aws

Guide de l’utilisateur

Amazon VPC Lattice

Amazon VPC Lattice: Guide de l’utilisateur

Table of Contents

Qu'est-ce qu'Amazon VPC Lattice ?

Amazon VPC Lattice est un service de mise en réseau d'applications entièrement géré que vous utilisez pour connecter, sécuriser et surveiller les services de votre application. Vous pouvez utiliser VPC Lattice avec un seul cloud privé virtuel (VPC) ou sur plusieurs VPC à partir d'un ou de plusieurs comptes.

Les applications modernes peuvent consister en plusieurs petits services modulaires, souvent appelés microservices. Bien que la modernisation présente des avantages, elle peut également introduire des complexités et des défis en matière de réseau lorsque vous connectez ces microservices. Par exemple, si les développeurs sont répartis dans différentes équipes, ils peuvent créer et déployer des microservices sur plusieurs comptes ou VPC.

Dans VPC Lattice, nous faisons référence à un microservice en tant que service. C'est le libellé que vous voyez dans la documentation de VPC Lattice.

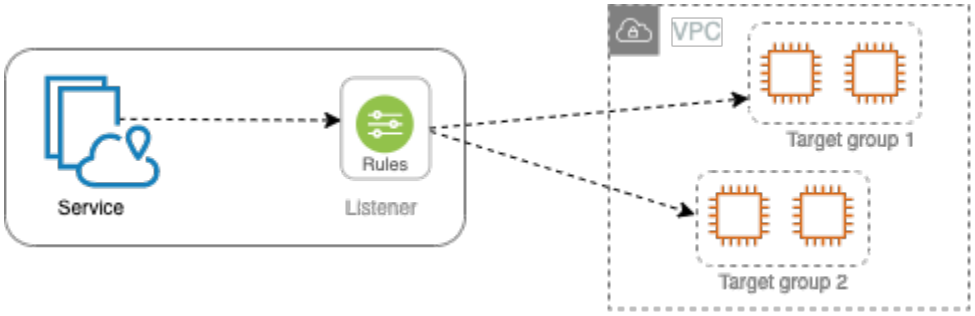
Table des matières

Composants clés

Pour utiliser Amazon VPC Lattice, vous devez connaître ses principaux composants.

Service

> Unité logicielle déployable indépendamment qui exécute une tâche ou une fonction spécifique. Un service peut être exécuté sur des instances EC2 ou des conteneurs ECS, ou en tant que fonctions Lambda, au sein d'un compte ou d'un cloud privé virtuel (VPC). Un service VPC Lattice comporte les composants suivants : groupes cibles, auditeurs et règles.



Groupe cible

Ensemble de ressources, également appelées cibles, qui exécutent votre application ou votre service. Les cibles peuvent être des instances EC2, des adresses IP, des fonctions Lambda, des équilibreurs de charge d'application ou des pods Kubernetes. Ils sont similaires aux groupes cibles fournis par Elastic Load Balancing, mais ils ne sont pas interchangeables.

Listener

Processus qui vérifie les demandes de connexion et les achemine vers les cibles d'un groupe cible. Un service peut avoir jusqu'à deux écouteurs, utilisant les protocoles HTTP et HTTPS et des numéros de port compris entre 1 et 65535.

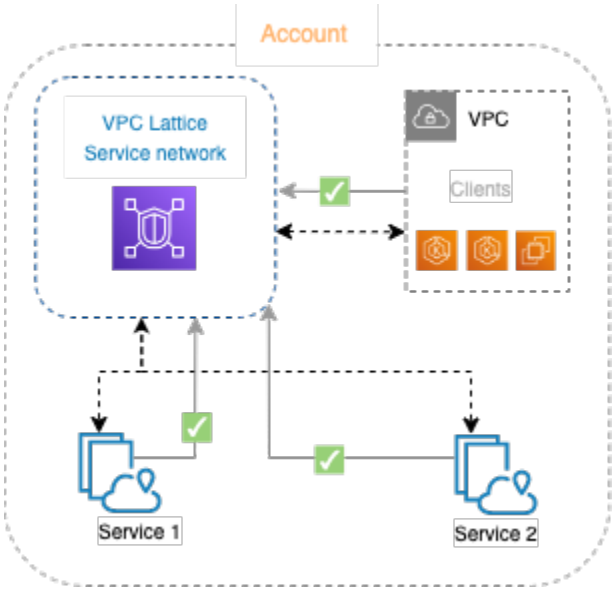
Règle

Composant par défaut d'un écouteur qui transmet les demandes aux cibles d'un groupe cible VPC Lattice. Chaque règle comprend une priorité, une ou plusieurs actions et une ou plusieurs conditions. Les règles déterminent la manière dont l'écouteur achemine les demandes des clients.

Réseau de services

Une limite logique pour un ensemble de services. Un client est une ressource déployée dans un VPC associée au réseau de services. Les clients et les services associés au même réseau de services peuvent communiquer entre eux s'ils y sont autorisés.

Dans la figure suivante, les clients peuvent communiquer avec les deux services, car le VPC et les services sont associés au même réseau de services.



Répertoire des services

Un registre central de tous les services VPC Lattice que vous possédez ou que vous partagez avec votre compte via AWS Resource Access Manager ().AWS RAM

Politiques d'authentification

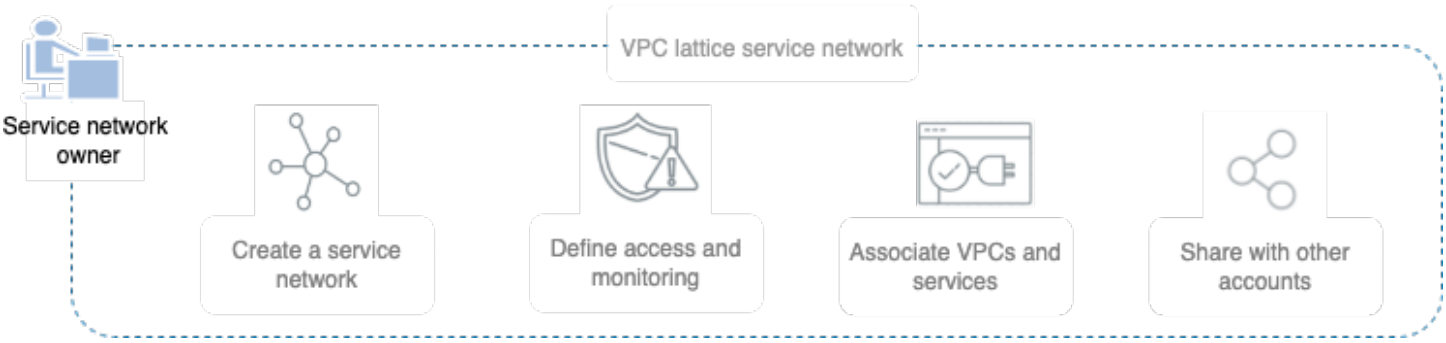
Politiques d'autorisation précises qui peuvent être utilisées pour définir l'accès aux services. Vous pouvez associer des politiques d'authentification distinctes à des services individuels ou au réseau de services. Par exemple, vous pouvez créer une politique concernant la manière dont un service de paiement exécuté sur un groupe d'instances EC2 à dimensionnement automatique doit interagir avec un service de facturation intégré. AWS Lambda

Rôles et responsabilités

Un rôle détermine qui est responsable de la configuration et du flux d'informations au sein d'Amazon VPC Lattice. Il existe généralement deux rôles, celui de propriétaire du réseau de services et celui de propriétaire du service, et leurs responsabilités peuvent se chevaucher.

Propriétaire du réseau de services : le propriétaire du réseau de services est généralement l'administrateur réseau ou l'administrateur cloud d'une organisation. Les propriétaires de réseaux de services créent, partagent et fournissent le réseau de service. Ils gèrent également qui peut accéder au réseau de services ou aux services au sein de VPC Lattice. Le propriétaire du réseau de service peut définir des paramètres d'accès grossiers pour les services associés au réseau de service. Ces contrôles sont utilisés pour gérer les communications entre les clients et les services à l'aide de

politiques d'authentification et d'autorisation. Le propriétaire du réseau de service peut également associer un service au réseau de service, si le service est partagé avec le compte du propriétaire du réseau de service.



Propriétaire du service — Le propriétaire du service est généralement un développeur de logiciels au sein d'une organisation. Les propriétaires de services créent des services au sein de VPC Lattice, définissent des règles de routage et associent également des services au réseau de services. Ils peuvent également définir des paramètres d'accès précis, qui peuvent restreindre l'accès aux seuls services et clients authentifiés et autorisés.

Fonctionnalités

Voici les principales fonctionnalités fournies par VPC Lattice.

Découverte de service

Tous les clients et services des VPC associés au réseau de services peuvent communiquer avec d'autres services au sein du même réseau de services. Directions DNS client-to-service et service-to-service trafic via le point de terminaison VPC Lattice. Lorsqu'un client souhaite envoyer une demande à un service, il utilise le nom DNS du service. Le résolveur Route 53 envoie le trafic à VPC Lattice, qui identifie ensuite le service de destination.

Connectivité

lient-to-service La connectivité C est établie à l'aide du plan de données VPC Lattice au sein de l' AWS infrastructure réseau. Lorsque vous associez un VPC au réseau de services, tous les clients du VPC peuvent se connecter aux services du réseau de services, s'ils disposent de l'accès requis.

Observabilité

VPC Lattice génère des métriques et des journaux pour chaque demande et réponse traversant le réseau de services, afin de vous aider à surveiller et à dépanner les applications. Par défaut, VPC Lattice publie les métriques dans le compte du propriétaire du service et vous donne la possibilité d'activer la journalisation. Si les clients sont également associés au même réseau de service, le propriétaire du réseau de service reçoit les journaux de tous les services associés au réseau de service. Le propriétaire du service reçoit les journaux de tous les clients qui font des demandes à son service.

VPC Lattice utilise les outils suivants pour vous aider à surveiller et à dépanner vos services : CloudWatch groupes de journaux, flux de diffusion Firehose et compartiments S3.

Sécurité

VPC Lattice fournit un cadre que vous pouvez utiliser pour mettre en œuvre une stratégie de défense sur plusieurs couches du réseau. La première couche est l'association entre le service et le VPC. Sans association de VPC et de service, les clients ne peuvent pas accéder au service. La deuxième couche permet aux utilisateurs d'associer des groupes de sécurité à l'association entre le VPC et le réseau de services. Les troisième et quatrième couches sont des politiques d'authentification qui peuvent être appliquées individuellement au niveau du réseau de service et au niveau du service.

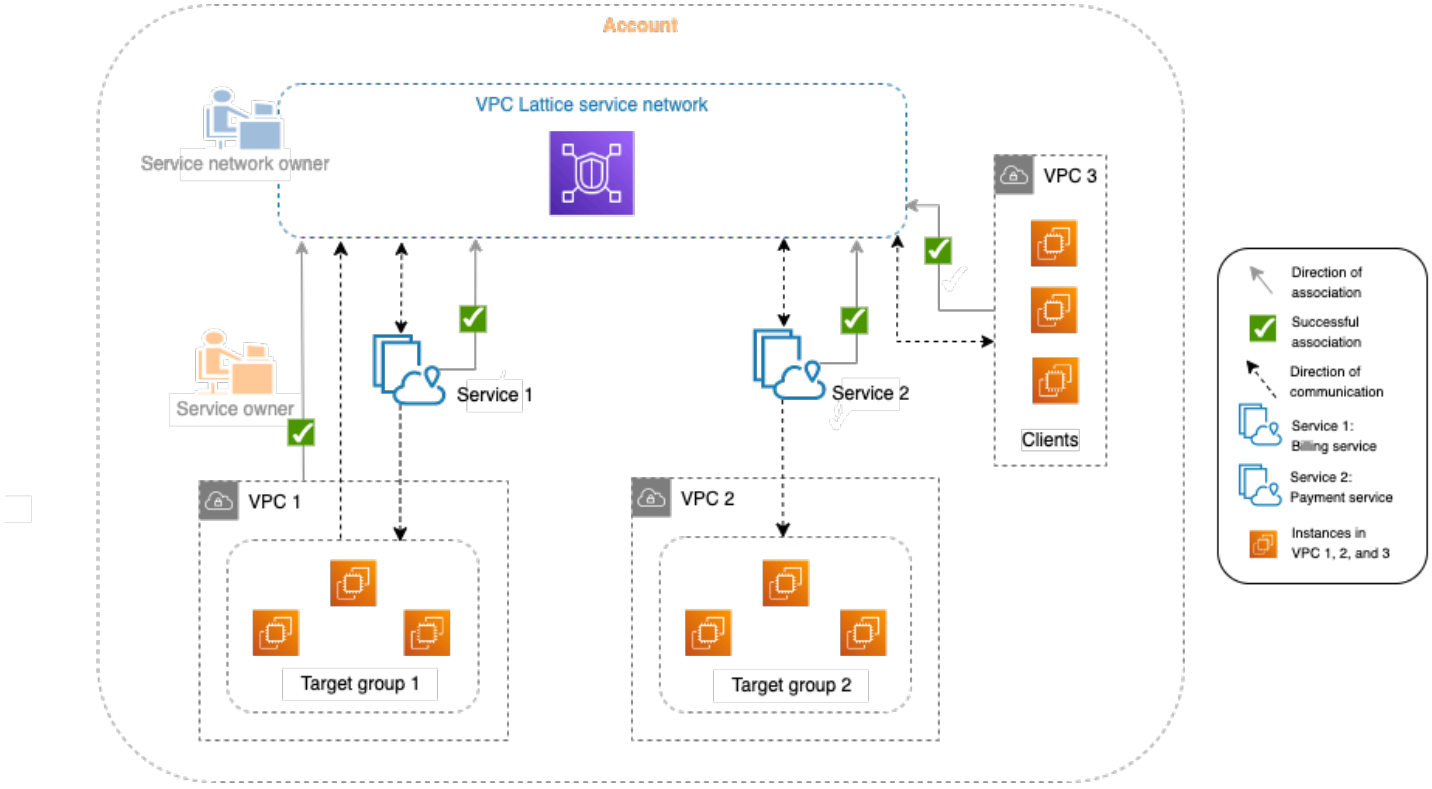
Comment fonctionne le VPC Lattice

VPC Lattice est conçu pour vous aider à découvrir, sécuriser, connecter et surveiller facilement et efficacement tous les services qu'il contient. Chaque composant de VPC Lattice communique de manière unidirectionnelle ou bidirectionnelle au sein du réseau de service en fonction de son association avec le réseau de service et de ses paramètres d'accès. Les paramètres d'accès comprennent les politiques d'authentification et d'autorisation requises pour cette communication.

Le résumé suivant décrit la communication entre les composants au sein de VPC Lattice :

- Les services associés au réseau de services peuvent recevoir des demandes de clients dont les VPC sont également associés au réseau de services.
- Un client peut envoyer des demandes aux services associés à un réseau de services uniquement s'il se trouve dans un VPC associé au même réseau de services. Le trafic client qui traverse une connexion d'appairage de VPC ou une passerelle de transit est refusé.
- Un client ne peut pas envoyer de demandes aux clients d'autres VPC associés au réseau de service.
- Les cibles des services dans les VPC associés au réseau de services sont également des clients et peuvent envoyer des demandes à d'autres services associés au réseau de services.
- Les cibles des services des VPC qui ne sont pas associés au réseau de services ne sont pas des clients et ne peuvent pas envoyer de demandes à d'autres services associés au réseau de services.

Le schéma de flux suivant utilise un exemple de scénario pour expliquer le flux d'informations et le sens de la communication entre les composants au sein de VPC Lattice. Deux services sont associés à un réseau de services. Les deux services et les trois VPC ont été créés dans le même compte que le réseau de services. Les deux services sont configurés pour autoriser le trafic provenant du réseau de service.



Le service 1 est une application de facturation exécutée sur un groupe d'instances enregistrées auprès du groupe cible 1 dans le VPC 1. Le service 2 est une application de paiement exécutée sur un groupe d'instances enregistrées auprès du groupe cible 2 dans le VPC 2. Le VPC 3 est dans le même compte, et il a des clients mais aucun service.

La liste suivante décrit, dans l'ordre, le flux de travail typique des tâches pour VPC Lattice.

1. Création d'un réseau de services

   Le propriétaire du réseau de service crée le réseau de service.

2. Créer un service

   Les propriétaires de services créent leurs services respectifs, le service 1 et le service 2. Lors de la création, le propriétaire du service ajoute des écouteurs et définit des règles d'acheminement des demandes vers le groupe cible pour chaque service.

3. Définir le routage

   Les propriétaires du service créent le groupe cible pour chaque service (groupe cible 1 et groupe cible 2). Pour ce faire, ils spécifient les ressources ciblées sur lesquelles les services s'exécutent, par exemple les instances. Ils spécifient également les VPC dans lesquels résident ces cibles.

   Dans le schéma précédent, les flèches en pointillés qui pointent vers les groupes cibles des services représentent le trafic circulant de chaque service vers son groupe cible respectif. Les flèches en pointillés indiquent le sens de communication entre le service et le groupe cible.

4. Associer des services au réseau de services

   Le propriétaire du réseau de service ou le propriétaire du service associe les services au réseau de services. Les associations apparaissent sous forme de flèches cochées pointant vers le réseau de service depuis le service. Lorsque vous associez un service à un réseau de services, ce service peut être découvert par d'autres services et clients dans les VPC associés au réseau de services.

   Les flèches en pointillés bidirectionnelles entre le service et le réseau de service représentent la communication bidirectionnelle résultant de l'association. Les flèches en pointillés reliant le réseau de services aux services représentent les services recevant des demandes de clients. Les flèches en pointillés dans le sens opposé, c'est-à-dire entre les services et le réseau de services, représentent les services répondant aux demandes des clients via le réseau de services.

5. Associer des VPC au réseau de services

Le propriétaire du réseau de service associe le VPC 1 et le VPC 3 au réseau de service. Les associations sont représentées par des flèches cochées pointées vers le réseau de service. Grâce à ces associations, les cibles de ces VPC deviennent des clients et peuvent adresser des demandes aux services associés. La flèche bidirectionnelle en pointillés entre le VPC 3 et le réseau de service représente la communication bidirectionnelle entre les clients (par exemple, les instances) du VPC 3 et le réseau de service résultant de l'association. De même, la flèche en pointillés pointant du groupe cible 1 vers le réseau de services représente les clients faisant des demandes à d'autres services associés au réseau de services.

Notez que le VPC 2 n'a pas de flèche ou de coche représentant une association. Cela signifie que le propriétaire du réseau de service ou le propriétaire du service n'a pas associé le VPC 2 au réseau de service. Cela est dû au fait que le service 2, dans cet exemple, n'a besoin que de recevoir des demandes et d'envoyer des réponses en utilisant la même demande. En d'autres termes, les cibles du service 2 ne sont pas les clients et il n'est pas nécessaire de faire des demandes aux autres services du réseau de services.

Accès à VPC Lattice

Vous pouvez créer, accéder et gérer VPC Lattice à l'aide de l'une des interfaces suivantes :

- AWS Management Console— Fournit une interface Web que vous pouvez utiliser pour accéder à VPC Lattice.
- AWS Command Line Interface (AWS CLI) — Fournit des commandes pour un large éventail de AWS services, y compris VPC Lattice. AWS CLI Il est pris en charge sur Windows, macOS et Linux. Pour plus d'informations sur la CLI, consultez AWS Command Line Interface. Pour plus d'informations sur les API, consultez le manuel Amazon VPC Lattice API Reference.
- Contrôleur VPC Lattice pour Kubernetes : gère les ressources VPC Lattice pour un cluster Kubernetes. Pour plus d'informations sur l'utilisation de VPC Lattice avec Kubernetes, consultez le guide de l'utilisateur duAWS Gateway API Controller.
- AWS CloudFormation— Vous aide à modéliser et à configurer vos AWS ressources. Pour plus d'informations, consultez la référence du type de ressource Amazon VPC Lattice.

Tarification

Avec VPC Lattice, vous payez en fonction de la durée de mise en service d'un service, de la quantité de données transférée via chaque service et du nombre de demandes. Pour plus d'informations, consultez la section Tarification d'Amazon VPC Lattice.

Configuration d'Amazon VPC Lattice

Effectuez les tâches décrites dans cette section pour configurer et lancer VPC Lattice pour la première fois :

Tâches

- Inscrivez-vous pour AWS
- Créer un utilisateur IAM

Inscrivez-vous pour AWS

Lorsque vous vous inscrivez à Amazon Web Services, vous Compte AWS êtes automatiquement enregistré pour utiliser tous les services AWS, y compris VPC Lattice. Seuls les services que vous utilisez vous sont facturés.

Si vous en avez Compte AWS déjà un, passez à la tâche suivante. Si vous n'avez pas de Compte AWS, utilisez la procédure suivante pour en créer un.

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

Créer un utilisateur IAM

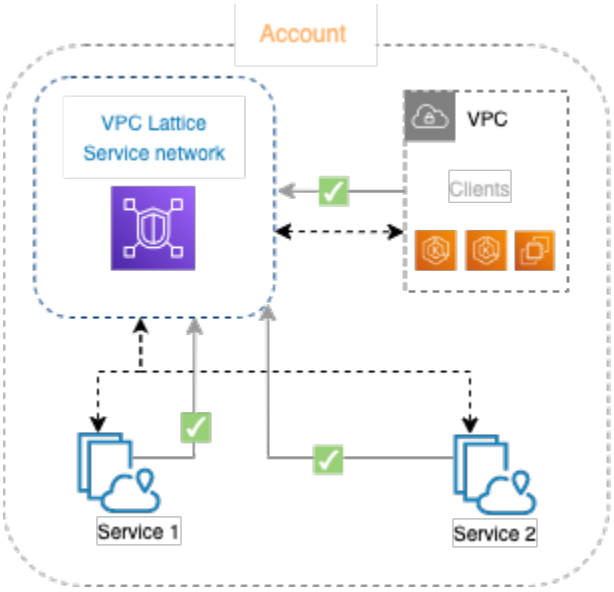
Afin de créer un utilisateur administrateur, choisissez l'une des options suivantes :

Choisissez un moyen de gérer votre administrateur	Pour	Par	Vous pouvez également
Dans IAM Identity Center (Recommandé)	Utiliser des identifiants à court terme pour accéder à AWS. Telles sont les meilleures pratiques en matière de sécurité. Pour plus d'informations sur les bonnes pratiques, veuillez consulter Security best practices in IAM (français non garanti) dans le Guide de l'utilisateur IAM.	Suivre les instructions de la section Mise en route dans le AWS IAM Identity Center Guide de l'utilisateur.	Configurez l'accès par programmation en configurant le AWS CLI à utiliser AWS IAM Identity Center dans le guide de l'AWS Command Line Interface utilisateur.
Dans IAM (Non recommandé)	Utiliser des identifiants à long terme pour accéder à AWS.	Suivre les instructions relatives à la Création de votre premier groupe utilisateur administrateur et utilisateur IAM dans le Guide de l'utilisateur IAM.	Configuration de l'accès par programmation via la Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Réseaux de service en VPC Lattice

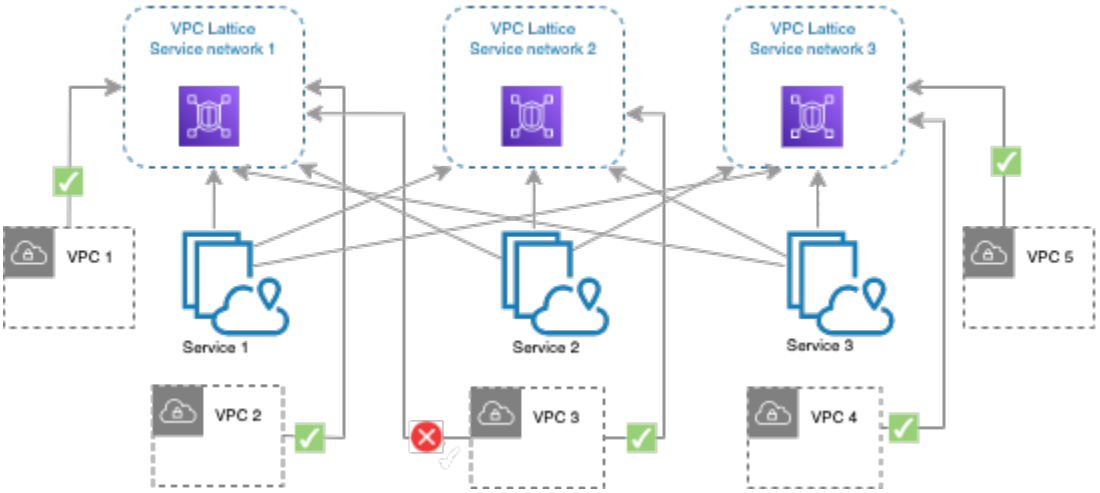
Un réseau de services est une limite logique pour un ensemble de services. Les services associés au réseau peuvent être autorisés à des fins de découverte, de connectivité, d'accessibilité et d'observabilité. Pour envoyer des demandes aux services du réseau, votre service ou client doit se trouver dans un VPC associé au réseau de services.

Le schéma suivant montre les composants clés d'un réseau de services typique au sein d'Amazon VPC Lattice. Les flèches sont cochées pour indiquer que les services et le VPC sont associés au réseau de services. Les clients du VPC associé au réseau de services peuvent communiquer avec les deux services via le réseau de services.



Vous pouvez associer un ou plusieurs services à plusieurs réseaux de services. Vous pouvez également associer plusieurs VPC à un réseau de services. Cependant, chaque VPC ne peut être associé qu'à un seul réseau de services.

Dans le schéma suivant, les flèches représentent les associations entre les services et les réseaux de services, ainsi que les associations entre les VPC et les réseaux de services. Vous pouvez constater que plusieurs services sont associés à plusieurs réseaux de services et que plusieurs VPC sont associés à chaque réseau de services. Cependant, le point X rouge sur le schéma indique que chaque VPC ne peut être associé qu'une seule fois à un réseau de services.



Pour de plus amples informations, veuillez consulter Quotas pour Amazon VPC Lattice.

Création d'un réseau de services

Utilisez la console pour créer un réseau de services et le configurer éventuellement avec des services, des associations, des paramètres d'accès et des journaux d'accès.

Pour créer un réseau de service à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Service networks.
3. Choisissez Créer un réseau de services.
4. Pour Identifiants, entrez un nom, une description facultative et des balises facultatives. Le nom doit comporter entre 3 et 63 caractères. Vous pouvez utiliser des lettres minuscules, des chiffres et des traits d'union. Le nom doit commencer et se terminer par une lettre ou un chiffre. N'utilisez pas de tirets consécutifs. La description peut comporter jusqu'à 256 caractères. Pour ajouter une balise, choisissez Ajouter une nouvelle balise et spécifiez une clé de balise et une valeur de balise.
5. (Facultatif) Pour associer un service, choisissez-le dans Associations de services, Services. La liste inclut les services présents dans votre compte et tous les services partagés avec vous à partir d'un autre compte. S'il n'y a aucun service dans la liste, vous pouvez créer un service en choisissant Create an VPC Lattice service.

   Vous pouvez également associer un service après avoir créé le réseau de services, voirthe section called "Gérer les associations de services".

6. (Facultatif) Pour associer un VPC, choisissez Ajouter une association VPC. Sélectionnez le VPC à associer à partir du VPC, puis sélectionnez jusqu'à cinq groupes de sécurité dans Groupes de sécurité. Pour créer un groupe de sécurité, choisissez Créer un nouveau groupe de sécurité.

   Vous pouvez également associer des VPC après avoir créé le réseau de service, consultezthe section called "Gérer les associations de VPC".

7. Pour l'accès au réseau, vous pouvez laisser le type d'authentification par défaut, None, si vous souhaitez que les clients des VPC associés accèdent aux services de ce réseau de services. Pour appliquer une politique d'authentification afin de contrôler l'accès à vos services, choisissez AWS IAM et effectuez l'une des opérations suivantes pour la politique d'authentification :

   - Entrez une politique dans le champ de saisie. Par exemple, des politiques que vous pouvez copier et coller, choisissez Exemples de politiques.
   - Choisissez Appliquer le modèle de politique et sélectionnez le modèle Autoriser les accès authentifiés et non authentifiés. Ce modèle permet à un client d'accéder au service depuis un autre compte soit en signant la demande (c'est-à-dire authentifié), soit de manière anonyme (c'est-à-dire non authentifié).
   - Choisissez Appliquer le modèle de politique et sélectionnez le modèle Autoriser uniquement l'accès authentifié. Ce modèle permet à un client d'un autre compte d'accéder au service uniquement en signant la demande (c'est-à-dire authentifiée).

8. (Facultatif) Pour activer les journaux d'accès, sélectionnez le commutateur Logs d'accès et spécifiez une destination pour vos journaux d'accès comme suit :

   - Sélectionnez Groupe de CloudWatch journaux, puis choisissez un groupe de CloudWatch journaux. Pour créer un groupe de journaux, choisissez Create a log group in CloudWatch.
   - Sélectionnez le compartiment S3 et entrez le chemin du compartiment S3, y compris tout préfixe. Pour effectuer une recherche dans vos compartiments S3, choisissez Browse S3.
   - Sélectionnez le flux de diffusion Kinesis Data Firehose, puis choisissez un flux de diffusion. Pour créer un flux de diffusion, choisissez Créer un flux de diffusion dans Kinesis.

9. (Facultatif) Pour partager votre réseau de service avec d'autres comptes, choisissez les partages de AWS RAM ressources dans Partages de ressources. Pour créer un partage de ressources, choisissez Créer un partage de ressources dans la console RAM.

10. Passez en revue votre configuration dans la section Résumé, puis choisissez Create service network.

Pour créer un réseau de service à l'aide du AWS CLI

Utilisez la commande create-service-network. Cette commande crée uniquement le réseau de service de base. Pour créer un réseau de services entièrement fonctionnel, vous devez également utiliser les commandes qui créent des associations de services, des associations VPC et des paramètres d'accès.

Gérer les associations d'un réseau de services

Lorsque vous associez un service au réseau de services, cela permet aux clients (ressources d'un VPC associé au réseau de services) d'adresser des demandes au service. Lorsque vous associez un VPC au réseau de services, toutes les cibles de ce VPC peuvent être des clients et communiquer avec d'autres services du réseau de services.

Table des matières

Gérer les associations de services

Vous pouvez associer des services qui se trouvent dans votre compte ou des services partagés avec vous à partir de différents comptes. Il s'agit d'une étape facultative lors de la création d'un réseau de service. Toutefois, un réseau de service n'est pas entièrement fonctionnel tant que vous n'associez pas un service. Les propriétaires de services peuvent associer leurs services à un réseau de services si leur compte dispose de l'accès requis. Pour de plus amples informations, veuillez consulter Comment fonctionne le VPC Lattice.

Lorsque vous supprimez une association de services, le service ne peut plus se connecter aux autres services du réseau de services.

Pour gérer les associations de services à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Service networks.
3. Sélectionnez le nom du réseau de service pour ouvrir sa page de détails.
4. Choisissez l'onglet Associations de services.
5. Pour créer une association, procédez comme suit :

    a. Choisissez Créer des associations.

b. Sélectionnez un service dans Services. Pour créer un service, choisissez Create an Amazon VPC Lattice service.

c. (Facultatif) Pour ajouter une balise, développez les balises d'association de services, choisissez Ajouter une nouvelle balise, puis entrez une clé de balise et une valeur de balise.

d. Sélectionnez Enregistrer les modifications.

6. Pour supprimer une association, cochez la case correspondante, puis choisissez Actions, Supprimer les associations de services. Lorsque vous êtes invité à confirmer, entrez **`confirm`**, puis choisissez Delete (Supprimer).

Pour créer une association de services à l'aide du AWS CLI

Utilisez la commande create-service-network-service-association.

Pour supprimer une association de services à l'aide du AWS CLI

Utilisez la commande delete-service-network-service-association.

Gérer les associations de VPC

Les clients peuvent envoyer des demandes aux services associés au réseau de services uniquement s'ils se trouvent dans des VPC associés au réseau de services. Le trafic client qui traverse une connexion d'appairage de VPC ou une passerelle de transit est refusé.

L'association d'un VPC est une étape facultative lorsque vous créez un réseau de services. Toutefois, le réseau de service n'est pas entièrement fonctionnel tant que vous n'associez pas un VPC. Les propriétaires de réseaux peuvent associer des VPC à un réseau de services si leur compte dispose de l'accès requis. Pour de plus amples informations, veuillez consulter Comment fonctionne le VPC Lattice.

Lorsque vous supprimez une association VPC, les clients des VPC ne peuvent plus se connecter aux services du réseau de services.

Pour gérer les associations de VPC à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Service networks.
3. Sélectionnez le nom du réseau de service pour ouvrir sa page de détails.

4. Choisissez l'onglet Associations VPC.
5. Pour créer une association VPC, procédez comme suit :
   a. Choisissez Create VPC associations.
   b. Choisissez Ajouter une association VPC.
   c. Sélectionnez un VPC dans un VPC et sélectionnez jusqu'à cinq groupes de sécurité dans Groupes de sécurité. Pour créer un groupe de sécurité, choisissez Créer un nouveau groupe de sécurité.
   d. (Facultatif) Pour ajouter une balise, développez les balises d'association VPC, choisissez Ajouter une nouvelle balise, puis entrez une clé de balise et une valeur de balise.
   e. Sélectionnez Enregistrer les modifications.
6. Pour modifier les groupes de sécurité d'une association, cochez la case correspondante, puis choisissez Actions, Modifier les groupes de sécurité. Ajoutez et supprimez des groupes de sécurité selon vos besoins.
7. Pour supprimer une association, cochez la case correspondante, puis choisissez Actions, Supprimer les associations VPC. Lorsque vous êtes invité à confirmer, entrez **`confirm`**, puis choisissez Delete (Supprimer).

Pour créer une association VPC à l'aide du AWS CLI

Utilisez la commande create-service-network-vpc-association.

Pour mettre à jour les groupes de sécurité d'une association VPC à l'aide du AWS CLI

Utilisez la commande update-service-network-vpc-association.

Pour supprimer une association VPC à l'aide du AWS CLI

Utilisez la commande delete-service-network-vpc-association.

Modifier les paramètres d'accès pour un réseau de service

Les paramètres d'accès vous permettent de configurer et de gérer l'accès des clients à un réseau de services. Les paramètres d'accès incluent le type d'authentification et les politiques d'authentification. Les politiques d'authentification vous aident à authentifier et à autoriser le trafic circulant vers les services au sein de VPC Lattice.

Vous pouvez appliquer des politiques d'authentification au niveau du réseau de service, au niveau du service ou aux deux. Généralement, les politiques d'authentification sont appliquées par les propriétaires du réseau ou les administrateurs du cloud. Ils peuvent mettre en œuvre une autorisation basée sur le cours, par exemple en autorisant les appels authentifiés provenant de l'organisation ou en autorisant les demandes GET anonymes répondant à certaines conditions. Au niveau du service, les propriétaires de services peuvent appliquer des contrôles précis, qui peuvent être plus restrictifs. Pour de plus amples informations, veuillez consulter Contrôlez l'accès aux services à l'aide de politiques d'authentification.

Pour ajouter ou mettre à jour des politiques d'accès à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Service networks.
3. Sélectionnez le nom du réseau de service pour ouvrir sa page de détails.
4. Cliquez sur l'onglet Accès pour vérifier les paramètres d'accès actuels.
5. Pour mettre à jour les paramètres d'accès, choisissez Modifier les paramètres d'accès.
6. Si vous souhaitez que les clients des VPC associés accèdent aux services de ce réseau de services, choisissez Aucun pour le type d'authentification.
7. Pour appliquer une politique de ressources au réseau de service, choisissez AWS IAM pour le type d'authentification et effectuez l'une des opérations suivantes pour la stratégie d'authentification :
   - Entrez une politique dans le champ de saisie. Par exemple, des politiques que vous pouvez copier et coller, choisissez Exemples de politiques.
   - Choisissez Appliquer le modèle de politique et sélectionnez le modèle Autoriser les accès authentifiés et non authentifiés. Ce modèle permet à un client d'accéder au service depuis un autre compte soit en signant la demande (c'est-à-dire authentifié), soit de manière anonyme (c'est-à-dire non authentifié).
   - Choisissez Appliquer le modèle de politique et sélectionnez le modèle Autoriser uniquement l'accès authentifié. Ce modèle permet à un client d'un autre compte d'accéder au service uniquement en signant la demande (c'est-à-dire authentifiée).
8. Sélectionnez Enregistrer les modifications.

Pour ajouter ou mettre à jour une politique d'accès à l'aide du AWS CLI

Utilisez la commande put-auth-policy.

Modifier les détails de surveillance d'un réseau de services

VPC Lattice génère des métriques et des journaux pour chaque demande et réponse, ce qui permet de surveiller et de dépanner les applications plus efficacement.

Vous pouvez activer les journaux d'accès et spécifier la ressource de destination pour vos journaux. VPC Lattice peut envoyer des journaux aux ressources suivantes : groupes de CloudWatch journaux, flux de diffusion Firehose et compartiments S3.

Pour activer les journaux d'accès ou mettre à jour une destination de journal à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Service networks.
3. Sélectionnez le nom du réseau de service pour ouvrir sa page de détails.
4. Sélectionnez l'onglet Monitoring (Surveillance). Consultez les journaux d'accès pour voir si les journaux d'accès sont activés.
5. Pour activer ou désactiver les journaux d'accès, choisissez Modifier les journaux d'accès, puis activez ou désactivez le bouton des journaux d'accès.
6. Lorsque vous activez les journaux d'accès, vous devez sélectionner le type de destination de livraison, puis créer ou choisir la destination des journaux d'accès. Vous pouvez également modifier la destination de livraison à tout moment. Par exemple :
   - Sélectionnez Groupe de CloudWatch journaux, puis choisissez un groupe de CloudWatch journaux. Pour créer un groupe de journaux, choisissez Create a log group in CloudWatch.
   - Sélectionnez le compartiment S3 et entrez le chemin du compartiment S3, y compris tout préfixe. Pour effectuer une recherche dans vos compartiments S3, choisissez Browse S3.
   - Sélectionnez le flux de diffusion Kinesis Data Firehose, puis choisissez un flux de diffusion. Pour créer un flux de diffusion, choisissez Créer un flux de diffusion dans Kinesis.
7. Sélectionnez Enregistrer les modifications.

Pour activer les journaux d'accès à l'aide du AWS CLI

Utilisez la commande create-access-log-subscription.

Pour mettre à jour la destination du journal à l'aide du AWS CLI

Utilisez la commande update-access-log-subscription.

Pour désactiver les journaux d'accès à l'aide du AWS CLI

Utilisez la commande delete-access-log-subscription.

Gestion des balises pour un réseau de services

Les balises vous aident à classer votre réseau de services de différentes manières, par exemple par objectif, propriétaire ou environnement.

Vous pouvez ajouter plusieurs balises à chaque réseau de service. Les clés de balise doivent être uniques pour chaque réseau de service. Si vous ajoutez une balise avec une clé déjà associée au réseau de service, la valeur de cette balise est mise à jour. Vous pouvez utiliser des caractères tels que des lettres, des espaces, des chiffres (en UTF-8) et les caractères spéciaux suivants : + - =. _ : / @. N'utilisez pas d'espaces de début ou de fin. Les valeurs de balise sont sensibles à la casse.

Pour ajouter ou supprimer des balises à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Service networks.
3. Sélectionnez le nom du réseau de service pour ouvrir sa page de détails.
4. Sélectionnez l'onglet Tags (Identifications).
5. Pour ajouter une étiquette, choisissez Ajouter des balises et entrez la clé et la valeur de la balise. Pour ajouter une autre balise, choisissez Ajouter une nouvelle balise. Après avoir ajouter les identifications, choisissez Enregistrer les modifications.
6. Pour supprimer une étiquette, cochez la case correspondante et choisissez Supprimer. Lorsque vous êtes invité à confirmer, entrez **`confirm`**, puis choisissez Delete (Supprimer).

Pour ajouter ou supprimer des balises à l'aide du AWS CLI

Utilisez les commandes tag-resource et untag-resource.

Supprimer un réseau de service

Avant de pouvoir supprimer un réseau de service, vous devez d'abord supprimer toutes les associations que le réseau de service peut avoir avec un service ou un VPC. Lorsque vous supprimez un réseau de service, nous supprimons également toutes les ressources associées

au réseau de service, telles que la politique de ressources, la politique d'authentification et les abonnements aux journaux d'accès.

Pour supprimer un réseau de service à l'aide de la console

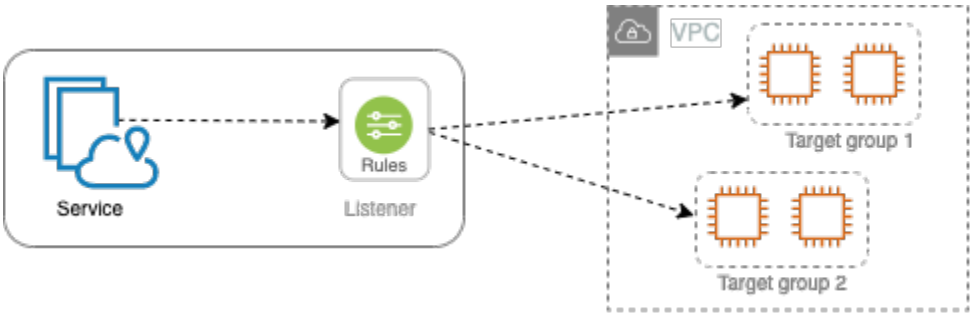
1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Service networks.
3. Cochez la case correspondant au réseau de service, puis choisissez Actions, Supprimer le réseau de service.
4. Lorsque vous êtes invité à confirmer, saisissez **`confirm`**, puis choisissez Delete (Supprimer).

Pour supprimer un réseau de service à l'aide du AWS CLI

Utilisez la commande delete-service-network.

Services en VPC Lattice

Un service au sein de VPC Lattice est une unité logicielle déployable indépendamment qui fournit une tâche ou une fonction spécifique. Un service peut être exécuté sur des instances, des conteneurs ou en tant que fonctions sans serveur au sein d'un compte ou d'un cloud privé virtuel (VPC). Un service possède un écouteur qui utilise des règles, appelées règles d'écouteur, que vous pouvez configurer pour aider à acheminer le trafic vers vos cibles. Les cibles peuvent être des instances EC2, des adresses IP, des fonctions Lambda sans serveur, des équilibreurs de charge d'application ou des pods Kubernetes. Pour plus d'informations, consultez Groupes cibles dans VPC Lattice. Vous pouvez associer un service à plusieurs réseaux de services. Le schéma suivant montre les composants clés d'un service typique au sein de VPC Lattice.



Vous pouvez créer un service en lui donnant un nom et une description. Toutefois, pour contrôler et surveiller le trafic vers votre service, il est important d'inclure les paramètres d'accès et les détails de surveillance. Pour envoyer le trafic de votre service vers vos cibles, vous devez configurer un écouteur et des règles. Pour permettre au trafic de circuler du réseau de service vers votre service, vous devez associer votre service au réseau de service.

Il existe un délai d'inactivité et un délai de connexion global pour les connexions aux cibles. Le délai d'inactivité de la connexion est de 1 minute, après quoi nous fermons la connexion. La durée maximale est de 10 minutes, après quoi nous n'autorisons pas de nouveaux flux via la connexion et nous entamons le processus de fermeture des flux existants.

Tâches

- Étape 1 : créer un service VPC Lattice
- Étape 2 : définir le routage
- Étape 3 : créer des associations réseau
- Étape 4 : vérifier et créer
- Gérer les associations pour un service VPC Lattice

- Modifier les paramètres d'accès pour un service VPC Lattice
- Modifier les détails de surveillance d'un service VPC Lattice
- Gérer les balises pour un service VPC Lattice
- Configurer un nom de domaine personnalisé pour votre service VPC Lattice
- Bring Your Own Certificate (BYOC) pour VPC Lattice
- Supprimer un service

Étape 1 : créer un service VPC Lattice

Créez un service VPC Lattice de base avec des paramètres d'accès et des informations de surveillance. Toutefois, le service n'est pas entièrement fonctionnel tant que vous n'avez pas défini sa configuration de routage et que vous ne l'avez pas associé à un réseau de services.

Pour créer un service de base à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Services.
3. Choisissez Créer un service.
4. Pour les identifiants, procédez comme suit :

   a. Entrez un nom pour le service. Le nom doit comporter entre 3 et 63 caractères et utiliser des lettres minuscules, des chiffres et des traits d'union. Il doit commencer et se terminer par une lettre ou un chiffre. N'utilisez pas de traits d'union doubles.

   b. (Facultatif) Entrez une description du réseau de service. Vous pouvez définir ou modifier la description pendant ou après la création. La description peut comporter jusqu'à 256 caractères.
5. Pour spécifier un nom de domaine personnalisé pour votre service, sélectionnez Spécifier une configuration de domaine personnalisée et entrez le nom de domaine personnalisé.

   Pour les écouteurs HTTPS, vous pouvez sélectionner le certificat que VPC Lattice utilisera pour effectuer la terminaison du protocole TLS. Si vous ne sélectionnez pas de certificat pour le moment, vous pouvez le sélectionner lorsque vous créez un écouteur HTTPS pour le service.

   Pour les écouteurs TCP, vous devez spécifier un nom de domaine personnalisé pour votre service. Si vous spécifiez un certificat, celui-ci n'est pas utilisé. Au lieu de cela, vous effectuez la terminaison du protocole TLS dans votre application.

6. Pour Accès au service, choisissez Aucun si vous souhaitez que les clients des VPC associés au réseau de service accèdent à votre service. Pour appliquer une politique d'authentification afin de contrôler l'accès au service, choisissez AWS IAM. Pour appliquer une politique de ressources au service, effectuez l'une des opérations suivantes pour la politique d'authentification :
   - Entrez une politique dans le champ de saisie. Par exemple, des politiques que vous pouvez copier et coller, choisissez Exemples de politiques.
   - Choisissez Appliquer le modèle de politique et sélectionnez le modèle Autoriser les accès authentifiés et non authentifiés. Ce modèle permet à un client d'accéder au service depuis un autre compte soit en signant la demande (c'est-à-dire authentifié), soit de manière anonyme (c'est-à-dire non authentifié).
   - Choisissez Appliquer le modèle de politique et sélectionnez le modèle Autoriser uniquement l'accès authentifié. Ce modèle permet à un client d'un autre compte d'accéder au service uniquement en signant la demande (c'est-à-dire authentifiée).
7. (Facultatif) Pour activer les journaux d'accès, activez le commutateur des journaux d'accès et spécifiez une destination pour vos journaux d'accès comme suit :
   - Sélectionnez Groupe de CloudWatch journaux, puis choisissez un groupe de CloudWatch journaux. Pour créer un groupe de journaux, choisissez Create a log group in CloudWatch.
   - Sélectionnez le compartiment S3 et entrez le chemin du compartiment S3, y compris tout préfixe. Pour effectuer une recherche dans vos compartiments S3, choisissez Browse S3.
   - Sélectionnez le flux de diffusion Kinesis Data Firehose, puis choisissez un flux de diffusion. Pour créer un flux de diffusion, choisissez Créer un flux de diffusion dans Kinesis.
8. (Facultatif) Pour partager votre service avec d'autres comptes, choisissez un partage de AWS RAM ressources dans Partages de ressources. Pour créer un partage de ressources, choisissez Créer un partage de ressources dans la console RAM.
9. Pour revoir votre configuration et créer le service, choisissez Ignorer pour vérifier et créer. Sinon, choisissez Next pour définir la configuration de routage de votre service.

Étape 2 : définir le routage

Définissez votre configuration de routage à l'aide d'écouteurs afin que votre service puisse envoyer du trafic vers les cibles que vous spécifiez.

Prérequis

Avant de pouvoir ajouter un écouteur, vous devez créer un groupe cible VPC Lattice. Pour plus d'informations, consultez the section called "Créer un groupe cible".

Pour définir le routage de votre service à l'aide de la console

1. Choisissez Add listener (Ajouter un écouteur).
2. Pour le nom de l'écouteur, vous pouvez soit fournir un nom d'écouteur personnalisé, soit utiliser le protocole et le port de votre écouteur comme nom d'écouteur. Le nom personnalisé que vous spécifiez peut comporter jusqu'à 63 caractères et doit être unique pour chaque service de votre compte. Les caractères valides sont a-z, 0-9 et les tirets (-). Vous ne pouvez pas utiliser de tiret comme premier ou dernier caractère, ni immédiatement après un autre tiret. Vous ne pouvez pas modifier le nom d'un écouteur après l'avoir créé.
3. Choisissez un protocole, puis entrez un numéro de port.
4. Pour l'action par défaut, choisissez le groupe cible du réseau VPC pour recevoir le trafic et choisissez le poids à attribuer à ce groupe cible. Vous pouvez éventuellement ajouter un autre groupe cible pour l'action par défaut. Choisissez Ajouter une action, puis choisissez un autre groupe cible et spécifiez son poids.
5. (Facultatif) Pour ajouter une autre règle, choisissez Ajouter une règle, puis entrez un nom, une priorité, une condition et une action pour la règle.

   Vous pouvez attribuer à chaque règle un numéro de priorité compris entre 1 et 100. Un écouteur ne peut pas avoir plusieurs règles ayant la même priorité. Les règles sont évaluées par ordre de priorité, de la valeur la plus basse à la valeur la plus haute. La règle par défaut est évaluée en dernier.

   Pour Condition, entrez un modèle de chemin pour la condition de correspondance du chemin. La taille maximale de chaque chaîne est de 200 caractères. La comparaison ne fait pas la distinction majuscules/minuscules.
6. (Facultatif) Pour ajouter des balises, développez les balises Listener, choisissez Ajouter une nouvelle balise, puis entrez une clé de balise et une valeur de balise.
7. Pour revoir votre configuration et créer le service, choisissez Ignorer pour vérifier et créer. Sinon, choisissez Next pour associer votre service à un réseau de services.

Étape 3 : créer des associations réseau

Associez votre service à un réseau de services afin que les clients puissent communiquer avec lui.

Pour associer un service à un réseau de services à l'aide de la console

1. Pour les réseaux de service VPC Lattice, sélectionnez le réseau de service. Pour créer un réseau de service, choisissez Create a VPC Lattice network. Vous pouvez associer votre service à plusieurs réseaux de services.
2. (Facultatif) Pour ajouter une balise, développez les balises d'association du réseau de services, choisissez Ajouter une nouvelle balise, puis entrez une clé de balise et une valeur de balise.
3. Choisissez Suivant.

Étape 4 : vérifier et créer

Pour revoir la configuration et créer le service à l'aide de la console

1. Vérifiez la configuration de votre service.
2. Choisissez Modifier si vous devez modifier une partie de la configuration du service.
3. Lorsque vous avez terminé de réviser ou de modifier votre configuration, choisissez Create VPC Lattice service.
4. Si vous avez spécifié un nom de domaine personnalisé pour le service, vous devez configurer le routage DNS une fois le service créé. Pour plus d'informations, consultez the section called "Configuration d'un nom de domaine personnalisé".

Gérer les associations pour un service VPC Lattice

Lorsque vous associez un service au réseau de services, cela permet aux clients (ressources d'un VPC associé au réseau de services) de faire des demandes à ce service. Vous pouvez associer des services présents dans votre compte ou des services partagés avec vous à partir de différents comptes. Cette étape est facultative lors de la création du service. Cependant, après sa création, le service ne peut pas communiquer avec d'autres services tant que vous ne l'avez pas associé à un réseau de services. Les propriétaires de services peuvent associer leurs services au réseau de services si leur compte dispose de l'accès requis. Pour plus d'informations, consultez Comment fonctionne le VPC Lattice.

Pour gérer les associations de réseaux de service à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Services.

3. Sélectionnez le nom du service pour ouvrir sa page de détails.
4. Choisissez l'onglet Associations de réseaux de services.
5. Pour créer une association, procédez comme suit :

    a. Choisissez Créer des associations.
    b. Sélectionnez un réseau de service parmi les réseaux de service VPC Lattice. Pour créer un réseau de service, choisissez Create a VPC Lattice network.
    c. (Facultatif) Pour ajouter une balise, développez les balises d'association de services, choisissez Ajouter une nouvelle balise, puis entrez une clé de balise et une valeur de balise.
    d. Sélectionnez Enregistrer les modifications.
6. Pour supprimer une association, cochez la case correspondante, puis choisissez Actions, Supprimer les associations réseau. Lorsque vous êtes invité à confirmer, entrez **`confirm`**, puis choisissez Delete (Supprimer).

Pour créer une association de réseau de service à l'aide du AWS CLI

Utilisez la commande create-service-network-service-association.

Pour supprimer une association de réseau de service à l'aide du AWS CLI

Utilisez la commande delete-service-network-service-association.

Modifier les paramètres d'accès pour un service VPC Lattice

Les paramètres d'accès vous permettent de configurer et de gérer l'accès des clients à un service. Les paramètres d'accès incluent le type d'authentification et les politiques d'authentification. Les politiques d'authentification vous aident à authentifier et à autoriser le trafic circulant vers les services au sein de VPC Lattice.

Vous pouvez appliquer des politiques d'authentification au niveau du réseau de service, au niveau du service ou aux deux. Au niveau du service, les propriétaires de services peuvent appliquer des contrôles précis, qui peuvent être plus restrictifs. Généralement, les politiques d'authentification sont appliquées par les propriétaires du réseau ou les administrateurs du cloud. Ils peuvent mettre en œuvre une autorisation basée sur le cours, par exemple en autorisant les appels authentifiés provenant de l'organisation ou en autorisant les demandes GET anonymes répondant à certaines conditions. Pour plus d'informations, consultez Contrôlez l'accès aux services à l'aide de politiques d'authentification.

Pour ajouter ou mettre à jour des politiques d'accès à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Services.
3. Sélectionnez le nom du service pour ouvrir sa page de détails.
4. Cliquez sur l'onglet Accès pour vérifier les paramètres d'accès actuels.
5. Pour mettre à jour les paramètres d'accès, choisissez Modifier les paramètres d'accès.
6. Si vous souhaitez que les clients des VPC du réseau de service associé accèdent à votre service, choisissez Aucun pour le type d'authentification.
7. Pour appliquer une politique de ressources afin de contrôler l'accès au service, choisissez AWS IAM pour le type d'authentification et effectuez l'une des opérations suivantes pour la politique d'authentification :
   - Entrez une politique dans le champ de saisie. Par exemple, des politiques que vous pouvez copier et coller, choisissez Exemples de politiques.
   - Choisissez Appliquer le modèle de politique et sélectionnez le modèle Autoriser les accès authentifiés et non authentifiés. Ce modèle permet à un client d'accéder au service depuis un autre compte soit en signant la demande (c'est-à-dire authentifié), soit de manière anonyme (c'est-à-dire non authentifié).
   - Choisissez Appliquer le modèle de politique et sélectionnez le modèle Autoriser uniquement l'accès authentifié. Ce modèle permet à un client d'un autre compte d'accéder au service uniquement en signant la demande (c'est-à-dire authentifiée).
8. Sélectionnez Enregistrer les modifications.

Pour ajouter ou mettre à jour une politique d'accès à l'aide du AWS CLI

Utilisez la commande put-auth-policy.

Modifier les détails de surveillance d'un service VPC Lattice

VPC Lattice génère des métriques et des journaux pour chaque demande et réponse, ce qui permet de surveiller et de dépanner les applications plus efficacement.

Vous pouvez activer les journaux d'accès et spécifier la ressource de destination pour vos journaux. VPC Lattice peut envoyer des journaux aux ressources suivantes : groupes de CloudWatch journaux, flux de diffusion Firehose et compartiments S3.

Pour activer les journaux d'accès ou mettre à jour une destination de journal à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Services.
3. Sélectionnez le nom du service pour ouvrir sa page de détails.
4. Choisissez l'onglet Surveillance, puis sélectionnez Logs. Consultez les journaux d'accès pour voir si les journaux d'accès sont activés.
5. Pour activer ou désactiver les journaux d'accès, choisissez Modifier les journaux d'accès, puis activez ou désactivez le bouton des journaux d'accès.
6. Lorsque vous activez les journaux d'accès, vous devez sélectionner le type de destination de livraison, puis créer ou choisir la destination des journaux d'accès. Vous pouvez également modifier la destination de livraison à tout moment. Par exemple :
   - Sélectionnez Groupe de CloudWatch journaux, puis choisissez un groupe de CloudWatch journaux. Pour créer un groupe de journaux, choisissez Create a log group in CloudWatch.
   - Sélectionnez le compartiment S3 et entrez le chemin du compartiment S3, y compris tout préfixe. Pour effectuer une recherche dans vos compartiments S3, choisissez Browse S3.
   - Sélectionnez le flux de diffusion Kinesis Data Firehose, puis choisissez un flux de diffusion. Pour créer un flux de diffusion, choisissez Créer un flux de diffusion dans Kinesis.
7. Sélectionnez Enregistrer les modifications.

Pour activer les journaux d'accès à l'aide du AWS CLI

Utilisez la commande create-access-log-subscription.

Pour mettre à jour la destination du journal à l'aide du AWS CLI

Utilisez la commande update-access-log-subscription.

Pour désactiver les journaux d'accès à l'aide du AWS CLI

Utilisez la commande delete-access-log-subscription.

Gérer les balises pour un service VPC Lattice

Les balises vous aident à classer votre service de différentes manières, par exemple par objectif, propriétaire ou environnement.

Vous pouvez ajouter plusieurs balises à chaque service. Les clés de tag doivent être uniques pour chaque service. Si vous ajoutez une balise avec une clé déjà associée au service, la valeur de cette balise est mise à jour. Vous pouvez utiliser des caractères tels que des lettres, des espaces, des chiffres (en UTF-8) et les caractères spéciaux suivants : + - =. _ : / @. N'utilisez pas d'espaces de début ou de fin. Les valeurs de balise sont sensibles à la casse.

Pour ajouter ou supprimer des balises à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Services.
3. Sélectionnez le nom du service pour ouvrir sa page de détails.
4. Sélectionnez l'onglet Tags (Identifications).
5. Pour ajouter une étiquette, choisissez Ajouter des balises et entrez la clé et la valeur de la balise. Pour ajouter une autre balise, choisissez Ajouter une nouvelle balise. Après avoir ajouter les identifications, choisissez Enregistrer les modifications.
6. Pour supprimer une étiquette, cochez la case correspondante et choisissez Supprimer. Lorsque vous êtes invité à confirmer, entrez **`confirm`**, puis choisissez Delete (Supprimer).

Pour ajouter ou supprimer des balises à l'aide du AWS CLI

Utilisez les commandes tag-resource et untag-resource.

Configurer un nom de domaine personnalisé pour votre service VPC Lattice

Lorsque vous créez un nouveau service, VPC Lattice génère un nom de domaine complet (FQDN) unique pour le service avec la syntaxe suivante.

```
service_name-service_id.partition_id.vpc-lattice-svcs.region.on.aws
```

Cependant, les noms de domaine fournis par VPC Lattice ne sont pas faciles à retenir pour vos utilisateurs. Les noms de domaine personnalisés sont des URL plus simples et plus intuitives que vous pouvez fournir à vos utilisateurs. Si vous préférez utiliser un nom de domaine personnalisé pour votre service, par exemple `www.parking.example.com` au lieu du nom DNS généré par VPC Lattice, vous pouvez le configurer lorsque vous créez un service VPC Lattice. Lorsqu'un client fait une demande en utilisant votre nom de domaine personnalisé, le serveur DNS la résout en utilisant

le nom de domaine généré par VPC Lattice. Toutefois, cela ne se produit que si vous mappez votre nom de domaine personnalisé au nom de domaine généré par VPC Lattice avec un enregistrement CNAME pour acheminer les requêtes vers votre service. Pour plus d'informations, consultez Associez un nom de domaine personnalisé à votre service.

Prérequis

- Vous devez avoir un nom de domaine enregistré pour votre service. Si vous n'avez pas encore de nom de domaine enregistré, vous pouvez en enregistrer un par le biais d'Amazon Route 53 ou de tout autre bureau d'enregistrement commercial.
- Pour recevoir des requêtes HTTPS, vous devez fournir votre propre certificat dans AWS Certificate Manager. VPC Lattice ne prend pas en charge les certificats par défaut comme solution de rechange. Par conséquent, si vous ne fournissez pas de certificat SSL/TLS correspondant à votre nom de domaine personnalisé, toutes les connexions HTTPS à votre nom de domaine personnalisé échoueront. Pour plus d'informations, consultez Bring Your Own Certificate (BYOC) pour VPC Lattice.

Limites et considérations

- Vous ne pouvez pas avoir plus d'un nom de domaine personnalisé pour un service.
- Vous ne pouvez pas modifier le nom de domaine personnalisé après avoir créé le service.
- Le nom de domaine personnalisé doit être unique pour un réseau de service. Cela signifie qu'un service ne peut pas être créé avec un nom de domaine personnalisé qui existe déjà (pour un autre service) dans le même réseau de services.

Pour configurer un nom de domaine personnalisé pour votre service à l'aide du AWS Management Console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Service.
3. Choisissez Create Service. Vous êtes redirigé vers l'étape 1 : créer un service.
4. Dans la section Configuration de domaine personnalisée, choisissez Spécifier une configuration de domaine personnalisée.
5. Entrez votre nom de domaine personnalisé.
6. Pour répondre aux demandes HTTPS, sélectionnez le certificat SSL/TLS correspondant à votre nom de domaine personnalisé dans Certificat SSL/TLS personnalisé. Si vous n'avez pas encore

de certificat ou si vous ne souhaitez pas en ajouter un maintenant, vous pouvez en ajouter un lors de la création de votre écouteur HTTPS. Toutefois, sans certificat, votre nom de domaine personnalisé ne sera pas en mesure de répondre aux requêtes HTTPS. Pour plus d'informations, consultez Ajout d'un écouteur HTTPS.

7. Lorsque vous avez terminé d'ajouter toutes les autres informations nécessaires à la création du service, choisissez Create.

Pour configurer un nom de domaine personnalisé pour votre service à l'aide du AWS CLI

Utilisez la commande create-service.

```
aws vpc-lattice create-service --name service_name --custom-domain-
name your_custom_domain_name --type https --certificate-arn arn:aws:acm:us-
east-1:123456789012:certificate/12345678-1234-1234-1234-123456789012
```

Dans la commande ci-dessus, pour`--name`, entrez le nom de votre service. Pour`--custom-domain-name`, entrez le nom de domaine de votre service tel que,`parking.example.com`. Pour `--certificate-arn` saisir l'ARN de votre certificat dans ACM. L'ARN du certificat est disponible dans votre compte en AWS Certificate Manager.

Si vous ne possédez pas votre propre certificat SSL/TLS dans AWS Certificate Manager (ACM), vous pouvez en créer ou en importer un avant de configurer un nom de domaine personnalisé. Toutefois, le certificat n'est requis que si vous souhaitez traiter des requêtes HTTPS à l'aide de votre nom de domaine personnalisé. Pour plus d'informations, consultez Bring Your Own Certificate (BYOC) pour VPC Lattice.

Associez un nom de domaine personnalisé à votre service

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

- Pour utiliser Amazon Route 53 pour enregistrer un nom de domaine, consultez Enregistrement de noms de domaines à l'aide de Route 53 dans le Guide du développeur Amazon Route 53.

- Pour une liste des serveurs d'inscriptions accrédités, consultez la page Accredited Registrar Directory.

Utilisez ensuite votre service DNS, tel que votre bureau d'enregistrement de domaines, pour créer un enregistrement CNAME afin d'acheminer les requêtes vers votre service. Pour plus d'informations, consultez la documentation de votre service DNS. Vous pouvez également utiliser Route 53 comme service DNS.

Si vous utilisez Route 53, vous devez d'abord créer une zone hébergée contenant des informations sur la manière d'acheminer le trafic sur Internet pour votre domaine. Après avoir créé la zone hébergée privée ou publique, créez un enregistrement CNAME de telle sorte que votre nom de domaine personnalisé, par exemple`parking.example.com`, soit mappé au nom de domaine généré automatiquement par VPC Lattice, par exemple,. `my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws` Sans ce mappage, votre nom de domaine personnalisé ne fonctionnera pas dans VPC Lattice. Pour plus d'informations, consultez la section Création d'enregistrements à l'aide de la console Amazon Route 53 dans le manuel du développeur Amazon Route 53. En outre, vous pouvez suivre les étapes ci-dessous pour créer une zone hébergée et un enregistrement CNAME afin de mapper votre nom de domaine personnalisé au point de terminaison VPC Lattice.

Pour créer une zone hébergée privée ou publique avec un enregistrement CNAME à l'aide de la console Amazon Route 53

1. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet de navigation, choisissez Hosted zones, puis Create hosted zone.
3. Dans Nom de domaine, choisissez le nom de la zone hébergée que vous souhaitez utiliser pour acheminer le trafic vers votre service VPC Lattice. Par exemple, si votre nom de domaine personnalisé est `parking.example.com` (http://parking.example.com/), le nom de domaine de votre zone hébergée sera `example.com` (http://example.com/), également connu sous le nom de domaine apex. Vous pouvez ensuite créer un enregistrement CNAME pour cette zone hébergée afin d'acheminer le trafic vers votre service VPC Lattice. Remarque : vous ne pouvez pas modifier le nom d'une zone hébergée après l'avoir créée.
4. Pour Type, choisissez Zone hébergée privée ou Zone hébergée publique selon les besoins.
5. Choisissez votre région et sélectionnez l'ID VPC d'un VPC que vous souhaitez associer à cette zone hébergée.

6. Ajoutez des tags si nécessaire, puis choisissez Create hosted zone. Une fois créée, votre zone hébergée est répertoriée sous Zones hébergées.
7. Pour créer un enregistrement CNAME dans la zone hébergée que vous venez de créer, sélectionnez la zone hébergée, puis sélectionnez Créer un enregistrement.
8. Spécifiez les valeurs suivantes sous Créer un enregistrement :

   a. Dans Nom de l'enregistrement, entrez le nom que vous souhaitez utiliser comme nom de domaine personnalisé. Si vous souhaitez utiliser `parking.example.com` (http://acme.example.com/) comme nom de domaine personnalisé, `parking` saisissez*. Cela signifie que vous devez saisir le nom du sous-domaine `parking` mais sans le nom de domaine de la zone hébergée `example.com` (http://example.com/).

   b. Pour Type d'enregistrement, choisissez CNAME.

   c. Gardez Alias désactivé.

   d. Dans Value, entrez le nom de domaine généré par le réseau VPC pour votre service (par exemple,). `my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws` Vous trouverez ce nom de domaine généré automatiquement dans la console VPC Lattice sur votre page de service. Si vous utilisez le AWS CLI, la sortie des `list-services` commandes `create-service` ou renverra ce nom de domaine généré automatiquement.

   e. Pour le TTL (secondes), acceptez la valeur par défaut de 300.

   f. Pour la stratégie de routage, choisissez la stratégie de routage applicable. Pour plus d'informations, consultez Choisir une politique de routage dans le manuel Amazon Route 53 Developer Guide.

9. Choisissez Create records (Créer des registres).

   Les changements se propagent généralement sur tous les serveurs Route 53 en 60 secondes. Une fois la propagation terminée, vous pourrez acheminer le trafic vers votre service en utilisant le nom de domaine personnalisé.

Pour créer un enregistrement d'alias dans votre zone hébergée à l'aide du AWS CLI

1. Obtenez le nom de domaine généré par VPC Lattice pour votre service (par exemple,`my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws`) et l'ID de zone hébergée en exécutant la commande. `get-service`
2. Pour définir l'alias, utilisez la commande suivante.

```
aws route53 change-resource-record-sets --hosted-zone-id hosted-zone-id-for-your-service-domain --change-batch file://~/Desktop/change-set.json
```

Pour le `change-set.json` fichier, créez un fichier JSON avec le contenu de l'exemple JSON suivant et enregistrez-le sur votre machine locale. Remplacez *`file : //~/desktop/change-set.json`* dans la commande ci-dessus par le chemin du fichier JSON enregistré sur votre machine locale. Notez que le « Type » dans le JSON suivant peut être un type d'enregistrement A ou AAAA.

```
{
    "Comment": "my-service-domain.com alias",
    "Changes": [
        {
            "Action": "CREATE",
            "ResourceRecordSet": {
                "Name": "my-custom-domain-name.com",
                "Type": "alias-record-type",
                "AliasTarget": {
                    "HostedZoneId": "hosted-zone-id-for-your-service-domain",
                    "DNSName": "lattice-generated-domain-name",
                    "EvaluateTargetHealth": true
                }
            }
        }
    ]
}
```

Bring Your Own Certificate (BYOC) pour VPC Lattice

Pour répondre aux requêtes HTTPS, vous devez disposer de votre propre certificat SSL/TLS prêt à l'emploi AWS Certificate Manager (ACM) avant de configurer un nom de domaine personnalisé. Ces certificats doivent avoir un nom alternatif d'objet (SAN) ou un nom commun (CN) correspondant au nom de domaine personnalisé de votre service. Si le SAN est présent, nous vérifions la correspondance uniquement dans la liste des SAN. Si le SAN est absent, nous vérifierons s'il y a une correspondance dans le CN.

VPC Lattice répond aux requêtes HTTPS à l'aide de l'indication du nom du serveur (SNI). Le DNS achemine la demande HTTPS vers votre service VPC Lattice en fonction du nom de domaine

personnalisé et du certificat correspondant à ce nom de domaine. Pour demander un certificat SSL/TLS pour un nom de domaine dans ACM ou en importer un dans ACM, voir Émission et gestion de certificats et importation de certificats dans le guide de l'utilisateur.AWS Certificate Manager Si vous ne pouvez pas demander ou importer votre propre certificat dans ACM, utilisez le nom de domaine et le certificat générés par VPC Lattice.

VPC Lattice n'accepte qu'un seul certificat personnalisé par service. Toutefois, vous pouvez utiliser un certificat personnalisé pour plusieurs domaines personnalisés. Cela signifie que vous pouvez utiliser le même certificat pour tous les services VPC Lattice que vous créez avec un nom de domaine personnalisé.

Pour consulter votre certificat à l'aide de la console ACM, ouvrez Certificats et sélectionnez votre ID de certificat. Vous devriez voir le service VPC Lattice associé à ce certificat sous Ressource associée.

Limites et considérations

- VPC Lattice autorise les correspondances génériques situées à un niveau du nom alternatif du sujet (SAN) ou du nom commun (CN) du certificat associé. Par exemple, si vous créez un service avec le nom de domaine personnalisé `parking.example.com` et associez votre propre certificat au SAN`*.example.com`. Lorsqu'une demande arrive`parking.example.com`, VPC Lattice associe le SAN à n'importe quel nom de domaine associé au domaine apex. `example.com` Toutefois, si vous avez le domaine personnalisé `parking.different.example.com` et que votre certificat possède le SAN`*.example.com`, la demande échoue.
- VPC Lattice prend en charge un niveau de correspondance de domaines génériques. Cela signifie qu'un caractère générique ne peut être utilisé que comme sous-domaine de premier niveau et qu'il ne sécurise qu'un seul niveau de sous-domaine. Par exemple, si le SAN de votre certificat l'est`*.example.com`, il n'`parking.*.example.com`est pas pris en charge.
- VPC Lattice prend en charge un caractère générique par nom de domaine. Cela signifie que ce n'`*.*.example.com`est pas valide. Pour plus d'informations, consultez la section Demander un certificat public dans le guide de AWS Certificate Manager l'utilisateur.
- VPC Lattice ne prend en charge que les certificats dotés de clés RSA de 2048 bits.
- Le certificat SSL/TLS dans ACM doit se trouver dans la même région que le service VPC Lattice auquel vous l'associez.

Sécurisation de la clé privée de votre certificat

Lorsque vous demandez un certificat SSL/TLS à l'aide d'ACM, ACM génère une paire de clés publique/privée. Lorsque vous importez un certificat, vous générez la paire de clés. La clé publique devient partie intégrante du certificat. Pour stocker la clé privée en toute sécurité, ACM crée une autre clé en utilisant AWS KMS, appelée clé KMS, l'alias aws/acm. AWS KMS utilise cette clé pour chiffrer la clé privée de votre certificat. Pour plus d'informations, consultez la section Protection des données AWS Certificate Manager dans le guide de AWS Certificate Manager l'utilisateur.

VPC Lattice utilise le gestionnaire de connexion AWS TLS, un service accessible uniquement à Services AWS, pour sécuriser et utiliser les clés privées de votre certificat. Lorsque vous utilisez votre certificat ACM pour créer un service VPC Lattice, VPC Lattice associe votre certificat au TLS Connection Manager. AWS Pour ce faire, nous créons une subvention associée AWS KMS à votre clé AWS gérée. Cette autorisation permet au Gestionnaire de connexions TLS de AWS KMS déchiffrer la clé privée de votre certificat. Le gestionnaire de connexion TLS utilise le certificat et la clé privée déchiffrée (texte brut) pour établir une connexion sécurisée (session SSL/TLS) avec les clients des services VPC Lattice. Lorsque le certificat est dissocié d'un service VPC Lattice, la subvention est retirée. Pour plus d'informations, consultez la section Subventions dans le guide du AWS Key Management Service développeur.

Pour plus d'informations, consultez Chiffrement au repos.

Supprimer un service

Pour supprimer un service VPC Lattice, vous devez d'abord supprimer toutes les associations que le service peut avoir avec n'importe quel réseau de services. Si vous supprimez un service, toutes les ressources associées au service, telles que la politique de ressources, la politique d'authentification, les écouteurs, les règles d'écoute et les abonnements aux journaux d'accès, sont également supprimées.

Pour supprimer un service à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Service.
3. Sur la page Services, sélectionnez le service que vous souhaitez supprimer, puis choisissez Actions, Supprimer le service.
4. Lorsque vous êtes invité à confirmer l'opération, choisissez Supprimer.

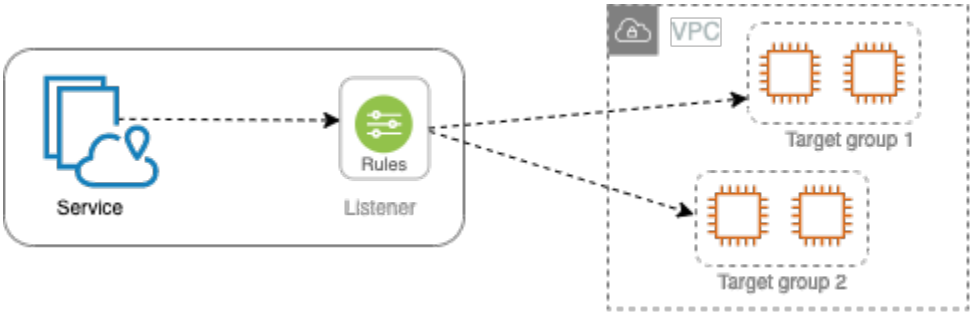
Pour supprimer un service à l'aide du AWS CLI

Utilisez la commande delete-service.

Groupes cibles dans VPC Lattice

Un groupe cible VPC Lattice est un ensemble de cibles, ou de ressources de calcul, qui exécutent votre application ou votre service. Les cibles peuvent être des instances EC2, des adresses IP, des fonctions Lambda, des équilibreurs de charge d'application ou des pods Kubernetes. Vous pouvez également associer des services existants à vos groupes cibles. Pour plus d'informations sur l'utilisation de Kubernetes avec VPC Lattice, consultez le guide de l'utilisateur du AWS Gateway API Controller.

Chaque groupe cible est utilisé pour acheminer les demandes vers une ou plusieurs cibles enregistrées. Lorsque vous créez une règle d'écoute, vous spécifiez un groupe cible et des conditions. Lorsqu'une condition est remplie, le trafic est transféré au groupe cible correspondant. 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 qui incluent des conditions de règle spécifiques, telles qu'un chemin ou une valeur d'en-tête.



Vous définissez les paramètres de contrôle de santé de votre service par 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 pour un écouteur, le service surveille en permanence l'état de toutes les cibles enregistrées auprès du groupe cible. Le service achemine les demandes vers les cibles enregistrées qui sont saines.

Pour spécifier un groupe cible dans une règle pour un service listener, le groupe cible doit être associé au même compte que le service.

Les groupes cibles VPC Lattice sont similaires aux groupes cibles fournis par Elastic Load Balancing, mais ils ne sont pas interchangeables.

Table des matières

- Enregistrer des cibles auprès d'un groupe cible VPC Lattice
- Contrôles de santé pour vos groupes cibles VPC Lattice
- Configuration du routage
- Algorithme de routage
- Type de cible
- Type d'adresse IP
- Cibles HTTP dans VPC Lattice
- Les fonctions Lambda sont des cibles dans VPC Lattice
- Les équilibreurs de charge des applications en tant que cibles dans VPC Lattice
- Version du protocole
- Tags pour votre groupe cible VPC Lattice
- Supprimer un groupe cible

Création d'un groupe cible VPC Lattice

Vous enregistrez les cibles avec le groupe cible. Par défaut, le service VPC Lattice envoie des demandes aux cibles enregistrées en utilisant le port et le 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, spécifiez le groupe cible dans une action lorsque vous créez un écouteur ou une règle pour votre écouteur. Pour plus d'informations, consultez Règles d'écoute pour votre service VPC Lattice. Vous pouvez spécifier le même groupe cible dans plusieurs écouteurs, mais ces derniers doivent appartenir au même service. Pour utiliser un groupe cible avec un service, vous devez vérifier que le groupe cible n'est pas utilisé par un écouteur pour un autre service.

Vous pouvez ajouter ou supprimer des cibles dans votre groupe cible à tout moment. Pour plus d'informations, consultez Enregistrer des cibles auprès d'un groupe cible VPC Lattice. Vous pouvez aussi modifier les paramètres de vérification de l'état de votre groupe cible. Pour plus d'informations, consultez Contrôles de santé pour vos groupes cibles VPC Lattice.

Créer un groupe cible

Vous pouvez créer un groupe cible et éventuellement enregistrer des cibles comme suit.

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

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Target groups.
3. Sélectionnez Créer un groupe cible.
4. Pour Choisir un type de cible, effectuez l'une des opérations suivantes :
   - Choisissez Instances pour enregistrer les cibles par ID d'instance.
   - Choisissez les adresses IP pour enregistrer les cibles par adresse IP.
   - Choisissez fonction Lambda pour enregistrer une fonction Lambda en tant que cible.
   - Choisissez Application Load Balancer pour enregistrer un Application Load Balancer en tant que cible.
5. Pour Nom du groupe cible, saisissez un nom pour le groupe cible. Ce nom doit être unique pour votre compte dans chaque AWS région, peut comporter un maximum de 32 caractères, ne doit contenir que des caractères alphanumériques ou des traits d'union, et ne doit pas commencer ou se terminer par un trait d'union.
6. Pour le protocole et le port, vous pouvez modifier les valeurs par défaut selon vos besoins. Le protocole par défaut est HTTPS et le port par défaut est 443.

   Si le type de cible est la fonction Lambda, vous ne pouvez pas spécifier de protocole ou de port.
7. Pour le type d'adresse IP, choisissez IPv4 pour enregistrer les cibles avec des adresses IPv4 ou choisissez IPv6 pour enregistrer les cibles avec des adresses IPv6. Vous ne pouvez pas modifier ce paramètre une fois le groupe cible créé.

   Cette option n'est disponible que si le type de cible est une adresse IP.
8. Pour VPC, sélectionnez un réseau Virtual Private Cloud (VPC).

   Cette option n'est pas disponible si le type de cible est la fonction Lambda.
9. Pour la version du protocole, modifiez la valeur par défaut selon vos besoins. La valeur par défaut est HTTP/1.

   Cette option n'est pas disponible si le type de cible est la fonction Lambda.
10. Pour les bilans de santé, modifiez les paramètres par défaut selon vos besoins. Pour plus d'informations, consultez Contrôles de santé pour vos groupes cibles VPC Lattice.

    Les contrôles de santé ne sont pas disponibles si le type de cible est la fonction Lambda.

11. Pour la version de structure d'événement Lambda, choisissez une version. Pour plus d'informations, consultez the section called "Recevez des événements du service VPC Lattice".

    Cette option n'est disponible que si le type de cible est la fonction Lambda

12. (Facultatif) Pour ajouter des balises, développez les balises, choisissez Ajouter une nouvelle balise, puis entrez la clé et la valeur de la balise.
13. Choisissez Suivant.
14. Pour les cibles de registre, vous pouvez soit ignorer cette étape, soit ajouter des cibles comme suit :
    - Si le type de cible est Instances, sélectionnez les instances, saisissez les ports, puis choisissez Inclure comme étant en attente ci-dessous.
    - Si la cible est de type Adresse IP, procédez comme suit :
        a. Pour Choisir un réseau, conservez le VPC que vous avez sélectionné pour le groupe cible ou choisissez Autre adresse IP privée.
        b. Pour Spécifier les adresses IP et définir les ports, entrez l'adresse IP et entrez les ports. Le port par défaut est le port du groupe cible.
        c. Choisissez Inclure comme en attente ci-dessous.
    - Si le type de cible est une fonction Lambda, choisissez-en une. Pour créer une fonction Lambda, choisissez Create a new Lambda function.
    - Si le type de cible est un Application Load Balancer, choisissez-en un Application Load Balancer. Pour créer un Application Load Balancer, choisissez Create an Application Load Balancer.
15. Sélectionnez Créer un groupe cible.

Pour créer un groupe cible à l'aide du AWS CLI

Utilisez la create-target-groupcommande pour créer le groupe cible et la commande register-targets pour ajouter des cibles.

Sous-réseaux partagés

Les participants peuvent créer des groupes cibles VPC Lattice dans un VPC partagé. Les règles suivantes s'appliquent aux sous-réseaux partagés :

- Toutes les parties d'un service VPC Lattice, telles que les auditeurs, les groupes cibles et les cibles, doivent être créées par le même compte. Ils peuvent être créés dans des sous-réseaux appartenant au propriétaire du service VPC Lattice ou partagés avec celui-ci.
- Les cibles enregistrées auprès d'un groupe cible doivent être créées par le même compte que le groupe cible.
- Seul le propriétaire d'un VPC peut associer le VPC à un réseau de services. Les ressources des participants d'un VPC partagé associé à un réseau de services peuvent envoyer des demandes aux services associés au réseau de services. Toutefois, l'administrateur peut empêcher cela en utilisant des groupes de sécurité, des ACL réseau ou des politiques d'authentification.

Pour plus d'informations sur les ressources partageables pour VPC Lattice, consultez. Partagez les ressources VPC Lattice

Enregistrer des cibles auprès d'un groupe cible VPC Lattice

Votre service sert de point de contact unique pour les clients et répartit le trafic entrant entre ses cibles enregistrées en bonne santé. 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 de plusieurs groupes cibles pour gérer la demande. Le service commence à acheminer les demandes vers une cible nouvellement enregistrée dès que le processus d'enregistrement est terminé et que la cible passe les tests de santé initiaux.

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 cible. L'annulation de l'enregistrement d'une cible supprime la cible de votre groupe cible, mais n'affecte pas autrement la cible. Le service arrête d'acheminer les demandes vers une cible dès qu'il est désenregistré. 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 des demandes par la cible.

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

Utilisez les procédures de console suivantes pour enregistrer ou désenregistrer des cibles. Vous pouvez également utiliser les commandes register-targets et deregister-targets du. AWS CLI

Table des matières

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

Les instances cibles doivent se trouver dans le cloud privé virtuel (VPC) que vous avez spécifié pour le groupe cible. L'état de l'instance doit également être `running` lorsque vous l'enregistrez.

Lorsque vous enregistrez des cibles par ID d'instance, vous pouvez utiliser votre service avec un groupe Auto Scaling. Une fois que vous avez attaché un groupe cible à un groupe Auto Scaling et que le groupe est redimensionné, les instances lancées par le groupe Auto Scaling sont automatiquement enregistrées auprès du groupe cible. Si vous détachez le groupe cible du groupe Auto Scaling, l'enregistrement des instances est annulé automatiquement dans le groupe cible. Pour plus d'informations, consultez la section Router le trafic vers votre groupe Auto Scaling avec un groupe cible VPC Lattice dans le guide de l'utilisateur Amazon EC2 Auto Scaling.

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

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Target groups.
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Choisissez l'onglet Cibles.
5. Pour enregistrer des instances, choisissez Enregistrer les cibles. Sélectionnez les instances, entrez le port de l'instance, puis choisissez Inclure en tant qu'instance en attente ci-dessous. Lorsque vous avez terminé d'ajouter des instances, choisissez Register targets.
6. Pour désenregistrer des instances, sélectionnez-les, puis choisissez Désenregistrer.

Enregistrer ou annuler l'enregistrement de cibles par adresse IP

Les adresses IP cibles doivent provenir des sous-réseaux du VPC que vous avez spécifiés pour le groupe cible. Vous ne pouvez pas enregistrer les adresses IP d'un autre service dans le même

VPC. Vous ne pouvez pas enregistrer de points de terminaison VPC ou d'adresses IP routables publiquement.

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

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Target groups.
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Choisissez l'onglet Cibles.
5. Pour enregistrer les adresses IP, sélectionnez Enregistrer les cibles. Pour chaque adresse IP, sélectionnez le réseau, entrez l'adresse IP et le port, et choisissez Inclure comme étant en attente ci-dessous. Lorsque vous avez fini de spécifier les adresses, choisissez Enregistrer les cibles.
6. Pour annuler l'enregistrement d'adresses IP, sélectionnez-les, puis choisissez Annuler l'enregistrement.

Enregistrement ou annulation de l'enregistrement d'une fonction Lambda

Vous pouvez enregistrer une seule fonction Lambda auprès du groupe cible. Si vous n'avez plus besoin d'envoyer le trafic vers votre fonction Lambda, vous pouvez annuler son enregistrement. Lorsque vous annulez l'enregistrement d'une fonction Lambda, les demandes en cours échouent avec des erreurs HTTP 5XX. Il est préférable de créer un nouveau groupe cible plutôt que de remplacer la fonction Lambda pour un groupe cible.

Pour enregistrer ou désenregistrer une fonction Lambda à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Target groups.
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Choisissez l'onglet Cibles.
5. Si aucune fonction Lambda n'est enregistrée, choisissez Register target. Sélectionnez la fonction Lambda et choisissez Register target.
6. Pour enregistrer ou annuler l'enregistrement d'une fonction Lambda, choisissez Deregister (Annuler l'enregistrement). Lorsque vous êtes invité à confirmer, entrez **`confirm`** puis choisissez Désenregistrer.

Enregistrer ou désenregistrer un Application Load Balancer

Vous pouvez enregistrer un seul Application Load Balancer auprès de chaque groupe cible. Si vous n'avez plus besoin d'envoyer du trafic vers votre équilibreur de charge, vous pouvez le désenregistrer. Une fois que vous avez désenregistré un équilibreur de charge, les requêtes en cours échouent avec des erreurs HTTP 5XX. Il est préférable de créer un nouveau groupe cible plutôt que de remplacer l'Application Load Balancer par un groupe cible.

Pour enregistrer ou désenregistrer un Application Load Balancer à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Target groups.
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Choisissez l'onglet Cibles.
5. Si aucun Application Load Balancer n'est enregistré, choisissez Register target. Sélectionnez l'Application Load Balancer et choisissez Register target.
6. Pour désenregistrer un Application Load Balancer, choisissez Désenregistrer. Lorsque vous êtes invité à confirmer, entrez **`confirm`** puis choisissez Désenregistrer.

Contrôles de santé pour vos groupes cibles VPC Lattice

Votre service envoie régulièrement des demandes à ses cibles enregistrées pour tester leur statut. Ces tests sont appelés vérifications de l'état.

Chaque service VPC Lattice achemine les demandes uniquement vers les cibles saines. Chaque service vérifie l'état de santé de chaque cible en utilisant les paramètres de contrôle de santé des groupes cibles auprès desquels la cible est enregistrée. Une fois que votre cible est enregistrée, elle doit passer avec succès une seule vérification de l'état pour être considérée comme saine. Une fois chaque contrôle de santé terminé, le service ferme la connexion établie pour le bilan de santé.

Limites et considérations

- Lorsque la version du protocole du groupe cible est HTTP/1, les contrôles de santé sont activés par défaut.
- Lorsque la version du protocole du groupe cible est HTTP/2, les contrôles de santé ne sont pas activés par défaut. Cependant, vous pouvez activer les contrôles de santé et définir manuellement la version du protocole sur HTTP/1 ou HTTP/2.

- Health checks ne prend pas en charge les versions du protocole du groupe cible gRPC. Toutefois, si vous activez les contrôles de santé, vous devez spécifier la version du protocole de contrôle de santé comme HTTP/1 ou HTTP/2.
- Les tests de santé ne prennent pas en charge les groupes cibles Lambda.
- Health checks ne prend pas en charge les groupes cibles d'Application Load Balancer. Cependant, vous pouvez activer les contrôles de santé pour les cibles de votre Application Load Balancer à l'aide d'Elastic Load Balancing. Pour plus d'informations, consultez la section État du groupe cible dans le guide de l'utilisateur des équilibreurs de charge d'application.

Paramètres de surveillance de l'état

Vous configurez les surveillances de l'état pour les cibles d'un groupe cible comme décrit dans le tableau suivant. Les noms de paramètres utilisés dans le tableau sont les noms utilisés dans l'API. Le service envoie une demande de contrôle de santé à chaque cible enregistrée toutes les HealthCheckIntervalSecondssecondes, en utilisant le port, le protocole et le chemin ping spécifiés. Chaque demande de vérification de l'état est indépendante et le résultat dure pendant la totalité de l'intervalle. Le temps nécessaire pour que la cible réponde n'affecte pas l'intervalle pour la demande de vérification de l'état suivante. Si les bilans de santé dépassent le nombre de défaillances UnhealthyThresholdCountconsécutives, le service met la cible hors service. Lorsque les bilans de santé dépassent les taux de réussite HealthyThresholdCountconsécutifs, le service remet la cible en service.

Paramètre	Description
HealthCheckProtocol	Protocole utilisé par le service pour effectuer des contrôles de santé sur des cibles. Les protocoles possibles sont HTTP et HTTPS. La valeur par défaut est le protocole HTTP.
HealthCheckPort	Port utilisé par le service pour effectuer des contrôles de santé sur des cibles. Par défaut, le port sur lequel chaque cible reçoit le trafic du service est utilisé.
HealthCheckPath	La destination des surveillances de l'état des cibles.

Paramètre	Description
	Si la version du protocole est HTTP/1 ou HTTP2, spécifiez un URI valide (/path ? requête). 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 1 et 120 secondes. La valeur par défaut est de 5 secondes si le type de cible est `INSTANCE` ou`IP`. Spécifiez 0 pour rétablir la valeur par défaut de ce paramètre.
HealthCheckIntervalSeconds	Durée approximative, en secondes, entre les vérifications de l'état d'une cible. La plage est comprise entre 5 et 300 secondes. La valeur par défaut est de 30 secondes si le type de cible est `INSTANCE` ou`IP`. Spécifiez 0 pour rétablir la valeur par défaut de ce paramètre.
HealthyThresholdCount	Le nombre de bilans de santé consécutifs réussis requis avant qu'une cible en mauvaise santé soit considérée comme saine. La plage est comprise entre 2 et 10. La valeur par défaut est 5. Spécifiez 0 pour rétablir la valeur par défaut de ce paramètre.
UnhealthyThresholdCount	Nombre d'échecs consécutifs de vérification de l'état à partir duquel la cible est considéré e comme défectueuse. La plage est comprise entre 2 et 10. La valeur par défaut est 2. Spécifiez 0 pour rétablir la valeur par défaut de ce paramètre.

Paramètre	Description
Matcher	Les codes à utiliser lors de la recherche d'une réponse positive provenant d'une cible. Ils sont appelés codes de réussite dans la console. Si la version du protocole est HTTP/1 ou HTTP/2, les valeurs possibles sont comprises entre 200 et 499. Vous pouvez spécifier plusieurs valeurs (par exemple, « 200,202 ») ou une plage de valeurs (par exemple, « 200-299 »). La valeur par défaut est 200. La version du protocole de contrôle de santé pour gRPC n'est actuellement pas prise en charge. Toutefois, si la version du protocole de votre groupe cible est gRPC, vous pouvez spécifier les versions du protocole HTTP/1 ou HTTP2 dans la configuration de votre bilan de santé.

Vérifier l'état de santé de vos cibles

Vous pouvez vérifier l'état de santé des cibles enregistrées auprès de vos groupes cible.

Pour vérifier l'état de santé de vos cibles à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Target groups.
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Cible, la colonne Statut d'état indique le statut de chaque cible. Si le statut est une valeur autre que`Healthy`, la colonne Détails de l'état de santé contient plus d'informations.

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

Utilisez la commande list-targets. La sortie de cette commande contient l'état de santé de la cible. Si le statut est différent de `Healthy`, la sortie inclut également un code de motif.

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

Utilisez des CloudWatch alarmes pour lancer une fonction Lambda afin d'envoyer des informations sur les cibles défectueuses.

Modifier les paramètres du bilan de santé

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

Pour modifier les paramètres du bilan de santé à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Target groups.
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Contrôles de santé, dans la section Paramètres des bilans de santé, choisissez Modifier.
5. Modifiez les paramètres du bilan de santé selon vos besoins.
6. Sélectionnez Enregistrer les modifications.

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

Utilisez la commande update-target-group.

Configuration du routage

Par défaut, un service achemine les demandes vers ses cibles en utilisant le protocole et le numéro de port que vous avez spécifiés lors de la création du 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 cible prennent en charge les protocoles et ports suivants :

- Protocoles : HTTP, HTTPS, TCP
- Ports : 1 à 65535

Si un groupe cible est configuré avec le protocole HTTPS ou utilise des contrôles de santé HTTPS, les connexions TLS aux cibles utilisent la politique de sécurité de l'écouteur. VPC Lattice établit des connexions TLS avec les cibles à l'aide de certificats que vous installez sur les cibles. VPC Lattice

ne valide pas ces certificats. Par conséquent, vous pouvez utiliser des certificats auto-signés ou des certificats qui ont expiré. Le trafic entre VPC Lattice et les cibles est authentifié au niveau des paquets. Il n'est donc pas exposé au risque d' man-in-the-middle attaques ou d'usurpation d'identité, même si les certificats des cibles ne sont pas valides.

Les groupes cibles TCP ne sont pris en charge qu'avec les écouteurs TLS.

Algorithme de routage

Par défaut, l'algorithme de routage Round Robin est utilisé pour acheminer les demandes vers des cibles saines.

Lorsque le service VPC Lattice reçoit une demande, il utilise le processus suivant :

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

Si un groupe cible ne contient que des cibles malsaines, les demandes sont acheminées vers toutes les cibles, quel que soit leur état de santé. Cela signifie que si toutes les cibles échouent aux tests de santé en même temps, le service VPC Lattice échoue à s'ouvrir. L'effet du fail-open est d'autoriser le trafic à destination de toutes les cibles, quel que soit leur état de santé, sur la base de l'algorithme du round robin.

Type de cible

Lorsque vous créez un groupe cible, vous spécifiez son type de cible, ce qui détermine le type de cible que vous indiquez lors de l'enregistrement des cibles auprès de ce groupe cible. 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 des adresses IP.

`LAMBDA`

La cible est une fonction Lambda.

`ALB`

La cible est un Application Load Balancer.

Considérations

- Lorsque le type de cible est`IP`, vous devez spécifier les adresses IP des sous-réseaux du VPC pour le groupe cible. Si vous devez enregistrer des adresses IP en dehors de ce VPC, créez un groupe cible de type `ALB` et enregistrez les adresses IP auprès de l'Application Load Balancer.
- Lorsque le type de cible est`IP`, vous ne pouvez pas enregistrer de points de terminaison VPC ou d'adresses IP routables publiquement.
- Lorsque le type de cible est`LAMBDA`, vous pouvez enregistrer une seule fonction Lambda. Lorsque le service reçoit une demande pour la fonction Lambda, il invoque la fonction Lambda. Si vous souhaitez enregistrer plusieurs fonctions lambda dans un service, vous devez utiliser plusieurs groupes cibles.
- Lorsque le type de cible est`ALB`, vous pouvez enregistrer un seul Application Load Balancer interne en tant que cible d'un maximum de deux services VPC Lattice. Pour ce faire, enregistrez l'Application Load Balancer auprès de deux groupes cibles distincts, utilisés par deux services VPC Lattice différents. En outre, l'Application Load Balancer ciblé doit disposer d'au moins un écouteur dont le port correspond au port du groupe cible.
- Pour enregistrer une tâche ECS en tant que cible, utilisez le type de `ALB` cible et enregistrez l'Application Load Balancer pour votre service Amazon ECS. Pour plus d'informations, consultez Répartition de charge des services dans le Guide du développeur Amazon Elastic Container Service.
- Pour enregistrer un pod EKS en tant que cible, utilisez le AWS Gateway API Controller, qui obtient les adresses IP du service Kubernetes.
- Si le protocole du groupe cible est TCP, les seuls types de cibles pris en charge sont `INSTANCE` et`IP`.

Type d'adresse IP

Lorsque vous créez un groupe cible avec un type de cible de`IP`, vous pouvez spécifier un type d'adresse IP pour le groupe cible. Cela indique le type d'adresses que l'équilibreur de charge utilise

pour envoyer des demandes et des contrôles de santé aux cibles. Les valeurs possibles sont `IPv4` et `IPv6`. La valeur par défaut est `IPV4`.

Considérations

- Si vous créez un groupe cible avec un type d'adresse IP de`IPv6`, le VPC que vous spécifiez pour le groupe cible doit avoir une plage d'adresses IPv6.
- Les adresses IP que vous enregistrez auprès d'un groupe cible doivent correspondre au type d'adresse IP du groupe cible. Par exemple, vous ne pouvez pas enregistrer une adresse IPv6 auprès d'un groupe cible si son type d'adresse IP est`IPv4`.
- Les adresses IP que vous enregistrez auprès d'un groupe cible doivent se situer dans la plage d'adresses IP du VPC que vous avez spécifié pour le groupe cible.

Cibles HTTP dans VPC Lattice

Les demandes HTTP et les réponses HTTP utilisent des champs d'en-tête pour envoyer des informations concernant les messages HTTP. Les en-têtes HTTP sont ajoutés automatiquement. Les champs d'en-tête sont des paires nom-valeur dont les noms et les valeurs sont séparés par un signe deux points, et qui sont séparées entre elles par un retour chariot (CR) et un saut de ligne (LF). Un ensemble standard de champs d'en-tête HTTP est défini dans la section du RFC 2616 concernant les en-têtes de message. Il existe également des en-têtes HTTP non standard qui sont automatiquement ajoutés et largement utilisés par les applications. Par exemple, il existe des en-têtes HTTP non standard avec le `x-forwarded` préfixe.

x-forwardeden-têtes

Amazon VPC Lattice ajoute les en-têtes suivants : `x-forwarded`

`x-forwarded-for`

Adresse IP source.

`x-forwarded-for-port`

Port de destination.

`x-forwarded-for-proto`

Le protocole de connexion (`http`|`https`).

En-têtes d'identité de l'appelant

Amazon VPC Lattice ajoute les en-têtes d'identité de l'appelant suivants :

`x-amzn-lattice-identity`

Les informations d'identité. Les champs suivants sont présents si AWS l'authentification est réussie.

- `Principal`— Le principal authentifié.
- `PrincipalOrgID`— L'identifiant de l'organisation pour le principal authentifié.
- `SessionName`— Le nom de la session authentifiée.

Les champs suivants sont présents si les informations d'identification de Roles Anywhere sont utilisées et que l'authentification est réussie.

- `X509Issuer/OU`— L'émetteur (OU).
- `X509SAN/DNS`— Le nom alternatif du sujet (DNS).
- `X509SAN/NameCN`— Le nom alternatif de l'émetteur (nom/CN).
- `X509SAN/URI`— Le nom alternatif du sujet (URI).
- `X509Subject/CN`— Le nom du sujet (CN).

`x-amzn-lattice-network`

Le VPC. Le format est le suivant :

```
SourceVpcArn=arn:aws:ec2:region:account:vpc/id
```

`x-amzn-lattice-target`

La cible. Le format est le suivant :

```
ServiceArn=arn;ServiceNetworkArn=arn;TargetGroupArn=arn
```

Pour plus d'informations sur les ARN des ressources pour VPC Lattice, consultez la section Types de ressources définis par Amazon VPC Lattice.

Les fonctions Lambda sont des cibles dans VPC Lattice

Vous pouvez enregistrer vos fonctions Lambda en tant que cibles auprès d'un groupe cible VPC Lattice et configurer une règle d'écoute pour transmettre les demandes de votre fonction Lambda au groupe cible. Lorsque le service transmet la demande à un groupe cible ayant une fonction Lambda comme cible, il invoque votre fonction Lambda et transmet le contenu de la demande à la fonction Lambda, au format JSON. Pour plus d'informations, consultez la section Utilisation AWS Lambda avec Amazon VPC Lattice dans le manuel du AWS Lambda développeur.

Limites

- La fonction Lambda et le groupe cible doivent être dans le même compte et dans la même région.
- La taille maximale du corps de requête que vous pouvez envoyer à une fonction Lambda est de 6 Mo.
- La taille maximale du JSON de réponse que la fonction Lambda peut envoyer est de 6 Mo.
- Le protocole doit être HTTP ou HTTPS.

Préparation de la fonction Lambda

Les recommandations suivantes s'appliquent si vous utilisez votre fonction Lambda avec un service VPC Lattice.

Autorisations pour invoquer la fonction Lambda

Lorsque vous créez le groupe cible et que vous enregistrez la fonction Lambda à l'aide du AWS Management Console ou du, AWS CLI VPC Lattice ajoute les autorisations requises à votre politique de fonction Lambda en votre nom.

Vous pouvez également ajouter vous-même des autorisations à l'aide de l'appel d'API suivant :

```
aws lambda add-permission \
  --function-name lambda-function-arn-with-alias-name \
  --statement-id vpc-lattice \
  --principal vpc-lattice.amazonaws.com \
  --action lambda:InvokeFunction \
  --source-arn target-group-arn
```

Gestion des versions de fonction Lambda

Vous pouvez enregistrer une seule fonction Lambda par groupe cible. Pour vous assurer que vous pouvez modifier votre fonction Lambda et que le service VPC Lattice invoque toujours la version actuelle de la fonction Lambda, créez un alias de fonction et incluez-le dans l'ARN de la fonction lorsque vous enregistrez la fonction Lambda auprès du service VPC Lattice. Pour plus d'informations, consultez Gestions des versions et alias des fonctions AWS Lambda et Déplacement du trafic à l'aide des alias dans le Guide du développeur AWS Lambda .

Création d'un groupe cible pour la fonction Lambda

Créez un groupe cible, qui sert à acheminer les demandes. Si le contenu de la demande correspond à une règle d'écoute assortie d'une action visant à le transmettre à ce groupe cible, le service VPC Lattice invoque la fonction Lambda enregistrée.

Pour créer un groupe cible et enregistrer la fonction Lambda à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Target groups.
3. Sélectionnez Créer un groupe cible.
4. Pour Choisir un type de cible, sélectionnez Fonction Lambda.
5. Pour Nom du groupe cible, saisissez un nom pour le groupe cible.
6. Pour la version de structure d'événement Lambda, choisissez une version. Pour plus d'informations, consultez the section called "Recevez des événements du service VPC Lattice".
7. (Facultatif) Pour ajouter des balises, développez les balises, choisissez Ajouter une nouvelle balise, puis entrez la clé et la valeur de la balise.
8. Choisissez Suivant.
9. Pour Lambda function (Fonction Lambda), effectuez l'une des opérations suivantes :
   - Sélectionnez une fonction Lambda existante.
   - Créez une nouvelle fonction Lambda et sélectionnez-la.
   - Enregistrez la fonction Lambda ultérieurement.
10. Sélectionnez Créer un groupe cible.

Pour créer un groupe cible et enregistrer la fonction Lambda à l'aide de l' AWS CLI

Utilisez les commandes create-target-groupet register-targets.

Recevez des événements du service VPC Lattice

Le service VPC Lattice prend en charge l'invocation Lambda pour les requêtes via HTTP et HTTPS. Le service envoie un événement au format JSON et ajoute l'`X-Forwarded-For`en-tête à chaque demande.

Encodage Base64

Le service Base64 code le corps si l'`content-encoding`en-tête est présent et que le type de contenu n'est pas l'un des suivants :

- `text/*`
- `application/json`
- `application/xml`
- `application/javascript`

Si l'en-tête `content-encoding` n'est pas présent, le codage Base64 dépend du type de contenu. Pour les types de contenu ci-dessus, le service envoie le corps tel quel, sans encodage Base64.

Format de structure de l'événement

Lorsque vous créez ou mettez à jour un groupe cible de type`LAMBDA`, vous pouvez spécifier la version de la structure d'événements que reçoit votre fonction Lambda. Les versions possibles sont `V1` et`V2`.

Example Exemple d'événement : V2

```
{
    "version": "2.0",
    "path": "/",
    "method": "GET|POST|HEAD|...",
    "headers": {
        "header-key": ["header-value", ...],
        ...
    },
    "queryStringParameters": {
        "key": "value", ...
    },
    "body": "request-body",
    "isBase64Encoded": true|false,
```

```
    "requestContext": {
        "serviceNetworkArn": "arn:aws:vpc-
lattice:region:123456789012:servicenetwork/sn-0bf3f2882e9cc805a",
        "serviceArn": "arn:aws:vpc-
lattice:region:123456789012:service/svc-0a40eebed65f8d69c",
        "targetGroupArn": "arn:aws:vpc-
lattice:region:123456789012:targetgroup/tg-6d0ecf831eec9f09",
        "identity": {
            "sourceVpcArn":
 "arn:aws:ec2:region:123456789012:vpc/vpc-0b8276c84697e7339",
            "type": "AWS_IAM",
            "principal": "arn:aws:iam::123456789012:assumed-role/my-role/my-session",
            "principalOrgID": "o-50dc6c495c0c9188",
            "sessionName": "i-0c7de02a688bde9f7",
            "x509IssuerOu": "string",
            "x509SanDns": "string",
            "x509SanNameCn": "string",
            "x509SanUri": "string",
            "x509SubjectCn": "string"
        },
        "region": "region",
        "timeEpoch": "1690497599177430"
    }
}
```

`body`

Le corps de la demande. Présent uniquement si le protocole est HTTP, HTTPS ou gRPC.

`headers`

Les en-têtes HTTP de la demande. Présent uniquement si le protocole est HTTP, HTTPS ou gRPC.

`identity`

Les informations d'identité. Les champs suivants sont possibles.

- `principal`— Le principal authentifié. Présent uniquement si AWS l'authentification est réussie.
- `principalOrgID`— L'identifiant de l'organisation pour le principal authentifié. Présent uniquement si AWS l'authentification est réussie.
- `sessionName`— Le nom de la session authentifiée. Présent uniquement si AWS l'authentification est réussie.

- `sourceVpcArn`— L'ARN du VPC d'où provient la demande. Présent uniquement si le VPC source peut être identifié.
- `type`— La valeur est `AWS_IAM` si une politique d'authentification est utilisée et si AWS l'authentification est réussie.

Si les informations d'identification de Roles Anywhere sont utilisées et que l'authentification est réussie, les champs suivants sont possibles.

- `x509IssuerOu`— L'émetteur (OU).
- `x509SanDns`— Le nom alternatif du sujet (DNS).
- `x509SanNameCn`— Le nom alternatif de l'émetteur (nom/CN).
- `x509SanUri`— Le nom alternatif du sujet (URI).
- `x509SubjectCn`— Le nom du sujet (CN).

`isBase64Encoded`

Indique si le corps a été codé en base64. Présent uniquement si le protocole est HTTP, HTTPS ou gRPC et que le corps de la requête n'est pas déjà une chaîne.

`method`

Méthode HTTP de la demande. Présent uniquement si le protocole est HTTP, HTTPS ou gRPC.

`path`

Le chemin d'accès de la demande. Présent uniquement si le protocole est HTTP, HTTPS ou gRPC.

`queryStringParameters`

Les paramètres de la chaîne de requête HTTP. Présent uniquement si le protocole est HTTP, HTTPS ou gRPC.

`serviceArn`

L'ARN du service qui reçoit la demande.

`serviceNetworkArn`

L'ARN du réseau de service qui fournit la demande.

`targetGroupArn`

L'ARN du groupe cible qui reçoit la demande.

`timeEpoch`

Le temps, en microsecondes.

Example Exemple d'événement : V1

```
{
    "raw_path": "/path/to/resource",
    "method": "GET|POST|HEAD|...",
    "headers": {"header-key": "header-value", ... },
    "query_string_parameters": {"key": "value", ...},
    "body": "request-body",
    "is_base64_encoded": true|false
}
```

Répondre au service VPC Lattice

La réponse de votre fonction Lambda doit inclure le statut d'encodage en Base64, le code de statut et des en-têtes. Vous pouvez omettre le corps.

Pour inclure un contenu binaire dans le corps de la réponse, vous devez encoder le contenu en Base64 et définir `isBase64Encoded` sur `true`. Le service décode le contenu pour récupérer le contenu binaire et l'envoie au client dans le corps de la réponse HTTP.

Le service VPC Lattice n'honore pas hop-by-hop les en-têtes tels que ou. `Connection` `Transfer-Encoding` Vous pouvez omettre l'`Content-Length`en-tête car le service le calcule avant d'envoyer des réponses aux clients.

Voici un exemple de réponse d'une fonction Lambda :

```
{
    "isBase64Encoded": false,
    "statusCode": 200,
    "statusDescription": "200 OK",
    "headers": {
        "Set-cookie": "cookies",
        "Content-Type": "application/json"
    },
    "body": "Hello from Lambda (optional)"
```

```
}
```

En-têtes à valeurs multiples

Par défaut, VPC Lattice prend en charge les demandes d'un client ou les réponses d'une fonction Lambda contenant des en-têtes comportant plusieurs valeurs ou contenant le même en-tête plusieurs fois. VPC Lattice prend également en charge les paramètres de requête comportant plusieurs valeurs pour la même clé.

Pour les en-têtes de demande, si plusieurs paramètres partagent le même nom, VPC Lattice transmettra les deux valeurs aux cibles. Voici un exemple où `header 1` figure le nom de deux en-têtes distincts :

```
header1 = foo
header1 = bar
```

VPC Lattice envoie ensuite les deux valeurs aux cibles :

```
"header1": ["foo", "bar"]
```

Pour les chaînes de requête, si plusieurs paramètres portent le même nom, la dernière valeur l'emporte. Cela signifie que les `_not_ coalesced` paramètres ont une valeur unique s'ils portent le même nom de clé.

Voici un exemple où `foo` et `bar` sont les valeurs des paramètres portant le même nom `QS1` :

```
http://www.example.com?&QS1=foo&QS1=bar
```

VPC Lattice envoie ensuite la dernière valeur aux cibles :

```
"QS1": "bar"
```

Annulation de l'enregistrement de la fonction Lambda

Si vous n'avez plus besoin d'envoyer le trafic vers votre fonction Lambda, vous pouvez annuler son enregistrement. Lorsque vous annulez l'enregistrement d'une fonction Lambda, les demandes en cours échouent avec des erreurs HTTP 5XX.

Pour remplacer une fonction Lambda, nous vous recommandons de créer un nouveau groupe cible, d'enregistrer la nouvelle fonction auprès du nouveau groupe cible et de mettre à jour les règles d'écouteur pour utiliser le nouveau groupe cible au lieu du groupe existant.

Pour désenregistrer une fonction Lambda à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Target groups.
3. Sélectionnez le nom du groupe cible pour afficher sa page de détails.
4. Dans l'onglet Cibles, choisissez Deregister (Annuler l'enregistrement).
5. Lorsque vous êtes invité à confirmer, entrez **`confirm`** puis choisissez Désenregistrer.

Pour annuler l'enregistrement de la fonction Lambda à l'aide du AWS CLI

Utilisez la commande deregister-targets.

Les équilibreurs de charge des applications en tant que cibles dans VPC Lattice

Vous pouvez créer un groupe cible VPC Lattice, enregistrer un seul Application Load Balancer interne comme cible et configurer votre service VPC Lattice pour transférer le trafic vers ce groupe cible. Dans ce scénario, l'Application Load Balancer prend en charge la décision de routage dès que le trafic l'atteint. Cette configuration vous permet d'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 VPC Lattice, telles que l'authentification et l'autorisation IAM, et la connectivité entre les VPC et les comptes.

Limites

- Vous pouvez enregistrer un seul Application Load Balancer interne en tant que cible dans un groupe cible de type VPC Lattice. `ALB`
- Vous pouvez enregistrer un Application Load Balancer en tant que cible d'un maximum de deux groupes cibles VPC Lattice, utilisés par deux services VPC Lattice différents.
- VPC Lattice ne fournit pas de tests de santé pour un `ALB` type de groupe cible. Cependant, vous pouvez configurer les contrôles de santé indépendamment au niveau de l'équilibreur de charge pour les cibles dans Elastic Load Balancing. Pour plus d'informations, consultez la section

Contrôles de santé de vos groupes cibles dans le guide de l'utilisateur pour les équilibreurs de charge d'application

Prérequis

Créez un Application Load Balancer à enregistrer en tant que cible auprès de votre groupe cible VPC Lattice. L'équilibreur de charge doit répondre aux critères suivants :

- Le schéma de l'équilibreur de charge est interne.
- L'Application Load Balancer doit se trouver sur le même compte que le groupe cible VPC Lattice et doit être à l'état actif.
- L'Application Load Balancer doit se trouver dans le même VPC que le groupe cible VPC Lattice.
- Vous pouvez utiliser des écouteurs HTTPS sur l'Application Load Balancer pour mettre fin au protocole TLS, mais uniquement si le service VPC Lattice utilise le même certificat SSL/TLS que l'équilibreur de charge.
- Pour conserver l'adresse IP du client du service VPC Lattice dans l'en-tête de `X-Forwarded-For` demande, vous devez définir l'attribut de l'Application Load Balancer sur. `routing.http.xff_header_processing.mode` `Preserve` Si la valeur est la `Preserve` même, l'équilibreur de charge préserve l'`X-Forwarded-For`en-tête de la requête HTTP et l'envoie aux cibles sans aucune modification. Pour plus d'informations, consultez X-Forwarded-For dans le guide de l'utilisateur des équilibreurs de charge d'application.

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 : Création d'un groupe cible de type ALB

Utilisez la procédure suivante pour créer le groupe cible. Notez que VPC Lattice ne prend pas en charge les contrôles de santé pour les groupes cibles ALB. Vous pouvez toutefois configurer des contrôles de santé pour les groupes cibles de votre Application Load Balancer. Pour plus d'informations, consultez la section État du groupe cible dans le guide de l'utilisateur des équilibreurs de charge d'application.

Pour créer le groupe cible

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le volet de navigation, sous VPC Lattice, choisissez Target groups.
3. Sélectionnez Créer un groupe cible.
4. Sur la page de détails du groupe cible, sous Configuration de base, choisissez Application Load Balancer comme type de cible.
5. Pour Nom du groupe cible, saisissez un nom pour le groupe cible.
6. Pour Protocole, sélectionnez **HTTP** ou **HTTPS**. Le protocole du groupe cible doit correspondre au protocole de l'écouteur de votre Application Load Balancer interne.
7. Pour Port, spécifiez le port pour votre groupe cible. Ce port doit correspondre au port de l'écouteur de votre Application Load Balancer interne. Vous pouvez également ajouter un port d'écoute sur l'Application Load Balancer interne pour qu'il corresponde au port du groupe cible que vous spécifiez ici.
8. Pour le VPC, sélectionnez le même cloud privé virtuel (VPC) que celui que vous avez sélectionné lors de la création de l'Application Load Balancer interne. Il doit s'agir du VPC qui contient vos ressources VPC Lattice.
9. Pour la version du protocole, choisissez la version du protocole prise en charge par votre Application Load Balancer.
10. (Facultatif) Ajoutez les balises requises.
11. Choisissez Suivant.

Étape 2 : enregistrer l'Application Load Balancer en tant que cible

Vous pouvez enregistrer l'équilibreur de charge en tant que cible maintenant ou ultérieurement.

Pour enregistrer un Application Load Balancer en tant que cible

1. Choisissez S'inscrire maintenant.
2. Pour Application Load Balancer, choisissez votre Application Load Balancer interne.
3. Pour Port, conservez la valeur par défaut ou spécifiez un port différent selon les besoins. Ce port doit correspondre à un port d'écoute existant sur votre Application Load Balancer. Si vous continuez sans port correspondant, le trafic n'atteindra pas votre Application Load Balancer.
4. Sélectionnez Créer un groupe cible.

Version du protocole

Par défaut, les services envoient des demandes aux cibles via HTTP/1.1. Vous pouvez utiliser la version du protocole pour envoyer des demandes à des cibles via HTTP/2 ou gRPC.

Le tableau suivant résume le résultat pour les combinaisons du protocole de demande et de la version du protocole du groupe cible.

Protocole de demande	Version du protocole	Résultat
HTTP/1.1	HTTP/1.1	Réussite
HTTP/2	HTTP/1.1	Réussite
gRPC	HTTP/1.1	Erreur
HTTP/1.1	HTTP/2	Erreur
HTTP/2	HTTP/2	Réussite
gRPC	HTTP/2	Succès si les cibles prennent en charge gRPC
HTTP/1.1	gRPC	Erreur
HTTP/2	gRPC	Succès si une demande POST
gRPC	gRPC	Réussite

Considérations relatives à la version du protocole gRPC

- Le seul protocole d'écouteur pris en charge est le HTTPS.
- Les seuls types de cibles pris en charge sont `INSTANCE` et `IP`.
- Le service analyse les demandes gRPC et achemine les appels gRPC vers les groupes cibles appropriés en fonction du package, du service et de la méthode.
- Vous ne pouvez pas utiliser les fonctions Lambda comme cibles.

Considérations relatives à la version du protocole HTTP/2

- Le seul protocole d'écouteur pris en charge est le HTTPS. Vous pouvez choisir HTTP ou HTTPS pour le protocole du groupe cible.
- Les seules règles d'écoute prises en charge sont les réponses directes et fixes.
- Les seuls types de cibles pris en charge sont `INSTANCE` et `IP`.
- Le service prend en charge le streaming depuis les clients. Le service ne prend pas en charge le streaming vers les cibles.

Tags pour votre groupe cible VPC Lattice

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

Vous pouvez ajouter plusieurs balises à chaque groupe cible. Les clés de balise doivent être uniques pour chaque groupe cible. Si vous ajoutez une balise avec une clé qui est déjà associée au groupe cible, cela met à jour la valeur de cette balise.

Lorsque vous avez terminé avec une balise, vous pouvez la supprimer.

Restrictions

- Nombre maximal de balises par ressource : 50
- Longueur de clé maximale : 127 caractères Unicode
- Longueur de valeur maximale – 255 caractères Unicode
- Les clés et valeurs de balise sont sensibles à la casse. Les caractères autorisés sont les lettres, les espaces et les chiffres représentables en UTF-8, ainsi que les caractères spéciaux suivants : + - = . _ : / @. N'utilisez pas d'espaces de début ou de fin.
- N'utilisez pas le `aws:` préfixe dans les noms ou les valeurs de vos balises, car il est réservé à AWS l'usage. Vous ne pouvez pas modifier ou supprimer des noms ou valeurs de balise ayant ce préfixe. Les balises avec ce préfixe ne sont pas comptabilisées comme vos balises pour la limite de ressources.

Pour mettre à jour les balises d'un groupe cible à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le volet de navigation, sous VPC Lattice, choisissez Target groups.
3. Sélectionnez le nom du groupe cible pour ouvrir sa page de détails.
4. Sélectionnez l'onglet Tags (Identifications).
5. Pour ajouter une étiquette, choisissez Ajouter des balises et entrez la clé et la valeur de la balise. Pour ajouter une autre balise, choisissez Ajouter une nouvelle balise. Après avoir ajouter les identifications, choisissez Enregistrer les modifications.
6. Pour supprimer une étiquette, cochez la case correspondante et choisissez Supprimer. Lorsque vous êtes invité à confirmer, entrez **`confirm`**, puis choisissez Delete (Supprimer).

Pour mettre à jour les balises d'un groupe cible à l'aide du AWS CLI

Utilisez les commandes tag-resource et untag-resource.

Supprimer un groupe cible

Vous pouvez supprimer un groupe cible s'il n'est pas référencé par les actions de transfert des règles d'écoute. La suppression d'un groupe cible n'affecte pas les cibles enregistrées auprès de ce groupe cible. Si vous n'avez plus besoin d'une instance EC2 enregistrée, vous pouvez l'arrêter ou la suspendre.

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

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez Target groups.
3. Cochez la case correspondant au groupe cible, puis choisissez Actions, Supprimer.
4. Lorsque vous êtes invité à confirmer, entrez **`confirm`**, puis choisissez Delete (Supprimer).

Pour supprimer un groupe cible à l'aide du AWS CLI

Utilisez la commande delete-target-group.

Écouteurs pour votre service VPC Lattice

Avant de commencer à utiliser votre service VPC Lattice, vous devez ajouter un ou plusieurs écouteurs. Un écouteur est un processus qui vérifie les demandes de connexion, en utilisant le protocole et le port que vous avez configurés. Les règles que vous définissez pour un écouteur déterminent la manière dont le service achemine les demandes vers ses cibles enregistrées.

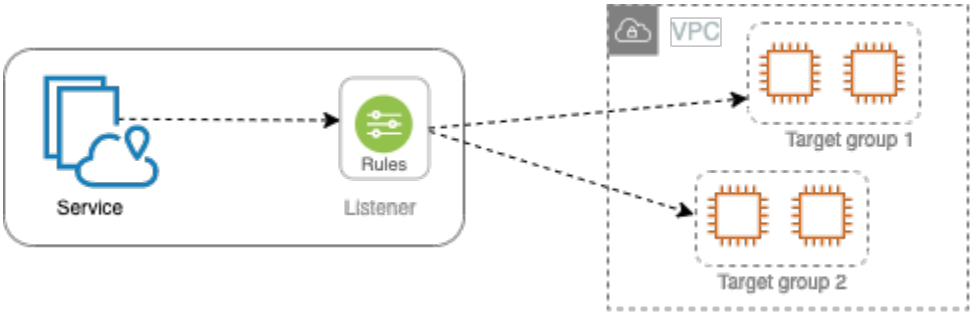


Table des matières

Configuration des écouteurs

Les écouteurs prennent en charge les protocoles et ports suivants :

- Protocoles : HTTP, HTTPS, TLS
- Ports : 1 à 65535

Si le protocole d'écoute est HTTPS, VPC Lattice fournira et gérera un certificat TLS associé au FQDN généré par VPC Lattice. VPC Lattice prend en charge le protocole TLS sur HTTP/1.1 et HTTP/2. Lorsque vous configurez un service avec un écouteur HTTPS, VPC Lattice détermine

automatiquement le protocole HTTP à l'aide de la négociation ALPN (Application-Layer Protocol Negotiation). Si ALPN est absent, VPC Lattice utilise par défaut HTTP/1.1. Pour plus d'informations, consultez Écouteurs HTTPS.

VPC Lattice peut écouter les protocoles HTTP, HTTPS, HTTP/1.1 et HTTP/2 et communiquer avec des cibles dans n'importe lequel de ces protocoles et versions. Nous n'exigeons pas que les protocoles de l'écouteur et du groupe cible correspondent. VPC Lattice gère l'ensemble du processus de mise à niveau et de rétrogradation entre les protocoles et les versions. Pour plus d'informations, consultez Version du protocole.

Vous pouvez créer un écouteur TLS pour vous assurer que votre application déchiffre le trafic chiffré au lieu du VPC Lattice. Pour plus d'informations, consultez Écouteurs TLS.

Le VPC Lattice n'est pas compatible. WebSockets

Créer un écouteur

Vous pouvez créer des écouteurs pour votre service VPC Lattice. Lorsque vous créez un écouteur, vous devez spécifier un nom, une action par défaut et un protocole. Un écouteur est fourni avec une règle par défaut. Vous pouvez également créer des règles supplémentaires pour votre auditeur.

Pour créer un écouteur à l'aide de la console

- the section called "Ajout d'un écouteur HTTP "
- the section called "Ajout d'un écouteur HTTPS"
- the section called "Ajouter un écouteur TLS"
- the section called "Ajout d'une règle"

Pour créer un écouteur à l'aide du AWS CLI

Utilisez les commandes create-listener et create-rule.

Écouteurs HTTP pour les services VPC Lattice

Un écouteur est un processus qui vérifie les demandes de connexion. Vous pouvez définir un écouteur lorsque vous créez votre service VPC Lattice. Vous pouvez ajouter des auditeurs à votre service à tout moment.

Les informations de cette page vous aident à créer un écouteur HTTP pour votre service. Pour plus d'informations sur la création d'écouteurs utilisant d'autres protocoles, reportez-vous aux sections Écouteurs HTTPS etÉcouteurs TLS.

Prérequis

- Pour ajouter une action directe à la règle d'écoute par défaut, vous devez spécifier un groupe cible VPC Lattice disponible. Pour plus d'informations, consultez Création d'un groupe cible VPC Lattice.
- Vous pouvez spécifier le même groupe cible dans plusieurs écouteurs, mais ces derniers doivent appartenir au même service. Pour utiliser un groupe cible avec un service VPC Lattice, vous devez vérifier qu'il n'est pas utilisé par un écouteur pour un autre service VPC Lattice.

Ajout d'un écouteur HTTP

Vous pouvez ajouter des écouteurs et des règles à votre service à tout moment. Vous configurez un écouteur avec un protocole et un port pour les connexions des clients au service, et un groupe cible VPC Lattice pour la règle d'écouteur par défaut. Pour plus d'informations, consultez Configuration des écouteurs.

Ajouter un écouteur HTTP à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Services.
3. Sélectionnez le nom du service pour ouvrir sa page de détails.
4. Dans l'onglet Routage, choisissez Ajouter un écouteur.
5. Pour le nom de l'écouteur, vous pouvez soit fournir un nom d'écouteur personnalisé, soit utiliser le protocole et le port de votre écouteur comme nom d'écouteur. Le nom personnalisé que vous spécifiez peut comporter jusqu'à 63 caractères et doit être unique pour chaque service de votre compte. Les caractères valides sont a-z, 0-9 et les tirets (-). Vous ne pouvez pas utiliser de tiret comme premier ou dernier caractère, ni immédiatement après un autre tiret. Vous ne pouvez pas modifier le nom après l'avoir créé.
6. Pour Protocole : port, choisissez HTTP et entrez un numéro de port.
7. Pour l'action par défaut, choisissez le groupe cible du réseau VPC pour recevoir le trafic et choisissez le poids à attribuer à ce groupe cible. Le poids que vous attribuez à un groupe cible définit sa priorité pour recevoir du trafic. Par exemple, si deux groupes cibles ont le même poids,

chaque groupe cible reçoit la moitié du trafic. Si vous n'avez spécifié qu'un seul groupe cible, 100 % du trafic est envoyé à ce groupe cible.

Vous pouvez éventuellement ajouter un autre groupe cible pour l'action par défaut. Choisissez Ajouter une action, puis choisissez un groupe cible et spécifiez son poids.

8. (Facultatif) Pour ajouter une autre règle, choisissez Ajouter une règle, puis entrez un nom, une priorité, une condition et une action pour la règle.

   Vous pouvez attribuer à chaque règle un numéro de priorité compris entre 1 et 100. Un écouteur ne peut pas avoir plusieurs règles ayant la même priorité. Les règles sont évaluées par ordre de priorité, de la valeur la plus basse à la valeur la plus haute. La règle par défaut est évaluée en dernier. Pour plus d'informations, consultez Règles d'un écouteur.
9. (Facultatif) Pour ajouter des balises, développez les balises Listener, choisissez Ajouter une nouvelle balise, puis entrez une clé de balise et une valeur de balise.
10. Vérifiez votre configuration, puis choisissez Ajouter.

Pour ajouter un écouteur HTTP à l'aide du AWS CLI

Utilisez la commande create-listener pour créer un écouteur avec une règle par défaut, et la commande create-rule pour créer des règles d'écouteur supplémentaires.

Écouteurs HTTPS pour les services VPC Lattice

Un écouteur est un processus qui vérifie les demandes de connexion. Vous définissez un écouteur lorsque vous créez votre service. Vous pouvez ajouter des écouteurs à votre service dans VPC Lattice à tout moment.

Vous pouvez créer un écouteur HTTPS, qui utilise TLS version 1.2 pour mettre fin directement aux connexions HTTPS avec VPC Lattice. VPC Lattice fournira et gérera un certificat TLS associé au nom de domaine complet (FQDN) généré par VPC Lattice. VPC Lattice prend en charge le protocole TLS sur HTTP/1.1 et HTTP/2. Lorsque vous configurez un service avec un écouteur HTTPS, VPC Lattice détermine automatiquement le protocole HTTP via la négociation du protocole ALPN (Application-Layer Protocol Negotiation). Si ALPN est absent, VPC Lattice utilise par défaut HTTP/1.1.

VPC Lattice utilise une architecture multi-tenant, ce qui signifie qu'il peut héberger plusieurs services sur le même point de terminaison. VPC Lattice utilise le protocole TLS avec indication du nom du serveur (SNI) pour chaque demande du client.

VPC Lattice peut écouter les protocoles HTTP, HTTPS, HTTP/1.1 et HTTP/2 et communiquer avec des cibles dans n'importe lequel de ces protocoles et versions. Il n'est pas nécessaire que ces configurations d'écouteur et de groupe cible correspondent. VPC Lattice gère l'ensemble du processus de mise à niveau et de rétrogradation entre les protocoles et les versions. Pour plus d'informations, consultez Version du protocole.

Pour vous assurer que votre application déchiffre le trafic, créez plutôt un écouteur TLS. Avec le relais TLS, VPC Lattice ne met pas fin au TLS. Pour plus d'informations, consultez Écouteurs TLS.

Table des matières

Politique de sécurité

VPC Lattice utilise une politique de sécurité qui combine le protocole TLSv1.2 et une liste de chiffrements SSL/TLS. Le protocole établit une connexion sécurisée entre un client et un serveur et permet de garantir que toutes les données transmises entre le client et votre service dans VPC Lattice 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. Au cours du processus de négociation de connexion, le client et VPC Lattice présentent une liste de chiffrements et de protocoles qu'ils prennent chacun en charge, par ordre de préférence. Par défaut, le premier chiffrement sur la liste du serveur qui correspond à l'un des chiffrements du client est sélectionné pour la connexion sécurisée.

VPC Lattice utilise le protocole TLSv1.2 et les chiffrements SSL/TLS suivants dans cet ordre de préférence :

- `ECDHE-RSA-AES128-GCM-SHA256`
- `ECDHE-RSA-AES128-SHA`
- `ECDHE-RSA-AES256-GCM-SHA384`
- `ECDHE-RSA-AES256-SHA`
- `AES128-GCM-SHA256`
- `AES128-SHA`
- `AES256-GCM-SHA384`

- `AES256-SHA`

Politique ALPN

La négociation du protocole ALPN (Application-Layer Protocol Negotiation) est une extension TLS envoyée lors des premiers messages d'accueil TLS. 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 initie une connexion ALPN, le service VPC Lattice compare la liste de préférences ALPN du client avec sa politique ALPN. Si le client prend en charge un protocole issu de la politique ALPN, le service VPC Lattice établit la connexion en fonction de la liste de préférences de la politique ALPN. Dans le cas contraire, le service n'utilise pas ALPN.

VPC Lattice prend en charge la politique ALPN suivante :

`HTTP2Preferred`

Préférez HTTP/2 à HTTP/1.1. La liste des préférences ALPN est h2, http/1.1.

Ajout d'un écouteur HTTPS

Vous configurez un écouteur avec un protocole et un port pour les connexions des clients au service, et un groupe cible pour la règle d'écouteur par défaut. Pour plus d'informations, consultez Configuration des écouteurs.

Prérequis

- Pour ajouter une action directe à la règle d'écoute par défaut, vous devez spécifier un groupe cible VPC Lattice disponible. Pour plus d'informations, consultez Création d'un groupe cible VPC Lattice.
- Vous pouvez spécifier le même groupe cible dans plusieurs écouteurs, mais ces écouteurs doivent appartenir au même service VPC Lattice. Pour utiliser un groupe cible avec un service VPC Lattice, vous devez vérifier qu'il n'est pas utilisé par un écouteur pour un autre service VPC Lattice.
- Vous pouvez utiliser le certificat fourni par VPC Lattice ou importer votre propre certificat dans. AWS Certificate Manager Pour plus d'informations, consultez the section called "BYOC".

Ajouter un écouteur HTTPS à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Services.
3. Sélectionnez le nom du service pour ouvrir sa page de détails.
4. Dans l'onglet Routage, choisissez Ajouter un écouteur.
5. Pour le nom de l'écouteur, vous pouvez soit fournir un nom d'écouteur personnalisé, soit utiliser le protocole et le port de votre écouteur comme nom d'écouteur. Le nom personnalisé que vous spécifiez peut comporter jusqu'à 63 caractères et doit être unique pour chaque service de votre compte. Les caractères valides sont a-z, 0-9 et les tirets (-). Vous ne pouvez pas utiliser de tiret comme premier ou dernier caractère, ni immédiatement après un autre tiret. Vous ne pouvez pas modifier le nom d'un écouteur après l'avoir créé.
6. Pour Protocole : port, choisissez HTTPS et entrez un numéro de port.
7. Pour l'action par défaut, choisissez le groupe cible du réseau VPC pour recevoir le trafic et choisissez le poids à attribuer à ce groupe cible. Le poids que vous attribuez à un groupe cible définit sa priorité pour recevoir du trafic. Par exemple, si deux groupes cibles ont le même poids, chaque groupe cible reçoit la moitié du trafic. Si vous n'avez spécifié qu'un seul groupe cible, 100 % du trafic est envoyé à ce groupe cible.

   Vous pouvez éventuellement ajouter un autre groupe cible pour l'action par défaut. Choisissez Ajouter une action, puis choisissez un groupe cible et spécifiez son poids.
8. (Facultatif) Pour ajouter une autre règle, choisissez Ajouter une règle, puis entrez un nom, une priorité, une condition et une action pour la règle.

   Vous pouvez attribuer à chaque règle un numéro de priorité compris entre 1 et 100. Un écouteur ne peut pas avoir plusieurs règles ayant la même priorité. Les règles sont évaluées par ordre de priorité, de la valeur la plus basse à la valeur la plus haute. La règle par défaut est évaluée en dernier. Pour plus d'informations, consultez Règles d'un écouteur.
9. (Facultatif) Pour ajouter des balises, développez les balises Listener, choisissez Ajouter une nouvelle balise, puis entrez une clé de balise et une valeur de balise.
10. Pour les paramètres du certificat d'écouteur HTTPS, si vous n'avez pas spécifié de nom de domaine personnalisé lors de la création du service, VPC Lattice génère automatiquement un certificat TLS pour sécuriser le trafic passant par l'écouteur.

    Si vous avez créé le service avec un nom de domaine personnalisé, mais que vous n'avez pas spécifié de certificat correspondant, vous pouvez le faire maintenant en choisissant le certificat dans Certificat SSL/TLS personnalisé. Dans le cas contraire, le certificat que vous avez spécifié lors de la création du service est déjà choisi.
11. Vérifiez votre configuration, puis choisissez Ajouter.

Pour ajouter un écouteur HTTPS à l'aide du AWS CLI

Utilisez la commande create-listener pour créer un écouteur avec une règle par défaut, et la commande create-rule pour créer des règles d'écouteur supplémentaires.

Écouteurs TLS pour les services VPC Lattice

Un écouteur est un processus qui vérifie les demandes de connexion. Vous pouvez définir un écouteur lorsque vous créez votre service VPC Lattice. Vous pouvez ajouter des auditeurs à votre service à tout moment.

Vous pouvez créer un écouteur TLS afin que VPC Lattice transmette le trafic chiffré à vos applications sans le déchiffrer.

Si vous préférez que VPC Lattice déchiffre le trafic chiffré et envoie le trafic non chiffré à vos applications, créez plutôt un écouteur HTTPS. Pour plus d'informations, consultez Écouteurs HTTPS.

Considérations

Les considérations suivantes s'appliquent aux écouteurs TLS :

- Le service VPC Lattice doit avoir un nom de domaine personnalisé. Le nom de domaine personnalisé du service est utilisé comme correspondance avec l'indication du nom de service (SNI). Si vous avez spécifié un certificat lors de la création du service, celui-ci n'est pas utilisé.
- La seule règle autorisée pour un écouteur TLS est la règle par défaut.
- L'action par défaut d'un écouteur TLS doit être une action de transfert vers un groupe cible TCP.
- Par défaut, les contrôles de santé sont désactivés pour les groupes cibles TCP. Si vous activez les contrôles de santé pour un groupe cible TCP, vous devez spécifier un protocole et une version du protocole.
- Les écouteurs TLS acheminent les demandes à l'aide du champ SNI du message client-hello. Vous pouvez utiliser des certificats Wildcard et SAN sur vos cibles si la condition correspondante correspond exactement au client-hello.
- Comme tout le trafic reste chiffré du client vers la cible, VPC Lattice ne peut pas lire les en-têtes HTTP et ne peut ni insérer ni supprimer d'en-têtes HTTP. Par conséquent, avec un écouteur TLS, les limites suivantes existent :
  - La durée de connexion est limitée à 10 minutes

- Les politiques d'authentification sont limitées aux principaux anonymes
- Les cibles Lambda ne sont pas prises en charge

Ajouter un écouteur TLS

Vous configurez un écouteur avec un protocole et un port pour les connexions des clients au service, et un groupe cible pour la règle d'écouteur par défaut. Pour plus d'informations, consultez Configuration des écouteurs.

Pour ajouter un écouteur TLS à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Services.
3. Sélectionnez le nom du service pour ouvrir sa page de détails.
4. Dans l'onglet Routage, choisissez Ajouter un écouteur.
5. Pour le nom de l'écouteur, vous pouvez soit fournir un nom d'écouteur personnalisé, soit utiliser le protocole et le port de votre écouteur comme nom d'écouteur. Le nom personnalisé que vous spécifiez peut comporter jusqu'à 63 caractères et doit être unique pour chaque service de votre compte. Les caractères valides sont a-z, 0-9 et les tirets (-). Vous ne pouvez pas utiliser de tiret comme premier ou dernier caractère, ni immédiatement après un autre tiret. Vous ne pouvez pas modifier le nom d'un écouteur après l'avoir créé.
6. Pour Protocole, choisissez TLS. Pour Port, entrez un numéro de port.
7. Pour Transférer vers le groupe cible, choisissez un groupe cible VPC Lattice qui utilise le protocole TCP pour recevoir le trafic, puis choisissez le poids à attribuer à ce groupe cible. Vous pouvez éventuellement ajouter un autre groupe cible. Choisissez Ajouter un groupe cible, puis choisissez un groupe cible et entrez son poids.
8. (Facultatif) Pour ajouter des balises, développez les balises Listener, choisissez Ajouter une nouvelle balise, puis entrez une clé de balise et une valeur de balise.
9. Vérifiez votre configuration, puis choisissez Ajouter.

Pour ajouter un écouteur TLS à l'aide du AWS CLI

Utilisez la commande create-listener pour créer un écouteur avec une règle par défaut. Spécifiez le protocole TLS_PASSTHROUGH.

Règles d'écoute pour votre service VPC Lattice

Chaque écouteur possède une règle par défaut et des règles supplémentaires que vous pouvez définir. Chaque règle comprend une priorité, une ou plusieurs actions et une ou plusieurs conditions. Vous pouvez ajouter ou modifier des règles à tout moment.

Table des matières

Règles par défaut

Lorsque vous créez un écouteur, vous définissez des actions pour la règle par défaut. Les règles par défaut ne peuvent pas avoir de conditions. Si aucune condition des règles d'un écouteur n'est satisfaite, l'action spécifiée pour la règle par défaut est effectuée.

Priorité de la règle

Chaque règle a une priorité. Les règles sont évaluées par ordre de priorité, de la valeur la plus basse à la valeur la plus haute. La règle par défaut est évaluée en dernier. Vous pouvez modifier la priorité d'une règle autre que celle par défaut à tout moment. Vous ne pouvez pas modifier la priorité de la règle par défaut.

Action de la règle

Les écouteurs des services VPC Lattice prennent en charge les actions avancées et les actions à réponse fixe.

Actions de réacheminement

Vous pouvez utiliser `forward` des actions pour acheminer les demandes vers un ou plusieurs groupes cibles VPC Lattice. Si vous spécifiez plusieurs groupes cibles pour une action `forward`,

vous devez spécifier une pondération pour chaque groupe cible. Le poids de chaque groupe cible est une valeur comprise entre 0 et 999. Les demandes qui correspondent à une règle d'écouteur avec des groupes cibles pondérés sont distribuées à ces groupes cibles en fonction de leur pondération. Par exemple, si vous spécifiez deux groupes cibles, chacun ayant une pondération de 10, chaque groupe cible reçoit la moitié des demandes. Si vous spécifiez deux groupes cibles, l'un avec une pondération de 10 et l'autre avec une pondération de 20, le groupe cible avec une pondération de 20 reçoit deux fois plus de demandes que l'autre groupe cible.

Actions de réponse fixe

Vous pouvez utiliser des actions `fixed-response` pour supprimer des demandes clients et renvoyer une réponse HTTP personnalisée. Vous pouvez utiliser cette action pour renvoyer un code de réponse 404.

Example Exemple d'action de réponse fixe pour le AWS CLI

Vous pouvez spécifier une action lorsque vous créez ou mettez à jour une règle. L'action suivante envoie une réponse fixe avec le code d'état spécifié.

```
"action": {
    "fixedResponse": {
        "statusCode": 404
},
```

Conditions de règle

Chaque condition de règle comporte un type et des informations de configuration. Lorsque les conditions d'une règle sont satisfaites, ses actions sont effectuées.

Les critères de correspondance pris en charge pour une règle sont les suivants :

Correspondance d'en-tête

Le routage est basé sur les en-têtes HTTP de chaque demande. Vous pouvez utiliser des conditions de l'en-tête HTTP pour configurer des règles qui acheminent des demandes, en fonction des en-têtes HTTP de la demande. Vous pouvez spécifier les noms des champs d'en-tête HTTP standard ou personnalisés. Le nom de l'en-tête et l'évaluation de la correspondance ne distinguent pas les majuscules et minuscules. Vous pouvez modifier ce paramètre en activant la distinction majuscules/majuscules. Les caractères génériques ne sont pas pris en charge par

le nom de l'en-tête. Les correspondances entre les préfixes, exacts et contenus sont prises en charge lors de la correspondance des en-têtes.

Correspondance des méthodes

Le routage est basé sur la méthode de requête HTTP de chaque demande.

Vous pouvez utiliser des conditions de méthode de demande HTTP pour configurer des règles qui acheminent des demandes, en fonction de la méthode de demande HTTP de la demande. Vous pouvez spécifier des méthodes HTTP standard ou personnalisées. La correspondance des méthodes fait la distinction majuscules/minuscules. Le nom de la méthode doit correspondre exactement. Les caractères génériques ne sont pas pris en charge.

Correspondance de trajectoire

Le routage est basé sur la correspondance des modèles de chemin dans les URL de demande.

Vous pouvez utiliser les conditions de chemin pour définir des règles qui acheminent les demandes en fonction de l'URL contenue dans la demande. Les caractères génériques ne sont pas pris en charge. Le préfixe et la correspondance exacte sur le chemin sont pris en charge.

Ajout d'une règle

Vous pouvez ajouter une règle d'écoute à tout moment.

Pour ajouter une règle d'écoute à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Services.
3. Sélectionnez le nom du service pour ouvrir sa page de détails.
4. Dans l'onglet Routage, choisissez Modifier l'écouteur.
5. Développez les règles du récepteur et choisissez Ajouter une règle.
6. Dans Nom de la règle, entrez le nom de la règle.
7. Pour Priorité, entrez une priorité comprise entre 1 et 100. Les règles sont évaluées par ordre de priorité, de la valeur la plus basse à la valeur la plus haute. La règle par défaut est évaluée en dernier.
8. Pour Condition, entrez un modèle de chemin pour la condition de correspondance du chemin. La taille maximale de chaque chaîne est de 200 caractères. La comparaison ne fait pas la distinction majuscules/minuscules. Les caractères génériques ne sont pas pris en charge.

Pour ajouter une condition de correspondance d'en-tête ou de règle de correspondance de méthode, utilisez le AWS CLI ou un AWS SDK.

9. Pour Action, choisissez un groupe cible VPC Lattice.
10. Sélectionnez Enregistrer les modifications.

Pour ajouter une règle à l'aide du AWS CLI

Utilisez la commande create-rule.

Mettre à jour une règle

Vous pouvez mettre à jour une règle d'écoute à tout moment. Vous pouvez modifier sa priorité, sa condition, son groupe cible et le poids de chaque groupe cible. Vous ne pouvez pas modifier le nom de la règle.

Pour mettre à jour une règle d'écoute à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Services.
3. Sélectionnez le nom du service pour ouvrir sa page de détails.
4. Dans l'onglet Routage, choisissez Modifier l'écouteur.
5. Modifiez les priorités, les conditions et les actions des règles selon vos besoins.
6. Passez en revue vos mises à jour et choisissez Enregistrer les modifications.

Pour mettre à jour une règle à l'aide du AWS CLI

Utilisez la commande update-rule.

Suppression d'une règle

Vous pouvez supprimer les règles autres que celles par défaut pour un écouteur à tout moment. Vous ne pouvez pas supprimer la règle par défaut pour un écouteur. Lorsque vous supprimez un écouteur, toutes ses règles sont supprimées.

Pour supprimer une règle d'écoute à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Services.
3. Sélectionnez le nom du service pour ouvrir sa page de détails.
4. Dans l'onglet Routage, choisissez Modifier l'écouteur.
5. Trouvez la règle et choisissez Supprimer.
6. Sélectionnez Enregistrer les modifications.

Pour supprimer une règle à l'aide du AWS CLI

Utilisez la commande delete-rule.

Mette à jour un écouteur

Après avoir créé un écouteur, vous pouvez remplacer le groupe cible pour l'action par défaut. Vous pouvez également ajouter un groupe cible à l'action par défaut et attribuer des pondérations aux groupes cibles. Vous ne pouvez pas mettre à jour le nom, le protocole ou le port de l'écouteur.

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

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Services.
3. Sélectionnez le nom du service pour ouvrir sa page de détails.
4. Dans l'onglet Routage, choisissez Modifier l'écouteur.
5. Pour l'action par défaut, vous pouvez mettre à jour le groupe cible ou le poids selon vos besoins.
6. Pour ajouter des groupes cibles supplémentaires, choisissez Ajouter une action, puis choisissez un groupe cible et spécifiez son poids.
7. Vous pouvez également ajouter, modifier ou supprimer des règles d'écoute. Pour plus d'informations, consultez Règles d'un écouteur.
8. Passez en revue vos mises à jour, puis choisissez Enregistrer les modifications.

Pour mettre à jour l'action par défaut d'un écouteur à l'aide du AWS CLI

Utilisez la commande update-listener.

Supprimer un écouteur

Vous pouvez supprimer un écouteur à tout moment. Lorsque vous supprimez un écouteur, toutes ses règles sont automatiquement supprimées.

Pour supprimer un écouteur à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Services.
3. Sélectionnez le nom du service pour ouvrir sa page de détails.
4. Dans l'onglet Routage, choisissez Supprimer l'écouteur.
5. Lorsque vous êtes invité à confirmer, entrez **`confirm`**, puis choisissez Delete (Supprimer).

Pour supprimer un écouteur à l'aide du AWS CLI

Utilisez la commande delete-listener.

Partagez vos ressources VPC Lattice

Amazon VPC Lattice s'intègre à AWS Resource Access Manager (AWS RAM) pour permettre le partage des ressources. AWS RAMest un service qui vous permet de partager certaines ressources VPC Lattice avec d'autres ou Comptes AWS via. AWS Organizations Avec AWS RAM, vous pouvez partager des ressources dont vous êtes propriétaire en créant un partage de ressources. Un partage de ressources spécifie les ressources à partager, ainsi que les consommateurs avec qui elles seront partagées. Les consommateurs peuvent inclure :

- Spécifique Comptes AWS à l'intérieur ou à l'extérieur de son organisation dansAWS Organizations.
- Une unité organisationnelle au sein de son organisation enAWS Organizations.
- Toute une organisation enAWS Organizations.

Pour plus d'informations sur AWS RAM, consultez le AWS RAMGuide de l'utilisateur .

Table des matières

Conditions préalables au partage des ressources VPC Lattice

- Pour partager une ressource, vous devez la posséder dans votreCompte AWS. Cela signifie que la ressource doit être allouée ou provisionnée dans votre compte. Vous ne pouvez pas partager une ressource qui a été partagée avec vous.
- Pour partager une ressource avec votre organisation ou une unité organisationnelle dansAWS Organizations, vous devez activer le partage avecAWS Organizations. Pour plus d'informations, voir Activer le partage des ressources AWS Organizations dans le Guide de AWS RAM l'utilisateur.

Partagez les ressources VPC Lattice

Pour partager une ressource, commencez par créer un partage de ressources à l'aide deAWS Resource Access Manager. Un partage de ressources indique les ressources à partager, les consommateurs avec lesquels elles sont partagées et les actions que les principaux peuvent effectuer.

Lorsque vous partagez une ressource VPC Lattice que vous possédez avec d'autres utilisateursComptes AWS, vous permettez à ces comptes d'associer leurs ressources aux ressources de votre compte. Lorsque vous créez une association avec une ressource partagée, nous générons un Amazon Resource Name (ARN) dans le compte du propriétaire de la ressource et un ARN dans le compte qui a créé l'association. Ainsi, le propriétaire de la ressource et le compte qui a créé l'association peuvent supprimer l'association.

Si vous faites partie d'une organisation AWS Organizations et que le partage au sein de votre organisation est activé, les consommateurs de votre organisation ont automatiquement accès à la ressource partagée. Dans le cas contraire, les consommateurs reçoivent une invitation à rejoindre le partage de ressources et ont accès à la ressource partagée après avoir accepté l'invitation.

Considérations

- Vous pouvez partager deux types de ressources VPC Lattice : les réseaux de services et les services.
- Vous pouvez partager vos ressources VPC Lattice avec n'importe qui. Compte AWS
- Vous ne pouvez pas partager vos ressources VPC Lattice avec des utilisateurs et des rôles IAM individuels.
- VPC Lattice prend en charge les autorisations gérées par le client pour les réseaux de services et les services.

Pour partager une ressource dont vous êtes propriétaire à l'aide de la console VPC Lattice

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Services ou Réseaux de services.
3. Choisissez le nom de la ressource pour ouvrir sa page de détails, puis choisissez Partager le service ou Partager le réseau de services dans l'onglet Partage.
4. Choisissez les partages de AWS RAM ressources dans Partages de ressources. Pour créer un partage de ressources, choisissez Créer un partage de ressources dans la console RAM.

5. Choisissez Partager le service ou Partager le réseau de services.

Pour partager une ressource dont vous êtes propriétaire à l'aide de la AWS RAM console

Suivez la procédure décrite dans la section Création d'un partage de ressources dans le guide de AWS RAM l'utilisateur.

Pour partager une ressource dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande associate-resource-share.

Arrêtez de partager les ressources VPC Lattice

Pour arrêter de partager une ressource VPC Lattice dont vous êtes propriétaire, vous devez la supprimer du partage de ressources. Les associations existantes sont conservées une fois que vous avez arrêté de partager votre ressource. Les nouvelles associations à une ressource précédemment partagée ne sont pas autorisées. Lorsque le propriétaire de la ressource ou le propriétaire de l'association supprime une association, celle-ci est supprimée des deux comptes. Si le titulaire d'un compte souhaite quitter un partage de ressources, il doit demander au propriétaire du partage de ressources de supprimer le compte.

Pour arrêter de partager une ressource dont vous êtes propriétaire à l'aide de la console VPC Lattice

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, sélectionnez Services ou Réseaux de services.
3. Choisissez le nom de la ressource pour ouvrir sa page de détails.
4. Dans l'onglet Partage, cochez la case correspondant au partage de ressources, puis choisissez Supprimer.

Pour arrêter de partager une ressource dont vous êtes propriétaire à l'aide de la AWS RAM console

Voir Mettre à jour un partage de ressources dans le guide de AWS RAM l'utilisateur.

Pour arrêter de partager une ressource dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande disassociate-resource-share.

Responsabilités et autorisations

Les responsabilités et autorisations suivantes s'appliquent lors de l'utilisation de ressources VPC Lattice partagées.

Propriétaires des ressources

- Le propriétaire du réseau de services ne peut pas modifier un service créé par un consommateur.
- Le propriétaire du réseau de services ne peut pas supprimer un service créé par un consommateur.
- Le propriétaire du réseau de service peut décrire toutes les associations de services du réseau de service.
- Le propriétaire du réseau de services peut dissocier tout service associé au réseau de services, quel que soit le créateur de l'association.
- Le propriétaire du réseau de service peut décrire toutes les associations VPC pour le réseau de service.
- Le propriétaire du réseau de service peut dissocier tout VPC associé au réseau de service par un consommateur.
- Le propriétaire du service peut décrire toutes les associations réseau avec le service.
- Le propriétaire du service peut dissocier un service de tout réseau de service auquel il est associé.
- Seul le compte qui a créé une association peut mettre à jour l'association entre le réseau de service et le VPC.

Consommateurs de ressources

- Le consommateur ne peut pas supprimer un service qu'il n'a pas créé.
- Le consommateur ne peut dissocier que les services qu'il a associés à un réseau de services.
- Le consommateur et le propriétaire du réseau peuvent décrire toutes les associations entre un réseau de services et un service.
- Le consommateur ne peut pas récupérer les informations de service d'un service dont il n'est pas le propriétaire.
- Le consommateur peut décrire toutes les associations de services associées à un réseau de services partagés.

- Le consommateur peut associer un service à un réseau de services partagés.
- Le consommateur peut voir toutes les associations VPC associées à un réseau de services partagés.
- Le consommateur peut associer un VPC à un réseau de services partagés.
- Le consommateur ne peut dissocier que les VPC qu'il a associés à un réseau de services.
- Le consommateur d'un service partagé ne peut pas associer un service à un réseau de services dont il n'est pas le propriétaire.
- Le consommateur d'un réseau de services partagés ne peut pas associer un VPC ou un service dont il n'est pas le propriétaire.
- Le consommateur peut décrire un service ou un réseau de services partagé avec lui.
- Le consommateur ne peut pas associer deux ressources si les deux sont partagées avec lui.

Événements multicomptes

Lorsque les propriétaires de ressources et les consommateurs effectuent des actions sur une ressource partagée, ces actions sont enregistrées en tant qu'événements entre comptes dansAWS CloudTrail.

`CreateServiceNetworkServiceAssociationBySharee`

Envoyé au propriétaire de la ressource lorsqu'un consommateur de ressources appelle CreateServiceNetworkServiceAssociationavec une ressource partagée. Si le service appartient à l'appelant, l'événement est envoyé au propriétaire du réseau de service. Si l'appelant possède le réseau de service, l'événement est envoyé au propriétaire du service.

`CreateServiceNetworkVpcAssociationBySharee`

Envoyé au propriétaire de la ressource lorsqu'un consommateur de ressources appelle CreateServiceNetworkVpcAssociationvia un réseau de services partagés.

`DeleteServiceNetworkServiceAssociationByOwner`

Envoyé au propriétaire de l'association lorsque le propriétaire de la ressource appelle DeleteServiceNetworkServiceAssociationavec une ressource partagée. Si le service appartient à l'appelant, l'événement est envoyé au propriétaire de l'association du réseau de services. Si l'appelant possède le réseau de service, l'événement est envoyé au propriétaire de l'association de services.

`DeleteServiceNetworkServiceAssociationBySharee`

Envoyé au propriétaire de la ressource lorsqu'un consommateur de ressources appelle DeleteServiceNetworkServiceAssociationavec une ressource partagée. Si le service appartient à l'appelant, l'événement est envoyé au propriétaire du réseau de service. Si l'appelant possède le réseau de service, l'événement est envoyé au propriétaire du service.

`DeleteServiceNetworkVpcAssociationByOwner`

Envoyé au propriétaire de l'association lorsque le propriétaire de la ressource appelle DeleteServiceNetworkVpcAssociationvia un réseau de services partagés.

`DeleteServiceNetworkVpcAssociationBySharee`

Envoyé au propriétaire de la ressource lorsqu'un consommateur de ressources appelle DeleteServiceNetworkVpcAssociationvia un réseau de services partagés.

`GetServiceBySharee`

Envoyé au propriétaire de la ressource lorsqu'un consommateur de ressources appelle GetServicevia un service partagé.

`GetServiceNetworkBySharee`

Envoyé au propriétaire de la ressource lorsqu'un consommateur de ressources appelle GetServiceNetworkvia un réseau de services partagés.

`GetServiceNetworkServiceAssociationBySharee`

Envoyé au propriétaire de la ressource lorsqu'un consommateur de ressources appelle GetServiceNetworkServiceAssociationavec une ressource partagée. Si le service appartient à l'appelant, l'événement est envoyé au propriétaire du réseau de service. Si l'appelant possède le réseau de service, l'événement est envoyé au propriétaire du service.

`GetServiceNetworkVpcAssociationBySharee`

Envoyé au propriétaire de la ressource lorsqu'un consommateur de ressources appelle GetServiceNetworkVpcAssociationvia un réseau de services partagés.

Voici un exemple d'entrée pour `CreateServiceNetworkServiceAssociationBySharee` cet événement.

```
{
    "eventVersion": "1.08",
```

```
    "userIdentity": {
        "type": "Unknown"
    },
    "eventTime": "2023-04-27T17:12:46Z",
    "eventSource": "vpc-lattice.amazonaws.com",
    "eventName": "CreateServiceNetworkServiceAssociationBySharee",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "vpc-lattice.amazonaws.com",
    "userAgent": "ec2.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "additionalEventData": {
        "callerAccountId": "111122223333"
    },
    "requestID": "ddabb0a7-70c6-4f70-a6c9-00cbe8a6a18b",
    "eventID": "bd03cdca-7edd-4d50-b9c9-eaa89f4a47cd",
    "readOnly": false,
    "resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::VpcLattice::ServiceNetworkServiceAssociation",
            "ARN": "arn:aws:vpc-
lattice:region:123456789012:servicenetworkserviceassociation/snsa-0d5ea7bc72EXAMPLE"
        }
    ],
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Sécurité dans Amazon VPC Lattice

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

La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon VPC Lattice, consultez la section AWS Services concernés par programme de conformitéAWS Services concernés par programme .
- Sécurité dans le cloud : vous êtes responsable de garder le contrôle sur votre contenu hébergé sur cette infrastructure. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de VPC Lattice. Les rubriques suivantes expliquent comment configurer VPC Lattice pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources VPC Lattice.

Table des matières

Gérez l'accès à vos services

VPC Lattice est sécurisé par défaut car vous devez indiquer clairement les services auxquels vous souhaitez donner accès et avec quels VPC. Pour les scénarios multicomptes, vous pouvez utiliser AWS Resource Access Managerpour partager des ressources au-delà des limites du compte. VPC Lattice fournit un cadre qui vous permet de mettre en œuvre une defense-in-depth stratégie sur plusieurs couches du réseau.

- Première couche : association du service et du VPC à un réseau de services. Si aucun VPC ou service spécifique n'est associé au réseau de services, les clients du VPC n'ont pas accès au service.
- Deuxième couche : protections de sécurité optionnelles au niveau du réseau pour le réseau de service, telles que les groupes de sécurité et les ACL réseau. En les utilisant, vous pouvez autoriser l'accès à des groupes de ressources spécifiques dans un VPC au lieu de toutes les ressources du VPC.
- Troisième couche : politique d'authentification VPC Lattice optionnelle. Vous pouvez appliquer une politique d'authentification aux réseaux de services et aux services individuels. Généralement, la politique d'authentification sur le réseau de service est gérée par l'administrateur du réseau ou du cloud, qui met en œuvre une autorisation grossière. Par exemple, autoriser uniquement les demandes authentifiées provenant d'une organisation spécifique dans AWS Organizations. Pour une politique d'authentification au niveau du service, le propriétaire du service définit généralement des contrôles précis, qui peuvent être plus restrictifs que l'autorisation grossière appliquée au niveau du réseau de service.

Méthodes de contrôle d'accès

- Politiques d'authentification
- Groupes de sécurité
- Listes ACL réseau

Contrôlez l'accès aux services à l'aide de politiques d'authentification

Les politiques d'authentification VPC Lattice sont des documents de politique IAM que vous attachez à des réseaux de services ou à des services pour contrôler si un principal spécifié a accès à un groupe de services ou à un service spécifique. Vous pouvez associer une politique d'authentification à chaque réseau de service ou service auquel vous souhaitez contrôler l'accès.

Les politiques d'authentification sont différentes des politiques basées sur l'identité IAM. Les politiques basées sur l'identité IAM sont associées aux utilisateurs, groupes ou rôles IAM et définissent les actions que ces identités peuvent effectuer sur quelles ressources. Les politiques d'authentification sont associées aux services et aux réseaux de services. Pour que l'autorisation réussisse, les politiques d'authentification et les politiques basées sur l'identité doivent comporter des instructions d'autorisation explicites. Pour plus d'informations, consultez Comment fonctionne l'autorisation.

Vous pouvez utiliser la console AWS CLI et pour afficher, ajouter, mettre à jour ou supprimer des politiques d'authentification sur les services et les réseaux de services. Lorsque vous utilisez le AWS CLI, n'oubliez pas que vos commandes s'exécutent dans la Région AWS configuration adaptée à votre profil. Si vous souhaitez exécuter les commandes dans une autre région, modifiez la région par défaut pour votre profil, ou utilisez le paramètre `--region` avec la commande.

Table des matières

Pour commencer à utiliser les politiques d'authentification, suivez la procédure de création d'une politique d'authentification qui s'applique à un réseau de services. Pour des autorisations plus restrictives que vous ne souhaitez pas appliquer à d'autres services, vous pouvez éventuellement définir des politiques d'authentification pour des services individuels.

Gérez l'accès à un réseau de services à l'aide de politiques d'authentification

Les AWS CLI tâches suivantes vous montrent comment gérer l'accès à un réseau de services à l'aide de politiques d'authentification. Pour obtenir des instructions relatives à l'utilisation de la console, reportez-vous àRéseaux de service en VPC Lattice.

Tâches

- Supprimer une politique d'authentification d'un réseau de service

Ajouter une politique d'authentification à un réseau de service

Suivez les étapes décrites dans cette section pour utiliser le AWS CLI pour :

- Activez le contrôle d'accès sur un réseau de service à l'aide d'IAM.
- Ajoutez une politique d'authentification au réseau de service. Si vous n'ajoutez pas de politique d'authentification, tout le trafic recevra un message d'erreur de refus d'accès.

Pour activer le contrôle d'accès et ajouter une politique d'authentification à un nouveau réseau de service

1. Pour activer le contrôle d'accès sur un réseau de service afin qu'il puisse utiliser une politique d'authentification, utilisez la create-service-network commande avec l'`--auth-type`option et la valeur de`AWS_IAM`.

   ```
   aws vpc-lattice create-service-network --name Name --auth-type AWS_IAM [--
   tags TagSpecification]
   ```

   Si elle aboutit, la commande renvoie un résultat semblable au suivant :

   ```
   {
      "arn": "arn",
      "authType": "AWS_IAM",
      "id": "sn-0123456789abcdef0",
      "name": "Name"
   }
   ```

2. Utilisez la put-auth-policy commande en spécifiant l'ID du réseau de service sur lequel vous souhaitez ajouter la politique d'authentification et la politique d'authentification que vous souhaitez ajouter.

   Par exemple, utilisez la commande suivante pour créer une politique d'authentification pour le réseau de service avec l'ID *sn-0123456789abcdef0*.

   ```
   aws vpc-lattice put-auth-policy --resource-identifier sn-0123456789abcdef0 --
   policy file://policy.json
   ```

Utilisez le JSON pour créer une définition de politique. Pour plus d'informations, consultez Éléments communs d'une politique d'authentification.

Si elle aboutit, la commande renvoie un résultat semblable au suivant :

```
{
   "policy": "policy",
   "state": "Active"
}
```

Pour activer le contrôle d'accès et ajouter une politique d'authentification à un réseau de service existant

1. Pour activer le contrôle d'accès sur un réseau de service afin qu'il puisse utiliser une politique d'authentification, utilisez la update-service-network commande avec l'`--auth-type`option et la valeur de`AWS_IAM`.

   ```
   aws vpc-lattice update-service-network --service-network-
   identifier sn-0123456789abcdef0 --auth-type AWS_IAM
   ```

   Si elle aboutit, la commande renvoie un résultat semblable au suivant :

   ```
   {
      "arn": "arn",
      "authType": "AWS_IAM",
      "id": "sn-0123456789abcdef0",
      "name": "Name"
   }
   ```

2. Utilisez la put-auth-policy commande en spécifiant l'ID du réseau de service sur lequel vous souhaitez ajouter la politique d'authentification et la politique d'authentification que vous souhaitez ajouter.

   ```
   aws vpc-lattice put-auth-policy --resource-identifier sn-0123456789abcdef0 --
   policy file://policy.json
   ```

   Utilisez le JSON pour créer une définition de politique. Pour plus d'informations, consultez Éléments communs d'une politique d'authentification.

Si elle aboutit, la commande renvoie un résultat semblable au suivant :

```
{
   "policy": "policy",
   "state": "Active"
}
```

Modifier le type d'authentification d'un réseau de services

Pour désactiver la politique d'authentification pour un réseau de service

Utilisez la update-service-network commande avec l'`--auth-type`option et la valeur de`NONE`.

```
aws vpc-lattice update-service-network --service-network-
identifier sn-0123456789abcdef0 --auth-type NONE
```

Si vous devez réactiver la politique d'authentification ultérieurement, exécutez cette commande en `AWS_IAM` spécifiant l'`--auth-type`option.

Supprimer une politique d'authentification d'un réseau de service

Pour supprimer une politique d'authentification d'un réseau de service

Utilisez la commande delete-auth-policy.

```
aws vpc-lattice delete-auth-policy --resource-identifier sn-0123456789abcdef0
```

La demande échoue si vous supprimez une politique d'authentification avant de changer le type d'authentification d'un réseau de service en. `NONE`

Gérer l'accès à un service à l'aide de politiques d'authentification

Les AWS CLI tâches suivantes vous montrent comment gérer l'accès à un service à l'aide de politiques d'authentification. Pour obtenir des instructions relatives à l'utilisation de la console, reportez-vous àServices en VPC Lattice.

Tâches

- Ajouter une politique d'authentification à un service

- Modifier le type d'authentification d'un service
- Supprimer une politique d'authentification d'un service

Ajouter une politique d'authentification à un service

Procédez comme suit pour utiliser le AWS CLI pour :

- Activez le contrôle d'accès sur un service à l'aide d'IAM.
- Ajoutez une politique d'authentification au service. Si vous n'ajoutez pas de politique d'authentification, tout le trafic recevra un message d'erreur de refus d'accès.

Pour activer le contrôle d'accès et ajouter une politique d'authentification à un nouveau service

1. Pour activer le contrôle d'accès sur un service afin qu'il puisse utiliser une politique d'authentification, utilisez la create-service commande avec l'`--auth-type`option et la valeur de`AWS_IAM`.

   ```
   aws vpc-lattice create-service --name Name --auth-type AWS_IAM [--
   tags TagSpecification]
   ```

   Si elle aboutit, la commande renvoie un résultat semblable au suivant :

   ```
   {
      "arn": "arn",
      "authType": "AWS_IAM",
      "dnsEntry": {
         ...
      },
      "id": "svc-0123456789abcdef0",
      "name": "Name",
      "status": "CREATE_IN_PROGRESS"
   }
   ```

2. Utilisez la put-auth-policy commande en spécifiant l'ID du service dans lequel vous souhaitez ajouter la politique d'authentification et la politique d'authentification que vous souhaitez ajouter.

   Par exemple, utilisez la commande suivante pour créer une politique d'authentification pour le service avec l'ID *svc-0123456789abcdef0*.

```
aws vpc-lattice put-auth-policy --resource-identifier svc-0123456789abcdef0 --
policy file://policy.json
```

Utilisez le JSON pour créer une définition de politique. Pour plus d'informations, consultez Éléments communs d'une politique d'authentification.

Si elle aboutit, la commande renvoie un résultat semblable au suivant :

```
{
   "policy": "policy",
   "state": "Active"
}
```

Pour activer le contrôle d'accès et ajouter une politique d'authentification à un service existant

1. Pour activer le contrôle d'accès sur un service afin qu'il puisse utiliser une politique d'authentification, utilisez la update-service commande avec l'`--auth-type`option et la valeur de`AWS_IAM`.

   ```
   aws vpc-lattice update-service --service-identifier svc-0123456789abcdef0 --auth-
   type AWS_IAM
   ```

   Si elle aboutit, la commande renvoie un résultat semblable au suivant :

   ```
   {
      "arn": "arn",
      "authType": "AWS_IAM",
      "id": "svc-0123456789abcdef0",
      "name": "Name"
   }
   ```

2. Utilisez la put-auth-policy commande en spécifiant l'ID du service dans lequel vous souhaitez ajouter la politique d'authentification et la politique d'authentification que vous souhaitez ajouter.

   ```
   aws vpc-lattice put-auth-policy --resource-identifier svc-0123456789abcdef0 --
   policy file://policy.json
   ```

Utilisez le JSON pour créer une définition de politique. Pour plus d'informations, consultez Éléments communs d'une politique d'authentification.

Si elle aboutit, la commande renvoie un résultat semblable au suivant :

```
{
   "policy": "policy",
   "state": "Active"
}
```

Modifier le type d'authentification d'un service

Pour désactiver la politique d'authentification d'un service

Utilisez la update-service commande avec l'`--auth-type`option et la valeur de`NONE`.

```
aws vpc-lattice update-service --service-identifier svc-0123456789abcdef0 --auth-type
 NONE
```

Si vous devez réactiver la politique d'authentification ultérieurement, exécutez cette commande en `AWS_IAM` spécifiant l'`--auth-type`option.

Supprimer une politique d'authentification d'un service

Pour supprimer une politique d'authentification d'un service

Utilisez la commande delete-auth-policy.

```
aws vpc-lattice delete-auth-policy --resource-identifier svc-0123456789abcdef0
```

La demande échoue si vous supprimez une politique d'authentification avant de changer le type d'authentification du service en. `NONE`

Si vous activez les politiques d'authentification qui nécessitent des demandes authentifiées adressées à un service, toutes les demandes adressées à ce service doivent contenir une signature de demande valide calculée à l'aide de la version 4 de signature (SigV4). Pour plus d'informations, consultez Exemples de demandes authentifiées de la version 4 de Signature.

Éléments communs d'une politique d'authentification

Les politiques d'authentification VPC Lattice sont spécifiées à l'aide de la même syntaxe que les politiques IAM. Pour plus d'informations, consultez les sections Politiques basées sur l'identité et politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Une politique d'authentification contient les éléments suivants :

- Principal : personne ou application autorisée à accéder aux actions et aux ressources de la déclaration. Dans une politique d'authentification, le principal est l'entité IAM destinataire de cette autorisation. Le principal est authentifié en tant qu'entité IAM pour envoyer des demandes à une ressource spécifique, ou à un groupe de ressources, comme dans le cas des services d'un réseau de services.

  Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou AWS des services. Pour plus d'informations, voir Éléments de politique AWS JSON : Principal dans le guide de l'utilisateur IAM.
- Effet : effet lorsque le principal spécifié demande l'action spécifique. Il peut correspondre à `Allow` ou `Deny`. Par défaut, lorsque vous activez le contrôle d'accès sur un service ou un réseau de services à l'aide d'IAM, les principaux ne sont pas autorisés à envoyer des demandes au service ou au réseau de services. Une valeur explicite remplace `Allow` donc la valeur par défaut.
- Actions — VPC Lattice prend en charge une action,. `vpc-lattice-svcs:Invoke` Cette autorisation permet au principal spécifié d'exécuter des demandes sur les ressources spécifiées dans l'`Resources`élément.
- Ressources : services concernés par l'action.
- État — Les conditions sont facultatives. Vous pouvez les utiliser pour contrôler la date d'entrée en vigueur de votre politique.

Lorsque vous créez et gérez des politiques d'authentification, vous souhaiterez peut-être utiliser le générateur de politiques IAM.

Exigence

La politique au format JSON ne doit pas contenir de nouvelles lignes ou de lignes vides.

Format de ressource pour les politiques d'authentification

Vous pouvez restreindre l'accès à des ressources spécifiques en créant une politique d'authentification qui utilise un schéma correspondant avec un `<serviceARN>/<path>` modèle et en codant l'`Resource`élément, comme indiqué dans les exemples suivants.

Exemples de ressources pour les politiques d'authentification

Protocole	Exemples
HTTP	• `"Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/rates"` • `"Resource": "*/rates"` • `"Resource": "*/*"`
gRPC	• `"Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/api.parking/GetRates"` • `"Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/api.parking/*"` • `"Resource": "arn:aws:vpc-lattice:us-west-2:1234567890:service/svc-0123456789abcdef0/*"`

Utilisez le format de ressource Amazon Resource Name (ARN) suivant pour `<serviceARN>` :

```
arn:aws:vpc-lattice:region:account-id:service/service-id
```

Par exemple :

```
"Resource": "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0"
```

Clés de condition pouvant être utilisées dans les politiques d'authentification

L'accès peut également être contrôlé par des clés de condition dans l'élément Condition des politiques d'authentification. Ces clés de condition sont présentes à des fins d'évaluation en fonction du protocole et du fait que la demande soit signée avec Signature Version 4 (SigV4) ou anonyme. Pour plus d'informations, consultez la section Clés de condition pour Amazon VPC Lattice Services dans la référence d'autorisation des services.

Exigence

Les clés de condition sont sensibles à la casse.

Clés de condition pour les politiques d'authentification

Clés de condition	Description	Exemple	Disponible pour les appelants anonymes (non authentifiés) ?	Disponible pour le gRPC ?
`vpc-lattice-svcs:Port`	Filtre l'accès par le port de service auquel la demande est envoyée	80	Oui	Oui
`vpc-lattice-svcs:RequestMethod`	Filtre l'accès en fonction de la méthode de la requête	GET	Oui	Publiez toujours
`vpc-lattice-svcs:RequestHeader/` *`header-name`* `:` *`value`*	Filtre l'accès en fonction d'une paire nom-valeur dans les en-têtes de la demande	content-type: application/json	Oui	Oui
`vpc-lattice-svcs:RequestQueryString/` *`key-name`*`:` *`value`*	Filtre l'accès en fonction des paires clé-valeur de la chaîne de requête dans l'URL de la demande	quux: [corge, grault]	Oui	Non

Clés de condition	Description	Exemple	Disponible pour les appelants anonymes (non authentifiés) ?	Disponible pour le gRPC ?
`vpc-lattice-svcs:ServiceNetworkArn`	Filtre l'accès par l'ARN du réseau de service du service qui reçoit la demande	arn:aws:vpc-lattice:us-west-2:123456789012:servicenetwork/sn-0123456789abcdef0	Oui	Oui
`vpc-lattice-svcs:ServiceArn`	Filtre l'accès par l'ARN du service qui reçoit la demande	arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0	Oui	Oui
`vpc-lattice-svcs:SourceVpc`	Filtre l'accès en fonction du VPC d'où provient la requête	vpc-1a2b3c4d	Oui	Oui
`vpc-lattice-svcs:SourceVpcOwnerAccount`	Filtre l'accès en fonction du compte propriétaire du VPC d'où provient la requête	123456789012	Oui	Oui

AWS fournit également des clés de condition supplémentaires que vous pouvez utiliser pour contrôler l'accès, telles que la clé de condition `aws:PrincipalOrgID` globale. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Principaux anonymes (non authentifiés)

Les principaux anonymes sont des appelants qui ne signent pas leurs AWS demandes avec Signature Version 4 (SigV4) et qui se trouvent au sein d'un VPC connecté au réseau de service. Les principaux anonymes peuvent envoyer des demandes non authentifiées aux services du réseau de services si une politique d'authentification le permet.

Exemples de politiques d'authentification

Voici des exemples de politiques d'authentification qui exigent que les demandes soient effectuées par des principaux authentifiés.

Tous les exemples utilisent la `us-west-2` région et contiennent des identifiants de compte fictifs.

Exemple 1 : Restreindre l'accès aux services d'une AWS organisation spécifique

L'exemple de politique d'authentification suivant accorde des autorisations à toute demande authentifiée pour accéder à tous les services du réseau de services auquel s'applique la politique. Cependant, la demande doit émaner de directeurs appartenant à l' AWS organisation spécifiée dans la condition.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": "vpc-lattice-svcs:Invoke",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "aws:PrincipalOrgID": [
                  "o-123456example"
               ]
            }
         }
```

```
      }
   ]
}
```

Exemple 2 : Restreindre l'accès à un service par un rôle IAM spécifique

L'exemple de politique d'authentification suivant accorde des autorisations à toute demande authentifiée utilisant le rôle IAM `rates-client` pour effectuer des requêtes HTTP GET sur le service spécifié dans l'élément. `Resource` La ressource de l'`Resource`élément est identique au service auquel la politique est attachée.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": [
               "arn:aws:iam::123456789012:role/rates-client"
            ]
         },
         "Action": "vpc-lattice-svcs:Invoke",
         "Resource": [
            "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0/
*"
         ],
         "Condition": {
            "StringEquals": {
               "vpc-lattice-svcs:RequestMethod": "GET"
            }
         }
      }
   ]
}
```

Exemple 3 : Restreindre l'accès aux services par des personnes authentifiées dans un VPC spécifique

L'exemple de politique d'authentification suivant autorise uniquement les demandes authentifiées provenant des principaux du VPC dont l'ID de VPC est. *vpc-1a2b3c4d*

```
{
```

```
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": "*",
         "Action": "vpc-lattice-svcs:Invoke",
         "Resource": "*",
         "Condition": {
            "StringNotEquals": {
               "aws:PrincipalType": "Anonymous"
            },
            "StringEquals": {
               "vpc-lattice-svcs:SourceVpc": "vpc-1a2b3c4d"
            }
         }
      }
   ]
}
```

Comment fonctionne l'autorisation

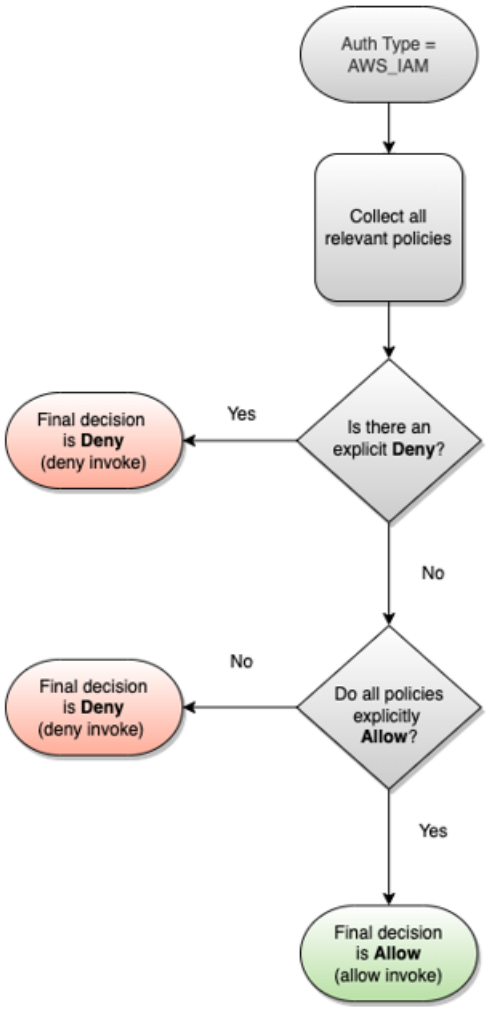
Lorsqu'un service VPC Lattice reçoit une demande, le code d' AWS application évalue ensemble toutes les politiques d'autorisation pertinentes afin de déterminer s'il convient d'autoriser ou de refuser la demande. Il évalue toutes les politiques basées sur l'identité IAM et les politiques d'authentification applicables dans le contexte de la demande lors de l'autorisation. Par défaut, toutes les demandes sont implicitement refusées lorsque le type d'authentification est. `AWS_IAM` Une autorisation explicite émanant de toutes les politiques pertinentes remplace la valeur par défaut.

L'autorisation inclut :

- Collecte de toutes les politiques basées sur l'identité IAM et des politiques d'authentification pertinentes.
- Évaluation de l'ensemble de politiques qui en résulte :
  - Vérifier que le demandeur (tel qu'un utilisateur ou un rôle IAM) est autorisé à effectuer l'opération depuis le compte auquel appartient le demandeur. S'il n'existe aucune instruction d'autorisation explicite, AWS cela n'autorise pas la demande.
  - Vérifier que la demande est autorisée par la politique d'authentification du réseau de service. Si une politique d'authentification est activée, mais qu'il n'existe aucune instruction d'autorisation explicite, AWS cela n'autorise pas la demande. S'il existe une instruction d'autorisation explicite, ou si le type d'authentification est le cas`NONE`, le code continue.

- Vérifier que la demande est autorisée par la politique d'authentification du service. Si une politique d'authentification est activée, mais qu'il n'existe aucune instruction d'autorisation explicite, AWS cela n'autorise pas la demande. S'il existe une instruction d'autorisation explicite, ou si le type d'authentification est le cas`NONE`, le code d'application renvoie la décision finale Allow.
- Un refus explicite dans n'importe quelle stratégie remplace toutes les autorisations.

Le schéma montre le flux de travail d'autorisation. Lorsqu'une demande est faite, les politiques pertinentes autorisent ou refusent à la demande l'accès à un service donné.



Contrôlez le trafic dans VPC Lattice à l'aide de groupes de sécurité

AWS les groupes de sécurité agissent comme des pare-feux virtuels, contrôlant le trafic réseau à destination et en provenance des ressources auxquelles ils sont associés. Avec VPC Lattice, vous pouvez créer des groupes de sécurité et les attribuer à l'association VPC qui relie un VPC à un

réseau de services afin d'appliquer des protections de sécurité supplémentaires au niveau du réseau pour votre réseau de services.

Table des matières

Liste de préfixes gérée

VPC Lattice fournit des listes de préfixes gérées qui incluent les adresses IP utilisées pour acheminer le trafic sur le réseau VPC Lattice. Vous pouvez faire référence aux listes de préfixes gérées par VPC Lattice dans les règles de votre groupe de sécurité. Cela permet au trafic de circuler depuis les clients, via le réseau de services VPC Lattice, et vers les cibles du service VPC Lattice.

Supposons, par exemple, qu'une instance EC2 soit enregistrée en tant que cible dans la région USA Ouest (Oregon) (`us-west-2`). Vous pouvez ajouter une règle au groupe de sécurité d'instance qui autorise l'accès HTTPS entrant depuis la liste de préfixes gérés par VPC Lattice, afin que le trafic VPC Lattice de cette région puisse atteindre l'instance. Si vous supprimez toutes les autres règles entrantes du groupe de sécurité, vous pouvez empêcher tout trafic autre que le trafic VPC Lattice d'atteindre l'instance.

Les noms des listes de préfixes gérées pour VPC Lattice sont les suivants :

- com.amazonaws.*region*.vpc-lattice
- com.amazonaws.*region*.ipv6.vpc-lattice

Pour plus d'informations, consultez les listes de préfixes gérés par AWS dans le Guide de l'utilisateur Amazon VPC.

Clients Windows

Les adresses figurant dans les listes de préfixes VPC Lattice sont des adresses locales de liens. Si vous vous connectez à VPC Lattice depuis un client Windows, vous devez mettre à jour la configuration du client Windows afin qu'il transfère les adresses de liaison locales utilisées par VPC Lattice à l'adresse IP principale du client. Voici un exemple de commande qui met à jour la configuration du client Windows, où se 169.254.171.0 trouve l'adresse lien-local utilisée par VPC Lattice.

```
C:\> route add 169.254.171.0 mask 255.255.255.0 primary-ip-address
```

Règles des groupes de sécurité

L'utilisation de VPC Lattice avec ou sans groupes de sécurité n'aura aucune incidence sur la configuration de votre groupe de sécurité VPC existant. Vous pouvez toutefois ajouter vos propres groupes de sécurité à tout moment.

Considérations clés

- Les règles de groupe de sécurité pour les clients contrôlent le trafic sortant vers VPC Lattice.
- Les règles de groupe de sécurité pour les cibles contrôlent le trafic entrant depuis le VPC Lattice vers les cibles, y compris le trafic de contrôle de santé.
- Les règles du groupe de sécurité pour l'association entre le réseau de service et le VPC contrôlent les clients qui peuvent accéder au réseau de service VPC Lattice.

Règles d'entrée recommandées pour les associations de réseaux de services et de VPC

Pour que le trafic circule des VPC clients vers les services associés au réseau de services, vous devez créer des règles entrantes pour les ports d'écoute et des protocoles d'écoute pour les services.

Entrant

Source	Protocole	Plage de ports	Comment
Bloc d'adresse du VPC	*listener*	*listener*	Autoriser le trafic des clients vers VPC Lattice

Règles sortantes recommandées pour le trafic circulant des instances clientes vers VPC Lattice

Par défaut, les groupes de sécurité autorisent la totalité du trafic sortant. Toutefois, si vous avez des règles de sortie personnalisées, vous devez autoriser le trafic sortant vers le préfixe VPC Lattice pour les ports et protocoles d'écoute afin que les instances clientes puissent se connecter à tous les services associés au réseau de services VPC Lattice. Vous pouvez autoriser ce trafic en référençant l'ID de la liste de préfixes pour VPC Lattice.

Sortant

Destination	Protocole	Plage de ports	Comment
ID de la liste des préfixes VPC Lattice	*listener*	*listener*	Autoriser le trafic des clients vers VPC Lattice

Règles entrantes recommandées pour le trafic circulant entre VPC Lattice et les instances cibles

Vous ne pouvez pas utiliser le groupe de sécurité client comme source pour les groupes de sécurité de votre cible, car le trafic provient de VPC Lattice. Vous pouvez référencer l'ID de la liste de préfixes pour VPC Lattice.

Entrant

Source	Protocole	Plage de ports	Comment
ID de la liste des préfixes VPC Lattice	*target*	*target*	Autoriser le trafic du VPC Lattice vers les cibles
ID de la liste des préfixes VPC Lattice	*health check*	*health check*	Autoriser le trafic de vérification de l'état du VPC Lattice vers les cibles

Gérer les groupes de sécurité pour une association VPC

Vous pouvez utiliser le AWS CLI pour afficher, ajouter ou mettre à jour des groupes de sécurité sur le VPC afin de desservir l'association réseau. Lorsque vous utilisez le AWS CLI, n'oubliez pas que vos commandes s'exécutent dans la Région AWS configuration adaptée à votre profil. Si vous souhaitez exécuter les commandes dans une autre région, modifiez la région par défaut pour votre profil, ou utilisez le paramètre `--region` avec la commande.

Avant de commencer, vérifiez que vous avez créé le groupe de sécurité dans le même VPC que le VPC que vous souhaitez ajouter au réseau de service. Pour plus d'informations, consultez la section

Contrôler le trafic vers les ressources à l'aide de groupes de sécurité dans le guide de l'utilisateur Amazon VPC

Pour ajouter un groupe de sécurité lorsque vous créez une association VPC à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Service networks.
3. Sélectionnez le nom du réseau de service pour ouvrir sa page de détails.
4. Dans l'onglet Associations VPC, choisissez Create VPC associations, puis choisissez Add VPC association.
5. Sélectionnez un VPC et jusqu'à cinq groupes de sécurité.
6. Sélectionnez Enregistrer les modifications.

Pour ajouter ou mettre à jour des groupes de sécurité pour une association VPC existante à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, sous VPC Lattice, choisissez Service networks.
3. Sélectionnez le nom du réseau de service pour ouvrir sa page de détails.
4. Dans l'onglet Associations VPC, cochez la case correspondant à l'association, puis choisissez Actions, Modifier les groupes de sécurité.
5. Ajoutez et supprimez des groupes de sécurité selon vos besoins.
6. Sélectionnez Enregistrer les modifications.

Pour ajouter un groupe de sécurité lorsque vous créez une association VPC à l'aide du AWS CLI

Utilisez la commande create-service-network-vpc-association, en spécifiant l'ID du VPC pour l'association VPC et l'ID des groupes de sécurité à ajouter.

```
aws vpc-lattice create-service-network-vpc-association \
    --service-network-identifier sn-0123456789abcdef0 \
    --vpc-identifier vpc-1a2b3c4d \
    --security-group-ids sg-7c2270198example
```

Si elle aboutit, la commande renvoie un résultat semblable au suivant :

```
{
  "arn": "arn",
  "createdBy": "464296918874",
  "id": "snva-0123456789abcdef0",
  "status": "CREATE_IN_PROGRESS",
  "securityGroupIds": ["sg-7c2270198example"]
}
```

Pour ajouter ou mettre à jour des groupes de sécurité pour une association VPC existante à l'aide du AWS CLI

Utilisez la commande update-service-network-vpc-association, en spécifiant l'ID du réseau de service et les ID des groupes de sécurité. Ces groupes de sécurité remplacent tous les groupes de sécurité précédemment associés. Définissez au moins un groupe de sécurité lors de la mise à jour de la liste.

```
aws vpc-lattice update-service-network-vpc-association
    --service-network-vpc-association-identifier sn-903004f88example \
    --security-group-ids sg-7c2270198example sg-903004f88example
```

> **Warning**
>
> Vous ne pouvez pas supprimer tous les groupes de sécurité. Au lieu de cela, vous devez d'abord supprimer l'association VPC, puis recréer l'association VPC sans aucun groupe de sécurité. Soyez prudent lorsque vous supprimez l'association VPC. Cela empêche le trafic d'atteindre les services qui se trouvent dans ce réseau de services.

Contrôlez le trafic vers VPC Lattice à l'aide des ACL réseau

Une liste de contrôle d'accès (ACL) réseau autorise ou refuse un trafic entrant ou sortant spécifique au niveau du sous-réseau. L'ACL réseau par défaut permet tout le trafic entrant et sortant. Vous pouvez créer des ACL réseau personnalisées pour vos sous-réseaux afin de fournir une couche de sécurité supplémentaire. Pour plus d'informations, consultez ACL réseau dans le Amazon VPC Guide de l'utilisateur.

Table des matières

ACL réseau pour les sous-réseaux de vos clients

Les ACL réseau pour les sous-réseaux clients doivent autoriser le trafic entre les clients et VPC Lattice. Vous pouvez obtenir la plage d'adresses IP à autoriser dans la liste des préfixes gérés pour VPC Lattice.

Entrant

Source	Protocole	Plage de ports	Comment
vpc_lattice_cidr_block	TCP	1025-65535	Autoriser le trafic entre VPC Lattice et les clients

Sortant

Destination	Protocole	Plage de ports	Comment
vpc_lattice_cidr_block	*listener*	*listener*	Autoriser le trafic des clients vers VPC Lattice

ACL réseau pour vos sous-réseaux cibles

Les ACL réseau pour les sous-réseaux cibles doivent autoriser le trafic entre les cibles et le VPC Lattice à la fois sur le port cible et sur le port de contrôle de santé. Vous pouvez obtenir la plage d'adresses IP à autoriser dans la liste des préfixes gérés pour VPC Lattice.

Entrant

Source	Protocole	Plage de ports	Comment
vpc_lattice_cidr_block	*target*	*target*	Autoriser le trafic du VPC Lattice vers les cibles
vpc_lattice_cidr_block	*health check*	*health check*	Autoriser le trafic de vérification de l'état du

Source	Protocole	Plage de ports	Comment
			VPC Lattice vers les cibles

Sortant

Destination	Protocole	Plage de ports	Comment
vpc_latti ce_cidr_block	*target*	1024-65535	Autoriser le trafic des cibles vers le VPC Lattice
vpc_latti ce_cidr_block	*health check*	1024-65535	Autoriser le trafic de contrôle de santé entre les cibles et le VPC Lattice

Exemples de demandes authentifiées de la version 4 de Signature

VPC Lattice utilise la version de signature 4 (Sigv4) ou la version de signature 4A (SigV4a) pour l'authentification du client. Pour plus d'informations, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Considérations

- VPC Lattice tente d'authentifier toute demande signée avec SigV4 ou SigV4a. La demande échoue sans authentification.
- VPC Lattice ne prend pas en charge la signature de la charge utile. Vous devez envoyer un `x-amz-content-sha256` en-tête dont la valeur est définie sur`"UNSIGNED-PAYLOAD"`.

Exemples

- Python
- Java avec intercepteur
- Java sans intercepteur
- Node.js

Python

Cet exemple envoie les demandes signées via une connexion sécurisée à un service enregistré sur le réseau. Si vous préférez utiliser des requêtes, le package botocore simplifie le processus d'authentification, mais n'est pas strictement obligatoire. Pour plus d'informations, consultez la section Credentials dans la documentation de Boto3.

Pour installer les `awscrt` packages `botocore` et, utilisez la commande suivante. Pour plus d'informations, consultez AWS CRT Python.

```
pip install botocore awscrt
```

Dans l'exemple suivant, remplacez les valeurs de l'espace réservé par vos propres valeurs.

SIGv4

```
from botocore import crt
import requests
from botocore.awsrequest import AWSRequest
from botocore.credentials import Credentials
import botocore.session

if __name__ == '__main__':
    session = botocore.session.Session()
    signer = crt.auth.CrtS3SigV4Auth(session.get_credentials(), 'vpc-lattice-svcs',
 'us-west-2')
    endpoint = 'https://user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
west-2.on.aws/create'
    data = "some-data-here"
    headers = {'Content-Type': 'application/json'}
    request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)
    request.context["has_streaming_input"] = True # payload signing is not supported
    signer.add_auth(request)

    prepped = request.prepare()

    response = requests.post(prepped.url, headers=prepped.headers, data=data)
```

SIGv4A

```
from botocore import crt
import requests
```

```
from botocore.awsrequest import AWSRequest
from botocore.credentials import Credentials
import botocore.session

if __name__ == '__main__':
    session = botocore.session.Session()
    signer = crt.auth.CrtS3SigV4AsymAuth(session.get_credentials(), 'vpc-lattice-
svcs', 'us-west-2')
    endpoint = 'https://user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
west-2.on.aws/create'
    data = "some-data-here"
    headers = {'Content-Type': 'application/json'}
    request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)
    request.context["has_streaming_input"] = True # payload signing is not supported
    signer.add_auth(request)

    prepped = request.prepare()

    response = requests.post(prepped.url, headers=prepped.headers, data=data)
```

Java avec intercepteur

Cet exemple utilise Amazon Request Signing Interceptor pour gérer la signature des demandes.

```
import com.amazonaws.http.AwsRequestSigningApacheInterceptor;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.auth.signer.Aws4UnsignedPayloadSigner;
import software.amazon.awssdk.regions.Region;

import java.nio.charset.StandardCharsets;

import org.apache.http.client.methods.HttpPost;
import org.apache.http.entity.ByteArrayEntity;
import org.apache.http.impl.client.CloseableHttpClient;
import org.apache.http.impl.client.HttpClients;

public class App {
    public static void main(String[] args) {
      var interceptor = new AwsRequestSigningApacheInterceptor(
          "vpc-lattice-svcs",
          Aws4UnsignedPayloadSigner.create(), // requires HTTPS
          DefaultCredentialsProvider.create(),
```

```
          Region.US_WEST_2.id()
          );
      CloseableHttpClient client = HttpClients.custom()
        .addInterceptorLast(interceptor)
        .build();

      var httpPost = new HttpPost("https://user-02222f67d3a427111.1234abc.vpc-lattice-
svcs.us-west-2.on.aws/create");
      httpPost.addHeader("content-type", "application/json");

      var body = """
      {
        "name": "Jane Doe",
        "job": "Engineer"
      }
      """;
      httpPost.setEntity(new ByteArrayEntity(body.getBytes(StandardCharsets.UTF_8)));

      try (var response = client.execute(httpPost)) {
        System.out.println(new
 String(response.getEntity().getContent().readAllBytes()));
      } catch (Exception e) {
        throw new RuntimeException(e);
      }
    }
}
```

Java sans intercepteur

Cet exemple montre comment effectuer la signature des demandes à l'aide d'intercepteurs personnalisés. Il utilise la classe de fournisseur d'informations d'identification par défaut from AWS SDK for Java 2.x, qui obtient les informations d'identification correctes pour vous. Si vous préférez utiliser un fournisseur d'informations d'identification spécifique, vous pouvez en sélectionner un parmi. AWS SDK for Java 2.x AWS SDK for Java Autorise uniquement les charges utiles non signées via HTTPS. Cependant, vous pouvez étendre le signataire pour prendre en charge les charges utiles non signées via HTTP.

```
import java.io.ByteArrayInputStream;
import java.io.IOException;
import java.nio.charset.StandardCharsets;
import java.util.HashMap;
import java.util.List;
```

```
import java.util.Map;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.auth.signer.Aws4UnsignedPayloadSigner;
import software.amazon.awssdk.auth.signer.AwsSignerExecutionAttribute;
import software.amazon.awssdk.core.interceptor.ExecutionAttributes;
import software.amazon.awssdk.http.SdkHttpFullRequest;
import software.amazon.awssdk.http.SdkHttpMethod;
import software.amazon.awssdk.regions.Region;

import org.apache.http.client.methods.HttpPost;
import org.apache.http.entity.ByteArrayEntity;
import org.apache.http.impl.client.CloseableHttpClient;
import org.apache.http.impl.client.HttpClients;

public class App {

    public static void main(String[] args) {
        var signer = Aws4UnsignedPayloadSigner.create(); // requires HTTPS

        Map<String, String> headers = new HashMap<>();
        headers.put("content-type", "application/json");
        var body = """
        {
            "name": "Jane Doe",
            "job": "Engineer"
        }
        """;

        String endpoint = "https://user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
west-2.on.aws/create";

        var sdkRequest = SdkHttpFullRequest.builder().method(SdkHttpMethod.POST);

        sdkRequest.host("user-02222f67d3a427111.1234abc.vpc-lattice-svcs.us-
west-2.on.aws");
        sdkRequest.protocol("HTTPS");
        sdkRequest.encodedPath("/create");
        sdkRequest.contentStreamProvider(() -> new
 ByteArrayInputStream(body.getBytes(StandardCharsets.UTF_8)));


        for (Map.Entry<String, String> header : headers.entrySet()) {
            sdkRequest.putHeader(header.getKey(), header.getValue());
        }
```

```
        ExecutionAttributes attributes = ExecutionAttributes.builder()
                .put(AwsSignerExecutionAttribute.AWS_CREDENTIALS,
 DefaultCredentialsProvider.create().resolveCredentials())
                .put(AwsSignerExecutionAttribute.SERVICE_SIGNING_NAME, "vpc-lattice-
svcs")
                .put(AwsSignerExecutionAttribute.SIGNING_REGION, Region.US_WEST_2)
                .build();

        SdkHttpFullRequest prepRequest = signer.sign(sdkRequest.build(), attributes);

        HttpPost httpPost = new HttpPost(endpoint);
        for (Map.Entry<String, List<String>> header : prepRequest.headers().entrySet())
 {
            if (header.getKey().equalsIgnoreCase("host")) { continue; }
            for(var value : header.getValue()) {
                httpPost.addHeader(header.getKey(), value);
            }
        }

        CloseableHttpClient client = HttpClients.custom().build();

        httpPost.setEntity(new ByteArrayEntity(body.getBytes(StandardCharsets.UTF_8)));

        try (var response = client.execute(httpPost)){
            System.out.println(new
 String(response.getEntity().getContent().readAllBytes()));
        } catch (IOException e) {
            throw new RuntimeException(e);
        }
    }
}
```

Node.js

Cet exemple utilise les liaisons NodeJS aws-crt pour envoyer une demande signée via HTTPS.

Pour installer le `aws-crt` package, utilisez la commande suivante.

```
npm -i aws-crt
```

Si la variable d'`AWS_REGION`environnement existe, l'exemple utilise la région spécifiée par`AWS_REGION`. La région par défaut est`us-east-1`.

SIGv4

```
const https = require('https')
const crt = require('aws-crt')
const { HttpRequest } = require('aws-crt/dist/native/http')

function sigV4Sign(method, endpoint, service, algorithm) {
    const host = new URL(endpoint).host
    const request = new HttpRequest(method, endpoint)
    request.headers.add('host', host)
    // crt.io.enable_logging(crt.io.LogLevel.INFO)
    const config = {
        service: service,
        region: process.env.AWS_REGION ? process.env.AWS_REGION : 'us-east-1',
        algorithm: algorithm,
        signature_type: crt.auth.AwsSignatureType.HttpRequestViaHeaders,
        signed_body_header: crt.auth.AwsSignedBodyHeaderType.XAmzContentSha256,
        signed_body_value: crt.auth.AwsSignedBodyValue.UnsignedPayload,
        provider: crt.auth.AwsCredentialsProvider.newDefault()
    }

    return crt.auth.aws_sign_request(request, config)
}

if (process.argv.length === 2) {
  console.error(process.argv[1] + ' <url>')
  process.exit(1)
}

const algorithm = crt.auth.AwsSigningAlgorithm.SigV4;

sigV4Sign('GET', process.argv[2], 'vpc-lattice-svcs').then(
  httpResponse => {
    var headers = {}

    for (const sigv4header of httpResponse.headers) {
      headers[sigv4header[0]] = sigv4header[1]
    }

    const options = {
      hostname: new URL(process.argv[2]).host,
      path: '/',
      method: 'GET',
      headers: headers
```

```
    }

    req = https.request(options, res => {
      console.log('statusCode:', res.statusCode)
      console.log('headers:', res.headers)
      res.on('data', d => {
        process.stdout.write(d)
      })
    })
    req.on('error', err => {
      console.log('Error: ' + err)
    })
    req.end()
  }
)
```

SIGv4A

```
const https = require('https')
const crt = require('aws-crt')
const { HttpRequest } = require('aws-crt/dist/native/http')

function sigV4Sign(method, endpoint, service, algorithm) {
    const host = new URL(endpoint).host
    const request = new HttpRequest(method, endpoint)
    request.headers.add('host', host)
    // crt.io.enable_logging(crt.io.LogLevel.INFO)
    const config = {
        service: service,
        region: process.env.AWS_REGION ? process.env.AWS_REGION : 'us-east-1',
        algorithm: algorithm,
        signature_type: crt.auth.AwsSignatureType.HttpRequestViaHeaders,
        signed_body_header: crt.auth.AwsSignedBodyHeaderType.XAmzContentSha256,
        signed_body_value: crt.auth.AwsSignedBodyValue.UnsignedPayload,
        provider: crt.auth.AwsCredentialsProvider.newDefault()
    }

    return crt.auth.aws_sign_request(request, config)
}

if (process.argv.length === 2) {
  console.error(process.argv[1] + ' <url>')
  process.exit(1)
```

```
}

const algorithm = crt.auth.AwsSigningAlgorithm.SigV4Asymmetric;

sigV4Sign('GET', process.argv[2], 'vpc-lattice-svcs').then(
  httpResponse => {
    var headers = {}

    for (const sigv4header of httpResponse.headers) {
      headers[sigv4header[0]] = sigv4header[1]
    }

    const options = {
      hostname: new URL(process.argv[2]).host,
      path: '/',
      method: 'GET',
      headers: headers
    }

    req = https.request(options, res => {
      console.log('statusCode:', res.statusCode)
      console.log('headers:', res.headers)
      res.on('data', d => {
        process.stdout.write(d)
      })
    })
    req.on('error', err => {
      console.log('Error: ' + err)
    })
    req.end()
  }
)
```

Protection des données dans Amazon VPC Lattice

Le modèle de responsabilité AWS partagée Le modèle s'applique à la protection des données dans Amazon VPC Lattice. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Ce contenu comprend les tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour

en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

Chiffrement en transit

VPC Lattice est un service entièrement géré composé d'un plan de contrôle et d'un plan de données. Chaque avion a un objectif distinct dans le service. Le plan de contrôle fournit les API administratives utilisées pour créer, lire/décrire, mettre à jour, supprimer et répertorier les ressources (CRUDL) (par exemple, et. `CreateService` `UpdateService` Les communications avec le plan de contrôle de VPC Lattice sont protégées en transit par le protocole TLS. Le plan de données est l'API Invoke de VPC Lattice qui assure l'interconnexion entre les services. Le protocole TLS chiffre également les communications avec le plan de données de VPC Lattice. La suite de chiffrement et la version du protocole utilisent les valeurs par défaut fournies par VPC Lattice et ne sont pas configurables. Pour plus d'informations, consultez Écouteurs HTTPS pour les services VPC Lattice.

Chiffrement au repos

Par défaut, le chiffrement des données au repos permet de réduire la charge opérationnelle et la complexité liées à la protection des données sensibles. Dans le même temps, il vous permet de créer des applications sécurisées qui répondent aux exigences réglementaires et de conformité strictes en matière de chiffrement.

Table des matières

Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)

Lorsque vous utilisez le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3), chaque objet est chiffré à l'aide d'une clé unique. Comme protection supplémentaire, il chiffre la clé elle-même à l'aide d'une clé racine dont il effectue une rotation régulière. Le chiffrement côté serveur Amazon S3 utilise l'un des chiffrements par bloc les plus puissants qui existent, Advanced Encryption Standard 256 bits (AES-256) GCM, pour chiffrer vos données. Pour les objets chiffrés avant AES-GCM, AES-CBC est toujours pris en charge pour déchiffrer ces objets. Pour plus d'informations, consultez Utilisation du chiffrement côté serveur avec des clés de chiffrement gérées par Amazon S3 (SSE-S3).

Si vous activez le chiffrement côté serveur avec des clés de chiffrement gérées par Amazon S3 (SSE-S3) pour votre compartiment S3 pour les journaux d'accès VPC Lattice, chiffre AWS automatiquement chaque fichier journal d'accès avant qu'il ne soit stocké dans votre compartiment S3. Pour plus d'informations, consultez la section Logs envoyés à Amazon S3 dans le guide de CloudWatch l'utilisateur Amazon.

Chiffrement côté serveur avec AWS KMS clés stockées dans AWS KMS (SSE-KMS)

Le chiffrement par AWS KMS clés côté serveur (SSE-KMS) est similaire au SSE-S3, mais l'utilisation de ce service comporte des avantages et des frais supplémentaires. Il existe des autorisations distinctes pour l'utilisation d'une AWS KMS clé qui fournit une protection supplémentaire contre l'accès non autorisé à vos objets dans Amazon S3. SSE-KMS vous fournit également une piste d'audit qui indique quand votre AWS KMS clé a été utilisée et par qui. Pour plus d'informations, voir Utilisation du chiffrement côté serveur avec AWS Key Management Service (SSE-KMS).

Table des matières

Chiffrement et déchiffrement de la clé privée de votre certificat

Votre certificat ACM et votre clé privée sont chiffrés à l'aide d'une clé KMS AWS gérée portant l'alias aws/acm. Vous pouvez consulter l'ID de clé avec cet alias dans la AWS KMS console sous clés AWS gérées.

VPC Lattice n'accède pas directement à vos ressources ACM. Il utilise le gestionnaire de connexion AWS TLS pour sécuriser et accéder aux clés privées de votre certificat. Lorsque vous utilisez votre certificat ACM pour créer un service VPC Lattice, VPC Lattice associe votre certificat au TLS Connection Manager. AWS Cela se fait en créant une subvention associée à votre AWS KMS clé AWS gérée avec le préfixe aws/acm. Une subvention est un instrument de politique qui permet au TLS Connection Manager d'utiliser des clés KMS dans le cadre d'opérations cryptographiques. L'autorisation permet au bénéficiaire principal (TLS Connection Manager) d'appeler les opérations d'autorisation spécifiées sur la clé KMS pour déchiffrer la clé privée de votre certificat. TLS Connection Manager utilise ensuite le certificat et la clé privée déchiffrée (texte brut) pour établir une connexion sécurisée (session SSL/TLS) avec les clients des services VPC Lattice. Lorsque le certificat est dissocié d'un service VPC Lattice, la subvention est retirée.

Si vous souhaitez supprimer l'accès à la clé KMS, nous vous recommandons de remplacer ou de supprimer le certificat du service à l'aide de AWS Management Console ou avec la `update-service` commande utilisant le AWS CLI.

Contexte de chiffrement pour VPC Lattice

Un contexte de chiffrement est un ensemble facultatif de paires clé-valeur qui contiennent des informations contextuelles supplémentaires sur l'utilisation de votre clé privée. AWS KMS lie le contexte de chiffrement aux données chiffrées et les utilise comme données authentifiées supplémentaires pour prendre en charge le chiffrement authentifié.

Lorsque vos clés TLS sont utilisées avec VPC Lattice et le gestionnaire de connexions TLS, le nom de votre service VPC Lattice est inclus dans le contexte de chiffrement utilisé pour chiffrer votre clé au repos. Vous pouvez vérifier pour quel service VPC Lattice votre certificat et votre clé privée sont utilisés en consultant le contexte de chiffrement dans vos CloudTrail journaux, comme indiqué dans la section suivante, ou en consultant l'onglet Ressources associées de la console ACM.

Pour déchiffrer les données, le même contexte de chiffrement est inclus dans la demande. VPC Lattice utilise le même contexte de chiffrement dans toutes les opérations cryptographiques AWS KMS, où la clé `aws:vpc-lattice:arn` et la valeur sont le Amazon Resource Name (ARN) du service VPC Lattice.

L'exemple suivant montre le contexte de chiffrement dans le résultat d'une opération telle que `CreateGrant` :

```
"encryptionContextEquals": {
    "aws:acm:arn": "arn:aws:acm:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
    "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-west-2:111122223333:service/
svc-0b23c1234567890ab"
}
```

Surveillance de vos clés de chiffrement pour VPC Lattice

Lorsque vous utilisez une clé AWS gérée avec votre service VPC Lattice, vous pouvez l'utiliser AWS CloudTrailpour suivre les demandes auxquelles VPC Lattice envoie. AWS KMS

CreateGrant

Lorsque vous ajoutez votre certificat ACM à un service VPC Lattice, `CreateGrant` une demande est envoyée en votre nom pour que TLS Connection Manager puisse déchiffrer la clé privée associée à votre certificat ACM

Vous pouvez visualiser l'`CreateGrant`opération sous forme d'événement dans CloudTrail **>>** Historique des **`CreateGrant`** événements**>>**.

Voici un exemple d'enregistrement d'événement dans l'historique des CloudTrail événements de l'`CreateGrant`opération :

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111122223333:user/Alice",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "sessionContext": {
            "sessionIssuer": {
                "type": "IAMUser",
                "principalId": "EX_PRINCIPAL_ID",
                "arn": "arn:aws:iam::111122223333:user/Alice",
                "accountId": "111122223333",
                "userName": "Alice"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-02-06T23:30:50Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "acm.amazonaws.com"
    },
    "eventTime": "2023-02-07T00:07:18Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "acm.amazonaws.com",
    "userAgent": "acm.amazonaws.com",
    "requestParameters": {
        "granteePrincipal": "tlsconnectionmanager.amazonaws.com",
        "keyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
```

```
        "operations": [
            "Decrypt"
        ],
        "constraints": {
            "encryptionContextEquals": {
                "aws:acm:arn": "arn:aws:acm:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-
west-2:111122223333:service/svc-0b23c1234567890ab"
            }
        },
        "retiringPrincipal": "acm.us-west-2.amazonaws.com"
    },
    "responseElements": {
        "grantId": "f020fe75197b93991dc8491d6f19dd3cebb24ee62277a05914386724f3d48758",
        "keyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    },
    "requestID": "ba178361-8ab6-4bdd-9aa2-0d1a44b2974a",
    "eventID": "8d449963-1120-4d0c-9479-f76de11ce609",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Dans l'`CreateGrant`exemple ci-dessus, vous remarquerez que le bénéficiaire principal est TLS Connection Manager et que le contexte de chiffrement possède l'ARN du service VPC Lattice.

ListGrants

Vous pouvez utiliser votre identifiant de clé KMS et votre identifiant de compte pour appeler l'`ListGrants`API. Vous obtenez ainsi une liste de toutes les autorisations pour la clé KMS spécifiée. Pour plus d'informations, consultez ListGrants.

Utilisez la `ListGrants` commande suivante dans le AWS CLI pour voir le détail de toutes les subventions :

```
aws kms list-grants –key-id your-kms-key-id
```

Votre sortie doit ressembler à cet exemple :

```
{
    "Grants": [
        {
            "Operations": [
                "Decrypt"
            ],
            "KeyId": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "Name": "IssuedThroughACM",
            "RetiringPrincipal": "acm.us-west-2.amazonaws.com",
            "GranteePrincipal": "tlsconnectionmanager.amazonaws.com",
            "GrantId":
 "f020fe75197b93991dc8491d6f19dd3cebb24ee62277a05914386724f3d48758",
            "IssuingAccount": "arn:aws:iam::111122223333:root",
            "CreationDate": "2023-02-06T23:30:50Z",
            "Constraints": {
                "encryptionContextEquals": {
                  "aws:acm:arn": "arn:aws:acm:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
                  "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-
west-2:111122223333:service/svc-0b23c1234567890ab"
                }
            }
        }
    ]
}
```

Dans l'`ListGrants`exemple ci-dessus, vous remarquerez que le bénéficiaire principal est TLS Connection Manager et que le contexte de chiffrement possède l'ARN du service VPC Lattice.

Decrypt

VPC Lattice utilise le gestionnaire de connexions TLS pour appeler l'`Decrypt`opération de déchiffrement de votre clé privée afin de servir les connexions TLS dans votre service VPC Lattice.

Vous pouvez visualiser l'`Decrypt`opération sous forme d'événement dans CloudTrail **>>** Historique des événements **>>** **`Decrypt`**.

Voici un exemple d'enregistrement d'événement dans l'historique des CloudTrail événements de l'`Decrypt`opération :


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "tlsconnectionmanager.amazonaws.com"
    },
    "eventTime": "2023-02-07T00:07:23Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "tlsconnectionmanager.amazonaws.com",
    "userAgent": "tlsconnectionmanager.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "aws:acm:arn": "arn:aws:acm:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "aws:vpc-lattice:arn": "arn:aws:vpc-lattice:us-west-2:111122223333:service/
svc-0b23c1234567890ab"
        },
        "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
    },
    "responseElements": null,
    "requestID": "12345126-30d5-4b28-98b9-9153da559963",
    "eventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
    "readOnly": true,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "abcde202-ba1a-467c-b4ba-f729d45ae521",
```

```
    "eventCategory": "Management"
}
```

Gestion des identités et des accès pour Amazon VPC Lattice

Les sections suivantes décrivent comment vous pouvez utiliser AWS Identity and Access Management (IAM) pour sécuriser vos ressources VPC Lattice, en contrôlant qui peut effectuer les actions de l'API VPC Lattice.

Rubriques

- Comment Amazon VPC Lattice fonctionne avec IAM
- Autorisations de l'API VPC Lattice
- Politiques basées sur l'identité pour Amazon VPC Lattice
- Utilisation de rôles liés à un service pour VPC Lattice
- AWS politiques gérées pour VPC Lattice

Comment Amazon VPC Lattice fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à VPC Lattice, découvrez quelles fonctionnalités IAM peuvent être utilisées avec VPC Lattice.

Fonctionnalités IAM que vous pouvez utiliser avec Amazon VPC Lattice

Fonction IAM	Support en VPC Lattice
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Oui
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d'une politique	Oui
ACL	Non

Fonction IAM	Support en VPC Lattice
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui
Fonctions du service	Non
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont VPC Lattice et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le guide de l'utilisateur IAM.

Politiques basées sur l'identité pour VPC Lattice

Prend en charge les politiques basées sur l'identité	Oui

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

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

Politiques basées sur les ressources au sein de VPC Lattice

Prend en charge les politiques basées sur les ressources	Oui

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources.

VPC Lattice prend en charge les politiques d'authentification, une politique basée sur les ressources qui vous permet de contrôler l'accès aux services de votre réseau de services. Pour plus d'informations, consultez Contrôlez l'accès aux services à l'aide de politiques d'authentification.

VPC Lattice prend également en charge les politiques d'autorisation basées sur les ressources pour l'intégration avec. AWS Resource Access Manager Vous pouvez utiliser ces politiques basées sur les ressources pour accorder des autorisations d'utilisation à d'autres AWS comptes ou organisations afin de permettre le partage des ressources. Pour plus d'informations, consultez Partagez vos ressources VPC Lattice.

Actions politiques pour VPC Lattice

Prend en charge les actions de politique	Oui

Dans une déclaration de politique IAM, vous pouvez spécifier une action d'API à partir de n'importe quel service prenant en charge IAM. Pour VPC Lattice, utilisez le préfixe suivant avec le nom de l'action d'API :. `vpc-lattice:` Par exemple : `vpc-lattice:CreateService`, `vpc-lattice:CreateTargetGroup` et `vpc-lattice:PutAuthPolicy`.

Pour spécifier plusieurs actions dans une seule instruction, séparez-les par des virgules, comme suit :

```
"Action": [ "vpc-lattice:action1", "vpc-lattice:action2" ]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques. Par exemple, vous pouvez spécifier toutes les actions dont le nom commence par le mot`Get`, comme suit :

```
"Action": "vpc-lattice:Get*"
```

Pour obtenir la liste complète des actions de l'API VPC Lattice, consultez la section Actions définies par Amazon VPC Lattice dans le Service Authorization Reference.

Ressources relatives aux politiques pour VPC Lattice

Prend en charge les ressources de politique	Oui

Dans une instruction de politiqe IAM, l'élément `Resource` spécifie l'objet ou les objets couverts par l'instruction. Pour VPC Lattice, chaque déclaration de politique IAM s'applique aux ressources que vous spécifiez à l'aide de leurs ARN.

Le format Amazon Resource Name (ARN) spécifique dépend de la ressource. Lorsque vous fournissez un ARN, remplacez le texte en *italique* par des informations spécifiques à votre ressource.

- Abonnements aux journaux d'accès :

```
"Resource": "arn:aws:vpc-lattice:region:account-id:accesslogsubscription/access-log-subscription-id"
```

- Auditeurs :

```
"Resource": "arn:aws:vpc-lattice:region:account-id:service/service-id/
listener/listener-id"
```

- Règles :

```
"Resource": "arn:aws:vpc-lattice:region:account-id:service/service-id/
listener/listener-id/rule/rule-id"
```

- Services :

```
"Resource": "arn:aws:vpc-lattice:region:account-id:service/service-id"
```

- Réseaux de services :

```
"Resource": "arn:aws:vpc-lattice:region:account-id:servicenetwork/service-network-id"
```

- Associations de services du réseau de services :

```
"Resource": "arn:aws:vpc-lattice:region:account-
id:servicenetworkserviceassociation/service-network-service-association-id"
```

- Associations VPC du réseau de services :

```
"Resource": "arn:aws:vpc-lattice:region:account-
id:servicenetworkvpcassociation/service-network-vpc-association-id"
```

- Groupes cibles :

```
"Resource": "arn:aws:vpc-lattice:region:account-id:targetgroup/target-group-id"
```

Clés de condition de politique pour VPC Lattice

Prend en charge les clés de condition de politique spécifiques au service	Oui

Vous pouvez spécifier des conditions dans les politiques IAM qui contrôlent l'accès aux ressources VPC Lattice. L'Instruction de politique est en vigueur uniquement lorsque les conditions sont vérifiées.

VPC Lattice prend en charge les clés de condition définies par le service suivantes que vous pouvez utiliser dans les politiques basées sur l'identité afin de déterminer qui peut effectuer les actions de l'API VPC Lattice. Pour plus d'informations, consultez la section Clés de condition pour Amazon VPC Lattice Services dans la référence d'autorisation des services.

Clés de condition définies par le service pour les politiques basées sur l'identité

Clés de condition	Description	Soutenu pour ces actions
`vpc-lattice:AuthType`	Filtre l'accès en fonction du type d'authentification indiqué dans la demande (`AWS_IAMouNONE`)	• CreateService • CreateServiceNetwork • UpdateService • UpdateServiceNetwork
`vpc-lattice:Protocol`	Filtre l'accès par le protocole dans la demande (`HTTPouHTTPS`)	• CreateListener

Clés de condition	Description	Soutenu pour ces actions
`vpc-lattice:SecurityGroupIds`	Filtre l'accès en fonction des identifiants de groupe de sécurité figurant dans la demande	• CreateServiceNetworkVpcAssociation • UpdateServiceNetworkVpcAssociation
`vpc-lattice:ServiceArn`	Filtre l'accès par l'ARN d'un service dans la requête	• CreateServiceNetworkServiceAssociation • DeleteServiceNetworkServiceAssociation • GetServiceNetworkServiceAssociation • ListServiceNetworkServiceAssociations
`vpc-lattice:ServiceNetworkArn`	Filtre l'accès par l'ARN d'un réseau de service dans la requête	• CreateServiceNetworkServiceAssociation • CreateServiceNetworkVpcAssociation • DeleteServiceNetworkVpcAssociation • GetServiceNetworkServiceAssociation • GetServiceNetworkVpcAssociation • ListServiceNetworkServiceAssociations • ListServiceNetworkVpcAssociations • UpdateServiceNetworkVpcAssociation
`vpc-lattice:TargetGroupArns`	Filtre l'accès par les ARN des groupes cibles dans la demande	• CreateListener • CreateRule • UpdateListener • UpdateRule
`vpc-lattice:VpcId`	Filtre l'accès en fonction de l'ID d'un cloud privé virtuel (VPC) dans la demande	• CreateServiceNetworkVpcAssociation • CreateTargetGroup • DeleteServiceNetworkVpcAssociation • GetServiceNetworkVpcAssociation • ListServiceNetworkVpcAssociations • UpdateServiceNetworkVpcAssociation

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour plus d'informations sur les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Listes de contrôle d'accès (ACL) dans VPC Lattice

Prend en charge les listes ACL	Non

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

Contrôle d'accès basé sur les attributs (ABAC) avec VPC Lattice

Prend en charge ABAC (étiquettes dans les politiques)	Oui

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

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

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

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

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

Utilisation d'informations d'identification temporaires avec VPC Lattice

Prend en charge les informations d'identification temporaires	Oui

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

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

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

Rôles de service pour VPC Lattice

Prend en charge les fonctions de service	Non

Une fonction du service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM.

Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations pour un rôle de service peut interrompre les fonctionnalités de VPC Lattice. Modifiez les rôles de service uniquement lorsque VPC Lattice fournit des instructions à cet effet.

Rôles liés à un service pour VPC Lattice

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion de rôles liés à un service VPC Lattice, consultez. Utilisation de rôles liés à un service pour VPC Lattice

Autorisations de l'API VPC Lattice

Vous devez accorder aux identités IAM (telles que les utilisateurs ou les rôles) l'autorisation d'appeler les actions d'API VPC Lattice dont elles ont besoin, comme décrit dans. Actions politiques pour VPC Lattice En outre, pour certaines actions VPC Lattice, vous devez autoriser les identités IAM à appeler des actions spécifiques à partir d'autres API. AWS

Autorisations requises pour l'API

Lorsque vous appelez les actions suivantes depuis l'API, vous devez autoriser les utilisateurs IAM à appeler les actions spécifiées.

`CreateServiceNetworkVpcAssociation`

- `vpc-lattice:CreateServiceNetworkVpcAssociation`
- `ec2:DescribeVpcs`

- `ec2:DescribeSecurityGroups`(Nécessaire uniquement lorsque des groupes de sécurité sont fournis)

`UpdateServiceNetworkVpcAssociation`

- `vpc-lattice:UpdateServiceNetworkVpcAssociation`
- `ec2:DescribeSecurityGroups`(Nécessaire uniquement lorsque des groupes de sécurité sont fournis)

`CreateTargetGroup`

- `vpc-lattice:CreateTargetGroup`
- `ec2:DescribeVpcs`

`RegisterTargets`

- `vpc-lattice:RegisterTargets`
- `ec2:DescribeInstances`(Nécessaire uniquement lorsqu'il `INSTANCE` s'agit du type de groupe cible)
- `ec2:DescribeVpcs`(Nécessaire uniquement lorsque `INSTANCE` ou `IP` selon le type de groupe cible)
- `ec2:DescribeSubnets`(Nécessaire uniquement lorsque `INSTANCE` ou `IP` selon le type de groupe cible)
- `lambda:GetFunction`(Nécessaire uniquement lorsqu'il `LAMBDA` s'agit du type de groupe cible)
- `lambda:AddPermission`(Nécessaire uniquement si le groupe cible n'est pas déjà autorisé à invoquer la fonction Lambda spécifiée)

`DeregisterTargets`

- `vpc-lattice:DeregisterTargets`

`CreateAccessLogSubscription`

- `vpc-lattice:CreateAccessLogSubscription`
- `logs:GetLogDelivery`
- `logs:CreateLogDelivery`

`DeleteAccessLogSubscription`

- `vpc-lattice:DeleteAccessLogSubscription`
- `logs:DeleteLogDelivery`

`UpdateAccessLogSubscription`

- `vpc-lattice:UpdateAccessLogSubscription`
- `logs:UpdateLogDelivery`

Politiques basées sur l'identité pour Amazon VPC Lattice

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources VPC Lattice. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par VPC Lattice, y compris le format des ARN pour chacun des types de ressources, consultez Actions, ressources et clés de condition pour Amazon VPC Lattice dans la référence d'autorisation de service.

Pour plus d'informations, consultez la section Actions, ressources et clés de condition pour Amazon VPC Lattice dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Autorisations supplémentaires requises pour un accès complet
- Exemples de politiques basées sur l'identité pour VPC Lattice

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources VPC Lattice dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Autorisations supplémentaires requises pour un accès complet

Pour utiliser les autres AWS services auxquels VPC Lattice est intégré et l'ensemble des fonctionnalités de VPC Lattice, vous devez disposer d'autorisations supplémentaires spécifiques. Ces autorisations ne sont pas incluses dans la politique `VPCLatticeFullAccess` gérée en raison du risque d'augmentation confuse des privilèges des adjoints.

Vous devez associer la politique suivante à votre rôle et l'utiliser avec la stratégie `VPCLatticeFullAccess` gérée.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "firehose:TagDeliveryStream",
                "lambda:AddPermission",
                "s3:PutBucketPolicy"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutResourcePolicy"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": [
                        "vpc-lattice.amazonaws.com"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:PutRolePolicy"
            ],
```

```
            "Resource": "arn:aws:iam::*:role/aws-service-role/vpc-
lattice.amazonaws.com/AWSServiceRoleForVpcLattice"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/
delivery.logs.amazonaws.com/AWSServiceRoleForLogDelivery*"
        }
    ]
}
```

Cette politique fournit les autorisations supplémentaires suivantes :

- `iam:AttachRolePolicy`: vous permet d'associer la politique gérée spécifiée au rôle IAM spécifié.
- `iam:PutRolePolicy`: vous permet d'ajouter ou de mettre à jour un document de politique intégré au rôle IAM spécifié.
- `s3:PutBucketPolicy`: vous permet d'appliquer une politique de compartiment à un compartiment Amazon S3.
- `firehose:TagDeliveryStream`: vous permet d'ajouter ou de mettre à jour des balises pour les flux de diffusion Firehose.

Exemples de politiques basées sur l'identité pour VPC Lattice

Rubriques

- Gérer les associations de VPC à un réseau de services
- Création d'associations de services avec un réseau de services
- Ajoutez des balises aux ressources .
- Créer un rôle lié à un service

Gérer les associations de VPC à un réseau de services

L'exemple suivant illustre une stratégie qui donne aux utilisateurs dotés de cette stratégie l'autorisation de créer, de mettre à jour et de supprimer les associations de VPC à un réseau de

service, mais uniquement pour le VPC et le réseau de service spécifiés dans la condition. Pour plus d'informations sur la spécification des clés de condition, consultez Clés de condition de politique pour VPC Lattice.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "vpc-lattice:CreateServiceNetworkVpcAssociation",
            "vpc-lattice:UpdateServiceNetworkVpcAssociation",
            "vpc-lattice:DeleteServiceNetworkVpcAssociation"
         ],
         "Resource": [
            "*"
         ],
         "Condition": {
            "StringEquals": {
               "vpc-lattice:ServiceNetworkArn": "arn:aws:vpc-lattice:us-
west-2:123456789012:servicenetwork/sn-903004f88example",
               "vpc-lattice:VpcId": "vpc-1a2b3c4d"
            }
         }
      }
   ]
}
```

Création d'associations de services avec un réseau de services

Si vous n'utilisez pas de clés de condition pour contrôler l'accès aux ressources VPC Lattice, vous pouvez spécifier les ARN des ressources dans l'`Resource`élément pour contrôler l'accès à la place.

L'exemple suivant illustre une politique qui limite les associations de services à un réseau de services que les utilisateurs utilisant cette stratégie peuvent créer en spécifiant les ARN du service et du réseau de services qui peuvent être utilisés avec l'action d'`CreateServiceNetworkServiceAssociation`API. Pour plus d'informations sur la spécification des valeurs ARN, consultezRessources relatives aux politiques pour VPC Lattice.

```
{
   "Version": "2012-10-17",
   "Statement": [
```

```
      {
         "Effect": "Allow",
         "Action": [
            "vpc-lattice:CreateServiceNetworkServiceAssociation"
         ],
         "Resource": [
            "arn:aws:vpc-lattice:us-
west-2:123456789012:servicenetworkserviceassociation/*",
            "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-04d5cc9b88example",
            "arn:aws:vpc-lattice:us-west-2:123456789012:servicenetwork/
sn-903004f88example"
         ]
      }
   ]
}
```

Ajoutez des balises aux ressources .

L'exemple suivant illustre une politique qui autorise les utilisateurs dotés de cette politique à créer des balises sur les ressources VPC Lattice.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "vpc-lattice:TagResource"
         ],
         "Resource": "arn:aws:vpc-lattice:us-west-2:123456789012:*/*"
      }
   ]
}
```

Créer un rôle lié à un service

VPC Lattice a besoin d'autorisations pour créer un rôle lié à un service la première fois qu'un de vos utilisateurs crée Compte AWS des ressources VPC Lattice. Si le rôle lié au service n'existe pas déjà, VPC Lattice le crée dans votre compte. Le rôle lié au service donne des autorisations à VPC Lattice afin qu'il puisse appeler d'autres personnes en votre nom. Services AWS

Pour que cette création de rôle automatique aboutisse, les utilisateurs doivent disposer des autorisations nécessaires pour l'action `iam:CreateServiceLinkedRole`.

```
"Action": "iam:CreateServiceLinkedRole"
```

L'exemple suivant illustre une politique qui autorise les utilisateurs dotés de cette politique à créer un rôle lié à un service pour VPC Lattice.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/vpc-lattice.amazonaws.com/
AWSServiceRoleForVpcLattice",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName":"vpc-lattice.amazonaws.com"
            }
         }
      }
   ]
}
```

Utilisation de rôles liés à un service pour VPC Lattice

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

Autorisations de rôle liées à un service pour VPC Lattice

VPC Lattice utilise le rôle lié au service nommé. AWSServiceRoleForVpcLattice

Le rôle AWSServiceRoleForVpcLatticelié à un service fait confiance au service suivant pour assumer le rôle :

- `vpc-lattice.amazonaws.com`

La politique d'autorisation de rôle nommée `AWSVpcLatticeServiceRolePolicy` permet à VPC Lattice de publier des CloudWatch métriques dans l'espace de noms. `AWS/VpcLattice`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "cloudwatch:PutMetricData",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/VpcLattice"
                }
            }
        }
    ]
}
```

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour VPC Lattice

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez des ressources VPC Lattice dans l'API AWS Management Console, le ou l'API AWS CLI AWS , VPC Lattice crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez des ressources VPC Lattice, VPC Lattice crée à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour VPC Lattice

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

Suppression d'un rôle lié à un service pour VPC Lattice

Si vous n'avez plus besoin d'utiliser Amazon VPC Lattice, nous vous recommandons de le supprimer. AWSServiceRoleForVpcLattice

Vous ne pouvez supprimer ce rôle lié à un service qu'après avoir supprimé toutes les ressources VPC Lattice de votre. Compte AWS

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForVpcLatticeservice. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Après avoir supprimé un rôle lié à un service, VPC Lattice le crée à nouveau lorsque vous créez des ressources VPC Lattice dans votre. Compte AWS

Régions prises en charge pour les rôles liés au service VPC Lattice

VPC Lattice prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible.

AWS politiques gérées pour VPC Lattice

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

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

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

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

AWS politique gérée : VPC LatticeFullAccess

Cette politique fournit un accès complet à Amazon VPC Lattice et un accès limité aux autres services dépendants. Il inclut les autorisations permettant d'effectuer les opérations suivantes :

- ACM — Récupérez l'ARN du certificat SSL/TLS pour les noms de domaine personnalisés.
- CloudWatch — Afficher les journaux d'accès et les données de surveillance.
- CloudWatch Journaux — Configurez et envoyez des journaux d'accès à CloudWatch Logs.
- Amazon EC2 — Récupérez des informations sur les instances EC2 et les VPC pour créer des groupes cibles et enregistrer des cibles.
- Elastic Load Balancing : récupérez des informations sur un Application Load Balancer pour l'enregistrer en tant que cible.
- Firehose — Récupérez des informations sur les flux de diffusion utilisés pour stocker les journaux d'accès.
- Lambda — Récupérez des informations sur une fonction Lambda pour l'enregistrer en tant que cible.
- Amazon S3 — Récupérez des informations sur les compartiments S3 utilisés pour stocker les journaux d'accès.

Pour consulter les autorisations associées à cette politique, consultez la section VPC LatticeFullAccess dans le manuel AWS Managed Policy Reference.

Pour utiliser les autres AWS services auxquels VPC Lattice est intégré et l'ensemble des fonctionnalités de VPC Lattice, vous devez disposer d'autorisations supplémentaires spécifiques. Ces autorisations ne sont pas incluses dans la politique `VPCLatticeFullAccess` gérée en raison du risque d'augmentation confuse des privilèges des adjoints. Pour plus d'informations, consultez Autorisations supplémentaires requises pour un accès complet.

AWS politique gérée : VPC LatticeReadOnlyAccess

Cette politique fournit un accès en lecture seule à Amazon VPC Lattice et un accès limité aux autres services dépendants. Il inclut les autorisations permettant d'effectuer les opérations suivantes :

- ACM — Récupérez l'ARN du certificat SSL/TLS pour les noms de domaine personnalisés.
- CloudWatch — Afficher les journaux d'accès et les données de surveillance.
- CloudWatch Journaux : affichez les informations de livraison des journaux pour les abonnements aux journaux d'accès.
- Amazon EC2 — Récupérez des informations sur les instances EC2 et les VPC pour créer des groupes cibles et enregistrer des cibles.
- Elastic Load Balancing — Récupérez des informations sur un Application Load Balancer.

- Firehose — Récupérez des informations sur les flux de diffusion pour la livraison des journaux d'accès.
- Lambda : affiche les informations relatives à une fonction Lambda.
- Amazon S3 — Récupérez des informations sur les compartiments S3 pour la livraison des journaux d'accès.

Pour consulter les autorisations associées à cette politique, consultez la section VPC LatticeReadOnlyAccess dans le manuel AWS Managed Policy Reference.

AWS politique gérée : VPC LatticeServicesInvokeAccess

Cette politique permet d'invoquer les services Amazon VPC Lattice.

Pour consulter les autorisations associées à cette politique, consultez la section VPC LatticeServicesInvokeAccess dans le manuel AWS Managed Policy Reference.

AWS politique gérée : AWSVpcLatticeServiceRolePolicy

Cette politique est associée à un rôle lié à un service nommé AWSServiceRoleForVpcLatticepour permettre à VPC Lattice d'effectuer des actions en votre nom. Vous ne pouvez pas attacher cette politique à vos entités IAM. Pour plus d'informations, consultez Utilisation de rôles liés à un service pour VPC Lattice.

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

Mises à jour des politiques gérées par VPC Lattice AWS

Consultez les détails des mises à jour des politiques AWS gérées pour VPC Lattice depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS du guide de l'utilisateur du VPC Lattice.

Modification	Description	Date
VPC LatticeFullAccess	VPC Lattice ajoute une nouvelle politique visant à accorder des autorisations pour un accès complet	31 mars 2023

Modification	Description	Date
	à Amazon VPC Lattice et un accès limité à d'autres services dépendants.	
VPC LatticeReadOnlyAccess	VPC Lattice ajoute une nouvelle politique pour accorder des autorisations d'accès en lecture seule à Amazon VPC Lattice et un accès limité à d'autres services dépendants.	31 mars 2023
VPC LatticeServicesInvokeAccess	VPC Lattice ajoute une nouvelle politique permettant d'autoriser l'accès aux services Amazon VPC Lattice.	31 mars 2023
AWSVpcLatticeServiceRolePolicy	VPC Lattice ajoute des autorisations à son rôle lié au service pour permettre à VPC Lattice de publier des métriques dans l'espace de noms. CloudWatch `AWS/VpcLattice` La `AWSVpcLatticeServiceRolePolicy` politique inclut l'autorisation d'appeler l'action d' CloudWatch PutMetricDataAPI. Pour plus d'informations, consultez Utilisation de rôles liés à un service pour VPC Lattice.	5 décembre 2022
VPC Lattice a commencé à suivre les modifications	VPC Lattice a commencé à suivre les modifications apportées à ses AWS politiques gérées.	5 décembre 2022

Validation de conformité pour Amazon VPC Lattice

Des auditeurs tiers évaluent la sécurité et la conformité d'Amazon VPC Lattice dans le cadre de plusieurs AWS programmes de conformité.

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

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

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

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

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

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans plusieurs cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier

votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.

- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Accédez à VPC Lattice à l'aide d'un point de terminaison d'interface () PrivateLink

Vous pouvez établir une connexion privée entre votre VPC et Amazon VPC Lattice en créant un point de terminaison VPC d'interface. Les points de terminaison d'interface sont alimentés par AWS PrivateLinkune technologie qui vous permet d'accéder en privé aux API VPC Lattice sans passerelle Internet, périphérique NAT, connexion VPN ou connexion. AWS Direct Connect Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les API VPC Lattice.

Chaque point de terminaison d'interface est représenté par une ou plusieurs interfaces réseau dans vos sous-réseaux.

Considérations relatives aux points de terminaison VPC d'interface

Avant de configurer un point de terminaison VPC d'interface pour VPC Lattice, assurez-vous de consulter la section Accès à un service à l' AWS aide d'un point de terminaison VPC d'interface dans le guide de l'utilisateur Amazon VPC.

VPC Lattice permet d'appeler toutes ses actions d'API depuis votre VPC.

Création d'un point de terminaison VPC d'interface pour VPC Lattice

Vous pouvez créer un point de terminaison VPC pour le service VPC Lattice à l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Créez un point de terminaison VPC pour VPC Lattice en utilisant le nom de service suivant :

`com.amazonaws.region.vpc-lattice`

Si vous activez le DNS privé pour le point de terminaison, vous pouvez envoyer des demandes d'API à VPC Lattice en utilisant son nom DNS par défaut pour la région, par exemple,. `vpc-lattice.us-east-1.amazonaws.com`

Pour plus d'informations, consultez la section Accès à un AWS service à l'aide d'un point de terminaison VPC d'interface dans le guide de l'utilisateur Amazon VPC.

Résilience dans Amazon VPC Lattice

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité.

Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant.

Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Sécurité de l'infrastructure dans Amazon VPC Lattice

En tant que service géré, Amazon VPC Lattice est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

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

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.

- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Surveillance d'Amazon VPC Lattice

Utilisez les fonctionnalités de cette section pour surveiller vos réseaux de services Amazon VPC Lattice, vos services, vos groupes cibles et vos connexions VPC.

Table des matières

CloudWatch métriques pour VPC Lattice

Amazon VPC Lattice envoie des données relatives à vos groupes cibles et à vos services à Amazon CloudWatch, et les traite en métriques lisibles en temps quasi réel. Ces statistiques sont conservées pendant 15 mois, afin que vous puissiez accéder aux informations historiques et avoir une meilleure idée des performances de votre application ou service Web. Vous pouvez également définir des alarmes qui surveillent certains seuils et envoient des notifications ou prennent des mesures lorsque ces seuils sont atteints. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

Amazon VPC Lattice utilise un rôle lié à un service dans votre AWS compte pour envoyer des métriques à Amazon. CloudWatch Pour plus d'informations, veuillez consulter Utilisation de rôles liés à un service pour VPC Lattice.

Table des matières

Afficher les CloudWatch statistiques Amazon

Vous pouvez consulter les CloudWatch statistiques Amazon relatives à vos groupes cibles et à vos services à l'aide de la CloudWatch console ouAWS CLI.

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

1. Ouvrez la CloudWatch console Amazon à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Metrics (Métriques).
3. Sélectionnez l'espace de noms `AWS/VpcLattice`.
4. (Facultatif) Pour afficher une métrique dans toutes les dimensions, entrez son nom dans le champ de recherche.
5. (Facultatif) Pour filtrer les métriques par dimension, sélectionnez l'une des options suivantes :
   - Pour afficher uniquement les statistiques signalées pour vos groupes cibles, choisissez Groupes cibles. Pour consulter les statistiques d'un seul groupe cible, entrez son nom dans le champ de recherche.
   - Pour afficher uniquement les statistiques signalées pour vos services, sélectionnez Services. Pour consulter les statistiques d'un seul service, entrez son nom dans le champ de recherche.

Pour consulter les statistiques à l'aide du AWS CLI

Utilisez la AWS CLI commande CloudWatch list-metrics suivante pour répertorier les métriques disponibles :

```
aws cloudwatch list-metrics --namespace AWS/VpcLattice
```

Pour plus d'informations sur chacune des mesures et leurs dimensions, reportez-vous aux sections Métriques du groupe cible etMétriques de service.

Métriques du groupe cible

VPC Lattice stocke automatiquement les métriques relatives aux groupes cibles dans l'espace de noms Amazon. `AWS/VpcLattice` CloudWatch Pour plus d'informations sur les groupes cibles, consultezGroupes cibles dans VPC Lattice.

Vous souhaiterez peut-être effectuer un suivi `HTTP code` et `RequestTime` des mesures pour les groupes cibles. Vous pouvez filtrer ces mesures par zone de disponibilité (AZ) afin de déterminer dans quelle zone se trouve le groupe cible.

Métrique	Description
`TotalConnectionCount`	Nombre total de connexions. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`. Dimensions • Nom :`TargetGroup` , Valeur : nom du groupe cible. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.
`ActiveConnectionCount`	Connexions actives. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`.

Métrique	Description
	Dimensions • Nom :`TargetGroup` , Valeur : nom du groupe cible. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.
`ConnectionErrorCount`	Nombre total d'échecs de connexion. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`. Dimensions • Nom :`TargetGroup` , Valeur : nom du groupe cible. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Métrique	Description
`HTTP1_ConnectionCount`	Nombre total de connexions HTTP/1.1. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`. Dimensions • Nom :`TargetGroup` , Valeur : nom du groupe cible. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Métrique	Description
`HTTP2_ConnectionCount`	Nombre total de connexions HTTP/2. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`. Dimensions • Nom :`TargetGroup` , Valeur : nom du groupe cible. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Métrique	Description
`ConnectionTimeoutCount`	Expiration totale des délais de connexion. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`. Dimensions • Nom :`TargetGroup` , Valeur : nom du groupe cible. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Métrique	Description
`TotalReceivedConnectionBytes`	Nombre total d'octets de connexion reçus. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`. Dimensions • Nom :`TargetGroup` , Valeur : nom du groupe cible. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Métrique	Description
`TotalSentConnectionBytes`	Nombre total d'octets de connexion envoyés. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`. Dimensions • Nom :`TargetGroup` , Valeur : nom du groupe cible. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Métrique	Description
`TotalRequestCount`	Nombre total de demandes. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`. Dimensions • Nom :`TargetGroup` , Valeur : nom du groupe cible. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Métrique	Description
`ActiveRequestCount`	Nombre total de demandes actives. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`. Dimensions • Nom :`TargetGroup` , Valeur : nom du groupe cible. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Métrique	Description
`RequestTime`	Durée de la demande en millisecondes. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • Les statistiques les plus utiles sont `Average` et `pNN.NN` (percentiles). Dimensions • Nom :`TargetGroup` , Valeur : nom du groupe cible. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Métrique	Description
`HTTPCode_2XX_Count`, `HTTPCode_3XX_Count`, `HTTPCode_4XX_Count`, `HTTPCode_5XX_Count`	Codes de réponse HTTP agrégés. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`. Dimensions • Nom :`TargetGroup` , Valeur : nom du groupe cible. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Métrique	Description
`TLSConnectionErrorCount`	Nombre total d'erreurs de connexion TLS, sans compter les échecs de vérification des certificats. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`. Dimensions • Nom :`TargetGroup` , Valeur : nom du groupe cible. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Métrique	Description
`TotalTLSConnection HandshakeCount`	Nombre total de connexions TLS réussies. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`. Dimensions • Nom :`TargetGroup` , Valeur : nom du groupe cible. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Métriques de service

VPC Lattice stocke automatiquement les métriques relatives aux services dans l'espace de noms Amazon. `AWS/VpcLattice` CloudWatch Pour plus d'informations sur les services, consultezServices en VPC Lattice.

Vous souhaiterez peut-être effectuer un suivi `HTTP code` et `RequestTime` des mesures pour les services. Vous pouvez filtrer ces mesures par zone de disponibilité (AZ) afin de déterminer dans quelle zone le service se trouve.

Métrique	Description
`RequestTimeoutCount`	Nombre total de demandes dont le délai d'attente d'une réponse a expiré.

Métrique	Description
	Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`. Dimensions • Nom :`Service`, Valeur : ID du service. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Métrique	Description
`TotalRequestCount`	Nombre total de demandes. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`. Dimensions • Nom :`Service`, Valeur : ID du service. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Métrique	Description
`RequestTime`	Durée de la demande en millisecondes. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • Les statistiques les plus utiles sont `Average` et `pNN.NN` (percentiles). Dimensions • Nom :`Service`, Valeur : ID du service. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Métrique	Description
`HTTPCode_2XX_Count` , `HTTPCode_3XX_Count` , `HTTPCode_4XX_Count` , `HTTPCode_5XX_Count`	Codes de réponse HTTP agrégés. Critères de notification • Toujours indiqué (qu'il s'agisse d'une valeur nulle ou non nulle) dès que la ressource reçoit du trafic. Fréquence des rapports • Une fois par minute Statistiques • La statistique la plus utile est`Sum`. Dimensions • Nom :`Service`, Valeur : ID du service. • Nom :`AvailabilityZone` , Valeur : L'AZ dans laquelle se trouve le groupe cible.

Journaux d'accès pour VPC Lattice

Les journaux d'accès capturent des informations détaillées sur vos services VPC Lattice. Vous pouvez utiliser ces journaux d'accès pour analyser les modèles de trafic et auditer tous les services du réseau.

Les journaux d'accès sont facultatifs et sont désactivés par défaut. Après avoir activé les journaux d'accès, vous pouvez les désactiver à tout moment.

Tarification

Des frais s'appliquent lorsque les journaux d'accès sont publiés. Les journaux publiés AWS nativement en votre nom sont appelés journaux automatiques. Pour plus d'informations sur la tarification des journaux vendus, consultez Amazon CloudWatch Pricing, choisissez Logs et consultez les tarifs sous Vended Logs.

Table des matières

Autorisations IAM requises pour activer les journaux d'accès

Pour activer les journaux d'accès et les envoyer à leur destination, les actions suivantes doivent figurer dans la politique attachée à l'utilisateur, au groupe ou au rôle IAM que vous utilisez.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Sid": "ManageVPCLatticeAccessLogSetup",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:GetLogDelivery",
                "logs:UpdateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
                "vpc-lattice:CreateAccessLogSubscription",
                "vpc-lattice:GetAccessLogSubscription",
                "vpc-lattice:UpdateAccessLogSubscription",
                "vpc-lattice:DeleteAccessLogSubscription",
                "vpc-lattice:ListAccessLogSubscriptions"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

Pour plus d'informations, veuillez consulter Ajout et suppression d'autorisations basées sur l'identité IAM dans le Guide de l'utilisateurAWS Identity and Access Management .

Après avoir mis à jour la politique associée à l'utilisateur, au groupe ou au rôle IAM que vous utilisez, rendez-vous sur. Activer les journaux d'accès

Accéder aux destinations du journal

Vous pouvez envoyer les journaux d'accès aux destinations suivantes.

Amazon CloudWatch Logs

- VPC Lattice fournit généralement les journaux aux CloudWatch journaux en 2 minutes. Cependant, gardez à l'esprit que le délai réel de livraison des journaux est le meilleur moyen possible et qu'il peut y avoir une latence supplémentaire.
- Une politique de ressources est créée automatiquement et ajoutée au groupe de CloudWatch journaux si le groupe de journaux ne dispose pas de certaines autorisations. Pour plus d'informations, consultez la section Logs envoyés à CloudWatch Logs dans le guide de CloudWatch l'utilisateur Amazon.
- Vous trouverez les journaux d'accès envoyés CloudWatch sous Groupes de journaux dans la CloudWatch console. Pour plus d'informations, consultez Afficher les données de journal envoyées à CloudWatch Logs dans le guide de CloudWatch l'utilisateur Amazon.

Amazon S3

- VPC Lattice fournit généralement des journaux à Amazon S3 dans un délai de 6 minutes. Cependant, gardez à l'esprit que le délai réel de livraison des journaux est le meilleur moyen possible et qu'il peut y avoir une latence supplémentaire.
- Une politique de compartiment sera créée automatiquement et ajoutée à votre compartiment Amazon S3 si celui-ci ne dispose pas de certaines autorisations. Pour plus d'informations, consultez la section Logs envoyés à Amazon S3 dans le guide de CloudWatch l'utilisateur Amazon.
- Les journaux d'accès envoyés à Amazon S3 utilisent la convention de dénomination suivante :

```
[bucket]/[prefix]/AWSLogs/[accountId]/VpcLattice/AccessLogs/[region]/[YYYY/
MM/DD]/[resource-id]/[accountId]_VpcLatticeAccessLogs_[region]_[resource-
id]_YYYYMMDDTHHmmZ_[hash].json.gz
```

Amazon Data Firehose

- VPC Lattice fournit généralement des journaux à Firehose en 2 minutes. Cependant, gardez à l'esprit que le délai réel de livraison des journaux est le meilleur moyen possible et qu'il peut y avoir une latence supplémentaire.
- Un rôle lié à un service est automatiquement créé pour autoriser VPC Lattice à envoyer des journaux d'accès à. Amazon Data FirehosePour que la création automatique de rôle réussisse, les utilisateurs doivent avoir l'autorisation pour l'action `iam:CreateServiceLinkedRole`. Pour plus d'informations, consultez la section Logs envoyés à Amazon Data Firehose dans le guide de CloudWatch l'utilisateur Amazon.
- Pour plus d'informations sur l'affichage des journaux envoyés à Amazon Data Firehose, consultez la section Monitoring Amazon Kinesis Data Streams dans Amazon Data Firehose le manuel du développeur.

Activer les journaux d'accès

Procédez comme suit pour configurer les journaux d'accès afin de capturer et de distribuer les journaux d'accès à la destination de votre choix.

Table des matières

Activer les journaux d'accès à l'aide de la console

Vous pouvez activer les journaux d'accès pour un réseau de services ou pour un service lors de la création. Vous pouvez également activer les journaux d'accès après avoir créé un réseau ou un service de service, comme décrit dans la procédure suivante.

Pour créer un service de base à l'aide de la console

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Sélectionnez le réseau ou le service de service.
3. Choisissez Actions, puis Modifier les paramètres du journal.
4. Activez le commutateur Access Logs.
5. Ajoutez une destination de livraison pour vos journaux d'accès comme suit :

- Sélectionnez Groupe de CloudWatch journaux, puis choisissez un groupe de journaux. Pour créer un groupe de journaux, choisissez Create a log group in CloudWatch.
- Sélectionnez le compartiment S3 et entrez le chemin du compartiment S3, y compris tout préfixe. Pour effectuer une recherche dans vos compartiments S3, choisissez Browse S3.
- Sélectionnez le flux de diffusion Kinesis Data Firehose, puis choisissez un flux de diffusion. Pour créer un flux de diffusion, choisissez Créer un flux de diffusion dans Kinesis.

6. Sélectionnez Enregistrer les modifications.

Activez les journaux d'accès à l'aide du AWS CLI

Utilisez la commande CLI create-access-log-subscriptionpour activer les journaux d'accès pour les réseaux ou les services de service.

Accès au contenu du journal

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

Champ	Description	Format
`hostHeader`	L'en-tête d'autorité de la demande.	chaîne
`sslCipher`	Le nom OpenSSL de l'ensemble de chiffreme nts utilisés pour établir la connexion TLS du client.	chaîne
`serviceNetworkArn`	L'ARN du réseau de service.	*arn:aws:vpc-lattic e : region : account:servicenet work/ id*
`resolvedUser`	L'ARN de l'utilisateur lorsque l'authentification est activée et que l'authentification est terminée.	null | ARN | « Anonyme » | « Inconnu »

Champ	Description	Format
`authDeniedReason`	La raison pour laquelle l'accès est refusé lorsque l'authent ification est activée.	null | « Service » | « Réseau » | « Identité »
`requestMethod`	L'en-tête de méthode de la demande.	chaîne
`targetGroupArn`	Le groupe d'hôtes cible auquel appartient l'hôte cible.	chaîne
`tlsVersion`	La version TLS.	*TLSv x*
`userAgent`	L'en-tête de l'agent utilisateur.	chaîne
`ServerNameIndication`	[HTTPS uniquement] Valeur définie sur le socket de connexion SSL pour l'indicat ion du nom du serveur (SNI).	chaîne
`destinationVpcId`	L'ID du VPC de destination.	*vpc- xxxxxxxx*
`sourceIpPort`	Adresse IP et:port de la source.	*IP* : *port*
`targetIpPort`	Adresse IP et port de la cible.	*IP* : *port*
`serviceArn`	L'ARN du service.	*arn:aws:vpc-lattic e : region : account:service/ id*
`sourceVpcId`	L'ID du VPC source.	*vpc- xxxxxxxx*
`requestPath`	Le chemin d'accès de la demande.	LatticePath? : *chemin*
`startTime`	Heure de début de la demande.	*YYYY - MM - DD T HH : MM : SS Z*

Champ	Description	Format
`protocol`	Protocole. Actuellement, soit HTTP/1.1 soit HTTP/2.	chaîne
`responseCode`	Le code de réponse HTTP. Seul le code de réponse pour les en-têtes finaux est enregistré. Pour de plus amples informations, veuillez consulter Résoudre les problèmes liés aux journaux d'accès.	entier
`bytesReceived`	Les octets de corps et d'en-tête reçus.	entier
`bytesSent`	Les octets du corps et de l'en-tête envoyés.	entier
`duration`	Durée totale en millisecondes de la demande entre l'heure de début et le dernier octet sortant.	entier
`requestToTargetDuration`	Durée totale en millisecondes de la demande entre l'heure de début et le dernier octet envoyé à la cible.	entier
`responseFromTargetDuration`	Durée totale en millisecondes de la demande entre le premier octet lu par l'hôte cible et le dernier octet envoyé au client.	entier

Champ	Description	Format
`grpcResponseCode`	Le code de réponse gRPC. Pour plus d'informations, consultez la section Codes d'état et leur utilisation dans gRPC. Ce champ est enregistré uniquement si le service prend en charge le gRPC.	entier
`callerPrincipal`	Le principal authentifié.	chaîne
`callerX509SubjectCN`	Le nom du sujet (CN).	chaîne
`callerX509IssuerOU`	L'émetteur (OU).	chaîne
`callerX509SANNameCN`	L'alternative de l'émetteur (nom/CN).	chaîne
`callerX509SANDNS`	Le nom alternatif du sujet (DNS).	chaîne
`callerX509SANURI`	Le nom alternatif du sujet (URI).	chaîne
`sourceVpcArn`	L'ARN du VPC d'où provient la demande.	*arn:aws:ec2 : région : compte : vpc/ id*

Exemple

Voici un exemple d'entrée de journal.

```
{
    "hostHeader": "example.com",
    "sslCipher": "-",
    "serviceNetworkArn": "arn:aws:vpc-lattice:us-west-2:123456789012:servicenetwork/
svn-1a2b3c4d",
    "resolvedUser": "Unknown",
    "authDeniedReason": "null",
```

```
    "requestMethod": "GET",
    "targetGroupArn": "arn:aws:vpc-lattice:us-west-2:123456789012:targetgroup/
tg-1a2b3c4d",
    "tlsVersion": "-",
    "userAgent": "-",
    "serverNameIndication": "-",
    "destinationVpcId": "vpc-0abcdef1234567890",
    "sourceIpPort": "178.0.181.150:80",
    "targetIpPort": "131.31.44.176:80",
    "serviceArn": "arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-1a2b3c4d",
    "sourceVpcId": "vpc-0abcdef1234567890",
    "requestPath": "/billing",
    "startTime": "2023-07-28T20:48:45Z",
    "protocol": "HTTP/1.1",
    "responseCode": 200,
    "bytesReceived": 42,
    "bytesSent": 42,
    "duration": 375,
    "requestToTargetDuration": 1,
    "responseFromTargetDuration": 1,
    "grpcResponseCode": 1
}
```


Résoudre les problèmes liés aux journaux d'accès

Cette section contient une explication des codes d'erreur HTTP que vous pouvez voir dans les journaux d'accès.

Code d'erreur	Causes possibles :
HTTP 400 : Demande erronée	• Le client a envoyé une demande mal formée qui ne répond pas à la spécification HTTP. • L'en-tête de demande dépassait 60 000 pour l'ensemble de l'en-tête de demande ou plus de 100 en-têtes. • Le client a fermé la connexion avant d'envoyer le corps complet de la demande.
HTTP 403 : Accès interdit	L'authentification a été configurée pour le service, mais la demande entrante n'est ni authentifiée ni autorisée.

Code d'erreur	Causes possibles :
HTTP 404 : Service inexistant	Vous essayez de vous connecter à un service qui n'existe pas ou qui n'est pas enregistré sur le réseau de service approprié.
HTTP 500 : Erreur de serveur interne	VPC Lattice a rencontré une erreur, telle qu'un échec de connexion aux cibles.
HTTP 502 : Passerelle erronée	VPC Lattice a rencontré une erreur.

CloudTrail journaux pour VPC Lattice

AWS CloudTrailest un AWS service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service. CloudTrail capture les appels d'API pour VPC Lattice sous forme d'événements. CloudTrail est activé sur votre ordinateur Compte AWS lorsque vous le créez. Lorsqu'une activité se produit dans VPC Lattice, cette activité est enregistrée en tant qu' CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Les appels capturés incluent des appels provenant de la console VPC Lattice et des appels de code aux opérations de l'API VPC Lattice. Pour plus d'informations sur CloudTrail, consultez le AWS CloudTrailGuide de l'utilisateur .

CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique. Un suivi est une CloudTrail configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment S3 que vous spécifiez.

Pour surveiller les actions supplémentaires, utilisez les journaux d'accès. Pour plus d'informations, veuillez consulter Journaux d'accès.

Comprendre les entrées du fichier journal VPC Lattice

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique

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

Pour plus d'informations sur les paires clé-valeur dans les journaux, voir le contenu des CloudTrail enregistrements dans le Guide de l'AWS CloudTrailutilisateur.

Voici un exemple d'entrée de journal pour un appel à l'action CreateServiceAPI.


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "abcdef01234567890",
    "arn": "arn:abcdef01234567890",
    "accountId": "abcdef01234567890",
    "accessKeyId": "abcdef01234567890",
    "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "abcdef01234567890",
            "arn": "arn:abcdef01234567890",
            "accountId": "abcdef01234567890",
            "userName": "abcdef01234567890"
        },
        "webIdFederationData": {},
        "attributes": {
            "creationDate": "2022-08-16T03:34:54Z",
            "mfaAuthenticated": "false"
        }
    }
  },
  "eventTime": "2022-08-16T03:36:12Z",
  "eventSource": "vpc-lattice.amazonaws.com",
  "eventName": "CreateService",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "abcdef01234567890",
  "userAgent": "abcdef01234567890",
  "requestParameters": {
    "name": "rates-service"
  },
  "responseElements": {
```

```
    "name": "rates-service",
    "id": "abcdef01234567890",
    "arn": "arn:abcdef01234567890",
    "status": "CREATE_IN_PROGRESS"
  },
  "requestID": "abcdef01234567890",
  "eventID": "abcdef01234567890",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "abcdef01234567890",
  "eventCategory": "Management"
}
```

Voici un exemple d'entrée de journal pour un appel à l'action DeleteServiceAPI.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "abcdef01234567890",
    "arn": "arn:ABCXYZ123456",
    "accountId": "abcdef01234567890",
    "accessKeyId": "abcdef01234567890",
    "sessionContext": {
        "sessionIssuer": {
            "type": "Role",
            "principalId": "abcdef01234567890",
            "arn": "arn:aws:iam::AIDACKCEVSQ6C2EXAMPLE:role/Admin",
            "accountId": "abcdef01234567890",
            "userName": "Admin"
        },
        "webIdFederationData": {},
        "attributes": {
            "creationDate": "2022-10-27T17:42:36Z",
            "mfaAuthenticated": "false"
        }
    }
  },
  "eventTime": "2022-10-27T17:56:41Z",
  "eventSource": "vpc-lattice.amazonaws.com",
  "eventName": "DeleteService",
  "awsRegion": "us-east-1",
```

```
  "sourceIPAddress": "72.21.198.64",
  "userAgent": "abcdef01234567890",
  "requestParameters": {
    "serviceIdentifier": "abcdef01234567890"
  },
  "responseElements": {
    "name": "test",
    "id": "abcdef01234567890",
    "arn": "arn:abcdef01234567890",
    "status": "DELETE_IN_PROGRESS"
  },
  "requestID": "abcdef01234567890",
  "eventID": "abcdef01234567890",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "abcdef01234567890",
  "eventCategory": "Management"
}
```

Quotas pour Amazon VPC Lattice

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chacun d'entre eux Service AWS. Sauf indication contraire, chaque quota est spécifique à la région. Vous pouvez demander des augmentations pour certains quotas, et d'autres quotas ne peuvent pas être augmentés.

Pour consulter les quotas de VPC Lattice, ouvrez la console Service Quotas. Dans le volet de navigation, choisissez Services AWSet sélectionnez VPC Lattice.

Pour demander une augmentation de quota, contactez le AWS Support ou consultez la section Demander une augmentation de quota dans le Guide de l'utilisateur du Service Quotas.

Vous Compte AWS disposez des quotas suivants liés à VPC Lattice.

Nom	Par défaut	Ajusta	Description
Taille de la politique d'authentification	Chaque région prise en charge : 10 kilo-octets	Non	Taille maximale d'un fichier JSON dans une politique d'authentification .
Auditeurs par service	Chaque région prise en charge : 2	Oui	Nombre maximal d'écouteurs que vous pouvez créer pour un service. Pour des capacités supplémen taires et des augmentat ions de limites, contactez AWS le Support.
Règles par auditeur	Chaque Région prise en charge : 5	Oui	Le nombre maximum de règles que vous pouvez définir pour votre service listener. Pour des capacités supplémen taires et des augmentat

Nom	Par défaut	Ajusta	Description
			ions de limites, contactez AWS le Support.
Groupes de sécurité par association	Chaque région prise en charge : 5	Non	Le nombre maximal de groupes de sécurité que vous pouvez ajouter à une association entre un VPC et un réseau de services.
Associations de services par réseau de services	Chaque région prise en charge : 500	Oui	Nombre maximal de services que vous pouvez associer à un réseau de services unique. Pour des capacités supplémen taires et des augmentat ions de limites, contactez AWS le Support.
Réseaux de services par région	Par région prise en charge : 10	Oui	Le nombre maximum de réseaux de service par région. Pour des capacités supplémen taires et des augmentat ions de limites, contactez AWS le Support.
Services par région	Chaque région prise en charge : 500	Oui	Le nombre maximum de services par région. Pour des capacités supplémen taires et des augmentat ions de limites, contactez AWS le Support.

Nom	Par défaut	Ajusta	Description
Groupes cibles par région	Chaque région prise en charge : 500	Oui	Le nombre maximum de groupes cibles par région. Pour des capacités supplémentaires et des augmentations de limites, contactez AWS le Support.
Groupes cibles par service	Chaque Région prise en charge : 5	Oui	Le nombre maximum de groupes cibles que vous pouvez associer à un service. Pour des capacités supplémen taires et des augmentat ions de limites, contactez AWS le Support.
Cibles par groupe cible	Chaque Région prise en charge : 1 000	Oui	Le nombre maximum de cibles que vous pouvez associer à un seul groupe cible. Pour des capacités supplémentaires et des augmentations de limites, contactez AWS le Support.
Associations VPC par réseau de services	Chaque région prise en charge : 500	Oui	Le nombre maximum de VPC que vous pouvez associer à un seul réseau de services. Pour des capacités supplémen taires et des augmentat ions de limites, contactez AWS le Support.

Les limites suivantes s'appliquent également.

Limite	Valeur
Bande passante par service et par zone de disponibilité	10 Gbit/s
Unité de transmission maximale (MTU) par connexion	8500 octets
Demandes par seconde, par service et par zone de disponibilité	10 000

Historique du document pour le guide de l'utilisateur du VPC Lattice

Le tableau suivant décrit les versions de documentation pour VPC Lattice.

Modification	Description	Date
Passthrough TLS	VPC Lattice prend désormais en charge le transfert TLS, ce qui vous permet d'effectuer la terminaison du protocole TLS dans votre application à des fins d'authentification. end-to-end	14 mai 2024
Version de la structure d'événements Lambda	VPC Lattice prend désormais en charge une nouvelle version de la structure d'événements Lambda.	7 septembre 2023
Support pour les VPC partagés	Les participants peuvent créer des groupes cibles VPC Lattice dans un VPC partagé.	5 juillet 2023
Version de disponibilité générale	La publication du guide de l'utilisateur VPC Lattice pour la disponibilité générale (GA)	31 mars 2023
VPC Lattice signale désormais les modifications apportées à ses politiques gérées AWS	Les modifications apportées aux politiques gérées sont signalées dans la section « Politiques AWS gérées pour VPC Lattice » du chapitre « Sécurité ».	29 mars 2023
Support pour le type de cible Application Load Balancer	VPC Lattice prend désormais en charge la création d'un	29 mars 2023

	groupe cible de type Application Load Balancer.	
Support pour tous les types d'instances	VPC Lattice prend désormais en charge tous les types d'instances.	27 mars 2023
Prise en charge d'IPv6	VPC Lattice prend désormais en charge les groupes cibles IP IPv4 et IPv6.	27 mars 2023
Version du protocole HTTP/2 pour les bilans de santé	Les contrôles de santé sont désormais pris en charge lorsque la version du protocole du groupe cible est HTTP/2.	27 mars 2023
Action de réponse fixe pour les règles de l'écouteur	Les écouteurs des services VPC Lattice prennent désormais en charge les actions de réponse fixe en plus des actions de transfert.	27 mars 2023
Support pour les noms de domaine personnalisés	Vous pouvez désormais configurer un nom de domaine personnalisé pour votre service VPC Lattice	14 février 2023
Support pour le BYOC (Bring Your Own Certificate)	VPC Lattice prend en charge l'utilisation de votre propre certificat SSL/TLS dans ACM pour les noms de domaine personnalisés.	14 février 2023
VPC Lattice affiche désormais une liste mise à jour des types d'instances non pris en charge	Trois instances supplémentaires ont été ajoutées à la liste des instances non prises en charge.	26 janvier 2023

VPC Lattice signale désormais les modifications apportées à ses politiques gérées AWS	À compter du 5 décembre 2022, les modifications apportées aux politiques gérées sont signalées dans la rubrique « Politiques AWS gérées pour VPC Lattice » du chapitre « Sécurité ». La première modification répertoriée est l'ajout des autorisations nécessaires à la CloudWatch surveillance.	5 décembre 2022
Première version	Publication initiale du guide de l'utilisateur VPC Lattice	5 décembre 2022

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.