun groupe cible ne répond à vos besoins, choisissez Créer un groupe cible pour en créer un maintenant. Pour de plus amples informations, veuillez consulter Créer un groupe cible.

   c. (Facultatif) Choisissez Ajouter une balise d'écoute et entrez une clé de balise et une valeur de balise.

   d. (Facultatif) Choisissez Ajouter un écouteur pour ajouter un autre écouteur (par exemple, un écouteur TLS).

9. Paramètres de l'écouteur sécurisé

   Cette section apparaît uniquement si vous ajoutez un écouteur TLS.

   a. Pour Stratégie de sécurité, choisissez une stratégie de sécurité qui répond à vos exigences. Pour de plus amples informations, veuillez consulter Stratégies de sécurité.

   b. Pour le certificat de SSL/TLS serveur par défaut, choisissez From ACM comme source du certificat. Sélectionnez un certificat que vous avez fourni ou importé à l'aide AWS Certificate Manager. Si aucun certificat n'est disponible dans ACM mais que vous possédez un certificat à utiliser avec votre équilibreur de charge, sélectionnez Importer un certificat et fournissez les informations requises. Sinon, choisissez Demander un nouveau certificat ACM. Pour plus d'informations, consultez la section sur AWS Certificate Manager les certificats dans le guide de AWS Certificate Manager l'utilisateur.

   c. (Facultatif) Pour la politique ALPN, choisissez une politique pour activer ALPN. Pour de plus amples informations, veuillez consulter the section called “Stratégies ALPN”.

10. Tags d'équilibreur de charge

(Facultatif) Développez les balises de l'équilibreur de charge. Choisissez Ajouter une nouvelle balise et entrez une clé de balise et une valeur de balise. Pour plus d'informations, veuillez consulter Balises.

11. Récapitulatif

    Examinez votre configuration, puis choisissez Create load balancer (Créer l'équilibreur de charge). Quelques attributs par défaut sont appliqués à votre Network Load Balancer lors de sa création. Vous pouvez les consulter et les modifier après avoir créé le Network Load Balancer. Pour de plus amples informations, veuillez consulter Attributs de l'équilibreur de charge.

AWS CLI

Pour créer un Network Load Balancer

Utilisez la commande create-load-balancer.

L'exemple suivant crée un équilibreur de charge connecté à Internet avec deux zones de disponibilité activées et un groupe de sécurité.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Pour créer un Network Load Balancer interne

Incluez l'`--scheme`option comme indiqué dans l'exemple suivant.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --scheme internal \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Pour créer un Network Load Balancer à double pile

Incluez l'`--ip-address-type`option comme indiqué dans l'exemple suivant.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --ip-address-type dualstack \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Pour ajouter un écouteur

Utilisez la commande create-listener. Pour obtenir des exemples, consultez Créer un écouteur.

CloudFormation

Pour créer un Network Load Balancer

Définissez un type de ressource AWS::ElasticLoadBalancingV2::LoadBalancer.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      IpAddressType: dualstack
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      Tags:
        - Key: 'department'
          Value: '123'
```

Pour ajouter un écouteur

Définissez un type de ressource AWS::ElasticLoadBalancingV2::Listener. Pour obtenir des exemples, consultez Créer un écouteur.

Testez l'équilibreur de charge

Après avoir créé votre Network Load Balancer, vous pouvez vérifier que vos EC2 instances ont passé avec succès le test de santé initial, puis vérifier que le Network Load Balancer envoie du trafic vers vos instances. EC2 Pour supprimer le Network Load Balancer, consultez. Suppression d'un Network Load Balancer

Pour tester le Network Load Balancer

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

Étapes suivantes

Après avoir créé votre équilibreur de charge, vous pouvez effectuer les opérations suivantes :

- Configurez les attributs de l'équilibreur de charge.
- Configurez les attributs du groupe cible.
- [Écouteurs TLS] Ajoutez des certificats à la liste des certificats facultatifs.
- Configurez les fonctionnalités de surveillance.

Mettez à jour les zones de disponibilité de votre Network Load Balancer

Vous pouvez activer ou désactiver les zones de disponibilité de votre Network Load Balancer à tout moment. Lorsque vous activez une zone de disponibilité, vous devez spécifier un sous-réseau à partir de cette zone de disponibilité. Une fois que vous avez activé une zone de disponibilité, l'équilibreur de charge commence à acheminer les demandes vers les cibles enregistrées dans cette zone de disponibilité. Votre équilibreur de charge est plus efficace si vous vous assurez que chaque zone de disponibilité activée a au moins une cible enregistrée. L'activation de plusieurs zones de disponibilité permet d'améliorer la tolérance aux pannes de vos applications.

Elastic Load Balancing crée un nœud Network Load Balancer dans la zone de disponibilité de votre choix, ainsi qu'une interface réseau pour le sous-réseau sélectionné dans cette zone de disponibilité. Chaque nœud Network Load Balancer de la zone de disponibilité utilise l'interface réseau pour obtenir une IPv4 adresse. Vous pouvez consulter ces interfaces réseau, mais elles ne peuvent pas être modifiées.

Considérations

- Pour les équilibreurs de charge réseau connectés à Internet, les sous-réseaux que vous spécifiez doivent disposer d'au moins 8 adresses IP disponibles. Pour les équilibreurs de charge réseau internes, cela n'est nécessaire que si vous autorisez la AWS sélection d'une IPv4 adresse privée dans le sous-réseau.
- Vous ne pouvez pas spécifier un sous-réseau dans une zone de disponibilité limitée. Toutefois, vous pouvez spécifier un sous-réseau dans une zone de disponibilité non contrainte et utiliser l'équilibrage de charge entre zones pour distribuer le trafic aux cibles de la zone de disponibilité restreinte.
- Vous ne pouvez pas spécifier de sous-réseau dans une zone locale.
- Vous ne pouvez pas supprimer un sous-réseau si le Network Load Balancer possède des associations de points de terminaison Amazon VPC actives.
- Lorsque vous ajoutez un sous-réseau précédemment supprimé, une nouvelle interface réseau est créée avec un identifiant différent.
- Les modifications de sous-réseau au sein d'une même zone de disponibilité doivent être des actions indépendantes. Vous devez d'abord terminer la suppression du sous-réseau existant, puis vous pouvez ajouter le nouveau sous-réseau.
- La suppression du sous-réseau peut prendre jusqu'à 3 minutes.

Lorsque vous créez un Network Load Balancer connecté à Internet, vous pouvez choisir de spécifier une adresse IP élastique pour chaque zone de disponibilité. Les adresses IP élastiques fournissent à votre Network Load Balancer des adresses IP statiques. Si vous choisissez de ne pas spécifier d'adresse IP élastique, une adresse IP élastique AWS sera attribuée à chaque zone de disponibilité.

Lorsque vous créez un Network Load Balancer interne, vous pouvez choisir de spécifier une adresse IP privée pour chaque sous-réseau. Les adresses IP privées fournissent à votre Network Load Balancer des adresses IP statiques. Si vous choisissez de ne pas spécifier d'adresse IP privée, AWS attribuez-en une pour vous.

Avant de mettre à jour les zones de disponibilité de votre Network Load Balancer, nous vous recommandons d'évaluer tout impact potentiel sur les connexions, les flux de trafic ou les charges de travail de production existants.

⚠ La mise à jour d'une zone de disponibilité peut être perturbatrice

- Lorsqu'un sous-réseau est supprimé, l'Elastic Network Interface (ENI) qui lui est associée est supprimée. Cela entraîne la résiliation de toutes les connexions actives dans la zone de disponibilité.
- Après la suppression d'un sous-réseau, toutes les cibles de la zone de disponibilité à laquelle il était associé sont marquées comme `unused` telles. Cela entraîne la suppression de ces cibles du pool de cibles disponible et l'interruption de toutes les connexions actives à ces cibles. Cela inclut toutes les connexions provenant d'autres zones de disponibilité lors de l'utilisation de l'équilibrage de charge entre zones.
- Les équilibreurs de charge réseau ont un délai de vie de 60 secondes (TTL) pour leur nom de domaine complet (FQDN). Lorsqu'une zone de disponibilité contenant des cibles actives est supprimée, toutes les connexions client existantes peuvent connaître des délais d'expiration jusqu'à ce que la résolution DNS se reproduise et que le trafic soit transféré vers les zones de disponibilité restantes.

Console

Pour modifier les zones de disponibilité

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

3. Sélectionnez l'équilibreur de charge.
4. Sous l'ongletNetwork mapping, choisissez Edit subnets.
5. Pour activer une zone de disponibilité, cochez sa case et sélectionnez un sous-réseau. S'il n'y a qu'un seul sous-réseau disponible, il est sélectionné pour vous.
6. Pour modifier le sous-réseau d'une zone de disponibilité activée, choisissez l'un des autres sous-réseaux dans la liste.
7. Pour désactiver une zone de disponibilité, décochez sa case.
8. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour modifier les zones de disponibilité

Utilisez la commande set-subnets.

```
aws elbv2 set-subnets \
    --load-balancer-arn load-balancer-arn \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890
```

CloudFormation

Pour modifier les zones de disponibilité

Mettez à jour la AWS::ElasticLoadBalancingV2::LoadBalancerressource.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref new-subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
```

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

Vous pouvez configurer votre Network Load Balancer afin que les clients puissent communiquer avec le Network Load Balancer en utilisant uniquement des adresses, ou IPv4 en utilisant à la IPv4 fois des adresses IPv6 et des adresses (dualstack). Le Network Load Balancer communique avec les cibles en fonction du type d'adresse IP du groupe cible. Pour de plus amples informations, veuillez consulter Type d'adresse IP.

Exigences en matière de double pile

- Vous pouvez définir le type d'adresse IP lorsque vous créez le Network Load Balancer et le mettre à jour à tout moment.
- Le cloud privé virtuel (VPC) et les sous-réseaux que vous spécifiez pour le Network Load Balancer doivent être associés à des blocs CIDR. IPv6 Pour plus d'informations, consultez les IPv6adresses dans le guide de EC2 l'utilisateur Amazon.
- Les tables de routage des sous-réseaux Network Load Balancer doivent acheminer le trafic. IPv6
- Le réseau ACLs des sous-réseaux Network Load Balancer doit autoriser le trafic. IPv6

Console

Pour mettre à jour le type d'adresse IP

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Cochez la case correspondant au Network Load Balancer.
4. Choisissez Actions, Edit IP address type.
5. Pour le type d'adresse IP, choisissez de prendre IPv4en charge les IPv4 adresses uniquement ou Dualstack pour prendre en charge à la fois les adresses IPv4 et IPv6 les adresses.
6. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour mettre à jour le type d'adresse IP

Utilisez la commande set-ip-address-type.

```
aws elbv2 set-ip-address-type \
    --load-balancer-arn load-balancer-arn \
    --ip-address-type dualstack
```

CloudFormation

Pour mettre à jour le type d'adresse IP

Mettez à jour la AWS::ElasticLoadBalancingV2::LoadBalancerressource.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      IpAddressType: dualstack
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
```

Modifier les attributs de votre Network Load Balancer

Après avoir créé un Network Load Balancer, vous pouvez modifier ses attributs.

Attributs de l'équilibreur de charge

- Protection contre la suppression
- Equilibrage de charge entre zones
- Affinité DNS de zone de disponibilité
- Adresses IP secondaires

Protection contre la suppression

Pour éviter que votre Network Load Balancer ne soit supprimé accidentellement, vous pouvez activer la protection contre la suppression. Par défaut, la protection contre les suppressions est désactivée pour votre Network Load Balancer.

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

Console

Pour activer ou désactiver la protection contre la suppression

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

AWS CLI

Pour activer ou désactiver la protection contre la suppression

Utilisez la modify-load-balancer-attributescommande avec l'`deletion_protection.enabled`attribut.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=deletion_protection.enabled,Value=true"
```

CloudFormation

Pour activer ou désactiver la protection contre la suppression

Mettez à jour la AWS::ElasticLoadBalancingV2::LoadBalancerressource pour inclure l'`deletion_protection.enabled`attribut.

```
Resources:
  myLoadBalancer:
```

```
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "deletion_protection.enabled"
          Value: "true"
```

Equilibrage de charge entre zones

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

Console

Pour activer ou désactiver l'équilibrage de charge entre zones pour un équilibreur de charge

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sous Équilibrage de charge, choisissez Équilibreurs de charge.
3. Sélectionnez le nom de l'équilibreur de charge afin d'ouvrir sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sur la page Modifier les attributs de l'équilibreur de charge, activez ou désactivez l'Équilibrage de charge entre zones.
6. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour activer ou désactiver l'équilibrage de charge entre zones pour un équilibreur de charge

Utilisez la modify-load-balancer-attributescommande avec l'`load_balancing.cross_zone.enabled`attribut.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=load_balancing.cross_zone.enabled,Value=true"
```

CloudFormation

Pour activer ou désactiver l'équilibrage de charge entre zones pour un équilibreur de charge

Mettez à jour la AWS::ElasticLoadBalancingV2::LoadBalancer ressource pour inclure l'`load_balancing.cross_zone.enabled`attribut.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "load_balancing.cross_zone.enabled"
          Value: "true"
```

Affinité DNS de zone de disponibilité

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

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

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

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

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

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

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

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

  Les requêtes DNS du client sont résolues entre des adresses IP Network Load Balancer saines dans toutes les zones de disponibilité du Network Load Balancer.

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

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

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

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

- L'affinité de zone de disponibilité entraîne des modifications sur tous les clients Network Load Balancers qui utilisent Route 53 Resolver.
  - Les clients ne sont pas en mesure de choisir entre les résolutions DNS zonales-locales et multizones. L'affinité de zone de disponibilité décide pour eux.
  - Les clients ne disposent pas d'une méthode fiable pour déterminer à quel moment ils sont concernés par l'affinité de zone de disponibilité ou comment savoir quelle adresse IP se trouve dans quelle zone de disponibilité.
- Lorsqu'ils utilisent l'affinité de zone de disponibilité avec les équilibreurs de charge réseau et le résolveur Route 53, nous recommandons aux clients d'utiliser le point de terminaison entrant du résolveur Route 53 dans leur propre zone de disponibilité.
- Les clients resteront affectés à leur adresse IP locale de zone jusqu'à ce qu'elle soit jugée totalement défectueuse selon les surveillances de l'état du DNS et qu'elle soit supprimée du DNS.
- L'utilisation de l'affinité de zone de disponibilité avec l'équilibrage de charge entre zones activé peut entraîner une répartition déséquilibrée des connexions client entre les zones de disponibilité. Il est recommandé de configurer votre pile d'applications pour qu'elle se mette à l'échelle indépendamment dans chaque zone de disponibilité, afin de garantir qu'elle puisse prendre en charge le trafic des clients zonaux.
- Si l'équilibrage de charge entre zones est activé, le Network Load Balancer est soumis à un impact entre zones.
- La charge sur chacune des zones de disponibilité des Network Load Balancers sera proportionnelle aux emplacements zonaux des demandes des clients. Si vous ne configurez pas

le nombre de clients exécutés dans chaque zone de disponibilité, vous devrez mettre à l'échelle chaque zone de disponibilité de manière réactive et indépendante.

Contrôle

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

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

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

Pour de plus amples informations, consultez CloudWatch métriques pour votre Network Load Balancer.

Activer l'affinité avec les zones de disponibilité

Console

Pour activer l'affinité avec les zones de disponibilité

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

AWS CLI

Pour activer l'affinité avec les zones de disponibilité

Utilisez la modify-load-balancer-attributescommande avec l'`dns_record.client_routing_policy`attribut.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes
 "Key=dns_record.client_routing_policy,Value=partial_availability_zone_affinity"
```

CloudFormation

Pour activer l'affinité avec les zones de disponibilité

Mettez à jour la AWS::ElasticLoadBalancingV2::LoadBalancerressource pour inclure l'`dns_record.client_routing_policy`attribut.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "dns_record.client_routing_policy"
          Value: "partial_availability_zone_affinity"
```

Adresses IP secondaires

Si vous rencontrez des erreurs d'allocation de ports et que vous ne pouvez pas ajouter de cibles au groupe cible pour les résoudre, vous pouvez ajouter des adresses IP secondaires aux interfaces réseau de l'équilibreur de charge. Pour chaque zone où l'équilibreur de charge est activé, nous sélectionnons des IPv4 adresses dans le sous-réseau de l'équilibreur de charge et les attribuons

à l'interface réseau correspondante. Ces adresses IP secondaires sont utilisées pour établir des connexions avec des cibles. Ils sont également utilisés pour les bilans de santé du trafic. Nous vous recommandons d'ajouter une adresse IP secondaire pour commencer, de surveiller la `PortAllocationErrors` métrique et d'ajouter une autre adresse IP secondaire uniquement si les erreurs d'allocation de port ne sont pas résolues.

> **Warning**
>
> Une fois que vous avez ajouté des adresses IP secondaires, vous ne pouvez pas les supprimer. La seule façon de libérer les adresses IP secondaires est de supprimer l'équilibreur de charge. Avant d'ajouter des adresses IP secondaires, vérifiez qu'il y a suffisamment d' IPv4adresses disponibles dans les sous-réseaux de l'équilibreur de charge.

Console

Pour ajouter une adresse IP secondaire

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Sélectionnez le nom du Network Load Balancer afin d'ouvrir sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Développez les attributs spéciaux, déverrouillez les adresses IP secondaires attribuées automatiquement par attribut de sous-réseau et choisissez le nombre d'adresses IP secondaires.
6. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour ajouter une adresse IP secondaire

Utilisez la modify-load-balancer-attributescommande avec l'`secondary_ips.auto_assigned.per_subnet`attribut.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=secondary_ips.auto_assigned.per_subnet,Value=1"
```

Vous pouvez utiliser la describe-network-interfacescommande pour obtenir les IPv4 adresses des interfaces réseau de l'équilibreur de charge. Le `--filters` paramètre étend les résultats aux interfaces réseau pour les équilibreurs de charge réseau et le `--query` paramètre étend ensuite les résultats à l'équilibreur de charge portant le nom spécifié et affiche uniquement les champs spécifiés. Vous pouvez inclure des champs supplémentaires si nécessaire.

```
aws elbv2 describe-network-interfaces \
    --filters "Name=interface-type,Values=network_load_balancer" \
    --query "NetworkInterfaces[?contains(Description,'my-nlb')].
{ID:NetworkInterfaceId,AZ:AvailabilityZone,Addresses:PrivateIpAddresses[*]}"
```

CloudFormation

Pour ajouter une adresse IP secondaire

Mettez à jour la AWS::ElasticLoadBalancingV2::LoadBalancerressource pour inclure l'`secondary_ips.auto_assigned.per_subnet`attribut.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "secondary_ips.auto_assigned.per_subnet"
          Value: "1"
```

Mettez à jour les groupes de sécurité pour votre Network Load Balancer

Vous pouvez associer un groupe de sécurité à votre Network Load Balancer pour contrôler le trafic autorisé à atteindre le Network Load Balancer et à le quitter. Vous spécifiez les ports, protocoles et sources à autoriser pour le trafic entrant, ainsi que les ports, protocoles et destinations à autoriser

pour le trafic sortant. Si vous n'attribuez aucun groupe de sécurité à votre Network Load Balancer, tout le trafic client peut atteindre les écouteurs Network Load Balancer et tout le trafic peut quitter le Network Load Balancer.

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

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

Table des matières

Considérations

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

Exemple : filtrer le trafic client

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

Entrant

Protocole	Source	Plage de ports	Comment
protocol	*client IP address range*	*listener port*	Autorise le trafic entrant depuis la plage d'adresses CIDR source sur le port d'écoute.
ICMP	0.0.0.0/0	Tous	Permet au trafic ICMP entrant de prendre en charge la MTU ou la détection de la MTU du chemin †.

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

Sortant

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

Exemple : accepter uniquement le trafic provenant du Network Load Balancer

Supposons que votre Network Load Balancer possède un groupe de sécurité sg-111112222233333. Utilisez les règles suivantes dans les groupes de sécurité associés à vos instances cibles pour vous assurer qu'elles n'acceptent que le trafic provenant du Network Load Balancer. Vous devez vous assurer que les cibles acceptent le trafic provenant du Network Load Balancer à la fois sur le port

cible et sur le port de contrôle de santé. Pour de plus amples informations, veuillez consulter the section called “Groupes de sécurité cibles”.

Entrant

Protocole	Source	Plage de ports	Comment
protocol	sg-111112 222233333	*target port*	Autorise le trafic entrant depuis le Network Load Balancer sur le port cible
protocol	sg-111112 222233333	*health check*	Autorise le trafic entrant depuis le Network Load Balancer sur le port de contrôle de santé

Sortant

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

Mise à jour des groupes de sécurité associés

Si vous avez associé au moins un groupe de sécurité à un Network Load Balancer lors de sa création, vous pouvez mettre à jour les groupes de sécurité de ce Network Load Balancer à tout moment.

Console

Pour mettre à jour les groupes de sécurité

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 Network Load Balancer.
4. Dans l'onglet Security, choisissez Edit.

5. Pour associer un groupe de sécurité à votre Network Load Balancer, sélectionnez-le. Pour supprimer un groupe de sécurité de votre Network Load Balancer, supprimez-le.
6. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour mettre à jour les groupes de sécurité

Utilisez la commande set-security-groups.

```
aws elbv2 set-security-groups \
    --load-balancer-arn load-balancer-arn \
    --security-groups sg-1234567890abcdef0 sg-0abcdef0123456789
```

CloudFormation

Pour mettre à jour les groupes de sécurité

Mettez à jour la AWS::ElasticLoadBalancingV2::LoadBalancerressource.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
        - !Ref myNewSecurityGroup
```

Mise à jour des paramètres de sécurité

Par défaut, nous appliquons les règles du groupe de sécurité entrant à tout le trafic envoyé au Network Load Balancer. Toutefois, il se peut que vous ne souhaitiez pas appliquer ces règles au trafic envoyé au Network Load Balancer via AWS PrivateLink, qui peut provenir d'adresses IP qui

se chevauchent. Dans ce cas, vous pouvez configurer le Network Load Balancer afin que nous n'appliquions pas les règles entrantes pour le trafic envoyé via le Network Load Balancer. AWS PrivateLink

Console

Pour mettre à jour les paramètres de sécurité

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 Network Load Balancer.
4. Dans l'onglet Security, choisissez Edit.
5. Sous Paramètre de sécurité, décochez Appliquer les règles de trafic entrant au PrivateLink trafic.
6. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour mettre à jour les paramètres de sécurité

Utilisez la commande set-security-groups.

```
aws elbv2 set-security-groups \
    --load-balancer-arn load-balancer-arn \
    --enforce-security-group-inbound-rules-on-private-link-traffic off
```

CloudFormation

Pour mettre à jour les paramètres de sécurité

Mettez à jour la AWS::ElasticLoadBalancingV2::LoadBalancerressource.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
```

```
      Scheme: internal
      EnforceSecurityGroupInboundRulesOnPrivateLinkTraffic: off
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
```

Surveiller les groupes de sécurité Network Load Balancer

Utilisez les `SecurityGroupBlockedFlowCount_Outbound` CloudWatch métriques `SecurityGroupBlockedFlowCount_Inbound` et pour surveiller le nombre de flux bloqués par les groupes de sécurité Network Load Balancer. Le trafic bloqué n'est pas reflété dans les autres métriques. Pour de plus amples informations, veuillez consulter the section called “CloudWatch métriques”.

Utilisez les journaux de flux VPC pour surveiller le trafic accepté ou rejeté par les groupes de sécurité Network Load Balancer. Pour plus d'informations, veuillez consulter Journaux de flux VPC dans le Guide de l'utilisateur Amazon VPC.

Marquer un Network Load Balancer

Les balises vous aident à classer vos équilibreurs de charge réseau de différentes manières. Par exemple, vous pouvez baliser une ressource par objectif, propriétaire ou environnement.

Vous pouvez ajouter plusieurs balises à chaque Network Load Balancer. Si vous ajoutez une balise avec une clé déjà associée au Network Load Balancer, la valeur de cette balise est mise à jour.

Lorsque vous avez terminé avec un tag, vous pouvez le supprimer de votre Network Load Balancer.

Restrictions

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

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

Console

Pour mettre à jour les balises d'un équilibreur de charge

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Cochez la case correspondant au Network Load Balancer.
4. Dans l'onglet Balises, choisissez Gérer les balises.
5. Pour ajouter une balise, choisissez Ajouter une balise, puis saisissez la clé et la valeur de la balise. Les caractères autorisés sont les lettres, les espaces et les chiffres (en UTF-8), ainsi que les caractères spéciaux suivants : + - =. _ : / @. N'utilisez pas d'espaces de début ou de fin. Les valeurs de balises sont sensibles à la casse.
6. Pour mettre à jour une balise, entrez de nouvelles valeurs dans Clé ou Valeur.
7. Pour supprimer une balise, choisissez Retirer en regard de la balise.
8. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour ajouter des tags

Utilisez la commande add tags. L'exemple suivant ajoute deux balises.

```
aws elbv2 add-tags \
    --resource-arns load-balancer-arn \
    --tags "Key=project,Value=lima" "Key=department,Value=digital-media"
```

Pour supprimer des balises

Utilisez la commande remove-tags. L'exemple suivant supprime les balises avec les clés spécifiées.

```
aws elbv2 remove-tags \
```

```
    --resource-arns load-balancer-arn \
    --tag-keys project department
```

CloudFormation

Pour ajouter des tags

Définissez une ressource de type AWS::ElasticLoadBalancingV2::LoadBalancerressource pour inclure la `Tags` propriété.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
          Value: 'digital-media'
```

Suppression d'un Network Load Balancer

Dès que votre Network Load Balancer est disponible, vous êtes facturé pour chaque heure ou heure partielle pendant laquelle il fonctionne. Lorsque vous n'avez plus besoin du Network Load Balancer, vous pouvez le supprimer. Dès que le Network Load Balancer est supprimé, vous cessez de payer des frais pour celui-ci.

Vous ne pouvez pas supprimer un Network Load Balancer si la protection contre la suppression est activée. Pour de plus amples informations, veuillez consulter Protection contre la suppression.

Vous ne pouvez pas supprimer un Network Load Balancer s'il est utilisé par un autre service. Par exemple, si le Network Load Balancer est associé à un service de point de terminaison VPC, vous

devez supprimer la configuration du service de point de terminaison avant de pouvoir supprimer le Network Load Balancer associé.

La suppression d'un Network Load Balancer entraîne également la suppression de ses écouteurs. La suppression d'un Network Load Balancer n'affecte pas ses cibles enregistrées. Par exemple, vos EC2 instances continuent de s'exécuter et sont toujours enregistrées auprès de leurs groupes cibles. Pour supprimer vos groupes cible, consultez la page Supprimer un groupe cible pour votre Network Load Balancer.

Console

Pour supprimer un Network Load Balancer

1. Si l'enregistrement DNS de votre domaine pointe vers votre Network Load Balancer, pointez-le vers un nouvel emplacement et attendez que la modification du DNS prenne effet avant de supprimer votre Network Load Balancer. Par exemple :
   - S'il s'agit d'un enregistrement CNAME avec une durée de vie (TTL) de 300 secondes, attendez au moins 300 secondes avant de passer à l'étape suivante.
   - Si l'enregistrement est un enregistrement Route 53 Alias(A), attendez au moins 60 secondes.
   - Si vous utilisez Route 53, la modification d'enregistrement prend 60 secondes pour se propager à tous les serveurs de noms Route 53 mondiaux. Ajoutez ce temps à la valeur TTL de l'enregistrement en cours de mise à jour.
2. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
3. Dans le volet de navigation, choisissez Load Balancers.
4. Cochez la case correspondant au Network Load Balancer.
5. Sélectionnez Actions, Delete load balancer.
6. Lorsque vous êtes invité à confirmer, saisissez **`confirm`**, puis choisissez Supprimer.

AWS CLI

Pour supprimer un Network Load Balancer

Utilisez la commande delete-load-balancer.

```
aws elbv2 delete-load-balancer \
```

```
    --load-balancer-arn load-balancer-arn
```

Afficher la carte des ressources du Network Load Balancer

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

Pour consulter la carte des ressources de votre équilibreur de charge

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

Composants de la carte des ressources

Vues cartographiques

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

La vue Malhealthy Target Map peut être utilisée pour dépanner les cibles dont les tests de santé échouent. Pour de plus amples informations, veuillez consulter Résoudre les problèmes liés aux cibles défectueuses à l'aide de la carte des ressources.

Colonnes de ressources

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

Tuiles de ressources

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

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

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

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

Exporter la carte des ressources

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

Changement de zone pour votre Network Load Balancer

Le changement de zone est une fonctionnalité d'Amazon Application Recovery Controller (ARC). Avec le changement de zone, vous pouvez déplacer une ressource Network Load Balancer 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 commencez un changement de zone, votre Network Load Balancer arrête d'acheminer le trafic vers les cibles situées dans la zone de disponibilité concernée. Les connexions existantes

aux cibles de la zone de disponibilité concernée ne sont pas interrompues par un changement de zone. Plusieurs minutes peuvent être nécessaires pour que ces connexions s'effectuent correctement.

Table des matières

Avant de commencer un changement de zone

- Le décalage de zone est désactivé par défaut et doit être activé sur chaque Network Load Balancer. Pour de plus amples informations, veuillez consulter Activez le changement de zone pour votre Network Load Balancer.
- Vous ne pouvez lancer un changement de zone pour un Network Load Balancer spécifique que pour une seule zone de disponibilité. Vous ne pouvez pas commencer un changement de zone pour plusieurs zones de disponibilité.
- AWS supprime de manière proactive les adresses IP zonales Network Load Balancer 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 vous utilisez un décalage de zone sur votre Network Load Balancer, la zone de disponibilité affectée par le décalage de zone perd également sa capacité cible.
- Lors du changement de zone sur les équilibreurs de charge réseau lorsque l'équilibrage de charge entre zones est activé, les adresses IP des équilibreurs de charge zonaux sont supprimées du DNS. Les connexions existantes aux cibles situées dans la zone de disponibilité altérée sont maintenues jusqu'à leur fermeture organique, tandis que les nouvelles connexions ne sont plus acheminées vers les cibles situées dans la zone de disponibilité altérée.

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

Dérogation administrative relative au changement de zone

Les cibles appartenant à un Network Load Balancer incluront un nouveau statut`AdministrativeOverride`, indépendant de l'`TargetHealth`état.

Lorsqu'un changement de zone est lancé pour un Network Load Balancer, toutes les cibles situées dans la zone à éloigner sont considérées comme étant remplacées administrativement. Le Network Load Balancer arrête d'acheminer le nouveau trafic vers des cibles administrativement remplacées. Les connexions existantes restent intactes jusqu'à ce qu'elles soient fermées de manière organique.

Les `AdministrativeOverride` états possibles sont les suivants :

inconnu

L'état ne peut pas être propagé en raison d'une erreur interne

no_override

Aucune dérogation n'est actuellement active sur la cible

zonal_shift_active

Le changement de zone est actif dans la zone de disponibilité cible

zonal_shift_delegated_to_dns

L'état de décalage de zone de cette cible n'est pas disponible `DescribeTargetHealth` mais peut être visualisé directement via l' AWS ARC - Zonal Shift API ou la console.

Activez le changement de zone pour votre Network Load Balancer

Le décalage de zone est désactivé par défaut et doit être activé sur chaque Network Load Balancer. Cela garantit que vous pouvez commencer un changement de zone en utilisant uniquement les équilibreurs de charge réseau spécifiques que vous souhaitez. Pour de plus amples informations, veuillez consulter the section called “Changement de zone”.

Prérequis

Si vous activez l'équilibrage de charge entre zones pour l'équilibreur de charge, chaque groupe cible rattaché à l'équilibreur de charge doit répondre aux exigences suivantes avant de pouvoir activer le décalage zonal.

- Le protocole du groupe cible doit être `TCP` ou`TLS`.

- Le type de groupe cible ne doit pas êtrealb.
- La terminaison de connexion pour les cibles défectueuses doit être désactivée.
- L'attribut du groupe `load_balancing.cross_zone.enabled` cible doit être `true` ou `use_load_balancer_configuration` (valeur par défaut).

Console

Pour activer le décalage de zone

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 Network Load Balancer.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sous Configuration du routage de la zone de disponibilité, pour l'intégration du décalage zonal ARC, sélectionnez Activer.
6. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour activer le décalage de zone

Utilisez la modify-load-balancer-attributescommande avec l'`zonal_shift.config.enabled`attribut.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes "Key=zonal_shift.config.enabled,Value=true"
```

CloudFormation

Pour activer le décalage de zone

Mettez à jour la AWS::ElasticLoadBalancingV2::LoadBalancerressource pour inclure l'`zonal_shift.config.enabled`attribut.

```
Resources:
  myLoadBalancer:
```

```
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        -Key: "zonal_shift.config.enabled"
         Value: "true"
```

Commencez un changement de zone pour votre Network Load Balancer

Le changement de zone dans ARC vous permet de déplacer temporairement le trafic vers les ressources prises en charge hors d'une zone de disponibilité afin que votre application puisse continuer à fonctionner normalement avec les autres zones de disponibilité d'une AWS région.

Prérequis

Avant de commencer, vérifiez que vous avez activé le décalage de zone pour l'équilibreur de charge.

Console

Cette procédure explique comment démarrer un changement de zone à l'aide de la EC2 console Amazon. Pour savoir comment démarrer un changement de zone à l'aide de la console ARC, consultez la section Commencer un changement de zone dans le manuel du développeur Amazon Application Recovery Controller (ARC).

Pour démarrer un changement de zone

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 Network Load Balancer.
4. Dans l'onglet Intégrations, développez Amazon Application Recovery Controller (ARC) et choisissez Start zonal Shift.
5. Sélectionnez la zone de disponibilité depuis laquelle vous voulez déplacer le trafic.

6. Choisissez ou saisissez une date d'expiration pour le changement de zone. Au départ, un changement de zone peut être défini entre 1 minute et 3 jours (72 heures).

   Tous les changements de zone sont temporaires. Vous devez définir une date d'expiration, mais vous pouvez mettre à jour les changements actifs ultérieurement pour définir une nouvelle date d'expiration.
7. Saisissez un commentaire. Vous pouvez mettre à jour le décalage de zone ultérieurement pour modifier le commentaire.
8. Cochez la case pour confirmer que le lancement d'un changement de zone réduit la capacité de votre application en déplaçant le trafic hors de la zone de disponibilité.
9. Choisissez Confirmer.

AWS CLI

Pour démarrer un changement de zone

Utilisez la start-zonal-shiftcommande Amazon Application Recovery Controller (ARC).

```
aws arc-zonal-shift start-zonal-shift \
    --resource-identifier load-balancer-arn \
    --away-from use2-az2 \
    --expires-in 2h \
    --comment "zonal shift due to scheduled maintenance"
```

Mettez à jour un décalage de zone pour votre Network Load Balancer

Vous pouvez mettre à jour un décalage de zone pour définir une nouvelle date d'expiration, ou modifier ou remplacer le commentaire correspondant au décalage de zone.

Console

Cette procédure explique comment mettre à jour un décalage de zone à l'aide de la EC2 console Amazon. Pour savoir comment mettre à jour un décalage de zone à l'aide de la console Amazon Application Recovery Controller (ARC), consultez la section Mise à jour d'un décalage de zone dans le manuel du développeur Amazon Application Recovery Controller (ARC).

Pour mettre à jour un décalage de zone

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 un Application Load Balancer avec un décalage de zone actif.
4. Dans l'onglet Intégrations, développez Amazon Application Recovery Controller (ARC) et choisissez Update zonal Shift.

   Cela ouvre la console ARC pour poursuivre le processus de mise à jour.
5. (Facultatif) Pour Définir l'expiration du décalage zonal, sélectionnez ou entrez une date d'expiration.
6. (Facultatif) Pour Commentaire, modifiez éventuellement le commentaire existant ou saisissez-en un nouveau.
7. Choisissez Mettre à jour.

AWS CLI

Pour mettre à jour un décalage de zone

Utilisez la update-zonal-shiftcommande Amazon Application Recovery Controller (ARC).

```
aws arc-zonal-shift update-zonal-shift \
    --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf57EXAMPLE \
    --expires-in 1h \
    --comment "extending zonal shift for scheduled maintenance"
```

Annuler un changement de zone pour votre Network Load Balancer

Vous pouvez annuler un changement de zone à tout moment avant son expiration. Vous pouvez annuler les changements de zone que vous initiez, ou les changements de zone qui AWS commencent pour une ressource dans le cadre d'une séance d'entraînement pour le changement automatique de zone.

Console

Cette procédure explique comment annuler un changement de zone à l'aide de la EC2 console Amazon. Pour savoir comment annuler un changement de zone à l'aide de la console Amazon Application Recovery Controller (ARC), consultez la section Annulation d'un changement de zone dans le manuel du développeur Amazon Application Recovery Controller (ARC).

Pour annuler un changement de zone

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 un Network Load Balancer avec un décalage de zone actif.
4. Dans l'onglet Intégrations, sous Amazon Application Recovery Controller (ARC), choisissez Annuler le changement de zone.

   Cela ouvre la console ARC pour poursuivre le processus d'annulation.
5. Choisissez Annuler le changement de zone.
6. Lorsque vous êtes invité à confirmer l'opération, choisissez Confirmer.

AWS CLI

Pour annuler un changement de zone

Utilisez la cancel-zonal-shiftcommande Amazon Application Recovery Controller (ARC).

```
aws arc-zonal-shift cancel-zonal-shift \
    --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf57EXAMPLE
```

Réservations de capacité pour votre Network Load Balancer

Les réservations d'unités de capacité de l'équilibreur de charge (LCU) vous permettent de réserver une capacité minimale statique pour votre équilibreur de charge. Les équilibreurs de charge réseau s'adaptent automatiquement pour prendre en charge les charges de travail détectées et répondre aux besoins en capacité. Lorsque la capacité minimale est configurée, votre équilibreur de charge continue à augmenter ou à diminuer en fonction du trafic reçu, mais empêche également la capacité de descendre en dessous de la capacité minimale configurée.

Envisagez d'utiliser la réservation LCU dans les situations suivantes :

- Vous avez un événement à venir qui connaîtra un trafic soudain et inhabituel et vous voulez vous assurer que votre équilibreur de charge peut supporter le pic de trafic soudain pendant l'événement.

- Vous êtes confronté à des pics de trafic imprévisibles en raison de la nature de votre charge de travail pendant une courte période.
- Vous configurez votre équilibreur de charge pour intégrer ou migrer vos services à une heure de début précise et vous devez commencer par une capacité élevée au lieu d'attendre que l'auto-scaling entre en vigueur.
- Vous migrez des charges de travail entre des équilibreurs de charge et vous souhaitez configurer la destination en fonction de l'échelle de la source.

Estimez la capacité dont vous avez besoin

Lorsque vous déterminez la capacité à réserver pour votre équilibreur de charge, nous vous recommandons d'effectuer des tests de charge ou de consulter les données historiques de charge de travail qui représentent le trafic à venir que vous attendez. À l'aide de la console Elastic Load Balancing, vous pouvez estimer la capacité à réserver en fonction du trafic examiné.

Vous pouvez également vous référer à la CloudWatch métrique ProcessedBytespour déterminer le bon niveau de capacité. La capacité de votre équilibreur de charge est réservée LCUs, chaque LCU étant égale à 2,2 Mbits/s. Vous pouvez utiliser la métrique Max (ProcessedBytes) pour connaître le trafic de débit maximal par minute sur l'équilibreur de charge, puis convertir ce débit en LCUs utilisant un taux de conversion de 2,2 Mbits/s égal à 1 LCU.

Si vous ne disposez pas de données historiques de charge de travail à référencer et que vous ne pouvez pas effectuer de tests de charge, vous pouvez estimer la capacité nécessaire à l'aide du calculateur de réservation LCU. Le calculateur de réservation LCU utilise des données basées sur l'historique des charges de travail AWS observées et peut ne pas représenter votre charge de travail spécifique. Pour plus d'informations, consultez la section Calculateur de réservation d'unités de capacité Load Balancer.

Régions prises en charge

Cette fonctionnalité n'est disponible que dans les régions suivantes :

- USA Est (Virginie du Nord)
- USA Est (Ohio)
- USA Ouest (Oregon)
- Asie-Pacifique (Hong Kong)
- Asie-Pacifique (Singapour)

- Asie-Pacifique (Sydney)
- Asie-Pacifique (Tokyo)
- Europe (Francfort)
- Europe (Irlande)
- Europe (Stockholm)

Valeurs minimales et maximales pour une réservation LCU

Le montant total de la demande de réservation doit être d'au moins 2 750 LCU par zone de disponibilité. La valeur maximale est déterminée par les quotas de votre compte. Pour de plus amples informations, veuillez consulter the section called “Unités de capacité Load Balancer”.

Demandez la réservation d'une unité de capacité d'équilibrage de charge pour votre Network Load Balancer

Avant d'utiliser la réservation LCU, vérifiez les points suivants :

- La réservation de LCU n'est pas prise en charge sur les équilibreurs de charge réseau utilisant des écouteurs TLS.
- La réservation de LCU prend uniquement en charge la réservation de capacité de débit pour les équilibreurs de charge réseau. Lorsque vous demandez une réservation de LCU, convertissez vos besoins en capacité de Mbits/s en LCUs utilisant le taux de conversion de 1 LCU à 2,2 Mbits/s.
- La capacité est réservée au niveau régional et est répartie uniformément entre les zones de disponibilité. Vérifiez que vous disposez de suffisamment d'objectifs répartis uniformément dans chaque zone de disponibilité avant d'activer la réservation de LCU.
- Les demandes de réservation de LCU sont traitées selon le principe du premier arrivé, premier servi, et dépendent de la capacité disponible pour une zone à ce moment-là. La plupart des demandes sont généralement traitées en une heure, mais cela peut prendre jusqu'à quelques heures.
- Pour mettre à jour une réservation existante, la demande précédente doit être provisionnée ou échouer. Vous pouvez augmenter la capacité réservée autant de fois que nécessaire, mais vous ne pouvez la diminuer que deux fois par jour.
- Vous continuerez de payer des frais pour toute capacité réservée ou mise en service jusqu'à ce qu'elle soit résiliée ou annulée.

Console

Pour demander une réservation LCU

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Load Balancers (Équilibreurs de charge).
3. Sélectionnez le nom de l'équilibreur de charge.
4. Dans l'onglet Capacité, choisissez Modifier la réservation LCU.
5. Sélectionnez Estimation basée sur des références historiques.
6. Sélectionnez la période de référence pour afficher le niveau de LCU réservé recommandé.
7. Si vous n'avez pas de charge de travail de référence historique, vous pouvez choisir Estimation manuelle et saisir le nombre de personnes LCUs à réserver.
8. Choisissez Enregistrer.

AWS CLI

Pour demander une réservation LCU

Utilisez la commande modify-capacity-reservation.

```
aws elbv2 modify-capacity-reservation \
    --load-balancer-arn load-balancer-arn \
    --minimum-load-balancer-capacity CapacityUnits=3000
```

CloudFormation

Pour demander une réservation LCU

Mettez à jour la AWS::ElasticLoadBalancingV2::LoadBalancerressource.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-alb
      Type: application
      Scheme: internal
      Subnets:
```

```
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      MinimumLoadBalancerCapacity:
        CapacityUnits: 3000
```

Mettre à jour ou annuler les réservations d'unités de capacité Load Balancer pour votre Network Load Balancer

Si les modèles de trafic de votre équilibreur de charge changent, vous pouvez mettre à jour ou annuler la réservation de LCU pour votre équilibreur de charge.

Console

Pour mettre à jour ou annuler une réservation LCU

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Load Balancers (Équilibreurs de charge).
3. Sélectionnez le nom de l'équilibreur de charge.
4. Dans l'onglet Capacité, effectuez l'une des opérations suivantes :
   a. Pour mettre à jour la réservation LCU, choisissez Modifier la réservation LCU.
   b. Pour annuler la réservation du LCU, choisissez Annuler la capacité.

AWS CLI

Pour annuler une réservation LCU

Utilisez la commande modify-capacity-reservation.

```
aws elbv2 modify-capacity-reservation \
    --load-balancer-arn load-balancer-arn \
    --reset-capacity-reservation
```

Surveillez la réservation d'unités de capacité d'équilibrage de charge pour votre Network Load Balancer

État de la réservation

Les valeurs de statut possibles pour une réservation LCU sont les suivantes :

- `pending`- Indique la réservation en cours de provisionnement.
- `provisioned`- Indique que la capacité réservée est prête et disponible pour être utilisée.
- `failed`- Indique que la demande ne peut pas être traitée pour le moment.
- `rebalancing`- Indique qu'une zone de disponibilité a été ajoutée ou supprimée et que l'équilibreur de charge rééquilibre la capacité.

Utilisation des LCU

Pour déterminer l'utilisation des LCU réservées, vous pouvez comparer la métrique par minute avec la `ProcessedBytes` métrique par heure. `Sum(ReservedLCUs)` Pour convertir des octets par minute en LCU par heure, utilisez (octets par minute) *8/60/ (10^6) /2.2.

Console

Pour consulter le statut d'une réservation LCU

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Load Balancers (Équilibreurs de charge).
3. Sélectionnez le nom de l'équilibreur de charge.
4. Dans l'onglet Capacité, vous pouvez consulter le statut de la réservation et la valeur de la LCU réservée.

AWS CLI

Pour surveiller le statut d'une réservation LCU

Utilisez la commande describe-capacity-reservation.

```
aws elbv2 describe-capacity-reservation \
    --load-balancer-arn load-balancer-arn
```

Écouteurs pour vos Network Load Balancers

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

Table des matières

Configuration des écouteurs

Les écouteurs prennent en charge les protocoles et ports suivants :

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

Vous pouvez utiliser un écouteur TLS pour confier le travail de chiffrement et de déchiffrement à votre équilibreur de charge afin que vos applications puissent se concentrer sur leur logique métier. Si le

protocole d'écoute est TLS, vous devez déployer au moins un certificat de serveur SSL sur l'écouteur. Pour de plus amples informations, veuillez consulter Certificats de serveur.

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

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

Un écouteur UDP pour un équilibreur de charge à double pile nécessite des groupes cibles. IPv6

WebSockets n'est pris en charge que sur les écouteurs TCP, TLS et TCP_UDP.

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

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

Attributs de l'écouteur

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

`tcp.idle_timeout.seconds`

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

Pour de plus amples informations, veuillez consulter Mettre à jour le délai d'inactivité.

Règles d'un écouteur

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

Auditeurs sécurisés

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

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

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

Les équilibreurs de charge réseau prennent en charge la reprise du protocole TLS à l'aide de PSK pour TLS 1.3 et de tickets de session pour TLS 1.2 et versions antérieures. Les reprises avec ID de session, ou lorsque plusieurs certificats sont configurés dans l'écouteur à l'aide du SNI, ne sont pas prises en charge. La fonctionnalité de données 0-RTT et l'extension early_data ne sont pas implémentées.

Pour les démonstrations associées, veuillez consulter Prise en charge de TLS sur Network Load Balancer et Prise en charge de SNI sur Network Load Balancer (langue française non garantie).

Stratégies ALPN

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

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

Stratégies ALPN prises en charge

Les stratégies ALPN prises en charge sont les suivantes :

`HTTP1Only`

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

`HTTP2Only`

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

`HTTP2Optional`

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

`HTTP2Preferred`

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

`None`

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

Activer les connexions ALPN

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

Création d'un écouteur pour votre Network Load Balancer

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

Prérequis

- Vous devez spécifier un groupe cible pour la règle d'écouteur. Pour de plus amples informations, veuillez consulter Création d'un groupe cible pour votre Network Load Balancer.
- Vous devez spécifier un certificat SSL pour un écouteur TLS. L'équilibreur de charge utilise le certificat pour mettre fin à la connexion et déchiffrer les demandes des clients avant de les acheminer vers les cibles. Pour de plus amples informations, veuillez consulter Certificats de serveur pour votre Network Load Balancer.
- Vous ne pouvez pas utiliser un groupe IPv4 cible avec un écouteur UDP comme équilibreur de `dualstack` charge.

Ajouter un écouteur

Vous configurez un écouteur avec un protocole et un port pour les connexions des clients vers l'équilibreur de charge, et un groupe cible pour la règle d'écouteur par défaut. Pour de plus amples informations, veuillez consulter Configuration des écouteurs.

Console

Pour ajouter un écouteur

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Sélectionnez le nom de l'équilibreur de charge afin d'ouvrir sa page de détails.
4. Sous l'onglet Écouteurs, choisissez Ajouter un écouteur.
5. Pour Protocole, choisissez TCP, UDP, TCP_UDP ou TLS. Conservez le port par défaut ou entrez un autre port.
6. Pour Action par défaut, choisissez un groupe cible disponible. Si aucun groupe cible ne répond à vos besoins, choisissez Créer un groupe cible pour en créer un maintenant. Pour de plus amples informations, veuillez consulter Créer un groupe cible.

7. [Écouteurs TLS] Pour Stratégie de sécurité, nous vous recommandons de conserver la stratégie de sécurité par défaut.
8. [Écouteurs TLS] Pour le certificat de SSL/TLS serveur par défaut, choisissez le certificat par défaut. Vous pouvez sélectionner le certificat à partir de l'une des sources suivantes :

   - Si vous avez créé ou importé un certificat à l'aide de AWS Certificate Manager, choisissez From ACM, puis choisissez le certificat from Certificate (from ACM).
   - Si vous avez importé un certificat via IAM, choisissez From IAM, puis sélectionnez le certificat depuis Certificate (from IAM).
   - Si vous avez un certificat, choisissez Importer un certificat. Choisissez Importer vers ACM ou Importer vers IAM. Pour la clé privée du certificat, copiez et collez le contenu du fichier de clé privée (codé PEM). Pour le corps du certificat, copiez et collez le contenu du fichier de certificat de clé publique (codé PEM). Pour la chaîne de certificats, copiez et collez le contenu du fichier de chaîne de certificats (codé PEM), sauf si vous utilisez un certificat auto-signé et qu'il n'est pas important que les navigateurs acceptent implicitement le certificat.
9. [Écouteurs TLS] Pour la stratégie ALPN, choisissez une stratégie pour activer ALPN ou choisissez Aucun pour désactiver ALPN. Pour de plus amples informations, veuillez consulter Stratégies ALPN.
10. Choisissez Ajouter.
11. [Écouteurs TLS] Pour ajouter des certificats à la liste des certificats facultatifs, consultez. Ajouter des certificats à la liste des certificats

AWS CLI

Pour créer un groupe cible

Si vous ne disposez pas d'un groupe cible que vous pouvez utiliser pour l'action par défaut, utilisez la create-target-groupcommande pour en créer un maintenant. Pour obtenir des exemples, consultez Créer un groupe cible.

Pour ajouter un écouteur TCP

Utilisez la commande create-listener en spécifiant le protocole TCP.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol TCP \
```

```
    --port 80 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

Pour ajouter un écouteur TLS

Utilisez la commande create-listener pour spécifier le protocole TLS.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol TLS \
    --port 443 \
    --certificates CertificateArn=certificate-arn \
    --ssl-policy ELBSecurityPolicy-TLS13-1-2-Res-2021-06 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

Pour ajouter un écouteur UDP

Utilisez la commande create-listener pour spécifier le protocole UDP.

```
aws elbv2 create-listener \
    --load-balancer-arn load-balancer-arn \
    --protocol UDP \
    --port 53 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

CloudFormation

Pour ajouter un écouteur TCP

Définissez un type de ressource AWS::ElasticLoadBalancingV2::Listenerà l'aide du protocole TCP.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Pour ajouter un écouteur TLS

Définissez un type de ressource AWS::ElasticLoadBalancingV2::Listenerà l'aide du protocole TLS.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-Res-2021-06"
      Certificates:
        - CertificateArn: "certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Pour ajouter un écouteur UDP

Définissez un type de ressource AWS::ElasticLoadBalancingV2::Listenerà l'aide du protocole UDP.

```
Resources:
  myUDPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: UDP
      Port: 53
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Certificats de serveur pour votre Network Load Balancer

Lorsque vous créez un écouteur sécurisé pour votre Network Load Balancer, vous devez déployer au moins un certificat sur l'équilibreur de charge. L'équilibreur de charge exige des certificats X.509 (certificats de serveur). Les certificats constituent une forme numérique d'identification émise par une

autorité de certification (AC). Un certificat contient les informations d'identification, une période de validité, une clé publique, un numéro de série et la signature numérique de l'émetteur.

Lorsque vous créez un certificat à utiliser avec votre équilibreur de charge, vous devez spécifier un nom de domaine. Le nom de domaine figurant sur le certificat doit correspondre à l'enregistrement du nom de domaine personnalisé, afin que nous puissions vérifier la connexion TLS. S'ils ne correspondent pas, le trafic n'est pas chiffré.

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

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

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

Algorithmes clés supportés

- RSA 1024 bits
- RSA 2048 bits
- RSA 3072 bits
- ECDSA 256 bits

- ECDSA 384 bits
- ECDSA 512 bits

Certificat par défaut

Lorsque vous créez un écouteur TLS, vous devez spécifier au moins un certificat. Ce certificat est connu comme le certificat par défaut. Vous pouvez remplacer le certificat par défaut après avoir créé l'écouteur TLS. Pour de plus amples informations, veuillez consulter Remplacer le certificat par défaut.

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

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

Liste de certificats

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

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

- Algorithme de clé publique (préférer ECDSA plutôt que RSA)
- Algorithme de hachage (préférez SHA à) MD5
- Longueur de clé (préférer la plus longue)

- Période de validité

Les entrées de journaux d'accès de l'équilibreur de charge indiquent le nom d'hôte spécifié par le client et le certificat présenté à ce dernier. Pour de plus amples informations, veuillez consulter Entrées des journaux d'accès.

Renouvellement des certificats

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

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

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

Politiques de sécurité pour votre Network Load Balancer

Lorsque vous créez un écouteur TLS, vous devez sélectionner une stratégie de sécurité. Une politique de sécurité détermine quels chiffrements et protocoles sont pris en charge lors des négociations SSL entre votre équilibreur de charge et les clients. Vous pouvez mettre à jour la politique de sécurité de votre équilibreur de charge si vos exigences changent ou lorsque nous publions une nouvelle politique de sécurité. Pour de plus amples informations, veuillez consulter Mettre à jour la stratégie de sécurité.

Considérations

- Un écouteur TLS nécessite une politique de sécurité. Si vous ne spécifiez pas de politique de sécurité lors de la création de l'écouteur, nous utilisons la politique de sécurité par défaut. La politique de sécurité par défaut dépend de la façon dont vous avez créé l'écouteur TLS :
  - Console — La politique de sécurité par défaut est`ELBSecurityPolicy-TLS13-1-2-Res-2021-06`.
  - Autres méthodes (par exemple, le AWS CLI AWS CloudFormation, et le AWS CDK) — La politique de sécurité par défaut est`ELBSecurityPolicy-2016-08`.
- Vous pouvez choisir la politique de sécurité à utiliser pour les connexions frontales, mais pas pour les connexions dorsales. La politique de sécurité pour les connexions dorsales dépend de la politique de sécurité de l'écouteur :
  - Si l'écouteur TLS utilise une politique de sécurité TLS 1.3, les connexions principales utilisent cette politique. `ELBSecurityPolicy-TLS13-1-0-2021-06`
  - Si l'écouteur TLS n'utilise pas de politique de sécurité TLS 1.3, les connexions principales utilisent cette politique. `ELBSecurityPolicy-2016-08`
- Vous pouvez activer les journaux d'accès pour obtenir des informations sur les requêtes TLS envoyées à votre Network Load Balancer, analyser les modèles de trafic TLS, gérer les mises à niveau des politiques de sécurité et résoudre les problèmes. Activez la journalisation des accès pour votre équilibreur de charge et examinez les entrées du journal d'accès correspondantes. Pour plus d'informations, consultez les journaux d'accès et les exemples de requêtes Network Load Balancer.
- Vous pouvez restreindre les politiques de sécurité accessibles aux utilisateurs de votre pays Comptes AWS et en AWS Organizations utilisant les clés de condition Elastic Load Balancing dans vos politiques IAM et de contrôle des services (SCPs), respectivement. Pour plus d'informations, voir Politiques de contrôle des services (SCPs) dans le guide de AWS Organizations l'utilisateur.
- Les politiques qui ne prennent en charge que le protocole TLS 1.3 prennent en charge le protocole FS (Forward Secrecy). Les politiques qui prennent en charge les protocoles TLS 1.3 et TLS 1.2 qui utilisent uniquement des chiffrements de la forme TLS_* et ECDHE_* fournissent également FS.
- Les équilibreurs de charge réseau prennent en charge l'extension Extended Master Secret (EMS) pour TLS 1.2.

Vous pouvez décrire les protocoles et les chiffrements à l'aide de la describe-ssl-policies AWS CLI commande ou consulter les tableaux ci-dessous.

Stratégies de sécurité

Stratégies de sécurité TLS

Vous pouvez utiliser les politiques de sécurité TLS pour respecter les normes de conformité et de sécurité qui nécessitent la désactivation de certaines versions du protocole TLS, ou pour prendre en charge les anciens clients qui nécessitent des chiffrements obsolètes.

Les politiques qui ne prennent en charge que le protocole TLS 1.3 prennent en charge le protocole FS (Forward Secrecy). Les politiques qui prennent en charge les protocoles TLS 1.3 et TLS 1.2 qui utilisent uniquement des chiffrements de la forme TLS_* et ECDHE_* fournissent également FS.

Table des matières

Protocoles par politique

Le tableau suivant décrit les protocoles pris en charge par chaque politique de sécurité TLS.

Stratégies de sécurité	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolitique- TLS13 -1-3-2021-06	Oui	Non	Non	Non
ELBSecurityPolitique- TLS13 -1-2-2021-06	Oui	Oui	Non	Non
ELBSecurityPolitique- TLS13 -1-2-Res-2021-06	Oui	Oui	Non	Non
ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06	Oui	Oui	Non	Non
ELBSecurityPolitique- TLS13 1-2-Ext1-2021-06	Oui	Oui	Non	Non
ELBSecurityPolitique- TLS13 -1-1-2021-06	Oui	Oui	Oui	Non
ELBSecurityPolitique- TLS13 -1-0-2021-06	Oui	Oui	Oui	Oui
ELBSecurityPolitique-TLS-1-2-Ext-2018-06	Non	Oui	Non	Non
ELBSecurityPolitique-TLS-1-2-2017-01	Non	Oui	Non	Non
ELBSecurityPolitique-TLS-1-1-2017-01	Non	Oui	Oui	Non
ELBSecurityPolitique-2016-08	Non	Oui	Oui	Oui
ELBSecurityPolitique-2015-05	Non	Oui	Oui	Oui

Chiffrements par politique

Le tableau suivant décrit les chiffrements pris en charge par chaque politique de sécurité TLS.

Politique de sécurité	Chiffrements
ELBSecurityPolitique- TLS13 -1-3-2021-06	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_ 05_ CHACHA2 POLY13 SHA256
ELBSecurityPolitique- TLS13 -1-2-2021-06	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384
ELBSecurityPolitique- TLS13 -1-2-Res-2021-06	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384
ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256

Politique de sécurité	Chiffrements
	• ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- -SHA AES256 • ECDHE-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Politique de sécurité	Chiffrements
ELBSecurityPolitique- TLS13 1-2-Ext1-2021-06	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • AES128-GCM- SHA256 • AES128-SHA256 • AES256-GCM- SHA384 • AES256-SHA256

Politique de sécurité	Chiffrements
ELBSecurityPolitique- TLS13 -1-1-2021-06	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- -SHA AES256 • ECDHE-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Politique de sécurité	Chiffrements
ELBSecurityPolitique- TLS13 -1-0-2021-06	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- -SHA AES256 • ECDHE-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Politique de sécurité	Chiffrements
ELBSecurityPolitique-TLS-1-2-Ext-2018-06	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- -SHA AES256 • ECDHE-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Politique de sécurité	Chiffrements
ELBSecurityPolitique-TLS-1-2-2017-01	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • AES128-GCM- SHA256 • AES128-SHA256 • AES256-GCM- SHA384 • AES256-SHA256

Politique de sécurité	Chiffrements
ELBSecurityPolitique-TLS-1-1-2017-01	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- -SHA AES256 • ECDHE-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Politique de sécurité	Chiffrements
ELBSecurityPolitique-2016-08	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- -SHA AES256 • ECDHE-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Politique de sécurité	Chiffrements
ELBSecurityPolitique-2015-05	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-ECDSA- -SHA AES256 • ECDHE-RSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Politiques par chiffrement

Le tableau suivant décrit les politiques de sécurité TLS qui prennent en charge chaque chiffrement.

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — TLS_AES_128_GCM_ SHA256 IANA — TLS_AES_128_GCM_ SHA256	• ELBSecurityPolitique- TLS13 -1-3-2021-06 • ELBSecurityPolitique- TLS13 -1-2-2021-06	1301

Nom du code	Stratégies de sécurité	Suite de chiffrement
	• ELBSecurityPolitique- TLS13 -1-2-Res-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext1-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06	
OpenSSL — TLS_AES_256_GCM_ SHA384 IANA — TLS_AES_256_GCM_ SHA384	• ELBSecurityPolitique- TLS13 -1-3-2021-06 • ELBSecurityPolitique- TLS13 -1-2-2021-06 • ELBSecurityPolitique- TLS13 -1-2-Res-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext1-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06	1302

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — TLS_ 0_ 05_ CHACHA2 POLY13 SHA256 IANA — TLS_ 0_ 05_ CHACHA2 POLY13 SHA256	• ELBSecurityPolitique- TLS13 -1-3-2021-06 • ELBSecurityPolitique- TLS13 -1-2-2021-06 • ELBSecurityPolitique- TLS13 -1-2-Res-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext1-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06	1303

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 128 GCM- ECDHE-ECDSA-AES SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityPolitique- TLS13 -1-2-2021-06 • ELBSecurityPolitique- TLS13 -1-2-Res-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext1-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2-Ext-2018-06 • ELBSecurityPolitique-TLS-1-2-2017-01 • ELBSecurityPolitique-TLS-1-1-2017-01 • ELBSecurityPolitique-2016-08	c02b

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 128 GCM- ECDHE-RSA-AES SHA256 IANA — TLS_ECDHE_RSA_WITH _AES_128_GCM_ SHA256	• ELBSecurityPolitique- TLS13 -1-2-2021-06 • ELBSecurityPolitique- TLS13 -1-2-Res-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext1-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2-Ext-2018-06 • ELBSecurityPolitique-TLS-1-2-2017-01 • ELBSecurityPolitique-TLS-1-1-2017-01 • ELBSecurityPolitique-2016-08	c02f

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 128- ECDHE-ECDSA-AES SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityPolitique- TLS13 -1-2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext1-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2-Ext-2018-06 • ELBSecurityPolitique-TLS-1-2-2017-01 • ELBSecurityPolitique-TLS-1-1-2017-01 • ELBSecurityPolitique-2016-08	c023

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 128- ECDHE-RSA-AES SHA256 IANA — TLS_ECDHE_RSA_WITH _AES_128_CBC_ SHA256	• ELBSecurityPolitique- TLS13 -1-2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 1-2- Ext1-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2- Ext-2018-06 • ELBSecurityPolitique-TLS-1- 2-2017-01 • ELBSecurityPolitique-TLS-1- 1-2017-01 • ELBSecurityPolitique-2016-08	c027
OpenSSL — 128 ECDHE-ECDSA-AES SHA IANA — TLS_ECDHE_ECDSA_WI TH_AES_128_CBC_SHA	• ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2- Ext-2018-06 • ELBSecurityPolitique-TLS-1- 1-2017-01 • ELBSecurityPolitique-2016-08	c009

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 128 ECDHE-RSA-AES SHA IANA — TLS_ECDHE_RSA_WITH _AES_128 CBC_SHA	• ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2-Ext-2018-06 • ELBSecurityPolitique-TLS-1-1-2017-01 • ELBSecurityPolitique-2016-08	c013
OpenSSL — 256 GCM- ECDHE-ECD SA-AES SHA384 IANA — TLS_ECDHE_ECDSA_WI TH_AES_256_GCM_ SHA384	• ELBSecurityPolitique- TLS13 -1-2-2021-06 • ELBSecurityPolitique- TLS13 -1-2-Res-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext1-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2-Ext-2018-06 • ELBSecurityPolitique-TLS-1-2-2017-01 • ELBSecurityPolitique-TLS-1-1-2017-01 • ELBSecurityPolitique-2016-08	c02c

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 256 GCM- ECDHE-RSA-AES SHA384 IANA — TLS_ECDHE_RSA_WITH _AES_256_GCM_ SHA384	• ELBSecurityPolitique- TLS13 -1-2-2021-06 • ELBSecurityPolitique- TLS13 -1-2-Res-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext1-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2-Ext-2018-06 • ELBSecurityPolitique-TLS-1-2-2017-01 • ELBSecurityPolitique-TLS-1-1-2017-01 • ELBSecurityPolitique-2016-08	C030

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 256 ECDHE-ECDSA-AES SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityPolitique- TLS13 -1-2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext1-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2-Ext-2018-06 • ELBSecurityPolitique-TLS-1-2-2017-01 • ELBSecurityPolitique-TLS-1-1-2017-01 • ELBSecurityPolitique-2016-08	C024

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 256 ECDHE-RSA-AES SHA384 IANA — TLS_ECDHE_RSA_WITH _AES_256_CBC_ SHA384	• ELBSecurityPolitique- TLS13 -1-2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext1-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2-Ext-2018-06 • ELBSecurityPolitique-TLS-1-2-2017-01 • ELBSecurityPolitique-TLS-1-1-2017-01 • ELBSecurityPolitique-2016-08	c028
OpenSSL — 256 ECDHE-ECDSA-AES SHA IANA — TLS_ECDHE_ECDSA_WI TH_AES_256_CBC_SHA	• ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2-Ext-2018-06 • ELBSecurityPolitique-TLS-1-1-2017-01 • ELBSecurityPolitique-2016-08	c00a

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 256 ECDHE-RSA-AES SHA IANA — TLS_ECDHE_RSA_WITH _AES_256_CBC_SHA	• ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2- Ext-2018-06 • ELBSecurityPolitique-TLS-1- 1-2017-01 • ELBSecurityPolitique-2016-08	c014
OpenSSL — -GCM - AES128 SHA256 IANA — TLS_RSA_WITH_AES_1 28_GCM_ SHA256	• ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 1-2- Ext1-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2- Ext-2018-06 • ELBSecurityPolitique-TLS-1- 2-2017-01 • ELBSecurityPolitique-TLS-1- 1-2017-01 • ELBSecurityPolitique-2016-08	9c

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — - AES128 SHA256 IANA — TLS_RSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext1-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2-Ext-2018-06 • ELBSecurityPolitique-TLS-1-2-2017-01 • ELBSecurityPolitique-TLS-1-1-2017-01 • ELBSecurityPolitique-2016-08	3 c
OpenSSL — AES128 -SHA IANA — TLS_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2-Ext-2018-06 • ELBSecurityPolitique-TLS-1-1-2017-01 • ELBSecurityPolitique-2016-08	2f

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — -GCM - AES256 SHA384 IANA — TLS_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext1-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2-Ext-2018-06 • ELBSecurityPolitique-TLS-1-2-2017-01 • ELBSecurityPolitique-TLS-1-1-2017-01 • ELBSecurityPolitique-2016-08	9d
OpenSSL — - AES256 SHA256 IANA — TLS_RSA_WITH_AES_256_CBC_ SHA256	• ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 1-2-Ext1-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2-Ext-2018-06 • ELBSecurityPolitique-TLS-1-2-2017-01 • ELBSecurityPolitique-TLS-1-1-2017-01 • ELBSecurityPolitique-2016-08	3d

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — AES256 -SHA IANA — TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolitique- TLS13 1-2-Ext 2-2021-06 • ELBSecurityPolitique- TLS13 -1-1-2021-06 • ELBSecurityPolitique- TLS13 -1-0-2021-06 • ELBSecurityPolitique-TLS-1-2-Ext-2018-06 • ELBSecurityPolitique-TLS-1-1-2017-01 • ELBSecurityPolitique-2016-08	35

Politiques de sécurité FIPS

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

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

> **Important**
>
> Les politiques `ELBSecurityPolicy-TLS13-1-1-FIPS-2023-04` `ELBSecurityPolicy-TLS13-1-0-FIPS-2023-04` sont fournies uniquement à des fins de compatibilité avec les anciennes versions. Bien qu'ils utilisent la cryptographie FIPS à l'aide du module FIPS14 0, ils peuvent ne pas être conformes aux dernières directives du NIST pour la configuration TLS.

Table des matières

Protocoles par politique

Le tableau suivant décrit les protocoles pris en charge par chaque politique de sécurité FIPS.

Stratégies de sécurité	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolitique- TLS13 -1-3-FIPS-2023-04	Oui	Non	Non	Non
ELBSecurityPolitique- TLS13 -1-2-FIPS-2023-04	Oui	Oui	Non	Non
ELBSecurityPolitique- TLS13 -1-2-RES-FIPS-2023-04	Oui	Oui	Non	Non
ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04	Oui	Oui	Non	Non
ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04	Oui	Oui	Non	Non
ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04	Oui	Oui	Non	Non
ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04	Oui	Oui	Oui	Non
ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	Oui	Oui	Oui	Oui

Chiffrements par politique

Le tableau suivant décrit les chiffrements pris en charge par chaque politique de sécurité FIPS.

Politique de sécurité	Chiffrements
ELBSecurityPolitique- TLS13 -1-3-FIPS -2023-04	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384
ELBSecurityPolitique- TLS13 -1-2-FIPS -2023-04	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384
ELBSecurityPolitique- TLS13 -1-2-RES-FIPS-2023-04	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384
ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384

Politique de sécurité	Chiffrements
	• ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- -SHA AES256 • ECDHE-ECDSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA
ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • AES128-GCM- SHA256 • AES128-SHA256 • AES256-GCM- SHA384 • AES256-SHA256

Politique de sécurité	Chiffrements
ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- -SHA AES256 • ECDHE-ECDSA- -SHA AES256

Politique de sécurité	Chiffrements
ELBSecurityPolitique- TLS13 -1-1-FIPS -2023-04	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- -SHA AES256 • ECDHE-ECDSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Politique de sécurité	Chiffrements
ELBSecurityPolitique- TLS13 -1-0-FIPS -2023-04	• TLS_AES_128_GCM_ SHA256 • TLS_AES_256_GCM_ SHA384 • ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- -SHA AES256 • ECDHE-ECDSA- -SHA AES256 • AES128-GCM- SHA256 • AES128-SHA256 • AES128-SHA • AES256-GCM- SHA384 • AES256-SHA256 • AES256-SHA

Politiques par chiffrement

Le tableau suivant décrit les politiques de sécurité FIPS qui prennent en charge chaque chiffrement.

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — TLS_AES_128_GCM_ SHA256	• ELBSecurityPolitique- TLS13 -1-3-FIPS-2023-04	1301

Nom du code	Stratégies de sécurité	Suite de chiffrement
IANA — TLS_AES_128_GCM_ SHA256	• ELBSecurityPolitique- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	
OpenSSL — TLS_AES_256_GCM_ SHA384 IANA — TLS_AES_256_GCM_ SHA384	• ELBSecurityPolitique- TLS13 -1-3-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	1302

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 128 GCM- ECDHE-ECDSA-AES SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityPolitique- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	c02b
OpenSSL — 128 GCM- ECDHE-RSA-AES SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityPolitique- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	c02f

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 128- ECDHE-ECDSA-AES SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityPolitique- TLS13 -1-2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	c023
OpenSSL — 128- ECDHE-RSA-AES SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityPolitique- TLS13 -1-2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	c027

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 128 ECDHE-ECDSA-AES SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	c009
OpenSSL — 128 ECDHE-RSA-AES SHA IANA — TLS_ECDHE_RSA_WITH_AES_128 CBC_SHA	• ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	c013

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 256 GCM- ECDHE-ECDSA-AES SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityPolitique- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	c02c
OpenSSL — 256 GCM- ECDHE-RSA-AES SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityPolitique- TLS13 -1-2-RES-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	C030

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 256 ECDHE-ECDSA-AES SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityPolitique- TLS13 -1-2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	C024
OpenSSL — 256 ECDHE-RSA-AES SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityPolitique- TLS13 -1-2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	c028

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 256 ECDHE-ECDSA-AES SHA IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	c00a
OpenSSL — 256 ECDHE-RSA-AES SHA IANA — TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT0-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	c014
OpenSSL — -GCM - AES128 SHA256 IANA — TLS_RSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	9c

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — - AES128 SHA256 IANA — TLS_RSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	3 c
OpenSSL — AES128 -SHA IANA — TLS_RSA_WITH_AES_128_CBC_SHA	• ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	2f
OpenSSL — -GCM - AES256 SHA384 IANA — TLS_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	9d

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — - AES256 SHA256 IANA — TLS_RSA_WITH_AES_256_CBC_ SHA256	• ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-2-EXT1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	3d
OpenSSL — AES256 -SHA IANA — TLS_RSA_WITH_AES_256_CBC_SHA	• ELBSecurityPolitique- TLS13 -1-2-EXT2-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-1-FIPS-2023-04 • ELBSecurityPolitique- TLS13 -1-0-FIPS-2023-04	35

Politiques de sécurité prises en charge par FS

Les politiques de sécurité prises en charge par FS (Forward Secrecy) fournissent des garanties supplémentaires contre l'écoute de données cryptées, grâce à l'utilisation d'une clé de session aléatoire unique. Cela empêche le décodage des données capturées, même si la clé secrète à long terme est compromise.

Les politiques décrites dans cette section prennent en charge FS, et le terme « FS » figure dans leur nom. Toutefois, ces politiques ne sont pas les seules à prendre en charge le FS. Les politiques qui prennent uniquement en charge le protocole TLS 1.3 prennent en charge le FS. Les politiques qui prennent en charge les protocoles TLS 1.3 et TLS 1.2 qui utilisent uniquement des chiffrements de la forme TLS_* et ECDHE_* fournissent également FS.

Table des matières

- Politiques par chiffrement

Protocoles par politique

Le tableau suivant décrit les protocoles pris en charge par chaque politique de sécurité prise en charge par FS.

Stratégies de sécurité	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
ELBSecurityPolitique-FS-1-2-RES-2020-10	Non	Oui	Non	Non
ELBSecurityPolitique-FS-1-2-RES-2019-08	Non	Oui	Non	Non
ELBSecurityPolitique-FS-1-2-2019-08	Non	Oui	Non	Non
ELBSecurityPolitique-FS-1-1-2019-08	Non	Oui	Oui	Non
ELBSecurityPolitique-FS-2018-06	Non	Oui	Oui	Oui

Chiffrements par politique

Le tableau suivant décrit les chiffrements pris en charge par chaque politique de sécurité prise en charge par FS.

Politique de sécurité	Chiffrements
ELBSecurityPolitique-FS-1-2-RES-2020-10	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384
ELBSecurityPolitique-FS-1-2-RES-2019-08	• ECDHE-ECDSA- -GCM- AES128 SHA256

Politique de sécurité	Chiffrements
	• ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384
ELBSecurityPolitique-FS-1-2-2019-08	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- -SHA AES256 • ECDHE-ECDSA- -SHA AES256

Politique de sécurité	Chiffrements
ELBSecurityPolitique-FS-1-1-2019-08	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- -SHA AES256 • ECDHE-ECDSA- -SHA AES256
ELBSecurityPolitique-FS-2018-06	• ECDHE-ECDSA- -GCM- AES128 SHA256 • ECDHE-RSA- -GCM- AES128 SHA256 • ECDHE-ECDSA- - AES128 SHA256 • ECDHE-RSA- - AES128 SHA256 • ECDHE-ECDSA- -SHA AES128 • ECDHE-RSA- -SHA AES128 • ECDHE-ECDSA- -GCM- AES256 SHA384 • ECDHE-RSA- -GCM- AES256 SHA384 • ECDHE-ECDSA- - AES256 SHA384 • ECDHE-RSA- - AES256 SHA384 • ECDHE-RSA- -SHA AES256 • ECDHE-ECDSA- -SHA AES256

Politiques par chiffrement

Le tableau suivant décrit les politiques de sécurité prises en charge par FS qui prennent en charge chaque chiffrement.

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 128 GCM- ECDHE-ECDSA-AES SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityPolitique-FS-1-2-RES-2020-10 • ELBSecurityPolitique-FS-1-2-RES-2019-08 • ELBSecurityPolitique-FS-1-2-2019-08 • ELBSecurityPolitique-FS-1-1-2019-08 • ELBSecurityPolitique-FS-2018-06	c02b
OpenSSL — 128 GCM- ECDHE-RSA-AES SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_GCM_ SHA256	• ELBSecurityPolitique-FS-1-2-RES-2020-10 • ELBSecurityPolitique-FS-1-2-RES-2019-08 • ELBSecurityPolitique-FS-1-2-2019-08 • ELBSecurityPolitique-FS-1-1-2019-08 • ELBSecurityPolitique-FS-2018-06	c02f
OpenSSL — 128- ECDHE-ECDSA-AES SHA256 IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityPolitique-FS-1-2-RES-2019-08 • ELBSecurityPolitique-FS-1-2-2019-08 • ELBSecurityPolitique-FS-1-1-2019-08 • ELBSecurityPolitique-FS-2018-06	c023
OpenSSL — 128- ECDHE-RSA-AES SHA256 IANA — TLS_ECDHE_RSA_WITH_AES_128_CBC_ SHA256	• ELBSecurityPolitique-FS-1-2-RES-2019-08 • ELBSecurityPolitique-FS-1-2-2019-08 • ELBSecurityPolitique-FS-1-1-2019-08 • ELBSecurityPolitique-FS-2018-06	c027
OpenSSL — 128 ECDHE-ECDSA-AES SHA	• ELBSecurityPolitique-FS-1-2-2019-08 • ELBSecurityPolitique-FS-1-1-2019-08 • ELBSecurityPolitique-FS-2018-06	c009

Nom du code	Stratégies de sécurité	Suite de chiffrement
IANA — TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA		
OpenSSL — 128 ECDHE-RSA-AES SHA IANA — TLS_ECDHE_RSA_WITH_AES_128 CBC_SHA	• ELBSecurityPolitique-FS-1-2-2019-08 • ELBSecurityPolitique-FS-1-1-2019-08 • ELBSecurityPolitique-FS-2018-06	c013
OpenSSL — 256 GCM- ECDHE-ECDSA-AES SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityPolitique-FS-1-2-RES-2020-10 • ELBSecurityPolitique-FS-1-2-RES-2019-08 • ELBSecurityPolitique-FS-1-2-2019-08 • ELBSecurityPolitique-FS-1-1-2019-08 • ELBSecurityPolitique-FS-2018-06	c02c
OpenSSL — 256 GCM- ECDHE-RSA-AES SHA384 IANA — TLS_ECDHE_RSA_WITH_AES_256_GCM_ SHA384	• ELBSecurityPolitique-FS-1-2-RES-2020-10 • ELBSecurityPolitique-FS-1-2-RES-2019-08 • ELBSecurityPolitique-FS-1-2-2019-08 • ELBSecurityPolitique-FS-1-1-2019-08 • ELBSecurityPolitique-FS-2018-06	C030
OpenSSL — 256 ECDHE-ECDSA-AES SHA384 IANA — TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384	• ELBSecurityPolitique-FS-1-2-RES-2019-08 • ELBSecurityPolitique-FS-1-2-2019-08 • ELBSecurityPolitique-FS-1-1-2019-08 • ELBSecurityPolitique-FS-2018-06	C024

Nom du code	Stratégies de sécurité	Suite de chiffrement
OpenSSL — 256 ECDHE-RSA-AES SHA384 IANA — TLS_ECDHE_RSA_WITH _AES_256_CBC_ SHA384	• ELBSecurityPolitique-FS-1-2-RES-2019-08 • ELBSecurityPolitique-FS-1-2-2019-08 • ELBSecurityPolitique-FS-1-1-2019-08 • ELBSecurityPolitique-FS-2018-06	c028
OpenSSL — 256 ECDHE-ECDSA-AES SHA IANA — TLS_ECDHE_ECDSA_WI TH_AES_256_CBC_SHA	• ELBSecurityPolitique-FS-1-2-2019-08 • ELBSecurityPolitique-FS-1-1-2019-08 • ELBSecurityPolitique-FS-2018-06	c00a
OpenSSL — 256 ECDHE-RSA-AES SHA IANA — TLS_ECDHE_RSA_WITH _AES_256_CBC_SHA	• ELBSecurityPolitique-FS-1-2-2019-08 • ELBSecurityPolitique-FS-1-1-2019-08 • ELBSecurityPolitique-FS-2018-06	c014

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

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

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

Lorsque le groupe cible pour l'action par défaut d'un écouteur TCP ou TLS est mis à jour, les nouvelles connexions sont routées vers le groupe cible nouvellement configuré. Toutefois, cela n'a aucun effet sur les connexions actives créées avant cette modification. Ces connexions actives restent associées à la cible dans le groupe cible d'origine pendant une heure au maximum si du trafic est envoyé, ou jusqu'à l'expiration du délai d'inactivité si aucun trafic n'est envoyé, selon la première

éventualité. Le paramètre `Connection termination on deregistration` n'est pas appliqué lors de la mise à jour de l'écouteur, comme il l'est lors de l'annulation d'enregistrement des cibles.

Console

Pour mettre à jour un écouteur

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

AWS CLI

Pour mettre à jour l'action par défaut

Utilisez la commande modify-listener suivante pour modifier le groupe cible de l'action par défaut.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --default-actions Type=forward,TargetGroupArn=new-target-group-arn
```

Pour ajouter des tags

Utilisez la commande add tags. L'exemple suivant ajoute deux balises.

```
aws elbv2 add-tags \
    --resource-arns listener-arn \
    --tags "Key=project,Value=lima" "Key=department,Value=digital-media"
```

Pour supprimer des balises

Utilisez la commande remove-tags. L'exemple suivant supprime les balises avec les clés spécifiées.

```
aws elbv2 remove-tags \
    --resource-arns listener-arn \
    --tag-keys project department
```

CloudFormation

Pour mettre à jour l'action par défaut

Mettez à jour la AWS::ElasticLoadBalancingV2::Listenerressource pour inclure le nouveau groupe cible.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref newTargetGroup
```

Pour ajouter des tags

Mettez à jour la AWS::ElasticLoadBalancingV2::Listenerressource pour inclure la propriété Tags.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
```

```
            Value: 'digital-media'
```

Mettez à jour le délai d'inactivité TCP pour votre écouteur Network Load Balancer

Pour chaque demande TCP effectuée via un Network Load Balancer, l'état de cette connexion est suivi. Si aucune donnée n'est envoyée via la connexion par le client ou la cible au cours d'une période plus longue que le délai d'inactivité, la connexion est fermée.

Considérations

- La valeur du délai d'inactivité par défaut pour les flux TCP est de 350 secondes.
- Le délai d'inactivité de la connexion pour les écouteurs TLS est de 350 secondes et ne peut pas être modifié.

Console

Pour mettre à jour le délai d'inactivité TCP

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sous Équilibrage de charge, choisissez Équilibreurs de charge.
3. Cochez la case correspondant au Network Load Balancer.
4. Dans l'onglet Écouteurs, cochez la case correspondant à l'écouteur TCP, puis choisissez Actions, Afficher les détails de l'écouteur.
5. Sur la page de détails de l'écouteur, dans l'onglet Attributs, sélectionnez Modifier. Si l'écouteur utilise un protocole autre que TCP, cet onglet n'est pas présent.
6. Entrez une valeur pour le délai d'inactivité TCP compris entre 60 et 6 000 secondes.
7. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour mettre à jour le délai d'inactivité TCP

Utilisez la modify-listener-attributescommande avec l'`tcp.idle_timeout.seconds`attribut.

```
aws elbv2 modify-listener-attributes \
```

```
    --listener-arn listener-arn \
    --attributes Key=tcp.idle_timeout.seconds,Value=500
```

Voici un exemple de sortie.

```
{
    "Attributes": [
        {
            "Key": "tcp.idle_timeout.seconds",
            "Value": "500"
        }
    ]
}
```

CloudFormation

Pour mettre à jour le délai d'inactivité TCP

Mettez à jour la AWS::ElasticLoadBalancingV2::Listenerressource pour inclure l'attribut `tcp.idle_timeout.seconds` listener.

```
Resources:
  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      ListenerAttributes:
        - Key: "tcp.idle_timeout.seconds"
          Value: "500"
```

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

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

Tâches

- Remplacer le certificat par défaut
- Ajouter des certificats à la liste des certificats
- Supprimer des certificats de la liste des certificats
- Mettre à jour la stratégie de sécurité
- Mettre à jour la stratégie ALPN

Remplacer le certificat par défaut

Vous pouvez remplacer le certificat par défaut de votre écouteur TLS selon vos besoins. Pour de plus amples informations, veuillez consulter Certificat par défaut.

Console

Pour remplacer le certificat par défaut

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Load Balancers (Équilibreurs de charge).
3. Sélectionnez l'équilibreur de charge.
4. Dans l'onglet Écouteurs, choisissez le texte dans la colonne Protocole : port pour ouvrir la page détaillée de l'écouteur.
5. Dans l'onglet Certificats, choisissez Modifier les valeurs par défaut.
6. Dans le tableau Certificats ACM et IAM, sélectionnez un nouveau certificat par défaut.
7. (Facultatif) Par défaut, nous sélectionnons Ajouter le certificat par défaut précédent à la liste des certificats d'écouteur. Nous vous recommandons de conserver cette option sélectionnée, sauf si vous ne possédez actuellement aucun certificat d'écouteur pour le SNI et que vous comptez sur la reprise de session TLS.
8. Choisissez Enregistrer par défaut.

AWS CLI

Pour remplacer le certificat par défaut

Utilisez la commande modify-listener.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --certificates CertificateArn=new-default-certificate-arn
```

CloudFormation

Pour remplacer le certificat par défaut

Mettez à jour la AWS::ElasticLoadBalancingV2::Listenerressource avec le nouveau certificat par défaut.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "new-default-certificate-arn"
```

Ajouter des certificats à la liste des certificats

Vous pouvez ajouter des certificats à la liste destinée à votre écouteur à l'aide de la procédure qui suit. Lorsque vous créez un écouteur TLS pour la première fois, la liste des certificats est vide. Vous pouvez ajouter le certificat par défaut à la liste des certificats pour vous assurer qu'il est utilisé avec le protocole SNI même s'il est remplacé en tant que certificat par défaut. Pour de plus amples informations, veuillez consulter Liste de certificats.

Console

Pour ajouter des certificats à la liste des certificats

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Choisissez le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.

4. Dans l'onglet Écouteurs, choisissez le texte dans la colonne Protocole : port pour ouvrir la page détaillée de l'écouteur.
5. Choisissez l'onglet Certificates (Certificats).
6. Pour ajouter le certificat par défaut à la liste, choisissez Ajouter le certificat par défaut à la liste.
7. Pour ajouter des certificats autres que ceux par défaut à la liste, procédez comme suit :
   a. Choisissez Ajouter un certificat.
   b. Pour ajouter des certificats déjà gérés par ACM ou IAM, sélectionnez les cases à cocher pour les certificats et choisissez Inclure comme étant en attente ci-dessous.
   c. Pour ajouter un certificat qui n'est pas géré par ACM ou IAM, choisissez Importer un certificat, complétez le formulaire, puis choisissez Importer.
   d. Choisissez Ajouter des certificats en attente.

AWS CLI

Pour ajouter des certificats à la liste des certificats

Utilisez la commande add-listener-certificates.

```
aws elbv2 add-listener-certificates \
    --listener-arn listener-arn \
    --certificates \
        CertificateArn=certificate-arn-1 \
        CertificateArn=certificate-arn-2 \
        CertificateArn=certificate-arn-3
```

CloudFormation

Pour ajouter des certificats à la liste des certificats

Définissez un type de ressource AWS::ElasticLoadBalancingV2::ListenerCertificate.

```
Resources:
  myCertificateList:
    Type: 'AWS::ElasticLoadBalancingV2::ListenerCertificate'
    Properties:
      ListenerArn: !Ref myTLSListener
```

```
      Certificates:
        - CertificateArn: "certificate-arn-1"
        - CertificateArn: "certificate-arn-2"
        - CertificateArn: "certificate-arn-3"

  myTLSListener:
    Type: AWS::ElasticLoadBalancingV2::Listener
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLSS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "certificate-arn-1"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Supprimer des certificats de la liste des certificats

Vous pouvez supprimer des certificats de la liste destinée à un écouteur TLS à l'aide de la procédure suivante. Une fois que vous avez supprimé un certificat, l'écouteur ne peut plus créer de connexions à l'aide de ce certificat. Pour vous assurer que les clients ne sont pas concernés, ajoutez un nouveau certificat à la liste et vérifiez que les connexions fonctionnent avant de supprimer un certificat de la liste.

Pour supprimer le certificat par défaut d'un écouteur TLS, consultez Remplacer le certificat par défaut.

Console

Pour supprimer des certificats de la liste des certificats

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Choisissez le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Dans l'onglet Écouteurs, choisissez le texte dans la colonne Protocole : port pour ouvrir la page détaillée de l'écouteur.
5. Dans l'onglet Certificats, cochez les cases des certificats, puis cliquez sur Supprimer.

6. À l'invite de confirmation, saisissez **`confirm`**, puis choisissez Supprimer.

AWS CLI

Pour supprimer des certificats de la liste des certificats

Utilisez la commande remove-listener-certificates.

```
aws elbv2 remove-listener-certificates \
    --listener-arn listener-arn \
    --certificates CertificateArn=certificate-arn
```

Mettre à jour la stratégie de sécurité

Lorsque vous créez un écouteur TLS, vous pouvez sélectionner la stratégie de sécurité qui correspond à vos besoins. Lorsqu'une nouvelle stratégie de sécurité est ajoutée, vous pouvez mettre à jour votre écouteur TLS afin de pouvoir l'utiliser. Les Network Load Balancers ne prennent pas en charge les stratégies de sécurité personnalisées. Pour de plus amples informations, veuillez consulter Politiques de sécurité pour votre Network Load Balancer.

La mise à jour de la politique de sécurité peut entraîner des perturbations si l'équilibreur de charge gère un volume de trafic élevé. Pour réduire les risques de perturbations lorsque votre équilibreur de charge gère un volume de trafic élevé, créez un équilibreur de charge supplémentaire pour aider à gérer le trafic ou demandez une réservation de LCU.

Console

Pour mettre à jour la politique de sécurité

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Choisissez le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Dans l'onglet Écouteurs, choisissez le texte dans la colonne Protocole : port pour ouvrir la page détaillée de l'écouteur.
5. Choisissez Actions, puis Modifier l'écouteur.
6. Dans la section Paramètres de l'écouteur sécurisé, sous Politique de sécurité, choisissez une nouvelle politique de sécurité.

7. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour mettre à jour la politique de sécurité

Utilisez la commande modify-listener.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --ssl-policy ELBSecurityPolicy-TLS13-1-2-Res-2021-06
```

CloudFormation

Pour mettre à jour la politique de sécurité

Mettez à jour la AWS::ElasticLoadBalancingV2::Listenerressource avec la nouvelle politique de sécurité.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-2021-06"
      Certificates:
        - CertificateArn: "default-certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Mettre à jour la stratégie ALPN

Vous pouvez mettre à jour la politique ALPN pour votre écouteur TLS selon vos besoins. Pour de plus amples informations, veuillez consulter Stratégies ALPN.

Console

Pour mettre à jour la politique ALPN

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Choisissez le nom de l'équilibreur de charge afin d'ouvrir sa page détaillée.
4. Dans l'onglet Écouteurs, choisissez le texte dans la colonne Protocole : port pour ouvrir la page détaillée de l'écouteur.
5. Choisissez Actions, puis Modifier l'écouteur.
6. Dans la section Paramètres de l'écouteur sécurisé, pour la politique ALPN, choisissez une politique pour activer ALPN ou choisissez None pour désactiver ALPN.
7. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour mettre à jour la politique ALPN

Utilisez la commande modify-listener.

```
aws elbv2 modify-listener \
    --listener-arn listener-arn \
    --alpn-policy HTTP2Preferred
```

CloudFormation

Pour mettre à jour la politique ALPN

Mettez à jour la AWS::ElasticLoadBalancingV2::Listenerressource pour inclure la politique ALPN.

```
Resources:
  myTLSListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TLS
      Port: 443
      SslPolicy: "ELBSecurityPolicy-TLS13-1-2-Res-2021-06"
      AlpnPolicy:
```

```
        - HTTP2Preferred
      Certificates:
        - CertificateArn: "certificate-arn"
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Suppression d'un écouteur pour votre Network Load Balancer

Avant de supprimer un écouteur, prenez en compte l'impact sur votre application :

- [Écouteurs TCP et TLS] L'équilibreur de charge arrête immédiatement d'accepter de nouvelles connexions sur l'écouteur. Toute poignée de main TLS en cours peut échouer. Les connexions existantes restent ouvertes jusqu'à ce qu'elles se ferment ou expirent naturellement. Les demandes en vol concernant les connexions existantes sont traitées avec succès.
- [Écouteurs UDP] Les paquets en transit risquent de ne pas atteindre leur destination.

Console

Pour supprimer un écouteur

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

AWS CLI

Pour supprimer un écouteur

Utilisez la commande delete-listener.

```
aws elbv2 delete-listener \
    --listener-arn listener-arn
```

Groupes cibles de vos Network Load Balancers

Chaque groupe cible est utilisé pour acheminer les demandes vers une ou plusieurs cibles enregistrées. Lorsque vous créez un écouteur, vous spécifiez un groupe cible pour son action par défaut. Le trafic est transféré vers le groupe cible spécifié dans la règle de l'écouteur. Vous pouvez créer différents groupes cibles pour les différents types de demandes. Par exemple, créez un groupe cible pour les demandes générales et d'autres groupes cibles pour les demandes adressées aux microservices pour votre application. Pour de plus amples informations, veuillez consulter Composants du Network Load Balancer.

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

Table des matières

- Supprimer un groupe cible pour votre Network Load Balancer

Configuration du routage

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

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

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

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

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

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

Type de cible

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

Les éléments suivants constituent les types de cibles possibles :

`instance`

Les cibles sont spécifiées par ID d'instance.

`ip`

Les cibles sont spécifiées par adresse IP.

`alb`

La cible est un Application Load Balancer.

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

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

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

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

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

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

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

Lorsque le type de cible est `alb`, vous pouvez enregistrer un Application Load Balancer unique en tant que cible. Pour de plus amples informations, veuillez consulter Utiliser un Application Load Balancer comme cible d'un Network Load Balancer.

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

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

Demande de routage et adresses IP

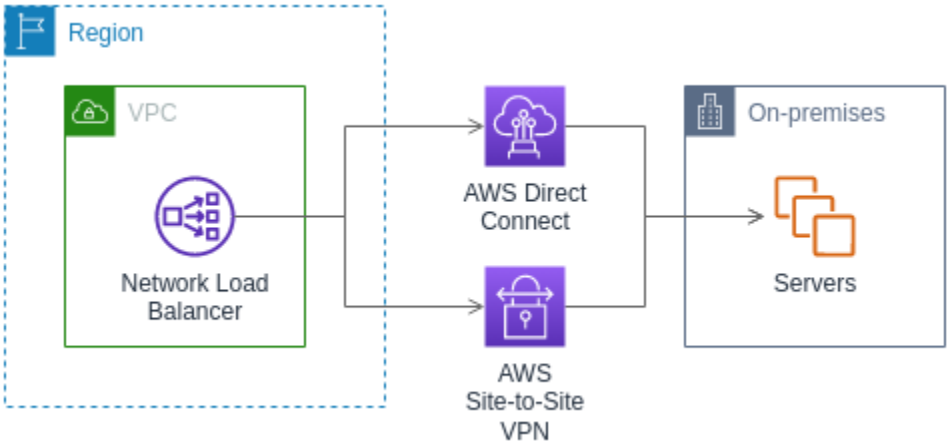
Si vous spécifiez des cibles à l'aide de l'ID d'une instance, le trafic est acheminé vers des instances à l'aide de l'adresse IP privée principale spécifiée dans l'interface réseau principale de l'instance. L'équilibreur de charge réécrit l'adresse IP de destination à partir du paquet de données avant de la transmettre à l'instance cible.

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

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

Ressources sur site en tant que cibles

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



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

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

Pour plus d'informations Direct Connect, voir Qu'est-ce que c'est Direct Connect ?

Pour plus d'informations AWS Site-to-Site VPN, voir Qu'est-ce que c'est AWS Site-to-Site VPN ?

Type d’adresse IP

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

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

`ipv4`

L'équilibreur de charge communique avec les cibles à l'aide IPv4 de.

`ipv6`

L'équilibreur de charge communique avec les cibles à l'aide IPv6 de.

Considérations

- L'équilibreur de charge communique avec les cibles en fonction du type d'adresse IP du groupe cible. Les cibles d'un groupe IPv4 cible doivent accepter le IPv4 trafic provenant de l'équilibreur de charge et les cibles d'un groupe IPv6 cible doivent accepter le IPv6 trafic provenant de l'équilibreur de charge.
- Vous ne pouvez pas utiliser un groupe IPv6 cible avec un équilibreur de `ipv4` charge.
- Vous ne pouvez pas utiliser un groupe IPv4 cible avec un écouteur UDP comme équilibreur de `dualstack` charge.
- Vous ne pouvez pas enregistrer un Application Load Balancer auprès d'un groupe IPv6 cible.

Cibles enregistrées

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

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

Si la demande diminue sur votre application ou que vous avez besoin de répondre aux demandes de vos cibles, vous pouvez annuler l'enregistrement des cibles dans vos groupes cibles. L'annulation de l'enregistrement d'une cible supprime la cible de votre groupe cible, mais n'affecte pas autrement la cible. L'équilibreur de charge arrête d'acheminer le trafic vers une cible dès que l'enregistrement de celle-ci a été annulé. La cible passe à l'état `draining` jusqu'à ce que les demandes en cours soient

terminées. Vous pouvez enregistrer à nouveau la cible auprès du groupe cible lorsque vous êtes prêt à reprendre la réception du trafic.

Si vous enregistrez des objectifs par ID d'instance, vous pouvez utiliser votre équilibreur de charge avec un groupe Auto Scaling. Une fois que vous avez attaché un groupe cible à un groupe Auto Scaling, Auto Scaling enregistre vos cibles auprès du groupe cible pour vous lorsqu'il les lance. Pour plus d'informations, consultez la section Attacher un équilibreur de charge à votre groupe Auto Scaling dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

Exigences et considérations

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

Attributs de groupe cible

Vous pouvez configurer un groupe cible en modifiant ses attributs. Pour de plus amples informations, veuillez consulter Modifier les attributs du groupe cible.

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

`deregistration_delay.timeout_seconds`

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

`deregistration_delay.connection_termination.enabled`

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

`load_balancing.cross_zone.enabled`

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

`preserve_client_ip.enabled`

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

`proxy_protocol_v2.enabled`

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

`stickiness.enabled`

Indique si les sessions permanentes sont activées. La valeur est `true` ou `false`. L'argument par défaut est `false`.

`stickiness.type`

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

`target_group_health.dns_failover.minimum_healthy_targets.count`

Nombre minimal de cibles qui doivent être saines. Si le nombre de cibles saines est inférieur à cette valeur, marquez la zone comme non saine dans le DNS, afin que le trafic soit acheminé

uniquement vers des zones saines. Les valeurs possibles sont `off` ou un entier compris entre 1 et le nombre maximal de cibles. Lorsque `off` la fonction DNS Fail Away est désactivée, ce qui signifie que même si toutes les cibles du groupe cible ne sont pas saines, la zone n'est pas supprimée du DNS. La valeur par défaut est 1.

`target_group_health.dns_failover.minimum_healthy_targets.percentage`

Pourcentage minimal de cibles qui doivent être saines. Si le pourcentage de cibles saines est inférieur à cette valeur, marquez la zone comme non saine dans le DNS, afin que le trafic soit acheminé uniquement vers des zones saines. Les valeurs possibles sont `off` ou un entier compris entre 1 et 100. Lorsque `off` la fonction DNS Fail Away est désactivée, ce qui signifie que même si toutes les cibles du groupe cible ne sont pas saines, la zone n'est pas supprimée du DNS. L'argument par défaut est `off`.

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.count`

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

`target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage`

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

`target_health_state.unhealthy.connection_termination.enabled`

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

`target_health_state.unhealthy.draining_interval_seconds`

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

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

État du groupe cible

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

Table des matières

Actions d'état défectueux

Vous pouvez configurer des seuils sains pour les actions suivantes :

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

Exigences et considérations

- Si vous spécifiez les deux types de seuils pour une action (nombre et pourcentage), l'équilibreur de charge réalise l'action lorsque l'un des seuils est dépassé.
- Si vous spécifiez des seuils pour les deux actions, le seuil de basculement DNS doit être supérieur ou égal au seuil de basculement du routage, afin que le basculement DNS se produise pendant ou avant le basculement du routage.

- Si vous spécifiez le seuil sous forme de pourcentage, nous calculons la valeur de manière dynamique, en fonction du nombre total de cibles enregistrées auprès des groupes cibles.
- Le nombre total de cibles est déterminé selon que la répartition de charge entre zones est activé ou non. Si la répartition de charge entre zones est désactivé, chaque nœud envoie du trafic uniquement aux cibles de sa propre zone, ce qui signifie que les seuils s'appliquent séparément au nombre de cibles dans chaque zone activée. Si l'équilibrage de charge entre zones est activé, chaque nœud envoie du trafic à toutes les cibles de toutes les zones activées, ce qui signifie que les seuils spécifiés s'appliquent au nombre total de cibles dans toutes les zones activées. Pour de plus amples informations, veuillez consulter Équilibrage de charge entre zones.
- Lorsque le basculement du DNS se produit, il a un impact sur tous les groupes cibles associés à l'équilibreur de charge. Assurez-vous de disposer d'une capacité suffisante dans les zones restantes pour gérer ce trafic supplémentaire, en particulier si la répartition de charge entre zones est désactivé.
- Avec le basculement du DNS, nous supprimons les adresses IP des zones défectueuses du nom d'hôte DNS de l'équilibreur de charge. Cependant, le cache DNS du client local peut contenir ces adresses IP jusqu'à ce que le time-to-live (TTL) de l'enregistrement DNS expire (60 secondes).
- Avec le basculement DNS, si plusieurs groupes cibles sont attachés à un Network Load Balancer et qu'un groupe cible est défectueux dans une zone, le basculement du DNS se produit, même si un autre groupe cible est sain dans cette zone.
- Avec le basculement DNS, si toutes les zones d'équilibreur de charge sont considérées comme défectueuses, l'équilibreur de charge envoie le trafic vers toutes les zones, y compris les zones défectueuses.
- Il existe des facteurs autres que le fait de savoir s'il existe suffisamment de cibles saines susceptibles d'entraîner un basculement DNS, tels que l'état de la zone.

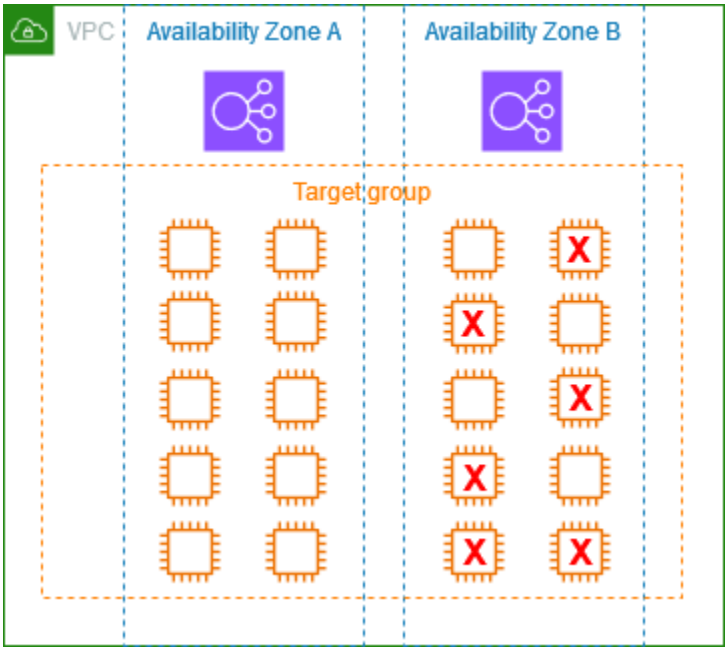
Exemple

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

Scénario

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

  - Basculement du routage : 50 %
- Six cibles échouent dans la zone de disponibilité B



Si la répartition de charge entre zones est désactivée

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

Si la répartition de charge entre zones est activée

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

Utiliser le basculement DNS Route 53 pour votre équilibreur de charge

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

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

Comment fonctionne l'évaluation de la santé cible

- Si l'option d'évaluation de l'état de la cible est définie `Yes` sur un enregistrement d'alias pour un Network Load Balancer, Route 53 évalue l'état de santé de la ressource spécifiée par la valeur. `alias target` Route 53 utilise les contrôles de santé du groupe cible.
- Si tous les groupes cibles attachés à un Network Load Balancer sont sains, Route 53 marque l'enregistrement d'alias comme sain. Si vous avez configuré un seuil pour un groupe cible et qu'il atteint son seuil, il passe avec succès les tests de santé. Sinon, si un groupe cible contient au moins une cible saine, il passe les tests de santé. Si les bilans de santé sont réussis, Route 53

renvoie les enregistrements conformément à votre politique de routage. Si une politique de routage en cas de basculement est utilisée, Route 53 renvoie l'enregistrement principal.

- Si tous les groupes cibles attachés à un Network Load Balancer ne fonctionnent pas correctement, l'enregistrement de l'alias échoue au contrôle de santé de Route 53 (ouverture en cas d'échec). Si vous utilisez Evaluate Target Health, la politique de routage en cas de basculement redirige le trafic vers la ressource secondaire.
- Si tous les groupes cibles d'un Network Load Balancer sont vides (aucune cible), Route 53 considère que l'enregistrement n'est pas sain (fail-open). Si vous utilisez Evaluate Target Health, la politique de routage en cas de basculement redirige le trafic vers la ressource secondaire.

Pour plus d'informations, consultez les sections Utilisation des seuils de santé du groupe cible de l'équilibreur de charge pour améliorer la disponibilité dans le AWS blog et Configuration du basculement du DNS dans le guide du développeur Amazon Route 53.

Création d'un groupe cible pour votre Network Load Balancer

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

Pour acheminer le trafic vers les cibles d'un groupe cible, créez un écouteur et spécifiez le groupe cible dans une action par défaut pour l'écouteur. Pour de plus amples informations, veuillez consulter Règles d'un écouteur. Vous pouvez spécifier le même groupe cible dans plusieurs écouteurs, mais ces écouteurs doivent appartenir au même Network Load Balancer. Pour utiliser un groupe cible avec un équilibreur de charge, vous devez vérifier que le groupe cible n'est pas utilisé par un écouteur pour un autre équilibreur de charge.

Vous pouvez ajouter ou supprimer des cibles dans votre groupe cible à tout moment. Pour de plus amples informations, veuillez consulter Enregistrez des cibles pour votre Network Load Balancer. Vous pouvez aussi modifier les paramètres de vérification de l'état de votre groupe cible. Pour de plus amples informations, veuillez consulter Mettre à jour les paramètres de contrôle de santé d'un groupe cible de Network Load Balancer.

Prérequis

- Une fois que vous avez créé un groupe cible, vous ne pouvez pas modifier son type de cible ni son type d'adresse IP.

- Toutes les cibles d'un groupe cible doivent avoir le même type d'adresse IP que le groupe cible : IPv4 ou IPv6.
- Vous devez utiliser un groupe IPv6 cible doté d'un équilibreur de charge à double pile.
- Vous ne pouvez pas utiliser un groupe IPv4 cible avec un écouteur UDP comme équilibreur de `dualstack` charge.

Console

Pour créer un groupe cible

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, sélectionnez Groupes cibles.
3. Sélectionnez Créer un groupe cible.
4. Sous le panneau Configuration de base, procédez comme suit :

   a. Pour Choisir un type de cible, sélectionnez Instances pour enregistrer les cibles par ID d'instance, Adresses IP pour enregistrer les cibles par adresse IP ou Application Load Balancer pour enregistrer un Application Load Balancer en tant que cible.

   b. Pour Nom du groupe cible, saisissez un nom pour le groupe cible. Ce nom doit être unique par région et par compte, peut comporter un maximum de 32 caractères, doit contenir uniquement des caractères alphanumériques ou des traits d'union et ne doit pas commencer ou se terminer par un trait d'union.

   c. Pour Protocole, choisissez un protocole comme suit :

      - Si l'écouteur est un protocole TCP, choisissez TCP ou TCP_UDP.
      - Si l'écouteur est un protocole TLS, choisissez TCP ou TLS.
      - Si l'écouteur est un protocole UDP, choisissez UDP ou TCP_UDP.
      - Si l'écouteur protocole est TCP_UDP, choisissez TCP_UDP.
      - Si le type de cible est Application Load Balancer, le protocole doit être TCP.

   d. Pour Port, modifiez la valeur par défaut selon vos besoins.

      Si le type de cible est Application Load Balancer, le port doit correspondre au port d'écoute de l'Application Load Balancer.

   e. Pour le type d'adresse IP, sélectionnez IPv4ou IPv6. Cette option n'est disponible que si le type de cible est Instances ou adresses IP.

f. Pour un VPC, sélectionnez le cloud privé virtuel (VPC) avec les cibles à enregistrer.

5. Pour le panneau Surveillances de l'état, modifiez les paramètres par défaut selon vos besoins. Pour les Paramètres avancés de surveillance de l'état, choisissez le port de surveillance de l'état, le nombre, le délai d'expiration, l'intervalle et spécifiez les codes de réussite. Si les surveillances de l'état dépassent consécutivement le Seuil de défectuosité, l'équilibreur de charge met la cible hors service. Lorsque les surveillances de l'état dépassent consécutivement le Seuil de défectuosité, l'équilibreur de charge remet la cible en service. Pour de plus amples informations, veuillez consulter ???.
6. (Facultatif) Pour ajouter une balise, choisissez Balises, puis Ajouter une balise et saisissez la clé et la valeur de la balise.
7. Choisissez Suivant.
8. (Facultatif) Enregistrez les cibles. Le type de cible du groupe cible détermine les informations que vous fournissez. Si vous n'êtes pas prêt à enregistrer des cibles maintenant, vous pourrez les enregistrer ultérieurement.
   - Instances : sélectionnez les EC2 instances, entrez les ports, puis choisissez Inclure comme étant en attente ci-dessous.
   - Adresses IP — Choisissez le VPC qui contient les adresses IP ou autres adresses IP privées, entrez les adresses IP et les ports, puis choisissez Inclure comme en attente ci-dessous.
   - Application Load Balancer : sélectionnez l'Application Load Balancer. Pour de plus amples informations, veuillez consulter Utiliser les équilibreurs de charge des applications comme cibles.
9. Sélectionnez Créer un groupe cible.

AWS CLI

Pour créer un groupe cible

Utilisez la commande create-target-group. L'exemple suivant crée un groupe cible avec le protocole TCP, des cibles enregistrées par adresse IP, une balise et les paramètres de contrôle de santé par défaut.

```
aws elbv2 create-target-group \
    --name my-target-group \
    --protocol TCP \
    --port 80 \
```

```
    --target-type ip \
    --vpc-id vpc-1234567890abcdef0 \
    --tags Key=department,Value=123
```

Pour enregistrer des cibles

Utilisez la commande register-targets pour enregistrer les cibles auprès du groupe cible. Pour obtenir des exemples, consultez the section called “Enregistrer des cibles”.

CloudFormation

Pour créer un groupe cible

Définissez un type de ressource AWS::ElasticLoadBalancingV2::TargetGroup. L'exemple suivant crée un groupe cible avec le protocole TCP, des cibles enregistrées par adresse IP, une balise, les paramètres de contrôle de santé par défaut et deux cibles enregistrées.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      Tags:
        - Key: 'department'
          Value: '123'
      Targets:
        - Id: 10.0.50.10
          Port: 80
        - Id: 10.0.50.20
          Port: 80
```

Mettez à jour les paramètres de santé du groupe cible pour votre Network Load Balancer

Par défaut, les équilibreurs de charge réseau surveillent l'état des cibles et acheminent les demandes vers des cibles saines. Toutefois, si l'équilibreur de charge ne dispose pas d'un nombre suffisant

de cibles saines, il envoie automatiquement le trafic vers toutes les cibles enregistrées (échec d'ouverture). Vous pouvez modifier les paramètres de santé du groupe cible pour votre groupe cible afin de définir les seuils de basculement du DNS et du basculement du routage. Pour de plus amples informations, veuillez consulter the section called “État du groupe cible”.

Console

Pour mettre à jour les paramètres de santé du groupe cible

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sous Répartition de charge, choisissez Groupes cibles.
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Développez Exigences en matière d'état du groupe cible.
6. Pour le type de configuration, nous vous recommandons de choisir la configuration unifiée, qui définit le même seuil pour le basculement du DNS et le basculement du routage.
7. Pour Exigences en matière d'état sain, exécutez l'une des actions suivantes :
   - Choisissez Nombre minimum de cibles saines, puis saisissez un nombre compris entre 1 et le nombre maximal de cibles pour votre groupe cible.
   - Choisissez Pourcentage minimum de cibles saines, puis saisissez un nombre compris entre 1 et 100.
8. Le texte d'information indique si l'équilibrage de charge entre zones est activé pour le groupe cible. Si l'équilibrage de charge entre zones est désactivé, vous pouvez l'activer pour vous assurer que vous disposez d'une capacité suffisante. Sous Configuration de la sélection de cibles, mettez à jour l'équilibrage de charge entre zones.

   Le texte suivant indique que l'équilibrage de charge entre zones est désactivé :

   ```
   Healthy state requirements apply to each zone independently.
   ```

   Le texte suivant indique que l'équilibrage de charge entre zones est activé :

   ```
   Healthy state requirements apply to the total targets across all applicable
    zones.
   ```
9. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour mettre à jour les paramètres de santé du groupe cible

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

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes \

 "Key=target_group_health.dns_failover.minimum_healthy_targets.percentage,Value=50"
 \

 "Key=target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage,Value=5
```

CloudFormation

Pour modifier les paramètres de santé du groupe cible

Mettez à jour la AWS::ElasticLoadBalancingV2::TargetGroupressource. L'exemple suivant définit à 50 % le seuil d'état sain pour les deux actions présentant un état défectueux.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "target_group_health.dns_failover.minimum_healthy_targets.percentage"
          Value: "50"
        - Key:
 "target_group_health.unhealthy_state_routing.minimum_healthy_targets.percentage"
          Value: "50"
```

Contrôles de santé pour les groupes cibles de Network Load Balancer

Vous pouvez enregistrer vos cibles auprès d'un ou de plusieurs groupes cibles. L'équilibreur de charge commence à acheminer les demandes vers une cible nouvellement enregistrée dès que le processus d'enregistrement est terminé et que les cibles passent les tests de santé initiaux. Quelques minutes peuvent être nécessaires pour que le processus d'inscription soit effectué et que les surveillances de l'état commencent.

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

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

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

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

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

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

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

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

Pour de plus amples informations, veuillez consulter the section called “État du groupe cible”.

Table des matières

Paramètres de surveillance de l'état

Vous configurez les vérifications de l'état actives pour les cibles d'un groupe cible en utilisant les paramètres suivants. Si les bilans de santé dépassent le nombre de défaillances

UnhealthyThresholdCountconsécutives, l'équilibreur de charge met la cible hors service. Lorsque les bilans de santé dépassent le nombre de réussites HealthyThresholdCountconsécutives, l'équilibreur de charge remet la cible en service.

Paramètre	Description	Par défaut
HealthCheckProtocol	Protocole utilisé par l'équilibreur de charge lors des vérifications de l'état des cibles. Les protocoles possibles sont HTTP, HTTPS et TCP. La valeur par défaut est le protocole TCP. Si le type de cible est `alb`, les protocole s de surveillance de l'état pris en charge sont HTTP et HTTPS.	TCP
HealthCheckPort	Port utilisé par l'équilibreur de charge lors des vérifications de l'état des cibles. La valeur par défaut consiste à utiliser le port sur lequel chaque cible reçoit le trafic depuis l'équilibreur de charge.	Port sur lequel chaque cible reçoit le trafic depuis l'équilibreur de charge.
HealthCheckPath	[Contrôles de santé HTTP/HTTPS] Le chemin du contrôle de santé qui est la destination des cibles pour les bilans de santé. La valeur par défaut est /.	/
HealthCheckTimeoutSeconds	Durée, en secondes, pendant laquelle l'absence de réponse d'une cible indique l'échec de la vérification de l'état. La plage est comprise entre 2 et 120 secondes. Cette valeur doit être de 6 secondes pour les surveillances de l'état HTTP et de 10 secondes pour les surveillances TCP et HTTPS.	6 secondes pour les surveilla nces de l'état HTTP et 10 secondes pour les surveilla

Paramètre	Description	Par défaut
		nces TCP et HTTPS.
HealthCheckIntervalSeconds	Durée approximative, en secondes, entre les vérifications de l'état d'une cible. La plage est comprise entre 5 et 300 secondes. Le durée par défaut est 30 secondes. Les surveillances de l'état pour un Network Load Balancer sont distribuées et utilisent un mécanisme de consensus pour déterminer l'état des cibles. Par conséquent, des cibles reçoivent plus de vérifications de l'état que le nombre configuré. Pour réduire l'impact sur vos cibles si vous utilisez des vérificat ions d'état HTTP, utilisez une destination plus simple sur les cibles, par exemple, un fichier HTML statique, ou basculez vers des vérificat ions d'état TCP.	30 secondes
HealthyThresholdCount	Le nombre de réussites consécutives de la vérification de l'état à partir duquel une cible défectueuse est considérée comme saine. La plage est comprise entre 2 et 10. La valeur par défaut est 5.	5
UnhealthyThresholdCount	Le nombre d'échecs consécutifs de la vérificat ion de l'état à partir duquel une cible est considérée comme défectueuse. La plage est comprise entre 2 et 10. La valeur par défaut est 2.	2

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

État de santé d'une cible

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

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

Valeur	Description
`initial`	L'équilibreur de charge est en train d'enregistrer la cible ou d'exécuter les vérifications de l'état initiales sur la cible. Codes de motif connexes : `Elb.RegistrationInProgress` | `Elb.InitialHealthChecking`
`healthy`	La cible est saine. Codes de motif connexes : aucun
`unhealthy`	La cible n'a pas répondu à un bilan de santé, a échoué au bilan de santé ou est à l'arrêt. Code motif connexe : `Target.FailedHealthChecks`

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

Codes de motif de vérification de l'état

Si l'état d'une cible correspond à une valeur autre que `Healthy`, l'API renvoie un code de motif et une description du problème, et la console affiche la même description dans une info-bulle. Notez que les codes de motif qui commencent par `Elb` proviennent de l'équilibreur de charge et que ceux qui commencent par `Target` proviennent de la cible.

Code de motif	Description
`Elb.InitialHealthChecking`	Vérifications de l'état initiales en cours
`Elb.InternalError`	Échec des vérifications de l'état initiales en raison d'une erreur interne
`Elb.RegistrationInProgress`	Enregistrement de la cible en cours
`Target.DeregistrationInProgress`	Annulation de l'enregistrement de la cible en cours
`Target.FailedHealthChecks`	Échec des vérifications de l'état
`Target.InvalidState`	La cible est à l'état arrêté. La cible est à l'état résilié. La cible est à l'état résilié ou arrêté. La cible est à un état non valide.
`Target.IpUnusable`	L'adresse IP ne peut pas être utilisée en tant que cible, car elle est utilisée par un équilibreur de charge
`Target.NotInUse`	Le groupe cible n'est pas configuré de façon à recevoir le trafic de l'équilibreur de charge La cible est dans une zone de disponibilité qui n'est pas activée pour l'équilibreur de charge
`Target.NotRegistered`	La cible n'est pas enregistrée auprès du groupe cible

Vérifiez l'état de vos cibles Network Load Balancer

Vous pouvez vérifier l'état de santé des cibles enregistrées auprès de vos groupes cible. Pour obtenir de l'aide en cas d'échec du bilan de santé, voir Résolution des problèmes : une cible enregistrée n'est pas en service.

Console

Pour vérifier l'état de santé de vos cibles

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

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

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

AWS CLI

Pour vérifier l'état de santé de vos cibles

Utilisez la commande describe-target-health. Cet exemple filtre la sortie pour n'inclure que les cibles qui ne sont pas saines. Pour les cibles qui ne sont pas saines, la sortie inclut un code de motif.

```
aws elbv2 describe-target-health \
    --target-group-arn target-group-arn \
    --query "TargetHealthDescriptions[?TargetHealth.State!='healthy'].
[Target.Id,TargetHealth.State,TargetHealth.Reason]" \
    --output table
```

Voici un exemple de sortie.

```
-------------------------------------------------
|            DescribeTargetHealth             |
+--------------+---------+--------------------+
```

```
|  172.31.0.57 |  unused |  Target.NotInUse  |
|  172.31.0.50 |  unused |  Target.NotInUse  |
+--------------+---------+-------------------+
```

États cibles et codes de motif

La liste suivante indique les codes de motif possibles pour chaque État cible.

L'état cible est healthy

Aucun code de motif n'est fourni.

L'état cible est initial

- `Elb.RegistrationInProgress`- La cible est en cours d'enregistrement auprès de l'équilibreur de charge.
- `Elb.InitialHealthChecking`- L'équilibreur de charge envoie toujours à la cible le nombre minimum de bilans de santé requis pour déterminer son état de santé.

L'état cible est unhealthy

- `Target.FailedHealthChecks`- L'équilibreur de charge a reçu une erreur lors de l'établissement d'une connexion avec la cible ou la réponse de la cible a été mal formée.

L'état cible est unused

- `Target.NotRegistered`- La cible n'est pas enregistrée auprès du groupe cible.
- `Target.NotInUse`- Le groupe cible n'est utilisé par aucun équilibreur de charge ou la cible se trouve dans une zone de disponibilité non activée pour son équilibreur de charge.
- `Target.InvalidState`- La cible est à l'état arrêté ou terminé.
- `Target.IpUnusable`- L'adresse IP cible est réservée à l'utilisation d'un équilibreur de charge.

L'état cible est draining

- `Target.DeregistrationInProgress`- La cible est en cours de désinscription et le délai de désinscription n'est pas expiré.

L'état cible est unavailable

- `Elb.InternalError`- L'état de santé cible n'est pas disponible en raison d'une erreur interne.

Mettre à jour les paramètres de contrôle de santé d'un groupe cible de Network Load Balancer

Vous pouvez mettre à jour les paramètres du bilan de santé de votre groupe cible à tout moment. Pour consulter la liste des paramètres du bilan de santé, voirthe section called “Paramètres de surveillance de l'état”.

Console

Pour mettre à jour les paramètres du bilan de santé

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sous Répartition de charge, choisissez Groupes cibles.
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Health checks, choisissez Edit.
5. Sur la page Modifier les paramètres du bilan de santé, modifiez les paramètres selon vos besoins.
6. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour mettre à jour les paramètres du bilan de santé

Utilisez la commande modify-target-group. L'exemple suivant met à jour les HealthCheckTimeoutSecondsparamètres HealthyThresholdCountet.

```
aws elbv2 modify-target-group \
    --target-group-arn target-group-arn \
    --healthy-threshold-count 3 \
    --health-check-timeout-seconds 20
```

CloudFormation

Pour mettre à jour les paramètres du bilan de santé

Mettez à jour la AWS::ElasticLoadBalancingV2::TargetGroupressource pour inclure les paramètres de contrôle de santé mis à jour. L'exemple suivant met à jour les HealthCheckTimeoutSecondsparamètres HealthyThresholdCountet.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: instance
      VpcId: !Ref myVPC
      HealthyThresholdCount: 3
      HealthCheckTimeoutSeconds: 20
```

Modifier les attributs du groupe cible pour votre Network Load Balancer

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

Attributs de groupe cible

- Préservation de l'IP du client
- Délai d'annulation d'enregistrement
- Protocole proxy
- Sessions permanentes
- Équilibrage de charge entre zones pour groupes cibles
- Interruption de connexion pour des cibles défectueuses
- Intervalle de vidange malsain

Préservation de l'IP du client

Les équilibreurs de charge réseau peuvent préserver les adresses IP sources des clients lors du routage des demandes vers des cibles principales. Lorsque vous désactivez la préservation de l'adresse IP du client, l'adresse IP source est l'adresse IP privée du Network Load Balancer.

Par défaut, la préservation des adresses IP client est activée (et ne peut pas être désactivée) pour les groupes cibles de type IP et instance utilisant les protocoles UDP et TCP_UDP. Toutefois, vous

pouvez activer ou désactiver la préservation des adresses IP client pour les groupes cibles TCP et TLS à l'aide de l'attribut de groupe cible `preserve_client_ip.enabled`.

Paramètres par défaut

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

Lorsque la préservation de l'adresse IP du client est activée

Le tableau suivant décrit les adresses IP que les cibles reçoivent lorsque la préservation de l'adresse IP du client est activée.

Cibles	IPv4 demandes des clients	IPv6 demandes des clients
Type d'instance (IPv4)	IPv4 Adresse du client	Adresse de l'équilibreur IPv4 de charge
Type d'adresse IP (IPv4)	IPv4 Adresse du client	Adresse de l'équilibreur IPv4 de charge
Type d'adresse IP (IPv6)	Adresse de l'équilibreur IPv6 de charge	IPv6 Adresse du client

Lorsque la préservation de l'adresse IP du client est désactivée

Le tableau suivant décrit les adresses IP que les cibles reçoivent lorsque la préservation de l'adresse IP du client est désactivée.

Cibles	IPv4 demandes des clients	IPv6 demandes des clients
Type d'instance (IPv4)	Adresse de l'équilibreur IPv4 de charge	Adresse de l'équilibreur IPv4 de charge
Type d'adresse IP (IPv4)	Adresse de l'équilibreur IPv4 de charge	Adresse de l'équilibreur IPv4 de charge

Cibles	IPv4 demandes des clients	IPv6 demandes des clients
Type d'adresse IP (IPv6)	Adresse de l'équilibreur IPv6 de charge	Adresse de l'équilibreur IPv6 de charge

Exigences et considérations

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

- La boucle NAT, également appelée hairpinning, n'est pas prise en charge lorsque la préservation des adresses IP client est activée. Cela se produit lorsque vous utilisez des Network Load Balancer internes et que la cible enregistrée derrière un Network Load Balancer crée des connexions avec le même Network Load Balancer. La connexion peut être routée vers la cible qui tente de créer la connexion, ce qui entraîne des erreurs de connexion. Nous vous recommandons de ne pas vous connecter à un Network Load Balancer à partir de cibles situées derrière le même Network Load Balancer. Vous pouvez également éviter ce type d'erreur de connexion en désactivant la préservation de l'adresse IP du client. Si vous avez besoin de l'adresse IP du client, vous pouvez l'utiliser pour la récupérer à l'aide du protocole Proxy v2. Pour de plus amples informations, veuillez consulter Protocole proxy.
- Lorsque la préservation des adresses IP client est désactivée, un Network Load Balancer prend en charge 55 000 connexions simultanées ou environ 55 000 connexions par minute sur chaque cible unique (adresse IP et port). Si vous dépassez ce nombre de connexions, il y a plus de risque d'erreurs d'attribution de port, ce qui entraîne l'échec d'établissement de nouvelles connexions. Pour de plus amples informations, veuillez consulter Erreurs d'allocation de ports pour les flux de backend.

Console

Pour modifier la conservation de l'adresse IP du client

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sous Load Balancing (Répartition de charge), choisissez Target Groups (Groupes cibles).
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Attributs, choisissez Modifier et recherchez le volet de configuration du trafic.
5. Pour activer la préservation des adresses IP client, activez l'option Préserver les adresses IP client. Pour désactiver la préservation des adresses IP client, désactivez l'option Préserver les adresses IP client.
6. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour activer la préservation de l'adresse IP du client

Utilisez la modify-target-group-attributescommande avec l'`preserve_client_ip.enabled`attribut.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=preserve_client_ip.enabled,Value=true"
```

CloudFormation

Pour activer la préservation de l'adresse IP du client

Mettez à jour la AWS::ElasticLoadBalancingV2::TargetGroup ressource pour inclure l'`preserve_client_ip.enabled`attribut.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "preserve_client_ip.enabled"
          Value: "true"
```

Délai d'annulation d'enregistrement

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

L'état initial d'une cible dont l'enregistrement est annulé est`draining`, pendant lequel la cible cessera de recevoir de nouvelles connexions. Cependant, la cible peut toujours recevoir des

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

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

Console

Pour modifier les attributs du délai de désenregistrement

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sous Load Balancing (Répartition de charge), choisissez Target Groups (Groupes cibles).
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Pour modifier le délai d'annulation de l'enregistrement, saisissez une nouvelle valeur pour Délai d'annulation de l'enregistrement. Pour vous assurer que les connexions existantes sont fermées après l'annulation d'enregistrement des cibles, sélectionnez Arrêter les connexions lors de l'annulation de l'enregistrement.
6. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour modifier les attributs du délai de désenregistrement

Utilisez la modify-target-group-attributescommande avec les `deregistration_delay.connection_termination.enabled` attributs `deregistration_delay.timeout_seconds` et.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes \
      "Key=deregistration_delay.timeout_seconds,Value=60" \
```

```
    "Key=deregistration_delay.connection_termination.enabled,Value=true"
```

CloudFormation

Pour modifier les attributs du délai de désenregistrement

Mettez à jour la AWS::ElasticLoadBalancingV2::TargetGroupressource pour inclure les `deregistration_delay.connection_termination.enabled` attributs `deregistration_delay.timeout_seconds` et.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "deregistration_delay.timeout_seconds"
          Value: "60"
        - Key: "deregistration_delay.connection_termination.enabled"
          Value: "true"
```

Protocole proxy

Les Network Load Balancers utilisent le protocole proxy version 2 pour envoyer des informations de connexion supplémentaires comme la source et la destination. Le protocole proxy version 2 fournit un codage binaire de l'en-tête de protocole proxy.

Avec les écouteurs TCP, l'équilibreur de charge ajoute un en-tête de protocole proxy aux données TCP. Il ne supprime ou ne remplace pas les données existantes, y compris les en-têtes de protocole proxy entrants envoyés par le client ou tous les autres proxys, les équilibreurs de charge ou les serveurs dans le chemin d'accès réseau. Par conséquent, il est possible de recevoir plusieurs en-têtes de protocole proxy. De même, s'il existe un autre chemin réseau vers vos cibles en dehors de votre Network Load Balancer, le premier en-tête du protocole proxy peut ne pas être celui provenant de l'équilibreur de charge.

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

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

- TCP et TLS : par défaut, la préservation de l'adresse IP du client est désactivée, et les adresses IP sources fournies à vos applications sont les adresses IP privées des nœuds de l'équilibreur de charge. Pour préserver l'adresse IP du client, assurez-vous que la cible se trouve dans le même VPC ou dans un VPC homologue et activez la préservation de l'adresse IP du client. Si vous avez besoin de l'adresse IP du client et que ces conditions ne sont pas remplies, activez le protocole proxy et obtenez l'adresse IP du client dans l'en-tête du protocole proxy.
- UDP et TCP_UDP : les adresses IP sources sont les adresses IP des clients, car la préservation de l'adresse IP des clients est activée par défaut pour ces protocoles et ne peut pas être désactivée. Si vous spécifiez des cibles par ID d'instance, les adresses IP source fournies à vos applications sont les adresses IP client. Toutefois, si vous préférez, vous pouvez activer le protocole proxy et obtenir les adresses IP client à partir de l'en-tête de protocole proxy.

Connexions de vérification de l'état

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

Les cibles peuvent échouer aux tests de santé si elles ne peuvent pas analyser l'en-tête du protocole proxy. Par exemple, ils peuvent renvoyer le message d'erreur suivant : HTTP 400 : Mauvaise demande.

Services de points de terminaison d’un VPC

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

L'en-tête de protocole proxy inclut également l'ID du point de terminaison. Ces informations sont codées à l'aide d'un vecteur personnalisé Type-Length-Value (TLV) comme suit.

Champ	Longueur (en octets)	Description
Type	1	PP2_TYPE_AWS (0xEA)
Longueur	2	Longueur de la valeur
Value	1	PP2AWS_VPCE_ID _SOUS-TYPE_ (0x01)
	variable (longueur de la valeur moins 1)	ID du point de terminaison

Pour un exemple qui analyse le type TLV 0xEA, voir/. https://github.com/aws/ elastic-load-balancing-tools tree/master/proprot

Activer le protocole proxy

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

Console

Pour activer la version 2 du protocole proxy

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sous Load Balancing (Répartition de charge), choisissez Target Groups (Groupes cibles).
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sur la page Modifier les attributs, sélectionnez Protocole proxy v2.
6. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour activer la version 2 du protocole proxy

Utilisez la modify-target-group-attributescommande avec l'`proxy_protocol_v2.enabled`attribut.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=proxy_protocol_v2.enabled,Value=true"
```

CloudFormation

Pour activer la version 2 du protocole proxy

Mettez à jour la AWS::ElasticLoadBalancingV2::TargetGroup ressource pour inclure l'`proxy_protocol_v2.enabled`attribut.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "proxy_protocol_v2.enabled"
          Value: "true"
```

Sessions permanentes

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

Considérations

- L'utilisation de sessions permanentes peut entraîner une distribution inégale des connexions et des flux, ce qui peut avoir un impact sur la disponibilité de vos cibles. Par exemple, tous les clients situés derrière le même périphérique NAT ont la même adresse IP source. Par conséquent, l'ensemble du trafic provenant de ces clients est acheminé vers la même cible.
- L'équilibreur de charge peut réinitialiser les sessions permanentes d'un groupe cible si l'état de l'une de ses cibles change ou si vous enregistrez ou annulez l'enregistrement des cibles au groupe cible.

- Lorsque l'attribut stickiness est activé pour un groupe cible, les contrôles de santé passifs ne sont pas pris en charge. Pour plus d'informations, consultez la section Contrôles de santé pour vos groupes cibles.
- Les sessions permanentes ne sont pas prises en charge pour les écouteurs TLS.

Console

Pour activer les sessions persistantes

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sous Load Balancing (Répartition de charge), choisissez Target Groups (Groupes cibles).
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sous Configuration de sélection de la cible, activez Permanence.
6. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour activer les sessions persistantes

Utilisez la modify-target-group-attributescommande avec l'`stickiness.enabled`attribut.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=stickiness.enabled,Value=true"
```

CloudFormation

Pour activer les sessions persistantes

Mettez à jour la AWS::ElasticLoadBalancingV2::TargetGroup ressource pour inclure l'`stickiness.enabled`attribut.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
```

```
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "stickiness.enabled"
          Value: "true"
```

Équilibrage de charge entre zones pour groupes cibles

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

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

Considérations

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

- Lorsque l'équilibrage de charge entre zones est désactivé, assurez-vous que tous les groupes cibles participent aux mêmes zones de disponibilité. Une zone de disponibilité vide est considérée comme défectueuse.
- Vous pouvez activer ou désactiver l'équilibrage de charge entre zones au niveau du groupe cible si le type de groupe cible est `instance` ou`ip`. Si le type de groupe cible est `alb`, le groupe cible hérite toujours du paramètre d'équilibrage de charge entre zones de l'équilibreur de charge.

Pour plus d'informations sur l'activation de l'équilibrage de charge entre zones au niveau de l'équilibreur de charge, consultez. the section called “Equilibrage de charge entre zones”

Console

Pour activer l'équilibrage de charge entre zones pour un groupe cible

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sous Répartition de charge, sélectionnez Groupes cibles.
3. Sélectionnez le nom du groupe cible pour ouvrir sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sur la page Modifier les attributs du groupe cible, sélectionnez Activé pour Équilibrage de charge entre zones.
6. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour activer l'équilibrage de charge entre zones pour un groupe cible

Utilisez la modify-target-group-attributescommande avec l'`load_balancing.cross_zone.enabled`attribut.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes "Key=load_balancing.cross_zone.enabled,Value=true"
```

CloudFormation

Pour activer l'équilibrage de charge entre zones pour un groupe cible

Mettez à jour la AWS::ElasticLoadBalancingV2::TargetGroup ressource pour inclure l'`load_balancing.cross_zone.enabled`attribut.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "load_balancing.cross_zone.enabled"
          Value: "true"
```

Interruption de connexion pour des cibles défectueuses

La terminaison de connexion est activée par défaut. Lorsque la cible d'un Network Load Balancer échoue aux tests de santé configurés et est jugée défectueuse, l'équilibreur de charge met fin aux connexions établies et arrête d'acheminer les nouvelles connexions vers la cible. Lorsque la terminaison de connexion est désactivée, la cible est toujours considérée comme défaillante et ne recevra pas de nouvelles connexions, mais les connexions établies restent actives, ce qui leur permet de se fermer correctement.

La terminaison de connexion pour les cibles défectueuses est configurée au niveau du groupe cible.

Console

Pour modifier l'attribut de terminaison de connexion

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sous Répartition de charge, choisissez Groupes cibles.
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sous Gestion des états non sains de la cible, choisissez d'activer ou de désactiver l'option Interrompre les connexions lorsque les cibles deviennent défectueuses.
6. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour désactiver l'attribut de terminaison de connexion

Utilisez la modify-target-group-attributescommande avec l'`target_health_state.unhealthy.connection_termination.enabled`attribut.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes
 "Key=target_health_state.unhealthy.connection_termination.enabled,Value=false"
```

CloudFormation

Pour désactiver l'attribut de terminaison de connexion

Mettez à jour la AWS::ElasticLoadBalancingV2::TargetGroup ressource pour inclure l'`target_health_state.unhealthy.connection_termination.enabled`attribut.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "target_health_state.unhealthy.connection_termination.enabled"
          Value: "false"
```

Intervalle de vidange malsain

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

Exigence

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

Console

Pour modifier l'intervalle de vidange insalubre

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sous Répartition de charge, choisissez Groupes cibles.
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Sous Gestion de l'état malsain de Target, assurez-vous que l'option Mettre fin aux connexions lorsque les cibles deviennent défectueuses est désactivée.
6. Entrez une valeur pour Intervalle de vidange insalubre.
7. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour modifier l'intervalle de vidange insalubre

Utilisez la modify-target-group-attributescommande avec l'`target_health_state.unhealthy.draining_interval_seconds`attribut.

```
aws elbv2 modify-target-group-attributes \
    --target-group-arn target-group-arn \
    --attributes
 "Key=target_health_state.unhealthy.draining_interval_seconds,Value=60"
```

CloudFormation

Pour modifier l'intervalle de vidange insalubre

Mettez à jour la AWS::ElasticLoadBalancingV2::TargetGroup ressource pour inclure l'`target_health_state.unhealthy.draining_interval_seconds`attribut.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
```

```
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      TargetGroupAttributes:
        - Key: "target_health_state.unhealthy.draining_interval_seconds"
          Value: "60"
```

Enregistrez des cibles pour votre Network Load Balancer

Lorsque votre cible est prête à traiter les demandes, vous l'inscrivez auprès d'un ou plusieurs groupes cibles. Le type de cible du groupe cible détermine la façon dont vous enregistrez les cibles. Par exemple, vous pouvez enregistrer une instance IDs, des adresses IP ou un Application Load Balancer. Votre Network Load Balancer commence à acheminer les demandes vers les cibles dès que le processus d'enregistrement est terminé et que la cible a réussi les surveillances de l'état initiales. Quelques minutes peuvent être nécessaires pour que le processus d'inscription soit effectué et que les surveillances de l'état commencent. Pour de plus amples informations, veuillez consulter Contrôles de santé pour les groupes cibles de Network Load Balancer.

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

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

Si vous enregistrez des objectifs par ID d'instance, vous pouvez utiliser votre équilibreur de charge avec un groupe Auto Scaling. Après avoir attaché un groupe cible à un groupe Auto Scaling et que ce groupe monte en puissance, les instances lancées par le groupe Auto Scaling sont automatiquement

enregistrées avec le groupe cible. Si vous détachez l'équilibreur de charge du groupe Auto Scaling, l'enregistrement des instances est annulé automatiquement dans le groupe cible. Pour plus d'informations, consultez la section Attacher un équilibreur de charge à votre groupe Auto Scaling dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

Table des matières

Groupes de sécurité cibles

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

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

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

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

- Pour autoriser le trafic client : si votre équilibreur de charge préserve les adresses IP client, ajoutez une règle qui accepte le trafic provenant des adresses IP de clients approuvés sur le port de trafic.

Sinon, ajoutez une règle qui accepte le trafic provenant des adresses IP privées de l'équilibreur de charge sur le port de trafic.

- Pour autoriser PrivateLink le trafic : ajoutez une règle qui accepte le trafic provenant des adresses IP privées de l'équilibreur de charge sur le port de trafic.
- Pour accepter les surveillances de l'état de l'équilibreur de charge : ajoutez une règle qui accepte le trafic de surveillance de l'état provenant des adresses IP privées de l'équilibreur de charge sur le port de surveillance.

Comment fonctionne la préservation des adresses IP client

Les Network Load Balancers ne préservent pas les adresses IP client, sauf si vous définissez l'attribut `preserve_client_ip.enabled` sur `true`. De plus, avec les équilibreurs de charge réseau à double pile, la préservation des adresses IP des clients ne fonctionne pas lors de la traduction d' IPv4 adresses vers ou vers IPv6 des adresses. IPv6 IPv4 La conservation de l'adresse IP du client ne fonctionne que lorsque les adresses IP du client et de la cible correspondent aux deux IPv4 ou aux deux IPv6.

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

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

Pour de plus amples informations, veuillez consulter Mettez à jour les groupes de sécurité pour votre Network Load Balancer.

Réseau ACLs

Lorsque vous enregistrez des EC2 instances en tant que cibles, vous devez vous assurer que le réseau ACLs des sous-réseaux de vos instances autorise le trafic à la fois sur le port d'écoute et sur le port de contrôle de santé. La liste de contrôle des accès (ACL) réseau par défaut pour un VPC autorise tout le trafic entrant et sortant. Si vous créez un réseau personnalisé ACLs, vérifiez qu'il autorise le trafic approprié.

Le réseau ACLs associé aux sous-réseaux de vos instances doit autoriser le trafic suivant pour un équilibreur de charge connecté à Internet.

Règles recommandées pour les sous-réseaux d'instance

Inbound

Source	Protocole	Plage de ports	Commentaire
Client IP addresses	*listener*	*target port*	Autoriser le trafic client (préservation de l'adresse IP :0N)
VPC CIDR	*listener*	*target port*	Autoriser le trafic client (préservation de l'adresse IP :0FF)
VPC CIDR	*health check*	*health check*	Autoriser le trafic de vérification de l'état

Outbound

Destination (Destination)	Protocole	Plage de ports	Commentaire
Client IP addresses	*listener*	1024-65535	Autoriser le retour du trafic vers le client (préservation de l'adresse IP :0N)
VPC CIDR	*listener*	1024-65535	Autoriser le retour du trafic vers le client (préservation de l'adresse IP :0FF)
VPC CIDR	*health check*	1024-65535	Autoriser le trafic de vérification de l'état

Le réseau ACLs associé aux sous-réseaux de votre équilibreur de charge doit autoriser le trafic suivant pour un équilibreur de charge connecté à Internet.

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

Inbound			
Source	Protocole	Plage de ports	Commentaire
Client IP addresses	*listener*	*listener*	Autoriser le trafic client
VPC CIDR	*listener*	1024-65535	Autoriser la réponse de la cible
VPC CIDR	*health check*	1024-65535	Autoriser le trafic de vérification de l'état
Outbound			
Destination (Destination)	Protocole	Plage de ports	Commentaire
Client IP addresses	*listener*	1024-65535	Autoriser les réponses aux clients
VPC CIDR	*listener*	*target port*	Autoriser les demandes aux cibles
VPC CIDR	*health check*	*health check*	Autoriser le bilan de santé des cibles

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

Sous-réseaux partagés

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

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

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

Enregistrer des cibles

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

Le type de cible de votre groupe cible détermine les cibles que vous pouvez enregistrer. Pour de plus amples informations, veuillez consulter Type de cible. Utilisez les informations ci-dessous pour enregistrer des cibles auprès d'un groupe cible de type `instance` ou`ip`. Si le type de cible est`alb`, voirUtiliser les équilibreurs de charge des applications comme cibles.

Exigences et considérations

- Une instance doit être à l'état `running` lorsque vous l'inscrivez.
- Vous ne pouvez pas enregistrer des instances par ID d'instance si elles utilisent l'un des types d'instance suivants : C1 CC1, CC2, CG1, CG2, CR1,, G1, G2, HI1, M1 HS1, M2, M3 ou T1.
- Lorsque vous enregistrez des cibles par ID d'instance, les instances doivent se trouver dans le même VPC que le Network Load Balancer. Vous ne pouvez pas enregistrer des instances par ID d'instance si elles se trouvent dans un VPC appairé au VPC de l'équilibreur de charge (même région ou région différente). Vous pouvez enregistrer ces instances par adresse IP.
- Lorsque vous enregistrez des cibles par ID d'instance pour un groupe IPv6 cible, une IPv6 adresse principale doit être attribuée aux cibles. Pour en savoir plus, consultez les IPv6 adresses dans le guide de EC2 l'utilisateur Amazon
- Lorsque vous enregistrez des cibles par adresse IP pour un groupe IPv4 cible, les adresses IP que vous enregistrez doivent provenir de l'un des blocs CIDR suivants :
  - Les sous-réseaux du groupe cible (VPC)
  - 10.0.0.0/8 (RFC 1918)
  - 100.64.0.0/10 (RFC 6598)
  - 172.16.0.0/12 (RFC 1918)
  - 192.168.0.0/16 (RFC 1918)

- Lorsque vous enregistrez des cibles par adresse IP pour un groupe IPv6 cible, les adresses IP que vous enregistrez doivent se trouver dans le bloc d'adresse IPv6 CIDR du VPC ou dans le bloc d'adresse IPv6 CIDR d'un VPC apparenté.
- Si vous enregistrez une cible par adresse IP et que l'adresse IP se trouve dans le même VPC que l'équilibreur de charge, ce dernier vérifie qu'elle provient d'un sous-réseau qu'elle peut atteindre.
- Pour les groupes cibles UDP et TCP_UDP, n'enregistrez pas les instances par adresse IP si elles résident en dehors du VPC de l'équilibreur de charge ou s'ils utilisent l'un des types d'instance suivants : C1,,,,,, G1 CC1 CC2, G2 CG1 CG2, CR1, M1, M2, M3 ou T1 HI1. HS1 Les cibles situées en dehors du VPC de l'équilibreur de charge ou utilisant un type d'instance non pris en charge peuvent être en mesure de recevoir du trafic en provenance de l'équilibreur de charge, mais ne pas être en mesure de répondre.

Console

Pour enregistrer des cibles

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sous Load Balancing (Répartition de charge), choisissez Target Groups (Groupes cibles).
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Choisissez l’onglet Cibles.
5. Choisissez Register targets (Enregistrer les cibles).
6. Si le type de cible du groupe cible est`instance`, sélectionnez les instances disponibles, remplacez le port par défaut si nécessaire, puis choisissez Inclure comme étant en attente ci-dessous.
7. Si le type de cible du groupe cible est`ip`, pour chaque adresse IP, sélectionnez le réseau, entrez l'adresse IP et les ports, puis choisissez Inclure comme en attente ci-dessous.
8. Si le type de cible du groupe cible est`alb`, remplacez le port par défaut si nécessaire et sélectionnez Application Load Balancer. Pour de plus amples informations, veuillez consulter Utiliser les équilibreurs de charge des applications comme cibles.
9. Choisissez Enregistrer les cibles en attente.

AWS CLI

Pour enregistrer des cibles

Utilisez la commande register-targets. L'exemple suivant enregistre les cibles par ID d'instance. Le port n'étant pas spécifié, l'équilibreur de charge utilise le port du groupe cible.

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

L'exemple suivant enregistre les cibles par adresse IP. Le port n'étant pas spécifié, l'équilibreur de charge utilise le port du groupe cible.

```
aws elbv2 register-targets \
    --target-group-arn target-group-arn \
    --targets Id=10.0.50.10 Id=10.0.50.20
```

L'exemple suivant enregistre un Application Load Balancer en tant que cible.

```
aws elbv2 register-targets \
    --target-group-arn target-group-arn \
    --targets Id=application-load-balancer-arn
```

CloudFormation

Pour enregistrer des cibles

Mettez à jour la AWS::ElasticLoadBalancingV2::TargetGroupressource pour inclure les nouvelles cibles. L'exemple suivant enregistre deux cibles par ID d'instance.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: HTTP
      Port: 80
      TargetType: instance
      VpcId: !Ref myVPC
      Targets:
        - Id: !GetAtt Instance1.InstanceId
          Port: 80
        - Id: !GetAtt Instance2.InstanceId
          Port: 80
```

Désenregistrer les cibles

Si la demande diminue sur votre application ou que vous avez besoin de répondre aux demandes de vos cibles, vous pouvez annuler l'enregistrement des cibles dans vos groupes cibles. L'annulation de l'enregistrement d'une cible supprime la cible de votre groupe cible, mais n'affecte pas autrement la cible. L'équilibreur de charge arrête d'acheminer le trafic vers une cible dès que l'enregistrement de celle-ci a été annulé. La cible passe à l'état `draining` jusqu'à ce que les demandes en cours soient terminées.

Console

Pour désenregistrer des cibles

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sous Load Balancing (Répartition de charge), choisissez Target Groups (Groupes cibles).
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Cibles, sélectionnez les cibles à supprimer.
5. Choisissez Deregister (Annuler l'enregistrement).

AWS CLI

Pour désenregistrer des cibles

Utilisez la commande deregister-targets. L'exemple suivant annule l'enregistrement de deux cibles enregistrées par ID d'instance.

```
aws elbv2 deregister-targets \
    --target-group-arn target-group-arn \
    --targets Id=i-1234567890abcdef0 Id=i-0abcdef1234567890
```

Utiliser un Application Load Balancer comme cible d'un Network Load Balancer

Vous pouvez créer un groupe cible avec un seul Application Load Balancer comme cible et configurer votre Network Load Balancer pour y transférer le trafic. Dans ce scénario, l'Application Load Balancer

prend en charge la décision d'équilibrage de charge dès que le trafic l'atteint. Cette configuration combine les fonctionnalités des deux équilibreurs de charge et offre les avantages suivants :

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

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

Considérations

- Vous ne pouvez enregistrer qu'un seul Application Load Balancer par groupe cible.
- Pour associer un Application Load Balancer en tant que cible d'un Network Load Balancer, les équilibreurs de charge doivent se trouver dans le même VPC au sein du même compte.
- Vous pouvez associer un Application Load Balancer en tant que cible de deux Network Load Balancers au maximum. Pour ce faire, enregistrez l'Application Load Balancer auprès d'un groupe cible distinct pour chaque Network Load Balancer.
- Chaque Application Load Balancer que vous enregistrez auprès d'un Network Load Balancer réduit de 50 le nombre maximum de cibles par zone de disponibilité et par Network Load Balancer. Vous pouvez désactiver l'équilibrage de charge entre zones dans les deux équilibreurs de charge afin de minimiser la latence et d'éviter les frais de transfert de données régionaux. Pour de plus amples informations, veuillez consulter Quotas de vos Network Load Balancers.
- Lorsque le type de groupe cible est `alb`, vous ne pouvez pas modifier les attributs du groupe cible. Ces attributs utilisent toujours leurs valeurs par défaut.
- Après avoir enregistré un Application Load Balancer en tant que cible, vous ne pouvez pas le supprimer tant que vous n'avez pas annulé son enregistrement depuis tous les groupes cibles.
- La communication entre un Network Load Balancer et un Application Load Balancer utilise toujours. IPv4

Tâches

Prérequis

Si vous n'avez pas encore d'Application Load Balancer à utiliser comme cible, créez l'équilibreur de charge, ses écouteurs et ses groupes cibles. Pour plus d'informations, consultez la section Créer un équilibreur de charge d'application dans le guide de l'utilisateur pour les équilibreurs de charge d'application.

Étape 1 : créer un groupe cible de type alb

Créez un groupe cible de type `alb`. Vous pouvez enregistrer votre Application Load Balancer en tant que cible lorsque vous créez le groupe cible ou ultérieurement.

Console

Pour créer un groupe cible pour un Application Load Balancer en tant que cible

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sous Load Balancing (Répartition de charge), choisissez Target Groups (Groupes cibles).
3. Sélectionnez Créer un groupe cible.
4. Dans le volet Configuration de base, pour Choisir un type de cible, choisissez Application Load Balancer.
5. Pour Nom du groupe cible, saisissez un nom pour le groupe cible.
6. Pour Protocole, seul le protocole TCP est autorisé. Sélectionnez le Port de votre groupe cible. Le port de ce groupe cible doit correspondre au port d'écoute de l'Application Load Balancer. Si vous choisissez un port différent pour ce groupe cible, vous pouvez mettre à jour le port d'écoute de l'Application Load Balancer pour qu'il corresponde à ce port.
7. Pour le VPC, sélectionnez le cloud privé virtuel (VPC) pour le groupe cible. Il doit s'agir du même VPC que celui utilisé par l'Application Load Balancer.
8. Pour Surveillances de l'état, choisissez HTTP ou HTTPS comme Protocole de surveillance de l'état. Les surveillances de l'état sont envoyées à l'Application Load Balancer et transmises

à ses cibles en utilisant le port, le protocole et le chemin ping spécifiés. Assurez-vous que votre Application Load Balancer peut recevoir ces surveillances de l'état en disposant d'un écouteur doté d'un port et d'un protocole qui correspondent au port et au protocole de la surveillance de l'état.

9. (Facultatif) Développez les balises. Pour chaque balise, choisissez Ajouter une nouvelle balise et entrez une clé de balise et une valeur de balise.
10. Choisissez Suivant.
11. Si vous êtes prêt à enregistrer l'Application Load Balancer, choisissez Register now, remplacez le port par défaut si nécessaire, puis sélectionnez l'Application Load Balancer. L'Application Load Balancer doit disposer d'un écouteur sur le même port que le groupe cible. Vous pouvez ajouter ou modifier un écouteur sur cet équilibreur de charge pour qu'il corresponde au port du groupe cible, ou revenir à l'étape précédente et modifier le port du groupe cible.

    Si vous n'êtes pas prêt à enregistrer l'Application Load Balancer en tant que cible, choisissez Register later et enregistrez la cible ultérieurement. Pour de plus amples informations, veuillez consulter the section called “Enregistrer des cibles”.
12. Sélectionnez Créer un groupe cible.

AWS CLI

Pour créer un groupe cible de type alb

Utilisez la commande create-target-group. Le protocole doit être TCP et le port doit correspondre au port d'écoute de l'Application Load Balancer.

```
aws elbv2 create-target-group \
    --name my-target-group \
    --protocol TCP \
    --port 80 \
    --target-type alb \
    --vpc-id vpc-1234567890abcdef0 \
    --tags Key=department,Value=123
```

CloudFormation

Pour créer un groupe cible de type alb

Définissez un type de ressource AWS::ElasticLoadBalancingV2::TargetGroup. Le protocole doit être TCP et le port doit correspondre au port d'écoute de l'Application Load Balancer.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: alb
      VpcId: !Ref myVPC
      Tags:
        - Key: 'department'
          Value: '123'
      Targets:
        - Id: !Ref myApplicationLoadBalancer
          Port: 80
```

Étape 2 : créer un Network Load Balancer et configurer le routage

Lorsque vous créez le Network Load Balancer, vous pouvez configurer l'action par défaut pour transférer le trafic vers l'Application Load Balancer.

Console

Pour créer le Network Load Balancer

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. Choisissez Créer un équilibreur de charge.
4. Sous Network Load Balancer, choisissez Créer.
5. Configuration de base

    a. Dans le champ Nom de l'équilibreur de charge, entrez le nom de votre Network Load Balancer.

    b. Pour Scheme (Méthode), choisissez Internet-facing (Accessible sur Internet) ou Internal (Interne). Un Network Load Balancer connecté à Internet achemine les demandes des

clients vers des cibles via Internet. Un Network Load Balancer interne achemine les demandes vers des cibles à l'aide d'adresses IP privées.

c. Pour le type d'adresse IP de l'équilibreur de charge, indiquez IPv4si vos clients utilisent des IPv4 adresses pour communiquer avec le Network Load Balancer ou Dualstack s'ils utilisent IPv4 les deux IPv6 adresses pour communiquer avec le Network Load Balancer.

6. Mappage du réseau

a. Pour le VPC, sélectionnez le même VPC que celui que vous avez utilisé pour votre Application Load Balancer. Dans le cas d'un équilibreur de charge connecté à Internet, seule VPCs une passerelle Internet est disponible pour la sélection.

b. Pour les zones de disponibilité et les sous-réseaux, sélectionnez au moins une zone de disponibilité, puis un sous-réseau par zone. Nous vous recommandons de sélectionner les mêmes zones de disponibilité que celles activées pour votre Application Load Balancer. Cela optimise la disponibilité, l'évolutivité et les performances.

(Facultatif) Pour utiliser des adresses IP statiques, choisissez Utiliser une adresse IP élastique dans les IPv4paramètres de chaque zone de disponibilité. Avec les adresses IP statiques, vous pouvez ajouter certaines adresses IP à une liste d'autorisation pour les pare-feux, ou vous pouvez coder en dur des adresses IP avec des clients.

7. Groupes de sécurité

Nous présélectionnons le groupe de sécurité par défaut pour le VPC de l'équilibreur de charge. Vous pouvez sélectionner des groupes de sécurité supplémentaires selon vos besoins. Si aucun groupe de sécurité ne répond à vos besoins, choisissez Créer un nouveau groupe de sécurité pour en créer un maintenant. Pour plus d'informations, veuillez consulter Création d'un groupe de sécurité dans le Guide de l'utilisateur Amazon VPC.

> **Warning**
>
> Si vous n'associez aucun groupe de sécurité à votre Network Load Balancer pour le moment, vous ne pourrez pas les associer ultérieurement.

8. Écouteurs et routage

a. La valeur par défaut est un écouteur qui accepte le trafic TCP sur le port 80. Seuls les écouteurs TCP peuvent transférer le trafic vers un groupe cible d'Application Load

Balancer. Pour Protocole, vous devez conserver la valeur TCP, mais vous pouvez modifier le Port si nécessaire.

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

b. Pour Action par défaut, sélectionnez le groupe cible que vous avez créé à l'étape précédente.

c. (Facultatif) Choisissez Ajouter une balise d'écoute et entrez une clé de balise et une valeur de balise.

9. Tags d'équilibreur de charge

(Facultatif) Développez les balises de l'équilibreur de charge. Choisissez Ajouter une nouvelle balise et entrez une clé de balise et une valeur de balise. Pour plus d'informations, veuillez consulter Balises.

10. Récapitulatif

Passez en revue votre configuration et choisissez Créer un équilibreur de charge.

AWS CLI

Pour créer le Network Load Balancer

Utilisez la commande create-load-balancer. Nous vous recommandons d'utiliser les mêmes zones de disponibilité que celles activées pour votre Application Load Balancer.

```
aws elbv2 create-load-balancer \
    --name my-load-balancer \
    --type network \
    --scheme internal \
    --subnets subnet-1234567890abcdef0 subnet-0abcdef1234567890 \
    --security-groups sg-1111222233334444
```

Pour ajouter un écouteur TCP

Utilisez la commande create-listener pour ajouter un écouteur TCP. Seuls les écouteurs TCP peuvent transférer le trafic vers un Application Load Balancer. Pour l'action par défaut, utilisez le groupe cible que vous avez créé à l'étape précédente.

```
aws elbv2 create-listener \
```

```
    --load-balancer-arn load-balancer-arn \
    --protocol TCP \
    --port 80 \
    --default-actions Type=forward,TargetGroupArn=target-group-arn
```

CloudFormation

Pour créer le Network Load Balancer

Définissez une ressource de type AWS::ElasticLoadBalancingV2::LoadBalanceret une ressource de type AWS::ElasticLoadBalancingV2::Listener. Seuls les écouteurs TCP peuvent transférer le trafic vers un Application Load Balancer. Pour l'action par défaut, utilisez le groupe cible que vous avez créé à l'étape précédente.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-load-balancer
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup

  myTCPListener:
    Type: 'AWS::ElasticLoadBalancingV2::Listener'
    Properties:
      LoadBalancerArn: !Ref myLoadBalancer
      Protocol: TCP
      Port: 80
      DefaultActions:
        - Type: forward
          TargetGroupArn: !Ref myTargetGroup
```

Étape 3 : (Facultatif) Création d'un service de point de terminaison VPC

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

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

1. Dans le volet de navigation, choisissez Load Balancers (Équilibreurs de charge).
2. Sélectionnez le nom du Network Load Balancer afin d'ouvrir sa page de détails.
3. Dans l'onglet Intégrations, développez Services de point de terminaison d'un VPC (AWS PrivateLink).
4. Choisissez Créer un point de terminaison pour ouvrir la page Services de point de terminaison. Pour les étapes restantes, veuillez consulter Créer un service de point de terminaison dans le Guide AWS PrivateLink .

Identifiez un groupe cible pour votre Network Load Balancer

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

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

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

Restrictions

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

préfixe. Les balises avec ce préfixe ne sont pas comptabilisées comme vos balises pour la limite de ressources.

Console

Pour gérer les tags d'un groupe cible

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sous Load Balancing (Répartition de charge), choisissez Target Groups (Groupes cibles).
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Balises, choisissez Gérer les balises, puis effectuez une ou plusieurs des actions suivantes :
   a. Pour mettre à jour une balise, saisissez de nouvelles valeurs pour Clé et Valeur.
   b. Pour ajouter une balise, sélectionnez Ajouter une balise et saisissez des valeurs pour Clé et Valeur.
   c. Pour supprimer une balise, choisissez Retirer en regard de la balise.
5. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour ajouter des tags

Utilisez la commande add tags. L'exemple suivant ajoute deux balises.

```
aws elbv2 add-tags \
    --resource-arns target-group-arn \
    --tags "Key=project,value=lima" "Key=department,Value=digital-media"
```

Pour supprimer des balises

Utilisez la commande remove-tags. L'exemple suivant supprime les balises avec les clés spécifiées.

```
aws elbv2 remove-tags \
    --resource-arns target-group-arn \
```

```
    --tag-keys project department
```

CloudFormation

Pour ajouter des tags

Mettez à jour la AWS::ElasticLoadBalancingV2::TargetGroupressource pour inclure la `Tags` propriété.

```
Resources:
  myTargetGroup:
    Type: 'AWS::ElasticLoadBalancingV2::TargetGroup'
    Properties:
      Name: my-target-group
      Protocol: TCP
      Port: 80
      TargetType: ip
      VpcId: !Ref myVPC
      Tags:
        - Key: 'project'
          Value: 'lima'
        - Key: 'department'
          Value: 'digital-media'
```

Supprimer un groupe cible pour votre Network Load Balancer

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

Console

Pour supprimer un groupe cible

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le panneau de navigation, sous Répartition de charge, choisissez Groupes cibles.
3. Sélectionnez le groupe cible et choisissez Actions, Supprimer.
4. Sélectionnez Delete (Supprimer).

AWS CLI

Pour supprimer un groupe cible

Utilisez la commande delete-target-group.

```
aws elbv2 delete-target-group \
    --target-group-arn target-group-arn
```

Surveillance de vos Network Load Balancers

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

CloudWatch métriques

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

Journaux de flux VPC

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

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

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

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

Amazon CloudWatch Internet Monitor

Vous pouvez utiliser Internet Monitor pour avoir une idée de l'impact des problèmes Internet sur les performances et la disponibilité entre vos applications hébergées sur AWS et vos utilisateurs finaux. Vous pouvez également découvrir, en temps quasi réel, comment améliorer la latence prévue de votre application en optant pour d'autres services ou en réacheminant le trafic vers votre charge de travail via différents Régions AWS moyens. Pour plus d'informations, consultez la section Utilisation d'Amazon CloudWatch Internet Monitor.

Journaux d'accès

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

CloudTrail journaux

Vous pouvez l'utiliser AWS CloudTrail pour capturer des informations détaillées sur les appels passés à l'API Elastic Load Balancing et les stocker sous forme de fichiers journaux dans Amazon S3. Vous pouvez utiliser ces CloudTrail journaux pour déterminer quels appels ont été passés, l'adresse IP source d'où provient l'appel, qui a effectué l'appel, quand l'appel a été passé, etc. Pour plus d'informations, consultez Log API calls for Elastic Load Balancing using CloudTrail.

CloudWatch métriques pour votre Network Load Balancer

Elastic Load Balancing publie des points de données sur Amazon CloudWatch pour vos équilibreurs de charge et vos cibles. CloudWatchvous permet de récupérer des statistiques sur ces points de données sous la forme d'un ensemble ordonné de séries chronologiques, appelées métriques. Considérez une métrique comme une variable à surveiller, et les points de données comme les valeurs de cette variable au fil du temps. Par exemple, vous pouvez surveiller le nombre total de cibles saines pour un équilibreur de charge sur une période spécifiée. Un horodatage et une unité de mesure facultative sont associés à chaque point de données.

Vous pouvez utiliser les métriques pour vérifier que le système fonctionne comme prévu. Par exemple, vous pouvez créer une CloudWatch alarme pour surveiller une métrique spécifiée et lancer une action (telle que l'envoi d'une notification à une adresse e-mail) si la métrique dépasse ce que vous considérez comme une plage acceptable.

Elastic Load Balancing communique les métriques CloudWatch uniquement lorsque les demandes transitent par l'équilibreur de charge. Si des demandes passent par l'équilibreur de charge, Elastic Load Balancing mesure et envoie ses métriques au cours d'intervalles de 60 secondes. Si aucune demande ne passe par l'équilibreur de charge ou s'il n'existe pas de données pour une métrique, cette dernière n'est pas présentée. Pour les équilibreurs de charge réseau dotés de groupes de sécurité, le trafic rejeté par les groupes de sécurité n'est pas pris en compte dans les CloudWatch métriques.

Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Table des matières

Métriques des Network Load Balancers

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

Métrique	Description
`ActiveFlowCount`	Nombre total de flux (ou connexions) simultanés provenant des clients vers des cibles. Cette métrique comprend les connexions dont l'état est SYN_SENT et ESTABLISHED. Les connexions TCP ne sont pas mises hors service au niveau de l'équilibreur de charge ; un client qui ouvre une connexion TCP avec une cible est donc comptabilisé comme un seul flux. Critères de notification : toujours signalé. Statistics : les statistiques les plus utiles sont `Average`, `Maximum` et `Minimum`. Dimensions • `LoadBalancer`

Métrique	Description
	• `AvailabilityZone` , `LoadBalancer`
`ActiveFlowCount_TCP`	Nombre total de flux (ou connexions) TCP simultanés provenant des clients vers des cibles. Cette métrique comprend les connexions dont l'état est SYN_SENT et ESTABLISHED. Les connexions TCP ne sont pas mises hors service au niveau de l'équilibreur de charge ; un client qui ouvre une connexion TCP avec une cible est donc comptabilisé comme un seul flux. Critères de notification : il existe une valeur différente de zéro Statistics : les statistiques les plus utiles sont `Average`, `Maximum` et `Minimum`. Dimensions • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ActiveFlowCount_TLS`	Nombre total de flux (ou connexions) TLS simultanés provenant des clients vers des cibles. Cette métrique comprend les connexions dont l'état est SYN_SENT et ESTABLISHED. Critères de notification : il existe une valeur différente de zéro. Statistics : les statistiques les plus utiles sont `Average`, `Maximum` et `Minimum`. Dimensions • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrique	Description
`ActiveFlowCount_UDP`	Nombre total de flux (ou connexions) UDP simultanés provenant des clients vers des cibles. Critères de notification : il existe une valeur différente de zéro. Statistics : les statistiques les plus utiles sont `Average`, `Maximum` et `Minimum`. Dimensions • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ActiveZonalShiftHostCount`	Le nombre de cibles qui participent activement au changement de zone actuellement. Critères de reporting : Signalé lorsque l'équilibreur de charge est activé pour le changement de zone. Statistiques : Les statistiques les plus utiles sont`Maximum`, et`Minimum`. Dimensions • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`
`ClientTLSNegotiationErrorCount`	Nombre total de liaisons TLS qui ont échoué lors de la négociation entre un client et un écouteur TLS. Critères de notification : il existe une valeur différente de zéro. Statistics : la statistique la plus utile est `Sum`. Dimensions • `LoadBalancer`

Métrique	Description
ConsumedLCUs	Nombre d'unités de capacité d'équilibreur de charge (LCU) utilisées par votre équilibreur de charge. Vous payez le montant LCUs que vous utilisez par heure. Pour plus d'informations, consultez Tarification Elastic Load Balancing. Critères de notification : toujours signalé. Statistics : All Dimensions • LoadBalancer
ConsumedLCUs_TCP	Nombre d'unités de capacité d'équilibreur de charge (LCU) utilisées par votre équilibreur de charge pour TCP. Vous payez le montant LCUs que vous utilisez par heure. Pour plus d'informations, consultez Tarification Elastic Load Balancing. Critères de notification : il existe une valeur différente de zéro. Statistics : All Dimensions • LoadBalancer
ConsumedLCUs_TLS	Nombre d'unités de capacité d'équilibreur de charge (LCU) utilisées par votre équilibreur de charge pour TLS. Vous payez le montant LCUs que vous utilisez par heure. Pour plus d'informations, consultez Tarification Elastic Load Balancing. Critères de notification : il existe une valeur différente de zéro. Statistics : All Dimensions • LoadBalancer

Métrique	Description
`ConsumedLCUs_UDP`	Nombre d'unités de capacité d'équilibreur de charge (LCU) utilisées par votre équilibreur de charge pour UDP. Vous payez le montant LCUs que vous utilisez par heure. Pour plus d'informations, consultez Tarification Elastic Load Balancing. Critères de notification : il existe une valeur différente de zéro. Statistics : All Dimensions • `LoadBalancer`
`HealthyHostCount`	Nombre de cibles considérées saines. Cette métrique n'inclut aucun Application Load Balancer enregistré comme cible. Critères de reporting : Signalé s'il existe des cibles enregistrées. Statistiques : les statistiques les plus utiles sont `Maximum` et `Minimum`. Dimensions • `LoadBalancer` , `TargetGroup` • `AvailabilityZone` , `LoadBalancer` , `TargetGroup`
`NewFlowCount`	Nombre total de nouveaux flux (ou connexions) établis entre les clients et les cibles pendant la période. Critères de notification : toujours signalé. Statistics : la statistique la plus utile est `Sum`. Dimensions • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrique	Description
NewFlowCount_TCP	Nombre total de nouveaux flux (ou connexions) TCP établis entre les clients et les cibles pendant la période. Critères de notification : il existe une valeur différente de zéro. Statistics : la statistique la plus utile est Sum. Dimensions • LoadBalancer • AvailabilityZone , LoadBalancer
NewFlowCount_TLS	Nombre total de nouveaux flux (ou connexions) TLS établis entre les clients et les cibles pendant la période. Critères de notification : il existe une valeur différente de zéro. Statistics : la statistique la plus utile est Sum. Dimensions • LoadBalancer • AvailabilityZone , LoadBalancer
NewFlowCount_UDP	Nombre total de nouveaux flux (ou connexions) UDP établis entre les clients et les cibles pendant la période. Critères de notification : il existe une valeur différente de zéro. Statistics : la statistique la plus utile est Sum. Dimensions • LoadBalancer • AvailabilityZone , LoadBalancer

Métrique	Description
PeakBytesPerSecond	Nombre moyen le plus élevé d'octets traités par seconde, calculé toutes les 10 secondes pendant la fenêtre d'échantillonnage. Cette métrique n'inclut pas le trafic lié aux bilans de santé. Critères de notification : toujours signalé Statistics : la statistique la plus utile est Maximum. Dimensions • LoadBalancer • AvailabilityZone , LoadBalancer
PeakPacketsPerSecond	Débit moyen de paquets le plus élevé (paquets traités par seconde), calculé toutes les 10 secondes pendant la fenêtre d'échantillonnage. Cette métrique inclut le trafic de surveillance de l'état. Critères de notification : toujours signalé. Statistics : la statistique la plus utile est Maximum. Dimensions • LoadBalancer • AvailabilityZone , LoadBalancer

Métrique	Description
`PortAllocationErrorCount`	Nombre total d'erreurs éphémères d'attribution de port lors d'une opération de traduction IP client. Une valeur différente de zéro indique l'interruption des connexions client. Remarque : un Network Load Balancer prend en charge 55 000 connexions simultanées ou environ 55 000 connexions par minute sur chaque cible unique (adresse IP et port) lors de la traduction des adresses IP client. Pour résoudre les erreurs d'attribution de port, ajoutez davantage de cibles au groupe cible. Critères de notification : toujours signalé. Statistics : la statistique la plus utile est `Sum`. Dimensions • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`ProcessedBytes`	Nombre total d'octets traités par l'équilibreur de charge, TCP/IP en-têtes compris. Ce nombre inclut le trafic vers et depuis les cibles, moins le trafic lié à la vérification de l'état. Critères de notification : toujours signalé. Statistics : la statistique la plus utile est `Sum`. Dimensions • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrique	Description
ProcessedBytes_TCP	Nombre total d'octets traités par les écouteurs TCP. Critères de notification : il existe une valeur différente de zéro. Statistics : la statistique la plus utile est Sum. Dimensions • LoadBalancer • AvailabilityZone , LoadBalancer
ProcessedBytes_TLS	Nombre total d'octets traités par les écouteurs TLS. Critères de notification : il existe une valeur différente de zéro. Statistics : la statistique la plus utile est Sum. Dimensions • LoadBalancer • AvailabilityZone , LoadBalancer
ProcessedBytes_UDP	Nombre total d'octets traités par les écouteurs UDP. Critères de notification : il existe une valeur différente de zéro Statistics : la statistique la plus utile est Sum. Dimensions • LoadBalancer • AvailabilityZone , LoadBalancer

Métrique	Description
`ProcessedPackets`	Nombre total de paquets traités par l'équilibreur de charge. Ce nombre inclut le trafic vers et depuis les cibles, y compris le trafic lié à la surveillance de l'état. Critères de notification : toujours signalé. Statistics : la statistique la plus utile est `Sum`. Dimensions • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`RejectedFlowCount`	Nombre total de flux (ou de connexions) rejetés par l'équilibreur de charge. Critères de notification : toujours signalé. Statistics : les statistiques les plus utiles sont `Average`, `Maximum` et `Minimum`. Dimensions • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`
`RejectedFlowCount_TCP`	Le nombre de flux TCP (ou de connexions) rejetés par l'équilibreur de charge. Critères de notification : il existe une valeur différente de zéro. Statistics : la statistique la plus utile est `Sum`. Dimensions • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrique	Description
`ReservedLCUs`	Le nombre d'unités de capacité de l'équilibreur de charge (LCUs) réservées à votre équilibreur de charge à l'aide de la réservation LCU. Critères de notification : il existe une valeur différente de zéro Statistics : All Dimensions • `LoadBalancer`
`SecurityGroupBlockedFlowCount_Inbound_ICMP`	Nombre de nouveaux messages ICMP rejetés par les règles entrantes des groupes de sécurité de l'équilibreur de charge. Critères de notification : il existe une valeur différente de zéro. Statistics : la statistique la plus utile est `Sum`. Dimensions • `LoadBalancer` • `AavailabilityZone` , `LoadBalancer`
`SecurityGroupBlockedFlowCount_Inbound_TCP`	Nombre de nouveaux flux TCP rejetés par les règles entrantes des groupes de sécurité de l'équilibreur de charge. Critères de notification : il existe une valeur différente de zéro. Statistics : la statistique la plus utile est `Sum`. Dimensions • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Métrique	Description
SecurityGroupBlockedFlowCount_Inbound_UDP	Nombre de nouveaux flux UDP rejetés par les règles entrantes des groupes de sécurité de l'équilibreur de charge. Critères de notification : il existe une valeur différente de zéro. Statistics : la statistique la plus utile est Sum. Dimensions • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Outbound_ICMP	Nombre de nouveaux messages ICMP rejetés par les règles sortantes des groupes de sécurité de l'équilibreur de charge. Critères de notification : il existe une valeur différente de zéro. Statistics : la statistique la plus utile est Sum. Dimensions • LoadBalancer • AvailabilityZone , LoadBalancer
SecurityGroupBlockedFlowCount_Outbound_TCP	Nombre de nouveaux flux TCP rejetés par les règles sortantes des groupes de sécurité de l'équilibreur de charge. Critères de notification : il existe une valeur différente de zéro. Statistics : la statistique la plus utile est Sum. Dimensions • LoadBalancer • AvailabilityZone , LoadBalancer

Métrique	Description
SecurityGroupBlockedFlowCount_Outbound_UDP	Nombre de nouveaux flux UDP rejetés par les règles sortantes des groupes de sécurité de l'équilibreur de charge. Critères de notification : il existe une valeur différente de zéro. Statistics : la statistique la plus utile est Sum. Dimensions • LoadBalancer • AvailabilityZone , LoadBalancer
TargetTLSNegotiationErrorCount	Nombre total de liaisons TLS qui ont échoué lors de la négociation entre un écouteur TLS et une cible. Critères de notification : il existe une valeur différente de zéro. Statistics : la statistique la plus utile est Sum. Dimensions • LoadBalancer
TCP_Client_Reset_Count	Nombre total de paquets de réinitialisation (RST) envoyés par un client à une cible. Les réinitialisations sont générées par le client et transférées par l'équilibreur de charge. Critères de notification : toujours signalé. Statistics : la statistique la plus utile est Sum. Dimensions • LoadBalancer • AvailabilityZone , LoadBalancer

Métrique	Description
TCP_ELB_Reset_Count	Nombre total de paquets de réinitialisation (RST) générés par l'équilibreur de charge. Pour plus d'informations, consultez Dépannage. Critères de notification : toujours signalé. Statistics : la statistique la plus utile est Sum. Dimensions • LoadBalancer • AvailabilityZone , LoadBalancer
TCP_Target_Reset_Count	Nombre total de paquets de réinitialisation (RST) envoyés par une cible à un client. Les réinitialisations sont générées par la cible et transférées par l'équilibreur de charge. Critères de notification : toujours signalé. Statistics : la statistique la plus utile est Sum. Dimensions • LoadBalancer • AvailabilityZone , LoadBalancer
UnHealthyHostCount	Nombre de cibles considérées non saines. Cette métrique n'inclut aucun Application Load Balancer enregistré comme cible. Critères de reporting : Signalé s'il existe des cibles enregistrées. Statistiques : les statistiques les plus utiles sont Maximum et Minimum. Dimensions • LoadBalancer , TargetGroup • AvailabilityZone , LoadBalancer , TargetGroup

Métrique	Description
`UnhealthyRoutingFlowCount`	Nombre de flux (ou de connexions) acheminés à l'aide de l'action de basculement du routage (fail-open). Cette métrique n'est pas prise en charge pour les écouteurs TLS. Critères de notification : il existe une valeur différente de zéro. Statistics : la statistique la plus utile est `Sum`.
`ZonalHealthStatus`	Nombre de zones de disponibilité considérées comme saines par l'équilibreur de charge. L'équilibreur de charge émet un 1 pour chaque zone de disponibilité saine et un 0 pour chaque zone de disponibilité non fonctionnelle. Critères de notification : signalé si les surveillances de l'état sont activées. Statistiques : les statistiques les plus utiles sont `Maximum` et `Minimum`. Dimensions • `LoadBalancer` • `AvailabilityZone` , `LoadBalancer`

Dimensions de métriques des Network Load Balancers

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

Dimension	Description
`AvailabilityZone`	Filtrer les données métriques par Zone de disponibilité.
`LoadBalancer`	Filtre les données métriques en fonction de l'équilibreur de charge. Spécifiez l'équilibreur de charge comme suit : net/ load-balancer-

Dimension	Description
	name/1234567890123456 (dernière partie de l'ARN de l'équilibreur de charge).
`TargetGroup`	Filtre les données métriques en fonction du groupe cible. Spécifiez le groupe cible comme suit : targetgroup/ target-group-name/1234567890123456 (dernière partie de l'ARN du groupe cible).

Statistiques des métriques Network Load Balancer

CloudWatch fournit des statistiques basées sur les points de données métriques publiés par Elastic Load Balancing. Les statistiques sont des regroupements de données de métrique sur une période donnée. Lorsque vous demandez des statistiques, le flux de données renvoyé est identifié par le nom et la dimension de la métrique. Une dimension est une name/value paire qui identifie une métrique de manière unique. Par exemple, vous pouvez demander des statistiques pour toutes les EC2 instances saines associées à un équilibreur de charge lancé dans une zone de disponibilité spécifique.

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

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

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

Afficher CloudWatch les statistiques de votre équilibreur de charge

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

Vous pouvez également afficher des métriques pour votre équilibreur de charge à l'aide de la console CloudWatch.

Pour afficher des métriques à l'aide de la console

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

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

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Sélectionnez l'espace de nom NetworkELB.
4. (Facultatif) Pour afficher une métrique pour toutes les dimensions, saisissez son nom dans le champ de recherche.

Pour consulter les statistiques à l'aide du AWS CLI

Utilisez la commande list-metrics suivante pour répertorier les métriques disponibles :

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

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

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

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

Voici un exemple de sortie :

```
{
    "Datapoints": [
        {
            "Timestamp": "2017-04-18T22:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2017-04-18T04:00:00Z",
            "Average": 0.0,
            "Unit": "Count"
        },
        ...
    ],
    "Label": "UnHealthyHostCount"
}
```

Journaux d'accès de votre Network Load Balancer

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

> **Important**
>
> Les journaux d'accès sont créés uniquement si l'équilibreur de charge dispose d'un écouteur TLS, et les journaux contiennent uniquement des informations sur les demandes TLS. Les journaux d'accès enregistrent les demandes dans la mesure du possible. Il est recommandé d'utiliser les journaux d'accès pour comprendre la nature des demandes, et non comme comptabilisation complète de toutes les demandes.

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

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

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

Table des matières

Fichiers journaux d'accès

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

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

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

bucket

Nom du compartiment S3.

prefix

Préfixe (hiérarchie logique) dans le compartiment. Si vous ne spécifiez pas de préfixe, les journaux sont placés à la racine du compartiment.

aws-account-id

L' Compte AWS identifiant du propriétaire.

region

Région pour votre équilibreur de charge et le compartiment S3.

aaaa/mm/jj

Date à laquelle le journal a été fourni.

load-balancer-id

ID de ressource de l'équilibreur de charge. Si l'ID de ressource contient des barres obliques (/), elles sont remplacées par des points (.).

end-time

Date et heure auxquelles l'intervalle de journalisation a pris fin. Par exemple, une heure de fin 20181220T2340Z contient des entrées pour les demandes effectuées entre 23h35 et 23h40.

random-string

Chaîne aléatoire générée par le système.

Voici un exemple de nom de fichier journal :

```
s3://my-bucket/prefix/AWSLogs/123456789012/elasticloadbalancing/us-
east-2/2020/05/01/123456789012_elasticloadbalancing_us-east-2_net.my-
loadbalancer.1234567890abcdef_20200501T0000Z_20sg8hgm.log.gz
```

Vous pouvez stocker vos fichiers journaux dans votre compartiment aussi longtemps que vous le souhaitez, mais vous pouvez également définir des règles de cycle de vie Amazon S3 pour archiver ou supprimer automatiquement les fichiers journaux. Pour plus d'informations, veuillez consulter Gestion du cycle de vie de votre stockage dans le Guide de l'utilisateur Amazon S3.

Entrées des journaux d'accès

Le tableau suivant décrit les champs d'une entrée de journal d'accès, dans l'ordre. Tous les champs sont délimités par des espaces. Lorsque de nouveaux champs sont insérés, ils sont ajoutés à la fin de l'entrée de journal. Lors du traitement des fichiers journaux, vous devez ignorer les champs situés à la fin de l'entrée de journal que vous n'attendiez pas.

Champ	Description
type	Le type d'écouteur. La valeur prise en charge est `tls`.
version	La version de l'entrée de journal. La version actuelle est 2.0.
time	Le temps enregistré à la fin de la connexion TLS, au format ISO 8601.
elb	ID de ressource de l'équilibreur de charge.

Champ	Description
écouteur	L'ID de ressource de l'écouteur TLS pour la connexion.
client:port	Adresse IP et port du client.
destination:port	Adresse IP et port de la destination. Si le client se connecte directeme nt à l'équilibreur de charge, la destination est l'écouteur. Si le client se connecte à l'aide d'un service de point de terminaison de VPC, la destination est le point de terminaison de VPC.
connection_time	Durée totale pour établir la connexion, du début à la fermeture, en millisecondes.
tls_handshake_time	Durée totale pour établir la liaison TLS après l'établissement de la connexion TCP, y compris les retards côté client, en millisecondes. Ce temps est inclus dans le `connection_time` champ. En l'absence de prise de contact TLS ou en cas d'échec de la prise de contact TLS, cette valeur est définie sur. `-`
received_bytes	Le nombre d'octets reçus par l'équilibreur de charge à partir du client, après déchiffrement.
sent_bytes	Le nombre d'octets envoyés par l'équilibreur de charge au client, après déchiffrement.
incoming_tls_alert	La valeur entière des alertes TLS reçues par l'équilibreur de charge à partir du client, le cas échéant. Dans le cas contraire, cette valeur est définie sur`-`.
chosen_cert_arn	ARN du certificat mis à la disposition du client. Si aucun message client valide n'est envoyé, cette valeur est définie sur`-`.
chosen_cert_serial	Réservé pour un usage futur. Cette valeur est toujours définie sur`-`.
tls_cipher	La suite de chiffrement négociée avec le client, au format OpenSSL. Si la négociation TLS n'aboutit pas, cette valeur est définie sur. `-`

Champ	Description
tls_protocol_version	Le protocole TLS négocié avec le client, au format chaîne. Les valeurs possibles sont `tlsv10`, `tlsv11`, `tlsv12` et `tlsv13`. Si la négociation TLS n'aboutit pas, cette valeur est définie sur. `-`
tls_named_group	Réservé pour un usage futur. Cette valeur est toujours définie sur`-`.
domain_name	Valeur de l'extension server_name dans le message Hello client. Ce champ est codé en URL. Si aucun message client valide n'est envoyé ou si l'extension n'est pas présente, cette valeur est définie sur`-`.
alpn_fe_protocol	Le protocole TLS négocié avec le client, au format chaîne. Les valeurs possibles sont `h2`, `http/1.1` et `http/1.0`. Si aucune politique ALPN n'est configurée dans l'écouteur TLS, si aucun protocole correspondant n'est trouvé ou si aucune liste de protocoles valide n'est envoyée, cette valeur est définie sur. `-`
alpn_be_protocol	Protocole d'application négocié avec la cible, au format chaîne. Les valeurs possibles sont `h2`, `http/1.1` et `http/1.0`. Si aucune politique ALPN n'est configurée dans l'écouteur TLS, si aucun protocole correspon dant n'est trouvé ou si aucune liste de protocoles valide n'est envoyée, cette valeur est définie sur. `-`
alpn_client_prefer ence_list	Valeur de l'extension application_layer_protocol_negotiation dans le message client Hello. Ce champ est codé en URL. Chaque protocole est entouré de guillemets doubles et les protocoles sont séparés par une virgule. Si aucune politique ALPN n'est configurée dans l'écouteur TLS, si aucun message client valide n'est envoyé ou si l'extension n'est pas présente, cette valeur est définie sur. `-` La chaîne est tronquée si elle dépasse 256 octets.
tls_connection_cre ation_time	Le temps enregistré au début de la connexion TLS, au format ISO 8601.

Exemple d'entrées de journal

Des modèles d'entrées de journal sont présentés ci-après : Notez que le texte ne s'affiche sur plusieurs lignes que pour en faciliter la lecture.

Voici un exemple pour un écouteur TLS sans stratégie ALPN.

```
tls 2.0 2018-12-20T02:59:40 net/my-network-loadbalancer/c6e77e28c25b2234
 g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
- - - 2018-12-20T02:59:30
```

Voici un exemple pour un écouteur TLS avec une stratégie ALPN.

```
tls 2.0 2020-04-01T08:51:42 net/my-network-loadbalancer/c6e77e28c25b2234
 g3d4b5e8bb8464cd
72.21.218.154:51341 172.100.100.185:443 5 2 98 246 -
arn:aws:acm:us-east-2:671290407336:certificate/2a108f19-aded-46b0-8493-c63eb1ef4a99 -
ECDHE-RSA-AES128-SHA tlsv12 -
my-network-loadbalancer-c6e77e28c25b2234.elb.us-east-2.amazonaws.com
h2 h2 "h2","http/1.1" 2020-04-01T08:51:20
```

Traitement des fichiers journaux d'accès

Les fichiers journaux d'accès sont compressés. Si vous ouvrez les fichiers à l'aide de la console Amazon S3, ils sont décompressés et les informations s'affichent. Si vous téléchargez les fichiers, vous devez les décompresser pour afficher les informations.

Si la demande est importante sur votre site web, votre équilibreur de charge peut générer des fichiers journaux avec des gigaoctets de données. Il se peut que vous ne puissiez pas traiter une telle quantité de données à l'aide du line-by-line traitement. Vous devrez donc peut-être utiliser des outils d'analyse qui proposent des solutions de traitement en parallèle. Par exemple, vous pouvez utiliser les outils d'analyse suivants pour analyser et traiter des journaux d'accès :

- Amazon Athena est un service de requête interactif qui facilite l'analyse des données dans Amazon S3 à l'aide du langage SQL standard. Pour plus d'informations, veuillez consulter Interrogation des journaux du dispositif du Network Load Balancer dans le Guide de l'utilisateur Amazon Athena.
- Loggly

- Splunk
- Sumo Logic

Activez les journaux d'accès pour votre Network Load Balancer

Pour activer la journalisation des accès pour votre équilibreur de charge, vous devez spécifier le nom du compartiment S3 dans lequel l'équilibreur de charge stockera les journaux. Le compartiment doit avoir une politique de compartiment qui accorde à Elastic Load Balancing l'autorisation d'écrire dans le compartiment.

> **Important**
>
> Les journaux d'accès sont créés uniquement si l'équilibreur de charge dispose d'un écouteur TLS, et les journaux contiennent uniquement des informations sur les demandes TLS.

Conditions requises pour le compartiment

Vous ou utiliser un compartiment existant ou créer un compartiment spécifique pour les journaux d'accès. Le compartiment doit répondre aux critères suivants :

Prérequis

- Le compartiment doit se situer dans la même région que l'équilibreur de charge. Le compartiment et l'équilibreur de charge peuvent être détenus par des comptes différents.
- Le préfixe que vous spécifiez ne doit pas inclure `AWSLogs`. Nous ajoutons la partie du nom de fichier commençant par `AWSLogs` après le nom du compartiment et le préfixe que vous avez spécifié.
- Le compartiment doit avoir une stratégie de compartiment qui octroie l'autorisation d'écrire les journaux d'accès dans votre compartiment. Les stratégies de compartiment sont une collection d'instructions JSON écrites dans le langage d'access policy permettant de définir des autorisations d'accès pour votre compartiment.

Exemple de politique de compartiment

Voici un exemple de politique . Pour les `Resource` éléments, *`amzn-s3-demo-destination-bucket`* remplacez-les par le nom du compartiment S3 pour vos journaux d'accès. Veillez à

omettre le préfixe de compartiment *Prefix/* si vous n'utilisez pas de préfixe de compartiment. Pour `aws:SourceAccount`, spécifiez l'ID du AWS compte auprès de l'équilibreur de charge. Pour `aws:SourceArn`, remplacez *region* et *012345678912* par la région et l'ID de compte de l'équilibreur de charge, respectivement.

JSON

```
{
    "Version":"2012-10-17",
    "Id": "AWSLogDeliveryWrite",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": [
                        "012345678912"
                    ]
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:logs:us-east-1:012345678912:*"
                    ]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-
bucket/Prefix/AWSLogs/account-ID/*",
            "Condition": {
```

```
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": [
                        "012345678912"
                    ]
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:logs:us-east-1:012345678912:*"
                    ]
                }
            }
        }
    ]
}
```

Chiffrement

Vous pouvez activer le chiffrement côté serveur pour votre compartiment de journaux d'accès Amazon S3 de l'une des manières suivantes :

- Clés gérées par Amazon S3 (SSE-S3)
- AWS KMS clés stockées dans AWS Key Management Service (SSE-KMS) †

† Avec les journaux d'accès de Network Load Balancer, vous ne pouvez pas utiliser de clés AWS gérées, vous devez utiliser des clés gérées par le client.

Pour plus d'informations, consultez les sections Spécification du chiffrement Amazon S3 (SSE-S3) et Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS) dans le guide de l'utilisateur Amazon S3.

La stratégie de clé doit permettre au service de chiffrer et de déchiffrer les journaux. Voici un exemple de politique .

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
      ],
      "Resource": "*"
    }
  ]
}
```

Configuration des journaux d'accès

Utilisez la procédure suivante pour configurer les journaux d'accès afin de capturer les informations relatives aux demandes et de transmettre les fichiers journaux à votre compartiment S3.

Console

Pour activer les journaux d'accès

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Sélectionnez le nom de votre équilibreur de charge afin d'ouvrir sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Pour Surveillance, activez Journaux d'accès.
6. Pour S3 URI, saisissez l'URI S3 de vos fichiers journaux. L'URI que vous spécifiez varie selon que vous utilisez ou non un préfixe.
   - URI avec préfixe : s3 :///*amzn-s3-demo-logging-bucketlogging-prefix*
   - URI sans préfixe : s3 ://*amzn-s3-demo-logging-bucket*
7. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour activer les journaux d'accès

Utilisez la modify-load-balancer-attributescommande avec les attributs associés.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes \
        Key=access_logs.s3.enabled,Value=true \
        Key=access_logs.s3.bucket,Value=amzn-s3-demo-logging-bucket \
        Key=access_logs.s3.prefix,Value=logging-prefix
```

CloudFormation

Pour activer les journaux d'accès

Mettez à jour la AWS::ElasticLoadBalancingV2::LoadBalancerressource pour inclure les attributs associés.

```
Resources:
  myLoadBalancer:
    Type: 'AWS::ElasticLoadBalancingV2::LoadBalancer'
    Properties:
      Name: my-nlb
      Type: network
      Scheme: internal
      Subnets:
        - !Ref subnet-AZ1
        - !Ref subnet-AZ2
      SecurityGroups:
        - !Ref mySecurityGroup
      LoadBalancerAttributes:
        - Key: "access_logs.s3.enabled"
          Value: "true"
        - Key: "access_logs.s3.bucket"
          Value: "amzn-s3-demo-logging-bucket"
        - Key: "access_logs.s3.prefix"
          Value: "logging-prefix"
```

Désactiver les journaux d'accès à votre Network Load Balancer

Vous pouvez désactiver la journalisation des accès pour votre équilibreur de charge à tout moment. Une fois que vous avez désactivé la journalisation des accès, vos journaux d'accès restent dans votre compartiment S3 jusqu'à ce que vous les supprimiez. Pour plus d'informations, consultez la section Création, configuration et utilisation des compartiments S3 dans le guide de l'utilisateur Amazon S3.

Console

Pour désactiver les journaux d'accès

1. Ouvrez la EC2 console Amazon à l'adresse https://console.aws.amazon.com/ec2/.
2. Dans le volet de navigation, choisissez Load Balancers.
3. Sélectionnez le nom de votre équilibreur de charge afin d'ouvrir sa page de détails.
4. Dans l'onglet Attributes, choisissez Edit.
5. Pour Surveillance, désactivez Journaux d'accès.
6. Sélectionnez Enregistrer les modifications.

AWS CLI

Pour désactiver les journaux d'accès

Utilisez la commande modify-load-balancer-attributes.

```
aws elbv2 modify-load-balancer-attributes \
    --load-balancer-arn load-balancer-arn \
    --attributes Key=access_logs.s3.enabled,Value=false
```

Dépannage de votre Network Load Balancer

Les informations suivantes peuvent vous aider à résoudre les problèmes liés à votre Network Load Balancer.

Une cible enregistrée n'est pas en service

Si le passage à l'état `InService` d'une cible est plus long que prévu, les vérifications de l'état risquent d'échouer. Votre cible ne sera pas en service tant que la vérification de l'état correspondante ne sera pas concluante. Pour de plus amples informations, veuillez consulter Contrôles de santé pour les groupes cibles de Network Load Balancer.

Vérifiez si les vérifications de l'état de votre instance ont échoué, puis contrôlez les points suivants :

Un groupe de configuration n'autorise pas le trafic

> Les groupes de sécurité associés à une instance doivent autoriser le trafic à partir de l'équilibreur de charge à l'aide du port et du protocole de vérification de l'état. Pour de plus amples informations, veuillez consulter Groupes de sécurité cibles. De même, le groupe de sécurité de votre équilibreur de charge doit autoriser le trafic vers les instances. Pour de plus amples informations, veuillez consulter Mettez à jour les groupes de sécurité pour votre Network Load Balancer.

Une liste de contrôle d'accès (ACL) réseau n'autorise pas le trafic

> La liste ACL réseau associée aux sous-réseaux de vos instances et aux sous-réseaux de votre équilibreur de charge doit autoriser le trafic et les surveillances de l'état depuis l'équilibreur de charge. Pour de plus amples informations, veuillez consulter Réseau ACLs.

Les demandes ne sont pas acheminées vers les cibles

Vérifiez les points suivants :

Un groupe de configuration n'autorise pas le trafic

> Les groupes de sécurité associés aux instances doivent autoriser le trafic sur le port d'écoute à partir d'adresses IP du client (si les cibles sont spécifiées par ID d'instance) ou de nœuds

d'équilibreur de charge (si les cibles sont spécifiées par adresse IP). Pour de plus amples informations, veuillez consulter Groupes de sécurité cibles. De même, le groupe de sécurité de votre équilibreur de charge doit autoriser le trafic vers les instances. Pour de plus amples informations, veuillez consulter Mettez à jour les groupes de sécurité pour votre Network Load Balancer.

Une liste de contrôle d'accès (ACL) réseau n'autorise pas le trafic

Le réseau ACLs associé aux sous-réseaux de votre VPC doit permettre à l'équilibreur de charge et aux cibles de communiquer dans les deux sens sur le port d'écoute. Pour de plus amples informations, veuillez consulter Réseau ACLs.

Les cibles sont dans une zone de disponibilité qui n'est pas activée

Si vous enregistrez des cibles dans une zone de disponibilité mais que vous n'activez pas la zone de disponibilité, ces cibles enregistrées ne reçoivent pas le trafic de l'équilibreur de charge.

L'instance n'est pas dans un VPC appairé

Si vous disposez d'instances dans un VPC appairé au VPC de l'équilibreur de charge, vous devez les enregistrer à l'aide de votre équilibreur de charge par adresse IP et non par ID d'instance.

Les cibles reçoivent plus de demandes de vérification de l'état que prévu

Les surveillances de l'état pour un Network Load Balancer sont distribuées et utilisent un mécanisme de consensus pour déterminer l'état des cibles. Par conséquent, des cibles reçoivent plus de vérifications de l'état que le nombre configuré via le paramètre `HealthCheckIntervalSeconds`.

Les cibles reçoivent moins de demandes de vérification de l'état que prévu

Vérifiez si `net.ipv4.tcp_tw_recycle` est activé. Ce paramètre est connu pour entraîner des problèmes liés aux équilibreurs de charge. Le paramètre `net.ipv4.tcp_tw_reuse` est considéré comme un paramètre plus sûr.

Des cibles non saines reçoivent des demandes de l'équilibreur de charge.

Cela se produit lorsque toutes les cibles enregistrées sont défectueuses. S'il existe au moins une cible enregistrée saine, votre Network Load Balancer achemine les demandes uniquement vers ses cibles enregistrées saines.

Lorsqu'il n'existe que des cibles enregistrées défectueuses, le Network Load Balancer achemine les demandes vers toutes les cibles enregistrées : il s'agit du mode fail-open. Le Network Load Balancer procède ainsi au lieu de supprimer toutes les adresses IP du DNS lorsque toutes les cibles sont défectueuses et que les zones de disponibilité respectives n'ont pas de cible saine à laquelle envoyer une demande.

La cible échoue aux vérifications d'intégrité HTTP ou HTTPS en raison d'une incompatibilité d'en-tête d'hôte

L'en-tête d'hôte HTTP dans la demande de vérification de l'intégrité contient l'adresse IP du nœud d'équilibrage et le port de l’écouteur, et non l'adresse IP de la cible et le port de vérification de l'intégrité. Si vous mappez des requêtes entrantes par en-tête d'hôte, vous devez vous assurer que les vérifications d'intégrité correspondent à n'importe quel en-tête d'hôte HTTP. Une autre option consiste à ajouter un service HTTP distinct sur un port différent et à configurer le groupe cible afin qu'il utilise ce port pour les vérifications d'intégrité à la place. Vous pouvez aussi envisager d'utiliser des contrôles d'intégrité TCP.

Impossible d'associer un groupe de sécurité à un équilibreur de charge

Si le Network Load Balancer a été créé sans groupes de sécurité, il ne peut pas prendre en charge les groupes de sécurité après sa création. Vous ne pouvez associer un groupe de sécurité qu'à un équilibreur de charge lors de sa création ou à un équilibreur de charge existant créé à l'origine avec des groupes de sécurité.

Impossible de supprimer tous les groupes de sécurité

Si le Network Load Balancer a été créé avec des groupes de sécurité, au moins un groupe de sécurité doit lui être associé à tout moment. Vous ne pouvez pas supprimer tous les groupes de sécurité de l'équilibreur de charge en même temps.

Augmentation de la métrique TCP_ELB_Reset_Count

Pour chaque demande TCP effectuée par un client via un Network Load Balancer, l'état de cette connexion est suivi. Si aucune donnée n'est envoyée via la connexion par le client ou la cible au cours d'une période plus longue que le délai d'inactivité, la connexion est fermée. Si un client ou une cible envoie des données après que le délai d'inactivité est écoulé, il reçoit un paquet TCP RST pour indiquer que la connexion n'est plus valide. Par ailleurs, si une cible devient défectueuse, l'équilibreur de charge envoie un TCP RST pour les paquets reçus sur les connexions client associées à la cible, sauf si la cible défectueuse déclenche le mode fail-open pour l'équilibreur de charge.

Si vous constatez une hausse de la métrique `TCP_ELB_Reset_Count` juste avant ou pendant l'augmentation de la métrique `UnhealthyHostCount`, il est probable que les paquets TCP RST aient été envoyés parce que la cible commençait à échouer, mais n'avait pas été signalée comme étant défectueuse. Si vous constatez des augmentations persistantes de `TCP_ELB_Reset_Count` sans que les cibles ne soient signalées comme défectueuses, vous pouvez consulter les journaux de flux VPC pour voir si les clients envoient des données sur des flux expirés.

Connexions expirées pour les demandes d'une cible vers son équilibreur de charge

Vérifiez si la préservation des adresses IP client est activée sur votre groupe cible. La boucle NAT, également appelée hairpinning, n'est pas prise en charge lorsque la préservation des adresses IP client est activée.

Si une instance est cliente d'un équilibreur de charge auprès duquel elle est enregistrée et que la préservation de l'adresse IP du client est activée, la connexion ne réussit que si la demande est acheminée vers une autre instance. Si la demande est acheminée vers la même instance à partir de laquelle elle a été envoyée, la connexion expire, car les adresses IP source et de destination sont identiques. Notez que cela s'applique aux pods Amazon EKS exécutés dans la même instance EC2 de nœud de travail, même s'ils ont des adresses IP différentes.

Si une instance doit envoyer des demandes à un équilibreur de charge auprès duquel elle est enregistrée, effectuez l'une des actions suivantes :

- Désactivez la préservation des adresses IP client. Utilisez plutôt le protocole Proxy v2 pour obtenir l'adresse IP du client.
- Assurez-vous que les conteneurs qui doivent communiquer sont sur des instances de conteneur différentes.

Diminution des performances lorsque des cibles sont déplacées vers un Network Load Balancer

Les Classic Load Balancers et les Application Load Balancers utilisent le multiplexage des connexions, mais pas les Network Load Balancers. Par conséquent, vos cibles peuvent recevoir plus de connexions TCP derrière un Network Load Balancer. Assurez-vous que vos cibles sont prêtes à gérer le volume de demandes de connexion qu'elles sont susceptibles de recevoir.

Erreurs d'allocation de ports pour les flux de backend

En cas de PrivateLink trafic ou lorsque la préservation de l'adresse IP du client est désactivée, un Network Load Balancer prend en charge 55 000 connexions simultanées ou environ 55 000 connexions par minute vers chaque cible unique (adresse IP et port). Si vous dépassez ces limites, le risque d'erreurs d'allocation de port augmente. Vous pouvez suivre les erreurs d'allocation de ports à l'aide de la `PortAllocationErrorCount` métrique. Vous pouvez suivre les connexions actives à l'aide de la `ActiveFlowCount` métrique. Pour de plus amples informations, veuillez consulter CloudWatch métriques pour votre Network Load Balancer.

Pour corriger les erreurs d'allocation de ports, nous vous recommandons d'ajouter des cibles au groupe cible.

Sinon, si vous ne pouvez pas ajouter de cibles au groupe cible, vous pouvez ajouter jusqu'à 7 adresses IP secondaires aux interfaces réseau de l'équilibreur de charge. Les adresses IP secondaires sont automatiquement attribuées à partir des blocs IPv4 CIDR des sous-réseaux correspondants. Chaque adresse IP secondaire consomme 6 unités d'adressage réseau. Notez qu'une fois que vous avez ajouté une adresse IP secondaire, vous ne pouvez pas la supprimer. La seule façon de libérer les adresses IP secondaires est de supprimer l'équilibreur de charge.

Défaillance intermittente de l'établissement de la connexion TCP ou retards d'établissement de la connexion TCP

Lorsque la conservation de l'adresse IP du client est activée, un client peut se connecter à une adresse IP de destination différente en utilisant le même port éphémère source. Ces adresses IP de destination peuvent provenir du même équilibreur de charge (dans différentes zones de disponibilité) lorsque l'équilibrage de charge entre zones est activé ou de différents équilibreurs de charge réseau utilisant la même adresse IP cible et le même port enregistrés. Dans ce cas, si ces connexions sont routées vers la même adresse IP cible et le même port, la cible verra une connexion dupliquée, car elles proviennent de la même adresse IP et du même port client. Cela entraîne des erreurs de connexion et des retards lors de l'établissement de l'une de ces connexions. Cela se produit fréquemment lorsqu'un périphérique NAT se trouve devant le client et que la même adresse IP source et le même port source sont alloués lors de la connexion simultanée à plusieurs adresses IP Network Load Balancer.

Vous pouvez réduire ce type d'erreur de connexion en augmentant le nombre de ports source éphémères alloués par le client ou le périphérique NAT, ou en augmentant le nombre de cibles pour l'équilibreur de charge. Nous recommandons aux clients de modifier le port source utilisé lors de la reconnexion après ces échecs de connexion. Pour éviter ce type d'erreur de connexion, si vous utilisez un seul Network Load Balancer, vous pouvez envisager de désactiver l'équilibrage de charge entre zones, ou si vous utilisez plusieurs Network Load Balancer, vous pouvez envisager de ne pas utiliser la même adresse IP cible et le même port enregistrés dans plusieurs groupes cibles. Vous pouvez également envisager de désactiver la préservation de l'adresse IP du client. Si vous avez besoin de l'adresse IP du client, vous pouvez l'utiliser pour la récupérer à l'aide du protocole proxy v2. Pour en savoir plus sur le protocole proxy v2, consultezProtocole proxy.

Défaillance potentielle lors du provisionnement de l'équilibreur de charge

L'une des raisons pour lesquelles un Network Load Balancer peut échouer lors de son approvisionnement est que vous utilisez une adresse IP déjà attribuée ou allouée ailleurs (par exemple, attribuée comme adresse IP secondaire pour une EC2 instance). Cette adresse IP empêche la configuration de l'équilibreur de charge, et son état est `failed`. Vous pouvez résoudre ce problème en annulant l'allocation de l'adresse IP associée et en relançant le processus de création.

Le trafic est réparti de manière inégale entre les cibles

Les écouteurs TCP et TLS acheminent les connexions TCP et les écouteurs UDP acheminent les flux UDP. L'équilibreur de charge sélectionne les cibles à l'aide d'un algorithme de hachage de flux. Une connexion unique provenant d'un client est intrinsèquement permanente.

Si vous remarquez que certaines cibles semblent recevoir plus de trafic que d'autres, nous vous recommandons de consulter les journaux de flux VPC. Comparez le nombre de connexions uniques pour chaque adresse IP cible. Veillez à ce que le créneau horaire soit le plus court possible, car l'enregistrement des cibles, la désinscription et les cibles malsaines influencent ces numéros de connexion.

Voici les scénarios possibles dans lesquels les connexions peuvent être réparties de manière inégale :

- Si vous commencez avec un petit nombre de cibles, puis que vous enregistrez des cibles supplémentaires ultérieurement, les cibles d'origine ont toujours des connexions avec les clients. Avec une charge de travail HTTP, keepalives garantit que les clients réutilisent les connexions. Si vous réduisez le nombre maximum de keepalives sur votre application Web, les clients ouvriront de nouvelles connexions plus souvent.
- Si l'adhérence au groupe cible est activée, qu'il y a un petit nombre de clients et que les clients communiquent via un périphérique NAT avec une adresse IP source unique, les connexions de ces clients sont acheminées vers la même cible.
- Si l'équilibrage de charge entre zones est désactivé et que les clients préfèrent utiliser l'adresse IP de l'équilibreur de charge provenant de l'une des zones d'équilibrage de charge, les connexions seront réparties de manière inégale entre les zones d'équilibreur de charge.

La résolution de noms DNS contient moins d'adresses IP que les zones de disponibilité activées

Dans l'idéal, votre Network Load Balancer fournit une adresse IP par zone de disponibilité activée, lorsqu'il possède au moins un hôte sain dans la zone de disponibilité. Lorsqu'aucun hôte sain n'est présent dans une zone de disponibilité donnée et que l'équilibrage de charge entre zones est désactivé, l'adresse IP du Network Load Balancer correspondant à cette zone de disponibilité est supprimée du DNS.

Supposons, par exemple, que votre Network Load Balancer dispose de trois zones de disponibilité activées, qui ont toutes au moins une instance cible enregistrée saine.

- Si les instances cibles enregistrées dans la zone de disponibilité A deviennent défectueuses, l'adresse IP correspondante de la zone de disponibilité A pour le Network Load Balancer est supprimée du DNS.
- Si deux des zones de disponibilité activées ne possèdent aucune instance cible enregistrée saine, les deux adresses IP respectives du Network Load Balancer seront supprimées du DNS.
- S'il n'y a aucune instance cible enregistrée saine dans toutes les zones de disponibilité activées, le mode d'ouverture automatique est activé et le DNS fournira toutes les adresses IP des trois activées AZs dans le résultat.

Les paquets IP fragmentés ne sont pas routés vers les cibles

Les équilibreurs de charge réseau ne prennent pas en charge les paquets IP fragmentés pour le trafic non UDP.

Résoudre les problèmes liés aux cibles défectueuses à l'aide de la carte des ressources

Si les tests de santé de vos cibles Network Load Balancer échouent, vous pouvez utiliser la carte des ressources pour détecter les cibles défectueuses et prendre des mesures en fonction du code de cause de l'échec. Pour de plus amples informations, veuillez consulter Afficher la carte des ressources du Network Load Balancer.

La carte des ressources fournit deux vues : Vue d'ensemble et Carte cible malsaine. L'option Vue d'ensemble est sélectionnée par défaut et affiche toutes les ressources de votre équilibreur de charge. La sélection de la vue Malhealthy Target Map affichera uniquement les cibles malsaines de chaque groupe cible associé au Network Load Balancer.

> **Note**
>
> L'option Afficher les détails des ressources doit être activée pour afficher le résumé du bilan de santé et les messages d'erreur pour toutes les ressources applicables dans la carte des ressources. Lorsque cette option n'est pas activée, vous devez sélectionner chaque ressource pour en afficher les détails.

La colonne Groupes cibles affiche un résumé des cibles saines et malsaines pour chaque groupe cible. Cela peut aider à déterminer si toutes les cibles échouent aux tests de santé ou si seules des cibles spécifiques échouent. Si toutes les cibles d'un groupe cible échouent aux tests de santé, vérifiez les paramètres du bilan de santé du groupe cible. Sélectionnez le nom d'un groupe cible pour ouvrir sa page détaillée dans un nouvel onglet.

La colonne Targets affiche le TargetID et l'état actuel du bilan de santé pour chaque cible. Lorsqu'une cible n'est pas saine, le code de la raison de l'échec du contrôle de santé s'affiche. Lorsqu'une cible échoue à un bilan de santé, vérifiez qu'elle dispose de ressources suffisantes. Sélectionnez l'ID d'une cible pour ouvrir sa page détaillée dans un nouvel onglet.

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

Vérifiez que les tests de santé de votre instance échouent, puis, en fonction du code de cause de l'échec, vérifiez les problèmes suivants :

- Malsain : le délai imparti pour la demande a expiré
  - Vérifiez que les groupes de sécurité et les listes de contrôle d'accès réseau (ACL) associés à vos cibles et à Network Load Balancer ne bloquent pas la connectivité.
  - Vérifiez que la cible dispose d'une capacité suffisante pour accepter les connexions depuis le Network Load Balancer.
  - Les réponses au bilan de santé du Network Load Balancer peuvent être consultées dans les journaux des applications de chaque cible. Pour plus d'informations, consultez la section Codes de raison du contrôle de santé.
- Malsain : FailedHealthChecks
  - Vérifiez que la cible écoute le trafic sur le port de contrôle de santé.

> **Lors de l'utilisation d'un écouteur TLS**
>
> Vous choisissez la politique de sécurité à utiliser pour les connexions frontales. La politique de sécurité utilisée pour les connexions dorsales est automatiquement sélectionnée en fonction de la stratégie de sécurité frontale utilisée.
>
> - Si votre écouteur TLS utilise une politique de sécurité TLS 1.3 pour les connexions frontales, la politique de `ELBSecurityPolicy-TLS13-1-0-2021-06` sécurité est utilisée pour les connexions dorsales.

- Si votre écouteur TLS n'utilise pas de stratégie de sécurité TLS 1.3 pour les connexions frontales, la stratégie de `ELBSecurityPolicy-2016-08` sécurité est utilisée pour les connexions dorsales.

Pour plus d'informations, consultez la section Politiques de sécurité.

- Vérifiez que la cible fournit un certificat de serveur et une clé au format correct spécifié par la politique de sécurité.
- Vérifiez que la cible prend en charge un ou plusieurs chiffrements correspondants, ainsi qu'un protocole fourni par le Network Load Balancer pour établir des handshakes TLS.

Quotas de vos Network Load Balancers

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

Pour afficher les quotas de vos Network Load Balancers ouvrez la console Service Quotas. Dans le panneau de navigation, choisissez Services AWS et sélectionnez Elastic Load Balancing. Vous pouvez également utiliser la commande describe-account-limits(AWS CLI) pour Elastic Load Balancing.

Pour demander une augmentation de quota, consultez Demande d'augmentation de quota dans le Guide de l'utilisateur Service Quotas. Si le quota n'est pas encore disponible dans Service Quotas, soumettez une demande d'augmentation du quota de service.

Quotas

- Équilibreur de charge
- Groupes cibles
- Unités de capacité Load Balancer

Équilibreur de charge

Vous Compte AWS disposez des quotas suivants relatifs aux équilibreurs de charge réseau.

Nom	Par défaut	Ajustable
Certificats par Network Load Balancer	25	Oui
Écouteurs par Network Load Balancer	50	Non
Network Load Balancer ENIs par VPC	1 200 [1]	Oui
Équilibreurs de charge réseau par région	50	Oui
Cibles par zone de disponibilité et par Network Load Balancer	500 [2, 3]	Oui

Nom	Par défaut	Ajustable
Cibles par Network Load Balancer	3 000 ₃	Oui

¹ Chaque Network Load Balancer utilise une interface réseau par zone. Le quota est défini au niveau du VPC. Lors du partage de sous-réseaux ou de sous-réseaux VPCs, l'utilisation est calculée pour tous les locataires.

² Si une cible est enregistrée avec N groupes cibles, cela compte comme N cibles pour atteindre cette limite. Chaque Application Load Balancer étant une cible du Network Load Balancer compte comme 50 cibles si l'équilibrage de charge entre zones est désactivé ou 100 cibles si l'équilibrage de charge entre zones est activé.

³ Si l'équilibrage de charge entre zones est activé, le maximum est de 500 cibles par équilibreur de charge, quel que soit le nombre de zones de disponibilité.

Groupes cibles

Les quotas suivants sont destinés aux groupes cibles.

Nom	Par défaut	Ajustable
Groupes cibles par région	3 000 ¹	Oui
Cibles par groupe cible et par région (instances ou adresses IP)	1 000	Oui
Cibles par groupe cible et par région (Application Load Balancers)	1	Non

* Ce quota est partagé par les Application Load Balancers et les Network Load Balancers.

Unités de capacité Load Balancer

Les quotas suivants concernent les unités de capacité Load Balancer ()LCUs.

Nom	Par défaut	Ajustable
Unités de capacité réservées au Network Load Balancer (LCUs) par Network Load Balancer, par zone de disponibilité	45000	Oui
Unités de capacité Network Load Balancer (LCU) réservées par région	0	Oui

Historique du document pour les Network Load Balancers

Le tableau suivant décrit les versions des Network Load Balancers.

Modification	Description	Date
IPv4 Adresses secondaires	Cette version ajoute la prise en charge de l'ajout d' IPv4 adresses secondaires aux interfaces réseau de l'équilib reur de charge.	29 juillet 2025
Désactiver les zones de disponibilité	Cette version ajoute la prise en charge de la désactivation d'une zone de disponibilité pour un équilibreur de charge existant.	13 février 2025
Réservation de l'unité de capacité	Cette version ajoute un support permettant de définir une capacité minimale pour votre équilibreur de charge.	20 novembre 2024
Suppression du support UDP IPv6 pour les équilibreurs de charge à double pile	Cette version permet aux clients d'accéder aux applicati ons basées sur UDP à l'aide de. IPv6	31 octobre 2024
Certificats RSA 3072 bits et ECDSA 256/384/521 bits	Cette version ajoute la prise en charge des certificats RSA 3072 bits et des certificats ECDSA (Elliptic Curve Digital Signature Algorithm) 256, 384 et 521 bits via (ACM). AWS Certificate Manager	19 janvier 2024
Terminaison TLS FIPS 140-3	Cette version ajoute des politiques de sécurité qui	20 novembre 2023

	utilisent les modules cryptographiques FIPS 140-3 lors de la terminaison des connexions TLS.	
Affinité DNS zonale	Cette version permet aux clients de résoudre le DNS de l'équilibreur de charge pour recevoir une adresse IP dans la même zone de disponibilité (AZ) dans laquelle ils se trouvent.	12 octobre 2023
Désactiver la terminaison d'une connexion cible défectueuse	Cette version ajoute la prise en charge du maintien de connexions actives aux cibles qui échouent aux tests de santé.	12 octobre 2023
Fin de connexion UDP par défaut	Cette version ajoute la prise en charge de la résiliation des connexions UDP à la fin du délai de désenregistrement par défaut.	12 octobre 2023
Enregistrez les cibles à l'aide de IPv6	Cette version ajoute la prise en charge de l'enregistrement des instances en tant que cibles lorsqu'elles sont traitées par IPv6.	2 octobre 2023
Groupes de sécurité de votre Network Load Balancer	Cette version permet d'associer des groupes de sécurité à vos Network Load Balancers lors de leur création.	10 août 2023

État du groupe cible	Cette version permet de configurer le nombre ou le pourcentage minimal de cibles qui doivent être saines, ainsi que les actions entreprises par l'équilibreur de charge lorsque le seuil n'est pas atteint.	17 novembre 2022
Configuration d'une surveillance de l'état	Cette version apporte des améliorations à la configuration de la surveillance de l'état.	17 novembre 2022
Equilibrage de charge entre zones	Cette version ajoute la prise en charge de la configuration de l'équilibrage de charge entre zones au niveau du groupe cible.	17 novembre 2022
IPv6 groupes cibles	Cette version ajoute la prise en charge de la configuration de groupes IPv6 cibles pour les équilibreurs de charge réseau.	23 novembre 2021
IPv6 équilibreurs de charge internes	Cette version ajoute la prise en charge de la configuration de groupes IPv6 cibles pour les équilibreurs de charge réseau.	23 novembre 2021
TLS 1.3	Cette version ajoute des stratégies de sécurité prenant en charge la version 1.3 de TLS.	14 octobre 2021

Application Load Balancers en tant que cibles	Cette version permet de configurer un Application Load Balancer en tant que cible d'un Network Load Balancer.	27 septembre 2021
Préservation des adresses IP client	Cette version permet de configurer la préservation des adresses IP client.	4 février 2021
Stratégie de sécurité pour la confidentialité persistante prenant en charge la version 1.2 de TLS	Cette version ajoute une stratégie de sécurité pour la confidentialité persistante (FS, Forward Secrecy) prenant en charge TLS version 1.2.	24 novembre 2020
Mode double pile	Cette version ajoute la prise en charge du mode double pile, qui permet aux clients de se connecter à l'équilibreur de charge en utilisant à la fois des IPv4 adresses et IPv6 des adresses.	13 novembre 2020
Fin de connexion en cas d'annulation d'enregistrement	Cette version permet d'interrompre les connexions aux cibles dont l'enregistrement a été annulé après la fin du délai d'expiration de l'annulation d'enregistrement.	13 novembre 2020
Stratégies ALPN	Cette version ajoute la prise en charge des listes de préférences ALPN (Application-Layer Protocol Negotiation).	27 mai 2020

Sessions permanentes	Cette version prend désormais en charge les sessions permanentes basées sur les adresses IP source et le protocole.	28 février 2020
Sous-réseaux partagés	Cette version permet de spécifier des sous-réseaux partagés avec vous par un autre Compte AWS.	26 novembre 2019
Adresses IP privées	Cette version vous permet de fournir une adresse IP privée à partir de la plage d' IPv4 adresses du sous-réseau que vous spécifiez lorsque vous activez une zone de disponibilité pour un équilibreur de charge interne.	25 novembre 2019
Ajout de sous-réseaux	Cette version ajoute la prise en charge de l'activation de zones de disponibilité supplémentaires après la création de votre équilibreur de charge.	25 novembre 2019
Politiques de sécurité pour FS	Cette version ajoute la prise en charge de trois politiques de sécurité de confidentialité prédéfinies supplémentaires.	8 octobre 2019
Prise en charge de SNI	Cette version ajoute la prise en charge de Server Name Indication (SNI).	12 septembre 2019
Protocole UDP	Cette version ajoute la prise en charge du protocole TLS.	24 juin 2019

Disponible dans une nouvelle région	Cette version ajoute la prise en charge des équilibreurs de charge réseau dans la région Asie-Pacifique (Osaka).	12 juin 2019
Protocole TLS	Cette version ajoute la prise en charge du protocole TLS.	24 janvier 2019
Équilibrage de charge entre zones	Cette version ajoute la prise en charge pour l'activation de l'équilibrage de charge entre zones.	le 22 février 2018
Protocole proxy	Cette version ajoute la prise en charge de l'activation du protocole proxy.	17 novembre 2017
Adresses IP en tant que cibles	Cette version prend en charge l'enregistrement d'adresses IP en tant que cibles.	21 septembre 2017
Nouveau type d'équilibreur de charge	Cette version d'Elastic Load Balancing introduit les Network Load Balancers.	7 septembre 2017

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.