aws

Guía del usuario

Amazon VPC Lattice

Amazon VPC Lattice: Guía del usuario

Table of Contents

¿Qué es Amazon VPC Lattice?

Amazon VPC Lattice es un servicio de redes de aplicaciones totalmente gestionado que se utiliza para conectar, proteger y supervisar los servicios y recursos de su aplicación. Puede usar VPC Lattice con una única nube privada virtual (VPC) o en varias VPCs de una o más cuentas.

Las aplicaciones modernas pueden constar de varios componentes pequeños y modulares que suelen denominarse microservicios, como una API HTTP, recursos, como bases de datos, y recursos personalizados compuestos por puntos finales de direcciones IP y DNS. Si bien la modernización tiene sus ventajas, también puede introducir complejidades y desafíos en la red al conectar estos microservicios y recursos. Por ejemplo, si los desarrolladores están repartidos en diferentes equipos, podrían crear e implementar microservicios y recursos en varias cuentas o. VPCs

En VPC Lattice, nos referimos a un microservicio como un servicio y representamos un recurso solo como una configuración de recursos. Estos son los términos que aparecen en la guía del usuario de VPC Lattice.

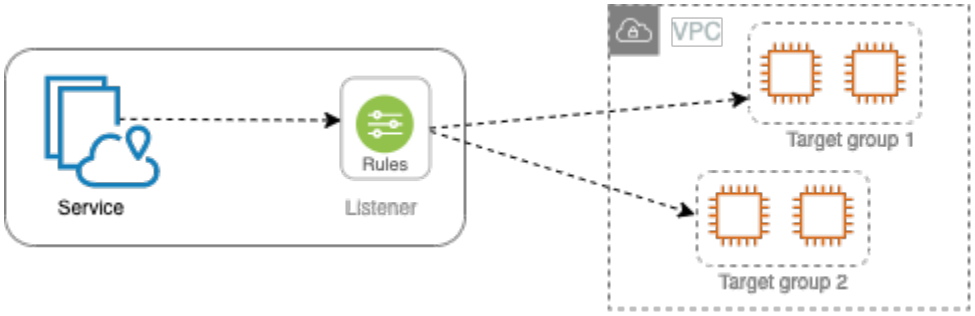
Contenido

Componentes principales

Para utilizar Amazon VPC Lattice, debe estar familiarizado con sus componentes principales.

Servicio

> Una unidad de software que se puede implementar de forma independiente y que ofrece una tarea o función específica. Un servicio puede ejecutarse en EC2 instancias o ECS/EKS/Fargate contenedores, o como funciones Lambda, dentro de una cuenta o una nube privada virtual (VPC). Un servicio de VPC Lattice tiene los siguientes componentes: grupos de destino, oyentes y reglas.



Grupo de destino

Conjunto de recursos, también conocidos como destinos, que ejecutan la aplicación o el servicio. Son similares a los grupos de destino que proporciona Elastic Load Balancing, pero no son intercambiables. Los tipos de destino compatibles incluyen EC2 instancias, direcciones IP, funciones Lambda, balanceadores de carga de aplicaciones, tareas de Amazon ECS y pods de Kubernetes.

Oyente

Proceso que comprueba las solicitudes de conexión y las enruta a los destinos de un grupo de destino. El listener se configura con un protocolo y un número de puerto.

Regla

Componente predeterminado de un oyente que reenvía las solicitudes a los destinos de un grupo de destino de VPC Lattice. Cada regla consta de una prioridad, una o más acciones y una o más condiciones. Las reglas determinan la forma en que el oyente enruta las solicitudes de clientes.

Recurso

Un recurso es una entidad como una base de datos del Amazon Relational Database Service (Amazon RDS), una instancia de EC2 Amazon, un punto final de aplicación, un destino de nombre de dominio o una dirección IP. Para compartir un recurso en su VPC, cree un recurso compartido en AWS Resource Access Manager (AWS RAM), cree una puerta de enlace de recursos y defina una configuración de recursos.

Puerta de enlace de recursos

Una puerta de enlace de recursos es un punto de entrada a la VPC en la que residen los recursos.

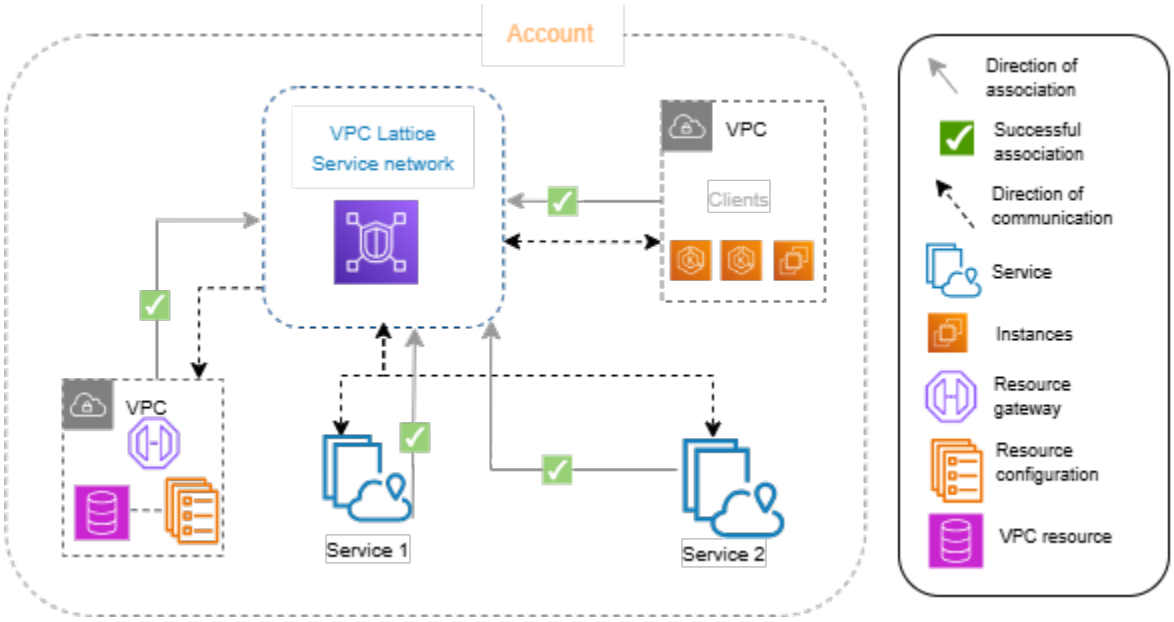
Configuración de recursos

Una configuración de recursos es un objeto lógico que representa un único recurso o un grupo de recursos. Un recurso puede ser una dirección IP, un destino de nombre de dominio o una base de datos de Amazon RDS.

Red de servicios

Límite lógico para un conjunto de configuraciones de servicios y recursos. Un cliente puede estar en una VPC asociada a la red de servicio. Los clientes y los servicios que están asociados a la misma red de servicios pueden comunicarse entre sí si están autorizados a hacerlo.

En la siguiente figura, los clientes pueden comunicarse con ambos servicios, ya que la VPC y los servicios están asociados a la misma red de servicios.



Directorio de servicios

Un registro central de todos los servicios de VPC Lattice que posees o a través de los cuales compartes con tu cuenta. AWS RAM

Políticas de autorización

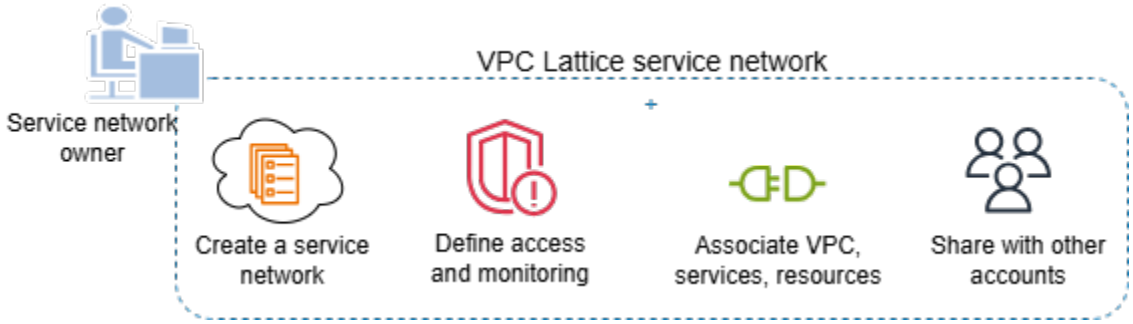
Políticas de autorización detalladas que se pueden utilizar para definir el acceso a los servicios. Puede asociar políticas de autorización independientes a los servicios individuales o a la red de servicios. Por ejemplo, puedes crear una política sobre cómo un servicio de pago que se ejecuta en un grupo de EC2 instancias con escalado automático debe interactuar con un servicio de facturación que se ejecuta en él AWS Lambda.

Las políticas de autenticación no se admiten en las configuraciones de recursos. Las políticas de autenticación de una red de servicios no se aplican a las configuraciones de recursos de la red de servicios.

Funciones y responsabilidades

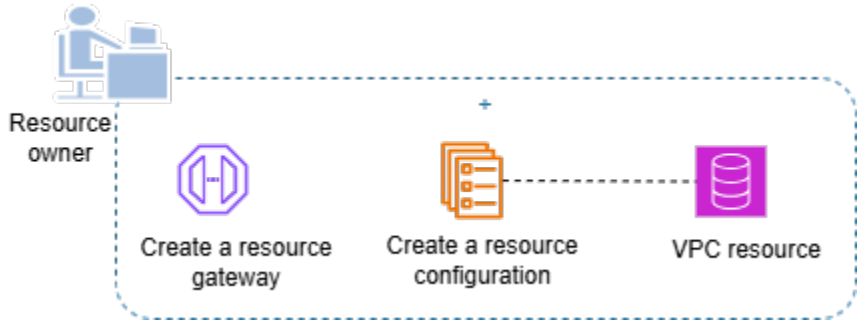
Un rol determina quién es responsable de la configuración y el flujo de información dentro de Amazon VPC Lattice. Por lo general, hay dos roles: propietario de la red de servicios y propietario del servicio, y sus responsabilidades pueden superponerse.

Propietario de la red de servicios: el propietario de la red de servicios suele ser el administrador de la red o el administrador de la nube de una organización. Los propietarios de la red de servicios crean, comparten y aprovisionan la red de servicios. También administran quién puede acceder a la red o los servicios dentro de VPC Lattice. El propietario de la red de servicio puede definir una configuración de acceso detallada para los servicios asociados a la red de servicios. Estos controles se utilizan para administrar la comunicación entre los clientes y los servicios mediante políticas de autenticación y autorización. El propietario de la red de servicio también puede asociar una configuración de servicio o recurso a una o varias redes de servicio, si la configuración del servicio o recurso se comparte con la cuenta del propietario de la red de servicio.



Propietario del servicio: el propietario del servicio suele ser un desarrollador de software de una organización. Los propietarios de servicios crean servicios dentro de VPC Lattice, definen las reglas de enrutamiento y también asocian los servicios a la red de servicios. También pueden definir una configuración de acceso detallada, que puede restringir el acceso únicamente a los servicios y clientes autenticados y autorizados.

Propietario del recurso: el propietario del recurso suele ser un desarrollador de software en una organización y actúa como administrador de un recurso, como una base de datos. El propietario del recurso crea una configuración de recursos para el recurso, define los ajustes de acceso para la configuración del recurso y asocia la configuración del recurso a las redes de servicio.



Características

Las siguientes son las características principales que ofrece VPC Lattice.

Detección de servicios

Todos los clientes y servicios VPCs asociados a la red de servicios pueden comunicarse con otros servicios dentro de la misma red de servicios. Direcciones de DNS client-to-service y service-to-service tráfico a través del punto final de VPC Lattice. Cuando un cliente quiere enviar una solicitud a un servicio, utiliza el nombre de DNS del servicio. El solucionador de Route 53 envía el tráfico a VPC Lattice, que luego identifica el servicio de destino.

Conectividad

Client-to-service y la client-to-resource conectividad se establece dentro de la infraestructura de AWS red. Al asociar una VPC a la red de servicio, cualquier cliente de la VPC puede conectarse con los servicios y recursos (mediante configuraciones de recursos) de la red de servicios, si tiene el acceso necesario. VPC Lattice admite la tecnología CIDR superpuesta.

Acceso local

Puede habilitar la conectividad a una red de servicio desde una VPC mediante un punto final de VPC (con tecnología). AWS PrivateLink Un punto final de VPC de tipo red de servicio le permite habilitar el acceso a los servicios y recursos de la red de servicios desde redes locales a través de Direct Connect y VPN. El tráfico que atraviesa el emparejamiento de VPC AWS Transit Gateway o que también puede acceder a los recursos y servicios a través de un punto final de VPC.

Observabilidad

VPC Lattice genera métricas y registros para cada solicitud y respuesta que atraviesa la red de servicios, para ayudarlo a monitorear y solucionar problemas de las aplicaciones. De forma predeterminada, las métricas se publican en la cuenta del propietario del servicio. Los propietarios de los servicios y los propietarios de los recursos tienen la opción de activar el registro y recibir los registros de todos los clientes access/requests to their services and resources. Service network owners can also turn on logging on the service network, to log all access/requests de los servicios y recursos de los clientes VPCs que están conectados a la red de servicios.

VPC Lattice funciona con las siguientes herramientas para ayudarle a supervisar sus servicios y solucionar sus problemas: Amazon CloudWatch grupos de registros, transmisiones de entrega de Firehose y buckets de Amazon S3.

Seguridad

VPC Lattice proporciona un marco que puede utilizar para implementar una estrategia de defensa en varios niveles de la red. La primera capa es la combinación de servicio, configuración de recursos, asociación de VPC y punto final de VPC de tipo red de servicio. Sin una VPC y una asociación de servicios o un punto final de VPC de tipo red de servicio, los clientes no pueden acceder a los servicios. Del mismo modo, sin una VPC y una configuración de recursos y una asociación de servicios o un punto final de VPC de tipo red de servicio, los clientes no pueden acceder a los recursos.

La segunda capa permite a los usuarios asociar grupos de seguridad a la asociación entre la VPC y la red de servicios. La tercera y cuarta capa son políticas de autorización que se pueden aplicar individualmente a nivel de red de servicios y a nivel de servicio.

Acceso a VPC Lattice

Puede crear, acceder y administrar VPC Lattice con cualquiera de las siguientes interfaces:

- AWS Management Console: proporciona una interfaz web que puede utilizar para acceder a VPC Lattice.
- AWS Command Line Interface (AWS CLI): proporciona comandos para un amplio conjunto de AWS servicios, incluido VPC Lattice. AWS CLI Es compatible con Windows, macOS y Linux. Para obtener más información acerca de la CLI, consulte AWS Command Line Interface. Para obtener más información sobre la APIs, consulte la referencia de la API Amazon VPC Lattice.
- Controlador de VPC Lattice para Kubernetes: administra los recursos de VPC Lattice para un clúster de Kubernetes. Para obtener más información sobre el uso de VPC Lattice con Kubernetes, consulte la Guía del usuario del controlador de AWS Gateway API.
- AWS CloudFormation: lo ayuda a diseñar y configurar sus recursos de AWS . Para obtener más información, consulte la referencia del tipo de recurso de Amazon VPC Lattice.

Puntos finales del servicio VPC Lattice

Un punto final es una URL que sirve como punto de entrada para un AWS servicio web. VPC Lattice admite los siguientes tipos de puntos finales:

- the section called “IPv4 puntos de enlace”
- Puntos finales de Dualstack (compatibles con y) IPv4 IPv6

Al realizar una solicitud, puede especificar el punto de conexión que se va a utilizar. Si no especifica un punto final, se usa el IPv4 punto final de forma predeterminada. Para utilizar un tipo de punto de conexión diferente, debe especificarlo en la solicitud. Para ver ejemplos prácticos, consulte the section called “Especificación de puntos de conexión”. Para ver una tabla de los puntos de enlace disponibles, consulte los puntos de enlace de Amazon VPC Lattice.

IPv4 puntos de enlace

IPv4 los puntos finales solo admiten IPv4 tráfico. IPv4 los puntos finales están disponibles en todas las regiones.

Si especifica el punto de conexión general `vpc-lattice.amazonaws.com`, utilizamos el punto de conexión para `us-east-1`. Para utilizar una región diferente, especifique su punto de conexión asociado. Por ejemplo, si especifica `vpc-lattice.us-east-2.amazonaws.com` como punto de conexión, dirigimos su solicitud al punto de conexión `us-east-2`.

IPv4 los nombres de los puntos finales utilizan la siguiente convención de nomenclatura:

- `vpc-lattice.region.amazonaws.com`

Por ejemplo, el nombre del IPv4 punto final de la `eu-west-1` región es`vpc-lattice.eu-west-1.amazonaws.com`.

Puntos finales de Dualstack (IPv4 y IPv6)

Los puntos finales de Dualstack admiten tanto el tráfico como el tráfico. IPv4 IPv6 Los puntos de conexión de Dualstack están disponibles para todas las regiones. Al realizar una solicitud a un punto final de doble pila, la URL del punto final pasa a ser una IPv6 o una IPv4 dirección, según el protocolo utilizado por la red y el cliente.

Los nombres de puntos de conexión de doble pila utilizan la siguiente convención de nomenclatura:

- `vpc-lattice.region.api.aws`

Por ejemplo, el nombre del punto de conexión de doble pila para la región `eu-west-1` es `vpc-lattice.eu-west-1.api.aws`.

Especificación de puntos de conexión

En los siguientes ejemplos se muestra cómo especificar un punto final para la `us-east-2` región mediante el AWS CLI comando for. `vpc-lattice`

- IPv4

```
aws vpc-lattice get-service --service-identifier svc-0285b53b2eEXAMPLE --region us-east-2 --endpoint-url https://vpc-lattice.us-east-2.amazonaws.com
```

- Pila doble

```
aws vpc-lattice get-service --service-identifier svc-0285b53b2eEXAMPLE --region us-east-2 --endpoint-url https://vpc-lattice.us-east-2.api.aws
```

Precios

Con VPC Lattice, paga por el tiempo que se aprovisiona un servicio, la cantidad de datos transferidos a través de cada servicio y el número de solicitudes. Como propietario de un recurso, usted paga por

los datos transferidos desde y hacia cada recurso. Como propietario de una red de servicios, paga por hora las configuraciones de recursos asociadas a su red de servicios. Como consumidor que tiene una VPC asociada a una red de servicio, usted paga por los datos transferidos desde y hacia los recursos de la red de servicio desde su VPC. Para obtener más información, consulte Precios de Amazon VPC Lattice.

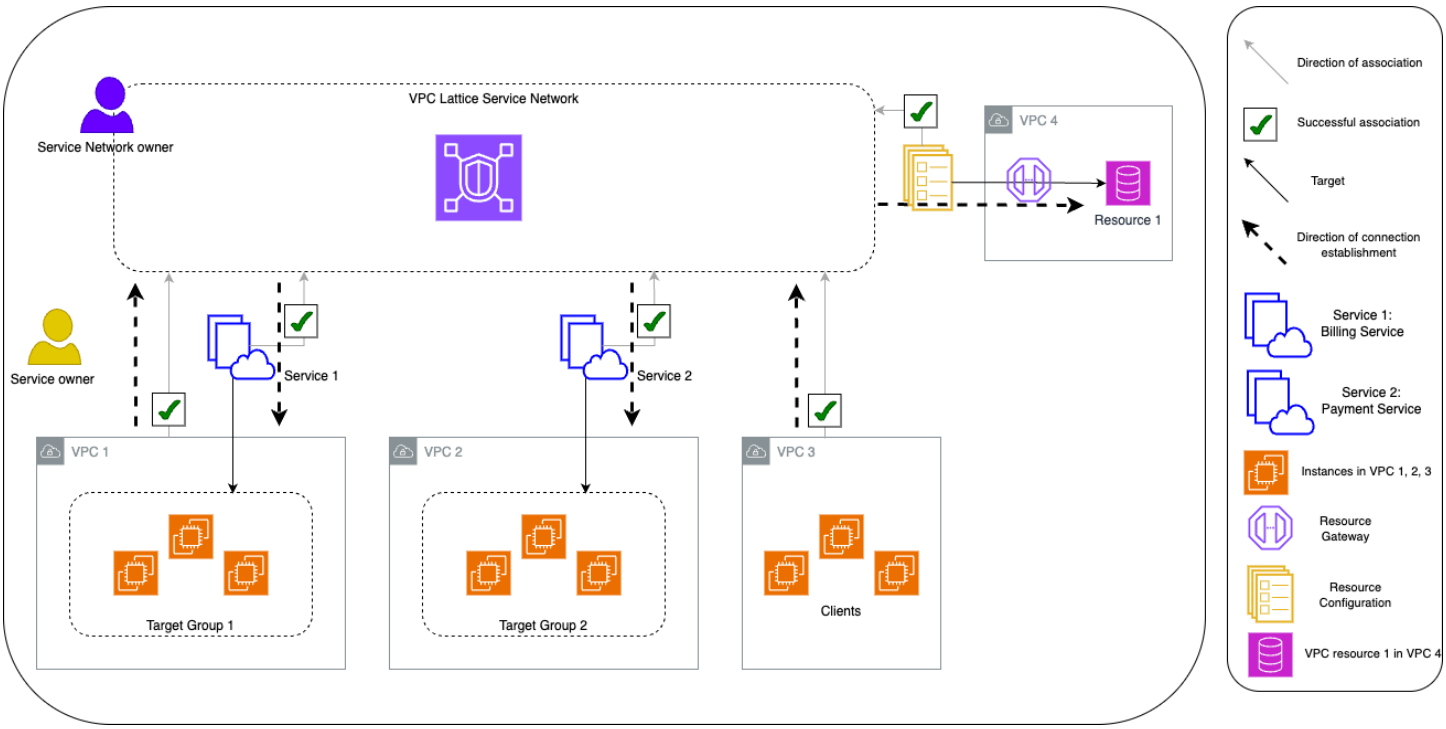
Cómo funciona VPC Lattice

VPC Lattice está diseñado para ayudarlo a descubrir, proteger, conectar y monitorear de manera fácil y efectiva todos los servicios y recursos que contiene. Cada componente de VPC Lattice se comunica de forma unidireccional o bidireccional dentro de la red de servicios en función de su asociación con la red de servicios y su configuración de acceso. La configuración de acceso se compone de las políticas de autenticación y autorización necesarias para esta comunicación.

El siguiente resumen describe la comunicación entre los componentes de VPC Lattice:

- Hay dos formas de conectar una VPC a una red de servicio: mediante una asociación de VPC y mediante un punto final de VPC del tipo red de servicio.
- Los servicios y recursos que están asociados a la red de servicios pueden recibir solicitudes de clientes que también VPCs estén conectados a la red de servicios.
- Un cliente puede enviar solicitudes a los servicios y recursos asociados a una red de servicio solo si se encuentra en una VPC que esté conectada a la misma red de servicio. El tráfico de clientes que atraviesa una conexión de emparejamiento de VPC, una puerta de enlace de tránsito, Direct Connect o una VPN solo puede llegar a los recursos y servicios si la VPC está conectada a la red de servicios a través de un punto final de la VPC.
- Los destinos de los servicios VPCs que están asociados a la red de servicios también son clientes y pueden enviar solicitudes a otros servicios y recursos asociados a la red de servicios.
- Los destinos de los servicios VPCs que no están asociados a la red de servicios no son clientes y no pueden enviar solicitudes a otros servicios y recursos asociados a la red de servicios.
- Los clientes VPCs que tienen recursos pero en los que la VPC no está asociada a la red de servicio no son clientes y no pueden enviar solicitudes a otros servicios y recursos asociados a la red de servicios.

El siguiente diagrama de flujo utiliza un escenario de ejemplo para explicar el flujo de información y la dirección de comunicación entre los componentes de VPC Lattice. Existen dos servicios asociados a una red de servicios. Ambos servicios y todos VPCs se crearon en la misma cuenta que la red de servicios. Ambos servicios están configurados para permitir el tráfico desde la red de servicios.



El servicio 1 es una aplicación de facturación que se ejecuta en un grupo de instancias registradas con el grupo de destino 1 en la VPC 1. El servicio 2 es una aplicación de pago que se ejecuta en un grupo de instancias registradas con el grupo de destino 2 en la VPC 2. La VPC 3 se encuentra en la misma cuenta y tiene clientes, pero no servicios. El recurso 1 es una base de datos que contiene datos de clientes en la VPC 4.

La siguiente lista describe, en orden, el flujo de trabajo típico de las tareas de VPC Lattice.

1. Creación de una red de servicios

   El propietario de la red de servicios crea la red de servicios.

2. Crear un servicio

   Los propietarios del servicio crean sus respectivos servicios, el servicio 1 y el servicio 2. Durante la creación, el propietario del servicio agrega los oyentes y define las reglas para enrutar las solicitudes al grupo de destino de cada servicio.

3. Definición del enrutamiento

   Los propietarios del servicio crean el grupo de destino para cada servicio (grupo de destino 1 y grupo de destino 2). Para ello, especifican las instancias de destino en las que se ejecutan los servicios. También especifican el lugar VPCs en el que residen estos objetivos.

En el diagrama anterior, las flechas continuas representan los servicios que enrutan el tráfico a los grupos de destino y las configuraciones de recursos que enrutan a los recursos.

4. Asociación de un servicio a la red de servicios

   El propietario de la red de servicios o el propietario del servicio asocian los servicios a la red de servicios. Las asociaciones se muestran como flechas con marcas de verificación que apuntan a la red de servicios desde el servicio. Al asociar un servicio a una red de servicios, otros servicios asociados a la red de servicios y los clientes que VPCs estén conectados a la red de servicios pueden detectarlo.

   Las flechas discontinuas entre la red de servicio y los grupos objetivo muestran la dirección del establecimiento de la conexión. El tráfico de retorno regresa a los clientes que utilizan la red de servicio. Las flechas que representan el tráfico de retorno no se incluyen en este diagrama.

5. Cree una puerta de enlace de recursos

   El propietario del recurso crea una puerta de enlace de recursos en la VPC 4 para poder habilitar la conectividad de los clientes al recurso 1.

6. Cree una configuración de recursos

   El propietario del recurso crea una configuración de recursos para representar el recurso 1 y especifica la puerta de enlace de recursos para el recurso 1.

7. Asocie las configuraciones de recursos a la red de servicios

   El propietario de la red de servicio o el propietario del recurso asocian la configuración del recurso a la red de servicio. La asociación se muestra como una flecha con una marca de verificación que apunta a la red de servicio desde la configuración de recursos. Al asociar una configuración de recursos a una red de servicios, otros servicios asociados a la red de servicios y los clientes de la red VPCs conectada a la red de servicios pueden detectar esa configuración de recursos.

   Las flechas discontinuas que van de la red de servicios al recurso representan el recurso que recibe las solicitudes de los clientes. El tráfico de retorno regresa al cliente mediante la red de servicio. Las flechas que representan el tráfico de retorno no se incluyen en este diagrama.

8. Conéctese VPCs con la red de servicio

   VPCs se puede conectar a la red de servicio de dos maneras: asociando la VPC a la red de servicio o creando un punto final de la VPC. En este caso, el propietario de la red de servicio asocia la VPC 1 y la VPC 3 con la red de servicio. Las asociaciones se muestran mediante flechas

con marcas de verificación que apuntan a la red de servicio. Con estas asociaciones, todos los recursos de la VPC pueden actuar como clientes y realizar solicitudes a los servicios de la red de servicios. Las flechas discontinuas entre la VPC 1 y la red de servicio muestran la dirección del establecimiento de la conexión. La red de servicio solo inicia conexiones hacia los recursos a los que se dirigen los grupos destinatarios del servicio 1. Cualquier recurso de la VPC 1 puede actuar como cliente e iniciar conexiones a los servicios y recursos de la red de servicios.

La VPC 2 no tiene una flecha ni una marca de verificación que represente una asociación. Esto significa que el propietario de la red de servicios o el propietario del servicio no han asociado la VPC 2 a la red de servicios. Esto se debe a que el servicio 2, en este ejemplo, solo necesita recibir solicitudes y enviar respuestas mediante la misma solicitud. En otras palabras, los destinos del servicio 2 no son clientes y no necesitan realizar solicitudes a otros servicios de la red de servicios.

Del mismo modo, la VPC 4 no tiene una flecha o una marca de verificación que represente una asociación. Esto significa que el propietario de la red de servicio o el propietario del recurso no han asociado la VPC 4 a la red de servicio. Esto se debe a que el recurso 1 solo recibe solicitudes y envía respuestas mediante la misma solicitud. No puede realizar solicitudes a otros servicios y recursos de la red de servicios.

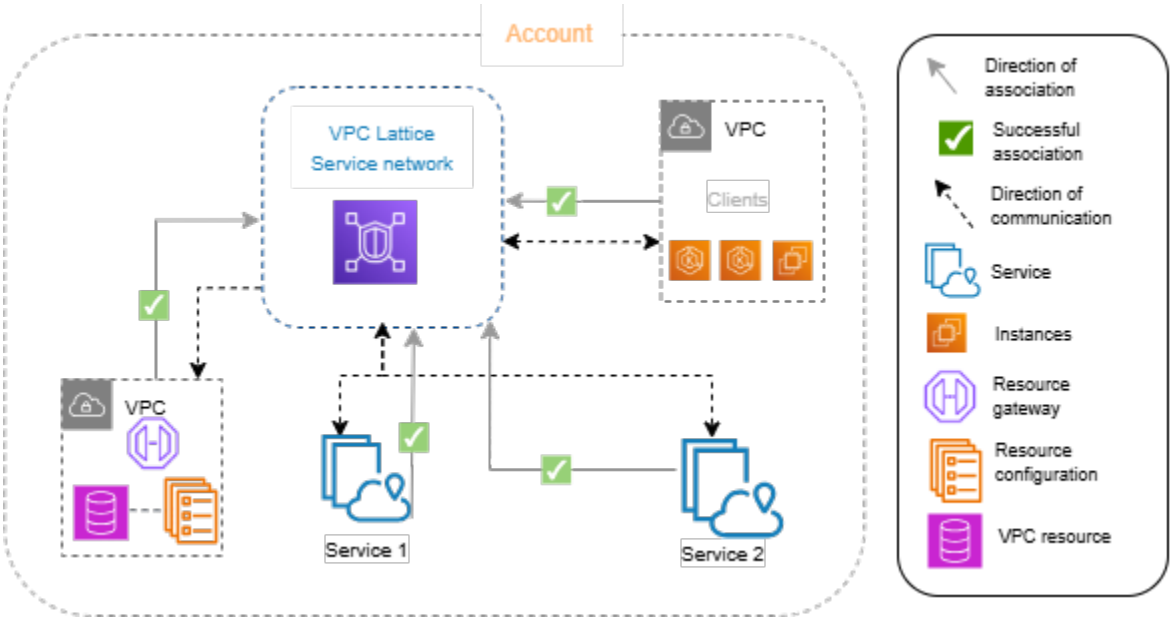
En resumen, el diagrama siguiente muestra los siguientes escenarios:

- VPCs con conexiones de entrada únicamente desde VPC Lattice a sus recursos. La VPC 2 y la VPC 4 representan estos escenarios.
- Una VPC con conexiones de salida únicamente desde sus recursos a VPC Lattice. La VPC 3 representa este escenario.
- Una VPC con conexiones de entrada desde VPC Lattice a sus recursos y con conexiones de salida desde sus recursos a VPC Lattice. La VPC 1 representa este escenario.

Redes de servicios en VPC Lattice

Una red de servicios es un límite lógico para un conjunto de configuraciones de servicios y recursos. Las configuraciones de servicios y recursos asociadas a la red se pueden autorizar para su detección, conectividad, accesibilidad y observabilidad. Para realizar solicitudes a las configuraciones de servicios y recursos de la red, el servicio o el cliente debe estar en una VPC que esté conectada a la red de servicios a través de una asociación o a través de un punto final de la VPC.

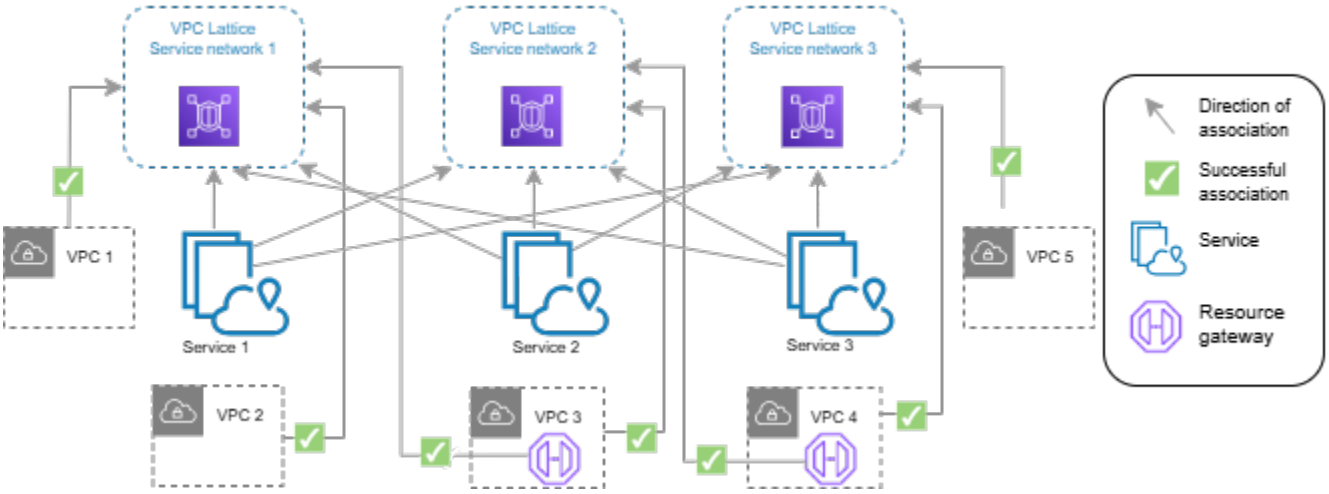
En el siguiente diagrama se muestran los componentes claves de una red de servicios propia de Amazon VPC Lattice. Las marcas de verificación en las flechas indican que los servicios y la VPC están asociados a la red de servicios. Los clientes de la VPC asociada a la red de servicios pueden comunicarse con ambos servicios a través de la red de servicios.



Puede asociar una o más configuraciones de servicios y recursos a varias redes de servicios. También puede conectar varias redes VPCs a una red de servicios. Puede conectar una VPC a una sola red de servicio a través de una asociación. Para conectar una VPC a varias redes de servicio, puede utilizar puntos finales de VPC del tipo red de servicio. Para obtener más información sobre los puntos finales de VPC de tipo red de servicio, consulte la guía del AWS PrivateLink usuario.

En el siguiente diagrama, las flechas representan las asociaciones entre los servicios y las redes de servicio, así como las asociaciones entre las redes VPCs y las de servicio. Puede ver que varios servicios están asociados a varias redes de servicios y que varios VPCs están asociados a cada red de servicio. Cada VPC tiene exactamente una asociación a una red de servicio. Sin embargo, la VPC 3 y la VPC 4 se conectan a dos redes de servicio. La VPC 3 se conecta a la red de servicio 1

a través de un punto final de la VPC. Del mismo modo, la VPC 4 se conecta a la red de servicio 2 a través de un punto final de la VPC.



Para obtener más información, consulte Cuotas de Amazon VPC Lattice.

Contenido

Cree una red de servicios VPC Lattice

Utilice la consola para crear una red de servicios y, si desea, configurarla con servicios, asociaciones, ajustes de acceso y registros de acceso.

Cómo crear una red de servicios mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Redes de servicios.
3. Elija Crear una red de servicios.

4. En el caso de los Identificadores, introduzca un nombre, una descripción opcional y etiquetas opcionales. El nombre debe tener entre 3 y 63 caracteres. Puede utilizar letras en minúscula, números y guiones. El nombre debe comenzar y terminar con una letra o un número. No utilice guiones consecutivos. La descripción puede tener hasta 256 caracteres. Para agregar una etiqueta, elija Añadir nueva etiqueta y la clave y el valor del registro.
5. (Opcional) Para asociar un servicio, elija el servicio dentro de Asociaciones de servicios, Servicios. La lista incluye los servicios que están en su cuenta y cualquier servicio que le hayan compartido desde una cuenta diferente. Si no hay ningún servicio en la lista, elija Crear un servicio VPC Lattice para crear uno.

   Como alternativa, para asociar un servicio después de haber creado la red de servicios, consulte the section called “Administración de asociaciones de servicios”.
6. (Opcional) Para asociar una configuración de recursos, elija el servicio de configuración de recursos en Asociaciones de configuración de recursos, Configuración de recursos. La lista incluye las configuraciones de recursos que se encuentran en su cuenta y cualquier configuración de recursos que se comparta con usted desde otra cuenta. Si no hay ninguna configuración de recursos en la lista, puede crear una configuración de recursos seleccionando Create an Amazon VPC Lattice resource configuration.

   Como alternativa, para asociar una configuración de recursos después de haber creado la red de servicios, consulte. the section called “Administre las asociaciones de configuración de recursos”
7. (Opcional) Para asociar una VPC, elija Agregar asociación de VPC. Seleccione la VPC que desee asociar desde VPC y seleccione hasta cinco grupos de seguridad dentro de Grupos de seguridad. Para crear un grupo de seguridad, elija Crear un grupo de seguridad.

   Como alternativa, puede omitir este paso y conectar una VPC a la red de servicio mediante un punto final de VPC (con tecnología). AWS PrivateLink Para obtener más información, consulte Acceder a las redes de servicios en la guía del AWS PrivateLink usuario.
8. Al crear una red de servicio, debe decidir si desea compartirla con otras cuentas o no. La selección es inmutable y no se puede cambiar después de crear la red de servicio. Si eliges permitir el uso compartido, la red de servicio se puede compartir con otras cuentas a través de. AWS Resource Access Manager

   Para compartir tu red de servicios con otras cuentas, selecciona los AWS RAM recursos compartidos en Recursos compartidos.

Para crear un recurso compartido, vaya a la AWS RAM consola y elija Crear un recurso compartido.

9. Para el acceso a la red, puede dejar el tipo de autenticación predeterminado, Ninguno, si desea que los clientes de la red asociada accedan VPCs a los servicios de esta red de servicios. Para aplicar una política de autenticación que controle el acceso a sus servicios, elija IAM de AWS y realice una de las siguientes acciones para la política de autenticación:
   - Escriba una política en el campo de entrada. Para ver políticas de ejemplo que puede copiar y pegar, elija Ejemplos de políticas.
   - Elija Aplicar la plantilla de política y seleccione la plantilla Permitir el acceso autenticado y no autenticado. Esta plantilla permite a un cliente de otra cuenta acceder al servicio ya sea firmando la solicitud (es decir, autenticada) o de forma anónima (es decir, no autenticada).
   - Elija Aplicar la plantilla de política y seleccione la plantilla Permitir solo el acceso autenticado. Esta plantilla permite a un cliente de otra cuenta acceder al servicio firmando la solicitud (es decir, autenticada).
10. (Opcional) Para activar los registros de acceso, seleccione el conmutador de registros de acceso y especifique un destino para esos registros de la siguiente manera:
   - Seleccione Grupo de CloudWatch registros y elija un grupo de CloudWatch registros. Para crear un grupo de registros, elija Crear un grupo de registros en CloudWatch.
   - Seleccione Bucket de S3 e introduzca la ruta del bucket de S3, incluido cualquier prefijo. Para buscar sus buckets de S3, elija Explorar S3.
   - Seleccione Flujo de entrega de Kinesis Data Firehose y elija un flujo de entrega. Para crear un flujo de entrega, elija Crear un flujo de entrega en Kinesis.
11. (Opcional) Para compartir su red de servicios con otras cuentas, elija los AWS RAM recursos compartidos en Recursos compartidos. Para crear un recurso compartido, elija Crear un recurso compartido en la consola RAM.
12. Revise su configuración en la sección Resumen y, a continuación, elija Crear red de servicios.

Para crear una red de servicios mediante AWS CLI

Utilice el comando create-service-network. Este comando crea únicamente la red de servicios básica. Para crear una red de servicios completamente funcional, también debe usar los comandos que crean asociaciones de servicios, asociaciones de VPC y configuraciones de acceso.

Gestione las asociaciones de una red de servicios de VPC Lattice

Al asociar un servicio o una configuración de recursos a la red de servicios, los clientes VPCs conectados a la red de servicios pueden realizar solicitudes a la configuración de servicios y recursos. Cuando conecta una VPC a la red de servicio, permite que todos los destinos de esa VPC sean clientes y se comuniquen con otros servicios y configuraciones de recursos de la red de servicios.

Contenido

Administración de asociaciones de servicios

Puede asociar los servicios que permanecen en su cuenta o los servicios que le hayan compartido desde diferentes cuentas. Este paso es opcional al momento de crear una red de servicios. Sin embargo, una red de servicios no es completamente funcional hasta que se asocie un servicio. Los propietarios de los servicios pueden asociar sus servicios a una red de servicios si su cuenta tiene el acceso necesario. Para obtener más información, consulte Ejemplos de políticas basadas en identidad de VPC Lattice.

Al eliminar una asociación de servicios, el servicio ya no se puede conectar a otros servicios de la red de servicios.

Cómo administrar asociaciones a servicios mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Redes de servicios.
3. Seleccione el nombre de la red de servicio para abrir su página de detalles.
4. Elija la pestaña Asociaciones de servicios.
5. Para crear una asociación, realice lo siguiente:
    a. Elija Crear asociaciones.

b. Seleccione un servicio en Servicios. Para crear un servicio, elija Crear un servicio de Amazon VPC Lattice.

c. (Opcional) Para agregar una etiqueta, expanda Etiquetas de asociación de servicios, elija Agregar etiqueta nueva e ingrese una clave y un valor de etiqueta.

d. Seleccione Save changes (Guardar cambios).

6. Para eliminar una asociación, seleccione la casilla de verificación de la asociación y, luego, elija Acciones, Eliminar asociaciones de servicios. Cuando le pidan confirmación, escriba **`confirm`** y elija Eliminar.

Para crear una asociación de servicios mediante el AWS CLI

Utilice el comando create-service-network-service-association.

Para eliminar una asociación de servicios mediante el AWS CLI

Utilice el comando delete-service-network-service-association.

Administre las asociaciones de configuración de recursos

Una configuración de recursos es un objeto lógico que representa un único recurso o un grupo de recursos. Puede asociar configuraciones de recursos que residan en su cuenta o configuraciones de recursos que se compartan con usted desde diferentes cuentas. Este paso es opcional al momento de crear una red de servicios. Los propietarios de las configuraciones de recursos pueden asociar sus configuraciones de recursos a una red de servicios si su cuenta tiene el acceso necesario. Para obtener más información, consulte Ejemplos de políticas basadas en identidad para VPC Lattice.

Gestione las asociaciones entre las redes de servicios y las configuraciones de recursos

Puede crear o eliminar la asociación entre la red de servicios y la configuración de recursos.

Para administrar las asociaciones de configuración de recursos mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en Lattice PrivateLink y Lattice, elija Redes de servicio.
3. Seleccione el nombre de la red de servicio para abrir su página de detalles.
4. Seleccione la pestaña Asociaciones de configuración de recursos.

5. Para crear una asociación, realice lo siguiente:

   a. Elija Crear asociaciones.
   b. Seleccione una configuración de recursos en Configuraciones de recursos. Elija Crear una configuración de recursos de Amazon VPC Lattice. .
   c. (Opcional) Para agregar una etiqueta, expanda Etiquetas de asociación de servicios, elija Agregar etiqueta nueva e ingrese una clave y un valor de etiqueta.
   d. Seleccione Save changes (Guardar cambios).
6. Para eliminar una asociación, active la casilla de verificación de la asociación y, a continuación, elija Acciones, Eliminar. Cuando le pidan confirmación, escriba **`confirm`** y elija Eliminar.

Para crear una asociación de configuración de recursos mediante el AWS CLI

Utilice el comando create-service-network-resource-association.

Para eliminar una asociación de configuración de recursos mediante el AWS CLI

Utilice el comando delete-service-network-resource-association.

Administración de asociaciones de VPC

Los clientes pueden enviar solicitudes a los servicios y recursos especificados en las configuraciones de recursos asociadas a una red de servicios si el cliente está VPCs asociado a la red de servicios. El tráfico de clientes que atraviesa una conexión de emparejamiento de VPC o una puerta de enlace de tránsito solo se permite a través de una red de servicio que utilice un punto final de VPC del tipo red de servicio.

Asociar una VPC es opcional al momento de crear una red de servicios. Los propietarios de la red pueden asociarse VPCs a una red de servicio si su cuenta tiene el acceso necesario. Para obtener más información, consulte Ejemplos de políticas basadas en identidad de VPC Lattice.

Al eliminar una asociación de VPC, los clientes de la ya no VPCs pueden conectarse a los servicios de la red de servicios.

Cómo administrar asociaciones VPC mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Redes de servicios.
3. Seleccione el nombre del servicio para abrir su página de detalles.

4. Elija la pestaña Asociaciones de VPC.
5. Para crear una asociación de VPC, realice lo siguiente:
   a. Elija Crear asociaciones de VPC.
   b. Elija Añadir asociación de VPC.
   c. Seleccione una VPC en VPC y seleccione hasta cinco grupos de seguridad de los grupos de seguridad. Para crear un grupo de seguridad, elija Crear un grupo de seguridad.
   d. (Opcional) Para agregar una etiqueta, expanda Etiquetas de asociación de VPC, elija Agregar etiqueta nueva e ingrese una clave y un valor de etiqueta.
   e. Seleccione Save changes (Guardar cambios).
6. Para editar los grupos de seguridad de una asociación, seleccione la casilla de verificación de la asociación y, luego, elija Acciones, Editar grupos de seguridad. Añada y elimine los grupos de seguridad cuando sea necesario.
7. Para eliminar una asociación, seleccione la casilla de verificación de la asociación y, luego, elija Acciones, Eliminar asociaciones de VPC. Cuando le pidan confirmación, escriba **`confirm`** y elija Eliminar.

Para crear una asociación de VPC mediante AWS CLI

Utilice el comando create-service-network-vpc-association.

Para actualizar los grupos de seguridad de una asociación de VPC mediante AWS CLI

Utilice el comando update-service-network-vpc-association.

Para eliminar una asociación de VPC mediante el AWS CLI

Utilice el comando delete-service-network-vpc-association.

Gestione las asociaciones de puntos finales de VPC

Los clientes pueden enviar solicitudes a los servicios y recursos especificados en las configuraciones de recursos a través de un punto final de VPC (con tecnología AWS PrivateLink) de su VPC. Un punto final de VPC de tipo red de servicio conecta una VPC a una red de servicio. El tráfico de clientes que proviene de fuera de la VPC a través de una conexión de emparejamiento de VPC, Transit Gateway, Direct Connect o una VPN puede usar el punto final de la VPC para llegar a las configuraciones de servicios y recursos. Con los puntos de conexión de VPC, puede conectar

una VPC a varias redes de servicios. Al crear un punto final de VPC en una VPC, se utilizan las direcciones IP de la VPC (y no las direcciones IP de la lista de prefijos gestionados) para establecer la conectividad con la red de servicio.

Para administrar las asociaciones de puntos de conexión de VPC mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Redes de servicios.
3. Seleccione el nombre de la red de servicio para abrir su página de detalles.
4. Seleccione la pestaña Asociaciones de puntos finales para ver los puntos finales de VPC conectados a su red de servicio.
5. Seleccione el ID de punto final del punto final de la VPC para abrir su página de detalles. A continuación, modifique o elimine la asociación de puntos finales de la VPC.

Para crear una nueva asociación de puntos de conexión de VPC mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Endpoints.
3. Elija Crear puntos de conexión.
4. En Tipo, elija Redes de servicio.
5. Seleccione la red de servicio que desee conectar a la VPC.
6. Seleccione la VPC, las subredes y los grupos de seguridad.
7. (Opcional) Para agregar una etiqueta, expanda Etiquetas de asociación de VPC, elija Agregar etiqueta nueva e ingrese una clave y un valor de etiqueta.
8. Elija Crear punto de conexión.

Para obtener más información sobre el punto final de la VPC y cómo conectarse a las redes de servicio, consulte Acceder a las redes de servicio en la guía del AWS PrivateLink usuario.

Edición de la configuración de acceso de una red de servicios de VPC Lattice

Los ajustes de acceso permiten configurar y administrar el acceso del cliente a una red de servicios. La configuración de acceso incluye el tipo de autenticación y las políticas de autenticación. Las

políticas de autenticación lo ayudan a autenticar y autorizar el tráfico que fluye a los servicios de VPC Lattice. La configuración de acceso de la red de servicio no se aplica a las configuraciones de recursos asociadas a la red de servicio.

Puede aplicar políticas de autenticación a nivel de red de servicio, nivel de servicio o ambos. Por lo general, las políticas de autenticación las aplican los propietarios de la red o los administradores de la nube. Pueden implementar autorizaciones más específicas, por ejemplo, permitiendo llamadas autenticadas desde dentro de la organización o permitiendo solicitudes GET anónimas que cumplan una condición determinada. A nivel de servicio, los propietarios del servicio pueden aplicar controles detallados, que pueden ser más restrictivos. Para obtener más información, consulte Controle el acceso a los servicios de VPC Lattice mediante políticas de autenticación.

Para añadir o actualizar políticas de acceso mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Redes de servicios.
3. Seleccione el nombre del servicio para abrir su página de detalles.
4. Elija la pestaña Acceso para comprobar las configuraciones de acceso actuales.
5. Para actualizar la configuración de acceso, elija Editar la configuración de acceso.
6. Si desea que los clientes de la red asociada accedan VPCs a los servicios de esta red de servicios, elija Ninguno como tipo de autenticación.
7. Para aplicar una política de recursos a la red de servicios, elija AWS IAM como tipo de autenticación y siga uno de los siguientes pasos para la política de autenticación:
   - Escriba una política en el campo de entrada. Para ver políticas de ejemplo que puede copiar y pegar, elija Ejemplos de políticas.
   - Elija Aplicar la plantilla de política y seleccione la plantilla Permitir el acceso autenticado y no autenticado. Esta plantilla permite a un cliente de otra cuenta acceder al servicio ya sea firmando la solicitud (es decir, autenticada) o de forma anónima (es decir, no autenticada).
   - Elija Aplicar la plantilla de política y seleccione la plantilla Permitir solo el acceso autenticado. Esta plantilla permite a un cliente de otra cuenta acceder al servicio solo firmando la solicitud (es decir, autenticada).
8. Seleccione Save changes (Guardar cambios).

Para añadir o actualizar una política de acceso mediante el AWS CLI

Utilice el comando put-auth-policy.

Edición de los detalles de supervisión de una red de servicios de VPC Lattice

VPC Lattice genera métricas y registros para cada solicitud y respuesta, lo que hace que sea más eficiente monitorear y solucionar problemas de las aplicaciones.

Puede habilitar los registros de acceso y especificar el recurso de destino para sus registros. VPC Lattice puede enviar registros a los siguientes recursos: grupos de CloudWatch registros, flujos de entrega de Firehose y depósitos de S3.

Cómo habilitar los registros de acceso o actualizar el destino de un registro mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Redes de servicios.
3. Seleccione el nombre del servicio para abrir su página de detalles.
4. Elija la pestaña Monitorización. Compruebe los registros de acceso para ver si los registros de acceso están habilitados.
5. Para activar o desactivar los registros de acceso, elija Editar registros de acceso y, a continuación, active o desactive el conmutador Registros de acceso.
6. Al habilitar los registros de acceso, debe seleccionar el tipo de destino de entrega y, a continuación, crear o elegir el destino de los registros de acceso. También puede cambiar el destino de entrega en cualquier momento. Por ejemplo:
   - Seleccione un grupo de CloudWatch registros y elija un grupo de registros. CloudWatch Para crear un grupo de registros, elija Crear un grupo de registros en CloudWatch.
   - Seleccione Bucket de S3 e introduzca la ruta del bucket de S3, incluido cualquier prefijo. Para buscar sus buckets de S3, elija Explorar S3.
   - Seleccione Flujo de entrega de Kinesis Data Firehose y elija un flujo de entrega. Para crear un flujo de entrega, elija Crear un flujo de entrega en Kinesis.
7. Seleccione Save changes (Guardar cambios).

Para habilitar los registros de acceso mediante el AWS CLI

Utilice el comando create-access-log-subscription.

Para actualizar el destino del registro mediante el AWS CLI

Utilice el comando update-access-log-subscription.

Para deshabilitar los registros de acceso mediante el AWS CLI

Utilice el comando delete-access-log-subscription.

Gestione las etiquetas de una red de servicios de VPC Lattice

Las etiquetas lo ayudan a clasificar su red de servicios de diferentes maneras, por ejemplo, según su finalidad, propietario o entorno.

Puede agregar varias etiquetas a cada red de servicio. Las claves de las etiquetas deben ser únicas para cada red de servicios. Si agrega una etiqueta con una clave que ya está asociada a la red de servicios, se actualiza el valor de esa etiqueta. Puede utilizar caracteres como letras, espacios, números (en UTF-8) y los siguientes caracteres especiales: + - =. _ : / @. No utilice espacios iniciales ni finales. Los valores de la etiqueta distinguen entre mayúsculas y minúsculas.

Cómo añadir o eliminar etiquetas a través de la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Redes de servicios.
3. Seleccione el nombre del servicio para abrir su página de detalles.
4. Elija la pestaña Etiquetas.
5. Para agregar una etiqueta, elija Agregar etiquetas e ingrese la clave y el valor de la etiqueta. Para agregar otra etiqueta, elija Agregar nueva etiqueta. Cuando haya terminado de añadir etiquetas, elija Guardar cambios.
6. Para eliminar una etiqueta, active la casilla de verificación de la etiqueta y elija Eliminar. Cuando le pidan confirmación, escriba **`confirm`** y elija Eliminar.

Para añadir o eliminar etiquetas mediante el AWS CLI

Utilice los comandos tag-resource y untag-resource.

Eliminar una red de servicios de VPC Lattice

Antes de poder eliminar una red de servicio, primero debe eliminar todas las asociaciones que la red de servicio pueda tener con cualquier servicio, configuración de recursos, VPC o punto final de VPC.

Al eliminar una red de servicios, también eliminamos todos los recursos relacionados con la red de servicios, como la política de recursos, la política de autenticación y las suscripciones al registro de acceso.

Cómo eliminar una red de servicios a través de la consola

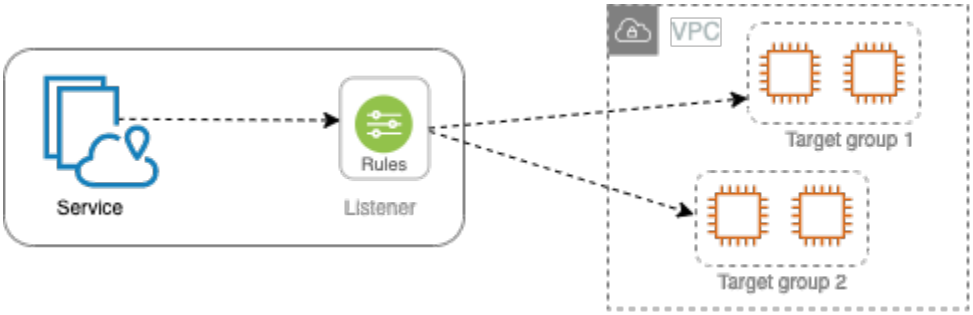
1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Redes de servicios.
3. Seleccione la casilla de verificación para la red de servicios y, a continuación, elija Acciones, Eliminar red de servicios.
4. Cuando se le pida confirmación, ingrese **`confirm`** y elija Delete (Eliminar).

Para eliminar una red de servicios mediante el AWS CLI

Utilice el comando delete-service-network.

Servicios en VPC Lattice

Un servicio en VPC Lattice es una unidad de software que se puede implementar de forma independiente y que ofrece una tarea o función específica. Un servicio puede ejecutarse en instancias, contenedores o funciones sin servidor dentro de una cuenta o nube privada virtual (VPC). Un servicio tiene un oyente que utiliza reglas, denominadas reglas del oyente, que usted puede configurar para ayudar a dirigir el tráfico a sus destinos. Los tipos de destino compatibles incluyen EC2 instancias, direcciones IP, funciones Lambda, balanceadores de carga de aplicaciones, tareas de Amazon ECS y pods de Kubernetes. Para obtener más información, consulte Grupos de destino en VPC Lattice. Puede asociar un servicio a varias redes de servicios. En el siguiente diagrama se muestran los componentes principales de un servicio típico de VPC Lattice.



Puede crear un servicio dándole un nombre y una descripción. Sin embargo, para controlar y monitorear el tráfico a su servicio, es importante que incluya la configuración de acceso y los detalles de supervisión. Para enviar el tráfico desde su servicio a sus destinos, debe configurar un oyente y las reglas. Para permitir que el tráfico fluya de la red de servicios a su servicio, debe asociar su servicio a la red de servicios.

Hay un tiempo de inactividad y un tiempo de espera de la conexión general para las conexiones a los destinos. El tiempo de espera de conexión inactiva es de 1 minuto, después del cual cerramos la conexión. La duración máxima es de 10 minutos, después de los cuales no permitimos nuevas transmisiones a través de la conexión y comenzamos el proceso de cierre de las transmisiones existentes.

Tareas

- Paso 1: crear un servicio de VPC Lattice
- Paso 2: definir el enrutamiento
- Paso 3: crear asociaciones de red
- Paso 4: Revisar y crear

- Gestión de asociaciones para un servicio de VPC Lattice
- Edición de la configuración de acceso de un servicio de VPC Lattice
- Edición de detalles de monitoreo de un servicio de VPC Lattice
- Administración de etiquetas de un servicio de VPC Lattice
- Configure un nombre de dominio personalizado para su servicio VPC Lattice
- Traiga su propio certificado (BYOC) para VPC Lattice
- Eliminar un servicio de VPC Lattice

Paso 1: crear un servicio de VPC Lattice

Cree un servicio básico de VPC Lattice con la configuración de acceso y los detalles de monitoreo. Sin embargo, el servicio no es del todo funcional hasta que defina su configuración de enrutamiento y lo asocie a una red de servicios.

Creación de un servicio básico mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Servicios.
3. Elija Crear servicio.
4. Para los identificadores, haga lo siguiente:

   a. Escriba un nombre para el servicio. El nombre debe tener entre 3 y 63 caracteres y usar letras en minúsculas, números y guiones. Debe comenzar y terminar con un número o una letra. No utilice guiones dobles.

   b. (Opcional) Escriba una descripción para la red de servicios. Puede establecer o cambiar la descripción durante o después de la creación. La descripción puede tener hasta 256 caracteres.
5. Para especificar un nombre de dominio personalizado para su servicio, seleccione Especificar una configuración de dominio personalizada e introduzca el nombre de dominio personalizado.

   Para los oyentes de HTTPS, puede seleccionar el certificado que utilizará VPC Lattice para realizar la terminación de TLS. Si no selecciona un certificado ahora, puede seleccionarlo al crear un agente de escucha HTTPS para el servicio.

En el caso de los agentes de escucha TCP, debe especificar un nombre de dominio personalizado para su servicio. Si especifica un certificado, no se utilizará. En su lugar, realiza la terminación de TLS en su aplicación.

6. Para el acceso al servicio, seleccione Ninguno si desea que los clientes de la red VPCs asociada a la red de servicio accedan a su servicio. Para aplicar una política de autenticación para controlar el acceso al servicio, elija AWS IAM. Para aplicar una política de recursos al servicio, realice una de las siguientes acciones para la política de autenticación:
   - Escriba una política en el campo de entrada. Para ver políticas de ejemplo que puede copiar y pegar, elija Ejemplos de políticas.
   - Elija Aplicar la plantilla de política y seleccione la plantilla Permitir el acceso autenticado y no autenticado. Esta plantilla permite a un cliente de otra cuenta acceder al servicio ya sea firmando la solicitud (es decir, autenticada) o de forma anónima (es decir, no autenticada).
   - Elija Aplicar la plantilla de política y seleccione la plantilla Permitir solo el acceso autenticado. Esta plantilla permite a un cliente de otra cuenta acceder al servicio solo firmando la solicitud (es decir, autenticada).
7. (Opcional) Para habilitar los registros de acceso, active el conmutador de registros de acceso y especifique un destino para los registros de acceso de la siguiente manera:
   - Seleccione Grupo de CloudWatch registros y elija un grupo de CloudWatch registros. Para crear un grupo de registros, elija Crear un grupo de registros en CloudWatch.
   - Seleccione Bucket de S3 e introduzca la ruta del bucket de S3, incluido cualquier prefijo. Para buscar sus buckets de S3, elija Explorar S3.
   - Seleccione Flujo de entrega de Kinesis Data Firehose y elija un flujo de entrega. Para crear un flujo de entrega, elija Crear un flujo de entrega en Kinesis.
8. (Opcional) Para compartir tu servicio con otras cuentas, selecciona un AWS RAM recurso compartido de entre Recursos compartidos. Para crear un recurso compartido, elija Crear un recurso compartido en la consola RAM.
9. Para revisar la configuración y crear el servicio, elija Omitir para revisar y crear. De lo contrario, elija Siguiente para definir la configuración de enrutamiento de su servicio.

Paso 2: definir el enrutamiento

Defina la configuración de enrutamiento mediante oyentes para que su servicio pueda enviar tráfico a los destinos que usted especifique.

Requisito previo

Para poder agregar un oyente, debe crear un grupo de destino de VPC Lattice. Para obtener más información, consulte the section called “Creación de un grupo de destino.”.

Cómo definir el enrutamiento de su servicio utilizando la consola

1. Elija Añadir oyente.
2. Para el nombre del oyente, puede proporcionar un nombre de oyente personalizado o utilizar el protocolo y el puerto del oyente como nombre del oyente. El nombre personalizado que especifique puede tener hasta 63 caracteres y debe ser único para cada servicio de su cuenta. Los caracteres válidos son a-z, 0-9 y guiones (-). No puede usar un guion como primer o último carácter, ni inmediatamente después de otro guion. No puede cambiar el nombre de un oyente después de crearlo.
3. Elija un protocolo y, a continuación, introduzca un número de puerto.
4. En Acción predeterminada, elija el grupo de destino de VPC Lattice que recibirá el tráfico y elija el peso que desee asignar a este grupo de destino. Si lo desea, puede añadir otro grupo de destino para la acción predeterminada. Elija Añadir acción y, a continuación, elija otro grupo de destino y especifique su peso.
5. (Opcional) Para añadir otra regla, elija Añadir regla y, luego, introduzca un nombre, una prioridad, una condición y una acción para la regla.

   Puede asignar a cada regla un número de prioridad entre 1 y 100. Un oyente no puede tener varias reglas con la misma prioridad. Las reglas se evalúan por orden de prioridad, desde el valor más bajo hasta el valor más alto. La regla predeterminada se evalúa en último lugar.

   En Condición, introduzca un patrón de ruta para la condición de coincidencia de ruta. El tamaño máximo de cada cadena es de 200 caracteres. La comparación no distingue entre mayúsculas y minúsculas.
6. (Opcional) Para agregar etiquetas, expanda Etiquetas del oyente, elija Agregar etiqueta nueva e ingrese una clave y un valor de etiqueta.
7. Para revisar la configuración y crear el servicio, elija Omitir para revisar y crear. De lo contrario, elija Siguiente para asociar el servicio a una red de servicios.

Paso 3: crear asociaciones de red

Asocie su servicio a una red de servicios para que los clientes puedan comunicarse con ella.

Cómo asociar un servicio a una red de servicios mediante la consola

1. Para las redes de servicios de VPC Lattice, seleccione la red de servicios. Para crear una red de servicios, elija Crear una red de VPC Lattice. Puede asociar un servicio a varias redes de servicios.
2. (Opcional) Para agregar una etiqueta, expanda Etiquetas de asociación de red de servicios, elija Agregar etiqueta nueva e ingrese una clave y un valor de etiqueta.
3. Elija Siguiente.

Paso 4: Revisar y crear

Cómo revisar la configuración y crear el servicio mediante la consola

1. Revise la configuración de su servicio.
2. Elija Editar si necesita modificar alguna parte de la configuración del servicio.
3. Cuando haya terminado de revisar o editar la configuración, elija Crear servicio de VPC Lattice.
4. Si especificó un nombre de dominio personalizado para el servicio, debe configurar el enrutamiento de DNS una vez creado el servicio. Para obtener más información, consulte the section called “Configuración de un nombre de dominio personalizado”.

Gestión de asociaciones para un servicio de VPC Lattice

Al asociar un servicio a la red de servicios, los clientes (recursos de una VPC asociada a la red de servicios) pueden realizar solicitudes a este servicio. Puede asociar los servicios que están en su cuenta o los servicios que se comparten con usted desde diferentes cuentas. Este paso es opcional al crear el servicio. Sin embargo, después de la creación, el servicio no podrá comunicarse con otros servicios hasta que lo asocie a una red de servicios. Los propietarios de los servicios pueden asociar sus servicios a la red de servicios si su cuenta tiene el acceso necesario. Para obtener más información, consulte Cómo funciona VPC Lattice.

Gestión de asociaciones a una red de servicios mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Servicios.
3. Seleccione el nombre del servicio para abrir la página de detalles.

4. Elija la pestaña Asociaciones de redes de servicios.
5. Para crear una asociación, realice lo siguiente:
   a. Elija Crear asociaciones.
   b. Seleccione una red de servicios en Red de servicios de VPC Lattice. Para crear una red de servicios, elija Crear una red de VPC Lattice.
   c. (Opcional) Para agregar una etiqueta, expanda Etiquetas de asociación de servicios, elija Agregar etiqueta nueva e ingrese una clave y un valor de etiqueta.
   d. Elija Guardar cambios.
6. Para eliminar una asociación, seleccione la casilla de verificación de la asociación y, luego, elija Acciones, Eliminar asociaciones de red. Cuando se le pida confirmación, ingrese **`confirm`** y elija Eliminar.

Para crear una asociación de red de servicios mediante el AWS CLI

Utilice el comando create-service-network-service-association.

Para eliminar una asociación de red de servicios mediante el AWS CLI

Utilice el comando delete-service-network-service-association.

Edición de la configuración de acceso de un servicio de VPC Lattice

La configuración de acceso le permite configurar y administrar el acceso de los clientes a un servicio. La configuración de acceso incluye el tipo de autenticación y las políticas de autenticación. Las políticas de autenticación lo ayudan a autenticar y autorizar el tráfico que fluye a los servicios de VPC Lattice.

Puede aplicar políticas de autenticación a nivel de red de servicio, nivel de servicio o ambos. A nivel de servicio, los propietarios del servicio pueden aplicar controles detallados, que pueden ser más restrictivos. Por lo general, las políticas de autenticación las aplican los propietarios de la red o los administradores de la nube. Pueden implementar una autorización específica, por ejemplo, que permita realizar llamadas autenticadas desde dentro de la organización o permitir solicitudes GET anónimas que cumplan una condición determinada. Para obtener más información, consulte Controle el acceso a los servicios de VPC Lattice mediante políticas de autenticación.

Para añadir o actualizar políticas de acceso mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Servicios.
3. Seleccione el nombre del servicio para abrir la página de detalles.
4. Elija la pestaña Acceso para comprobar la configuración de acceso actual.
5. Para actualizar la configuración de acceso, elija Editar la configuración de acceso.
6. Si desea que los clientes de la red VPCs de servicios asociada accedan a su servicio, elija Ninguno como tipo de autenticación.
7. Para aplicar una política de recursos para controlar el acceso al servicio, elija AWS IAM como tipo de autenticación y siga uno de estos procedimientos para la política de autenticación:
   - Escriba una política en el campo de entrada. Para ver políticas de ejemplo que puede copiar y pegar, elija Ejemplos de políticas.
   - Elija Aplicar la plantilla de política y seleccione la plantilla Permitir el acceso autenticado y no autenticado. Esta plantilla permite a un cliente de otra cuenta acceder al servicio ya sea firmando la solicitud (es decir, autenticada) o de forma anónima (es decir, no autenticada).
   - Elija Aplicar la plantilla de política y seleccione la plantilla Permitir solo el acceso autenticado. Esta plantilla permite a un cliente de otra cuenta acceder al servicio solo firmando la solicitud (es decir, autenticada).
8. Seleccione Save changes (Guardar cambios).

Para añadir o actualizar una política de acceso mediante el AWS CLI

Utilice el comando put-auth-policy.

Edición de detalles de monitoreo de un servicio de VPC Lattice

VPC Lattice genera métricas y registros para cada solicitud y respuesta, lo que hace que sea más eficiente monitorear y solucionar problemas de las aplicaciones.

Puede habilitar los registros de acceso y especificar el recurso de destino para sus registros. VPC Lattice puede enviar registros a los siguientes recursos: grupos de CloudWatch registros, flujos de entrega de Firehose y depósitos de S3.

Cómo habilitar los registros de acceso o actualizar el destino de un registro mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Servicios.
3. Seleccione el nombre del servicio para abrir la página de detalles.
4. Elija la pestaña Monitoreo y, a continuación, seleccione Registros. Compruebe los registros de acceso para ver si los registros de acceso están habilitados.
5. Para activar o desactivar los registros de acceso, elija Editar registros de acceso y, a continuación, active o desactive el conmutador Registros de acceso.
6. Al habilitar los registros de acceso, debe seleccionar el tipo de destino de entrega y, a continuación, crear o elegir el destino de los registros de acceso. También puede cambiar el destino de entrega en cualquier momento. Por ejemplo:
   - Seleccione un grupo de CloudWatch registros y elija un grupo de registros. CloudWatch Para crear un grupo de registros, elija Crear un grupo de registros en CloudWatch.
   - Seleccione Bucket de S3 e introduzca la ruta del bucket de S3, incluido cualquier prefijo. Para buscar sus buckets de S3, elija Explorar S3.
   - Seleccione Flujo de entrega de Kinesis Data Firehose y elija un flujo de entrega. Para crear un flujo de entrega, elija Crear un flujo de entrega en Kinesis.
7. Seleccione Save changes (Guardar cambios).

Para habilitar los registros de acceso mediante el AWS CLI

Utilice el comando create-access-log-subscription.

Para actualizar el destino del registro mediante el AWS CLI

Utilice el comando update-access-log-subscription.

Para deshabilitar los registros de acceso mediante el AWS CLI

Utilice el comando delete-access-log-subscription.

Administración de etiquetas de un servicio de VPC Lattice

Las etiquetas lo ayudan a clasificar su servicio de diferentes maneras, por ejemplo, según su finalidad, propietario o entorno.

Puede añadir varias etiquetas a cada servicio. Las claves de etiquetas deben ser únicas para cada servicio. Si agregas una etiqueta con una clave que ya está asociada al servicio, se actualiza el valor de esa etiqueta. Puede utilizar caracteres como letras, espacios, números (en UTF-8) y los siguientes caracteres especiales: + - =. _ : / @. No utilice espacios iniciales ni finales. Los valores de la etiqueta distinguen entre mayúsculas y minúsculas.

Cómo añadir o eliminar etiquetas a través de la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Servicios.
3. Seleccione el nombre del servicio para abrir la página de detalles.
4. Elija la pestaña Etiquetas.
5. Para agregar una etiqueta, elija Agregar etiquetas e ingrese la clave y el valor de la etiqueta. Para agregar otra etiqueta, elija Agregar nueva etiqueta. Cuando haya terminado de añadir etiquetas, elija Guardar cambios.
6. Para eliminar una etiqueta, active la casilla de verificación de la etiqueta y elija Eliminar. Cuando le pidan confirmación, escriba **`confirm`** y elija Eliminar.

Para añadir o eliminar etiquetas mediante el AWS CLI

Utilice los comandos tag-resource y untag-resource.

Configure un nombre de dominio personalizado para su servicio VPC Lattice

Al crear un servicio nuevo, VPC Lattice genera un nombre de dominio completo (FQDN) único para el servicio con la siguiente sintaxis.

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

Sin embargo, los nombres de dominio que proporciona VPC Lattice no son fáciles de recordar para sus usuarios. Los nombres de dominio personalizados son más simples e intuitivos URLs y puede proporcionarlos a sus usuarios. Si prefiere usar un nombre de dominio personalizado para su servicio, por ejemplo, `www.parking.example.com` en lugar del nombre del DNS generado por VPC Lattice, puede configurarlo al crear un servicio de VPC Lattice. Cuando un cliente realiza una

solicitud utilizando su nombre de dominio personalizado, el servidor del DNS lo resuelve para hallar el nombre de dominio generado por VPC Lattice.

Requisitos previos

- Debe tener un nombre de dominio registrado para su servicio. Si aún no tiene un nombre de dominio registrado, puede registrar uno a través de Amazon Route 53 o cualquier otro registrador comercial.
- Para recibir solicitudes HTTPS, debe proporcionar su propio certificado en AWS Certificate Manager. VPC Lattice no admite un certificado predeterminado como alternativa. Por lo tanto, si no proporciona un SSL/TLS certificado correspondiente a su nombre de dominio personalizado, fallarán todas las conexiones HTTPS a su nombre de dominio personalizado. Para obtener más información, consulte Traiga su propio certificado (BYOC) para VPC Lattice.

Limitaciones y consideraciones

- No puede tener más de un nombre de dominio personalizado para un servicio.
- No puede modificar el nombre de dominio personalizado después de crear el servicio.
- El nombre de dominio personalizado debe ser único en una red de servicios. Esto significa que no se puede crear un servicio con un nombre de dominio personalizado que ya exista (para otro servicio) en la misma red de servicios.

El siguiente procedimiento muestra cómo configurar un nombre de dominio personalizado para tu servicio.

AWS Management Console

Para configurar un nombre de dominio personalizado para su servicio

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Servicio.
3. Elija Crear servicio. Acceda al Paso 1: crear un servicio.
4. En la sección Configuración de dominio personalizado, elija Especificar una configuración de dominio personalizado.
5. Introduzca su nombre de dominio personalizado.

6. Para atender las solicitudes HTTPS, seleccione el SSL/TLS certificado que coincida con su nombre de dominio personalizado en SSL/TLS Certificado personalizado. Si aún no tiene un certificado o no quiere añadir uno ahora, puede añadir uno al crear su oyente HTTPS. Sin embargo, sin un certificado, su nombre de dominio personalizado no podrá atender las solicitudes HTTPS. Para obtener más información, consulte Adición de un oyente HTTPS.
7. Cuando haya terminado de añadir el resto de la información para crear el servicio, elija Crear.

AWS CLI

Para configurar un nombre de dominio personalizado para tu servicio

Utilice el comando 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
```

En el comando anterior, para `--name`, introduzca un nombre para el servicio. Para `--custom-domain-name`, introduzca el nombre de dominio de su servicio, como `parking.example.com`. Para `--certificate-arn`, introduzca el ARN de su certificado en ACM. El ARN del certificado está disponible en su cuenta en AWS Certificate Manager.

Asocie un nombre de dominio personalizado a su servicio

En primer lugar, si aún no lo ha hecho, registre su nombre de dominio personalizado. La Internet Corporation for Assigned Names and Numbers (ICANN, Corporación de Internet para la Asignación de Nombres y Números) administra los nombres de dominios de Internet. Los nombres de dominios se registran mediante un registrador de nombres de dominio, una organización acreditada por la ICANN que administra el registro de los nombres de dominios. En el sitio web de su registrador, se detallarán las instrucciones y la información sobre los precios del registro del nombre de dominio. Para obtener más información, consulte los siguientes recursos:

- Para registrar el nombre de un dominio mediante Amazon Route 53, consulte Registro de nombres de dominio mediante Route 53 en la Guía para desarrolladores de Amazon Route 53.
- Para obtener una lista de registradores acreditados, consulte el Accredited Registrar Directory.

A continuación, usa tu servicio de DNS, como el registrador de dominios, para crear un registro que dirija las consultas a tu servicio. Para obtener más información, consulte la documentación de su servicio de DNS. También puede usar Route 53 como su servicio DNS.

Si usas Route 53, puedes usar un registro de alias o un registro CNAME para enrutar las consultas a tu servicio. Le recomendamos que utilice un registro de alias, ya que puede crear un registro de alias en el nodo superior de un espacio de nombres DNS, también conocido como vértice de zona.

Si utiliza Route 53, primero debe crear una zona alojada, que contiene información sobre cómo dirigir el tráfico en Internet para el dominio. Después de crear la zona alojada pública o privada, cree un registro de modo que su nombre de dominio personalizado, por ejemplo`parking.example.com`, se asigne al nombre de dominio generado automáticamente por VPC Lattice, por ejemplo,. `my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws` Sin esta asignación, el nombre de dominio personalizado no funcionará en VPC Lattice.

Los siguientes procedimientos muestran cómo crear una zona alojada pública o privada mediante Route 53

AWS Management Console

Para crear un registro de alias que dirija las consultas a su servicio mediante Route 53, consulte Enrutamiento del tráfico al punto final del dominio del servicio Amazon VPC Lattice.

Utilice el nombre de dominio generado por VPC Lattice para su servicio, por ejemplo, para Value**`my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws`**. Puedes encontrar este nombre de dominio generado automáticamente en la consola de VPC Lattice, en tu página de servicio.

AWS CLI

Para crear un registro de alias en tu zona alojada

1. Obtenga el nombre de dominio generado por VPC Lattice para su servicio (por ejemplo, `my-service-02031c045478f6ddf1.7d67968.vpc-lattice-svcs.us-west-2.on.aws`) y el ID de la zona alojada ejecutando el comando `get-service`.
2. Para establecer el alias, utilice el siguiente comando.

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

Para el archivo `change-set.json`, cree un archivo JSON con el contenido del siguiente ejemplo de JSON y guárdelo en su máquina local. Sustituya *`file://~/Desktop/change-set.json`* el comando anterior por la ruta del archivo JSON guardado en su máquina local. Tenga en cuenta que el término “Tipo” en el siguiente JSON puede ser un tipo de registro A o 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
                }
            }
        }
    ]
}
```

Traiga su propio certificado (BYOC) para VPC Lattice

Para atender las solicitudes HTTPS, debes tener tu propio SSL/TLS certificado listo AWS Certificate Manager (ACM) antes de configurar un nombre de dominio personalizado. Estos certificados deben tener un nombre alternativo del sujeto (SAN) o un nombre común (CN) que coincida con el nombre de dominio personalizado de su servicio. Si el SAN está presente, comprobamos si solo hay una coincidencia en la lista de SAN. Si el SAN está ausente, comprobamos si hay alguna coincidencia en el CN.

VPC Lattice atiende las solicitudes HTTPS mediante el uso de la indicación de nombre de servidor (SNI). El DNS enruta la solicitud HTTPS a su servicio de VPC Lattice en función del nombre de dominio personalizado y el certificado que coincide con este nombre de dominio. Para solicitar un SSL/TLS certificado para un nombre de dominio en ACM o importar uno a ACM, consulte Emisión y administración de certificados e importación de certificados en la Guía del AWS Certificate Manager

usuario. Si no puede solicitar o importar su propio certificado en ACM, utilice el nombre de dominio y el certificado generados por VPC Lattice.

VPC Lattice solo acepta un certificado personalizado por servicio. Sin embargo, puede usar un certificado personalizado para varios dominios personalizados. Esto significa que puede usar el mismo certificado para todos los servicios de VPC Lattice que cree con un nombre de dominio personalizado.

Para ver su certificado mediante la consola ACM, abra Certificados y seleccione el ID de su certificado. Debería ver el servicio de VPC Lattice que está asociado a ese certificado en Recurso asociado.

Limitaciones y consideraciones

- VPC Lattice permite coincidencias con caracteres comodín que estén a un nivel de profundidad en el nombre alternativo del sujeto (SAN) o el nombre común (CN) del certificado asociado. Por ejemplo, si crea un servicio con el nombre de dominio personalizado `parking.example.com` y asocia su propio certificado al SAN `*.example.com`. Cuando se recibe una solicitud para `parking.example.com`, VPC Lattice hace coincidir el SAN con cualquier nombre de dominio con el dominio apex `example.com`. Sin embargo, si tiene el dominio personalizado `parking.different.example.com` y su certificado tiene el SAN `*.example.com`, la solicitud fallará.
- VPC Lattice admite un nivel de coincidencia de dominios comodín. Esto significa que un comodín solo se puede usar como subdominio de primer nivel y que solo protege un nivel de subdominio. Por ejemplo, si el SAN de su certificado es `*.example.com`, entonces `parking.*.example.com` no es compatible.
- VPC Lattice admite un comodín por nombre de dominio. Esto significa que `*.*.example.com` no es válido. Para obtener más información, consulte Solicitud de un certificado público en la Guía del usuario de AWS Certificate Manager .
- VPC Lattice solo admite certificados con claves RSA de 2048 bits.
- El SSL/TLS certificado de ACM debe estar en la misma región que el servicio VPC Lattice al que lo está asociando.

Protección de la clave privada de su certificado

Cuando solicita un SSL/TLS certificado mediante ACM, ACM genera un public/private key pair. Cuando importa un certificado, es usted quien genera el par de claves. La clave pública pasa a

formar parte del certificado. Para almacenar la clave privada de forma segura, ACM crea otra clave AWS KMS, denominada clave KMS, con el alias aws/acm. AWS KMS utiliza esta clave para cifrar la clave privada del certificado. Para obtener más información, consulte Protección de datos en AWS Certificate Manager en la Guía del usuario de AWS Certificate Manager .

VPC Lattice usa AWS TLS Connection Manager, un servicio al que solo pueden acceder Servicios de AWS, para proteger y usar las claves privadas de su certificado. Cuando usa su certificado ACM para crear un servicio de VPC Lattice, VPC Lattice asocia su certificado con TLS Connection Manager. AWS Para ello, creamos una concesión en función de su clave gestionada. AWS KMS AWS Esta concesión permite que TLS Connection Manager lo utilice AWS KMS para descifrar la clave privada de su certificado. TLS Connection Manager utiliza el certificado y la clave privada descifrada (texto sin formato) para establecer una conexión segura (sesión SSL/TLS) con los clientes de los servicios de VPC Lattice. Cuando el certificado se desvincula de un servicio de VPC Lattice, la concesión se retira. Para obtener más información, consulte Concesiones en la Guía para desarrolladores de AWS Key Management Service .

Para obtener más información, consulte Cifrado en reposo.

Eliminar un servicio de VPC Lattice

Para eliminar un servicio de VPC Lattice, primero debe eliminar todas las asociaciones que el servicio pueda tener con cualquier red de servicios. Si elimina un servicio, también se eliminan todos los recursos relacionados con el servicio, como la política de recursos, la política de autenticación, los oyentes, las reglas de los oyentes y las suscripciones al registro de acceso.

Cómo eliminar un servicio utilizando la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Servicio.
3. En la página Servicios, seleccione el servicio que desea eliminar y, a continuación, elija Acciones, Eliminar servicio.
4. Cuando se le pida confirmación, elija Eliminar.

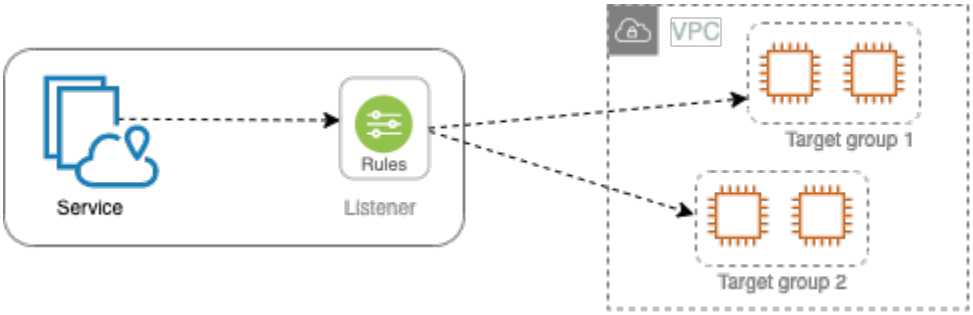
Para eliminar un servicio mediante el AWS CLI

Utilice el comando delete-service.

Grupos de destino en VPC Lattice

Un grupo de destino de VPC Lattice es un conjunto de destinos, o recursos de cómputo, que ejecutan su aplicación o servicio. Los tipos de destino compatibles incluyen EC2 instancias, direcciones IP, funciones de Lambda, equilibradores de carga de aplicación, tareas de Amazon ECS y pods de Kubernetes. También puede asociar los servicios existentes a sus grupos de destino. Para obtener más información sobre el uso de Kubernetes con VPC Lattice, consulte la Guía del usuario del controlador de AWS Gateway API.

Cada grupo de destino se utiliza para direccionar solicitudes a uno o varios destinos registrados. Cuando crea la regla del oyente, especifica un grupo de destino y condiciones. Cuando se cumple la condición de una regla, el tráfico se reenvía al grupo de destino correspondiente. Puede crear grupos de destino diferentes para los distintos tipos de solicitudes. Por ejemplo, cree un grupo de destino para las solicitudes generales y otros grupos de destino para las solicitudes que incluyan condiciones de regla específicas, como una ruta o un valor de encabezado.



Puede definir la configuración de comprobación de estado de su servicio para cada grupo de destino. Cada grupo de destino utiliza la configuración de comprobación de estado predeterminada, a menos que la anule al crear el grupo de destino o la modifique posteriormente. Después de especificar un grupo de destino en una regla para un oyente, el servicio monitoriza constantemente el estado de todos los destinos registrados en el grupo de destino. El servicio dirige las solicitudes a los destinos registrados que se encuentran en buen estado.

Para especificar un grupo de destino en una regla para un oyente de servicios, el grupo de destino debe estar en la misma cuenta que el servicio.

Los grupos de destino de VPC Lattice son similares a los grupos de destino proporcionados por Elastic Load Balancing, pero no son intercambiables.

Contenido

- Cómo registrar destinos con un grupo de destino de VPC Lattice
- Comprobaciones de estado de sus grupos de destino de VPC Lattice
- Configuración de enrutamiento
- Algoritmo de enrutamiento
- Tipo de destino
- Tipo de dirección IP
- Destinos HTTP en VPC Lattice
- Funciones de Lambda como destinos en VPC Lattice
- Equilibradores de carga de aplicación como destinos en VPC Lattice
- Versión del protocolo
- Etiquetas para su grupo de destino de VPC Lattice
- Para eliminar un grupo de destino de VPC Lattice

Creación de un grupo de destino de VPC Lattice

Los destinos se registran en un grupo de destino. De forma predeterminada, el servicio de VPC Lattice envía las solicitudes a los destinos registrados mediante el protocolo y el puerto que ha especificado para el grupo de destino. Puede anular este puerto al registrar cada destino en el grupo de destino.

Para dirigir el tráfico a los destinos de un grupo de destino, especifique el grupo de destino en una acción al crear un oyente o crear una regla para este último. Para obtener más información, consulte Reglas del oyente para su servicio de VPC Lattice. Puede especificar el mismo grupo de destino en varios oyentes, pero estos oyentes deben pertenecer al mismo servicio. Para usar un grupo de destino con un servicio, debe comprobar que ningún oyente utilice el grupo de destino para ningún otro servicio.

Puede agregar o eliminar destinos del grupo de destino en cualquier momento. Para obtener más información, consulte Cómo registrar destinos con un grupo de destino de VPC Lattice. También puede modificar la configuración de la comprobación de estado del grupo de destino. Para obtener más información, consulte Comprobaciones de estado de sus grupos de destino de VPC Lattice.

Creación de un grupo de destino.

Puede crear un grupo de destino y, si lo desea, registrar los destinos de la siguiente manera.

Para crear un grupo de destino desde la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Grupos de destino.
3. Elija Crear grupo de destino.
4. En Elegir un tipo de destino, seleccione una de las siguientes opciones:
   - Elija Instancias para registrar destinos por ID de instancia.
   - Elija Direcciones IP para registrar destinos por dirección IP.
   - Elija Función de Lambda para registrar una función de Lambda como destino.
   - Elija Equilibrador de carga de aplicación para registrar un equilibrador de carga de aplicación como destino.
5. En Nombre del grupo de destino, escriba el nombre del grupo de destino. Este nombre debe ser único para su cuenta en cada AWS región, puede tener un máximo de 32 caracteres, debe contener únicamente caracteres alfanuméricos o guiones y no puede comenzar ni terminar con un guion.
6. (Opcional) En Protocolo y Puerto, puede modificar los valores predeterminados según sea necesario. El protocolo predeterminado es HTTPS y el puerto predeterminado es 443.

   Si el tipo de destino es Función de Lambda, no puede especificar un protocolo o un puerto.
7. Para el tipo de dirección IP, elija IPv4registrar los destinos con IPv4 direcciones o registrar los destinos con direcciones. IPv6 IPv6 No puede cambiar esta configuración una vez que se creó el grupo de destino.

   Esta opción solo está disponible si el tipo de destino son direcciones IP.
8. En VPC, seleccione una nube privada virtual (VPC).

   Esta opción no está disponible si el tipo de destino es Función de Lambda.
9. En Versión del protocolo, modifique el valor predeterminado según sea necesario. El valor predeterminado es HTTP1.

   Esta opción no está disponible si el tipo de destino es Función de Lambda.
10. En Comprobaciones de estado, modifique la configuración predeterminada según sea necesario. Para obtener más información, consulte Comprobaciones de estado de sus grupos de destino de VPC Lattice.

    Las comprobaciones de estado no están disponibles si el tipo de destino es Función de Lambda.

11. En Versión de estructura de eventos de Lambda, elija una versión. Para obtener más información, consulte the section called “Recepción de eventos del servicio de VPC Lattice”.

    Esta opción solo está disponible si el tipo de destino es la función de Lambda

12. (Opcional) Para agregar etiquetas, expanda Etiquetas, elija Agregar nueva etiqueta e ingrese la clave y el valor de la etiqueta.
13. Elija Siguiente.
14. En el caso de Registrar destinos, puede omitir este paso o añadir destinos de la siguiente manera:
    - Si el tipo de destino es Instancias, seleccione las instancias, introduzca los puertos y, a continuación, elija Incluir como pendiente debajo.
    - Si el tipo de destino es Direcciones IP, haga lo siguiente:
        a. En Elegir una red, conserve la VPC que seleccionó para el grupo de destino o elija Otra dirección IP privada.
        b. En Especificar IPs y definir puerto, introduzca la dirección IP e introduzca los puertos. El puerto predeterminado es el puerto de grupo de destino.
        c. Elija Incluir como pendiente debajo.
    - Si el tipo de destino es una función de Lambda, elija una función de Lambda. Para crear una función de Lambda, elija Crear una nueva función de Lambda.
    - Si el tipo de destino es un Equilibrador de carga de aplicación, elija un equilibrador de carga de aplicación. Para crear un Equilibrador de carga de aplicación, elija Crear un equilibrador de carga de aplicación.
15. Elija Crear grupo de destino.

    VPC Lattice puede tardar unos minutos en registrar los destinos. Para obtener más información, consulte ¿Por qué mis cambios de DNS tardan tanto en propagarse en Route 53 y en los dispositivos de resolución públicos?

Creación de un grupo de destino desde la AWS CLI

Utilice el create-target-groupcomando para crear el grupo objetivo y el comando register-targets para añadir objetivos.

Subredes compartidas

Los participantes pueden crear grupos de destinos de VPC Lattice en una VPC compartida. Las siguientes reglas se aplican a las subredes compartidas:

- Todas las partes de un servicio de VPC Lattice, como los oyentes, los grupos de destino y los destinos, deben crearse con la misma cuenta. Se pueden crear en subredes que son propiedad del propietario del servicio de VPC Lattice o se pueden compartir con él.
- Los destinos registrados en un grupo de destino deben crearse con la misma cuenta que el grupo de destino.
- Solo el propietario de una VPC puede asociar la VPC a una red de servicios. Los recursos participantes de una VPC compartida que está asociada a una red de servicios pueden enviar solicitudes a los servicios que están asociados a la red de servicios. Sin embargo, el administrador puede evitarlo mediante grupos de seguridad ACLs, red o políticas de autenticación.

Para obtener más información acerca de los recursos compartibles de VPC Lattice, consulte Comparta entidades de VPC Lattice.

Cómo registrar destinos con un grupo de destino de VPC Lattice

Su servicio sirve como un único punto de contacto para los clientes y distribuye el tráfico entrante entre los destinos registrados en buen estado. Puede registrar cada destino en uno o varios grupos de destino.

Si aumenta la demanda en la aplicación, puede registrar destinos adicionales en uno o más grupos de destino para controlar la demanda. El servicio comienza a dirigir las solicitudes a un destino recién registrado tan pronto como se completa el proceso de registro y el destino supera las comprobaciones de estado iniciales.

Si la demanda de la aplicación se reduce o cuando es preciso realizar el mantenimiento de los destinos, puede anular el registro de los destinos en los grupos de destino. Al anular el registro de un destino, este se quita del grupo de destino, pero no se ve afectado de ningún otro modo. El servicio deja de dirigir solicitudes a un destino tan pronto como se anula su registro. El destino adquiere el estado `DRAINING` hasta que se completan las solicitudes en tránsito. Puede volver a registrar el destino en el grupo de destino cuando esté preparado para reanudar la recepción de solicitudes.

El tipo de destino de su grupo de destino determina cómo se registran los destinos en ese grupo de destino. Para obtener más información, consulte Tipo de destino.

Utilice los siguientes procedimientos de consola para registrar o anular el registro de los destinos. Como alternativa, utilice los comandos register-targets y deregister-targets de la AWS CLI.

Contenido

Registro o anulación del registro de destinos por ID de instancia

Las instancias de destino deben encontrarse en la nube privada virtual (VPC) que ha especificado para el grupo de destino. La instancia debe estar además en el estado `running` al registrarla.

Al registrar los destinos por ID de instancia, puede usar su servicio con un grupo de escalado automático. Después de asociar un grupo de destino a un grupo de escalado automático y cuando el grupo se escale horizontalmente, las instancias lanzadas por el grupo de escalado automático se registran automáticamente en el grupo de destino. Si separa el grupo de destino del grupo de escalado automático, automáticamente se anula el registro de las instancias en el grupo de destino. Para obtener más información, consulte Enrutar el tráfico a su grupo de escalado automático con un grupo de destino de VPC Lattice en la Guía del usuario de Amazon EC2 Auto Scaling.

Para registrar un destino o anular su registro mediante el ID de instancia desde la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Grupos de destino.
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. Elija la pestaña Destinos.
5. Para registrar instancias, elija Registrar destinos. Seleccione las instancias, introduzca el puerto de la instancia y, a continuación, elija Incluir como pendiente debajo. Cuando haya terminado de agregar instancias, elija Registrar destinos.
6. Para anular el registro de instancias, seleccione las instancias y, a continuación, elija Anular registro.

Registro o anulación del registro de destinos por dirección IP

Las direcciones IP de destino deben provenir de las subredes de la VPC que especificó para el grupo de destino. No puede registrar las direcciones IP de otro servicio en la misma VPC. No puede registrar puntos de conexión de VPC ni direcciones IP enrutables públicamente.

Para registrar un destino o anular su registro mediante la dirección IP desde la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Grupos de destino.
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. Elija la pestaña Destinos.
5. Para registrar direcciones IP, elija Registrar destinos. Para cada dirección IP, seleccione la red, introduzca la dirección IP y el puerto y elija Incluir como pendiente debajo. Cuando haya terminado de especificar direcciones, elija Registrar destinos.
6. Para anular el registro de direcciones IP, selecciónelas y, a continuación, elija Anular registro.

Registrar o anular el registro de una función de Lambda

Puede registrar una sola función de Lambda con el grupo de destino. Si ya no necesita enviar tráfico a la función de Lambda, puede anular su registro. Después de anular el registro de una función de Lambda, las solicitudes en tránsito producirán errores HTTP 5XX. Es mejor crear un nuevo grupo de destino en lugar de sustituir la función de Lambda para un grupo de destino.

Cómo registrar o anular el registro de una función de Lambda mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Grupos de destino.
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. Elija la pestaña Destinos.
5. Si no hay ninguna función de Lambda registrada, elija Registrar destino. Seleccione la función de Lambda y elija Registrar destino.
6. Para anular el registro de una función de Lambda, elija Anular registro. Cuando se le pida confirmación, ingrese **`confirm`** y luego elija Anular registro.

Registrar o anular el registro de un equilibrador de carga de aplicación

Puede registrar un único equilibrador de carga de aplicación con cada grupo de destino. Si ya no necesita enviar tráfico al equilibrador de carga, puede anular su registro. Después de anular el registro de un equilibrador de carga, las solicitudes en tránsito producirán errores HTTP 5XX. Es mejor crear un grupo de destino nuevo en lugar de reemplazar el equilibrador de carga de aplicación para un grupo de destino.

Para registrar o anular el registro de un equilibrador de carga de aplicación mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Grupos de destino.
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. Elija la pestaña Destinos.
5. Si no hay ningún equilibrador de carga de aplicación registrado, elija Registrar destino. Seleccione el equilibrador de carga de aplicación y elija Registrar destino.
6. Para anular el registro de un equilibrador de carga de aplicación, elija Anular registro. Cuando se le pida confirmación, ingrese **`confirm`** y luego elija Anular registro.

Comprobaciones de estado de sus grupos de destino de VPC Lattice

Su servicio envía periódicamente solicitudes a los destinos registrados para comprobar su estado. Estas pruebas se denominan comprobaciones de estado.

Cada servicio de VPC Lattice enruta las solicitudes solo a los destinos en buen estado. Cada servicio comprueba el estado de cada destino; para ello, utiliza la configuración de comprobación de estado de los grupos de destino con los que está registrado el destino. Una vez que el destino está registrado, debe superar una comprobación de estado para que se considere que se encuentra en buen estado. Después de completar cada comprobación de estado, el servicio cierra la conexión que se estableció para la comprobación de estado.

Limitaciones y consideraciones

- Cuando la versión del protocolo del grupo de destino es HTTP1, las comprobaciones de estado están habilitadas de forma predeterminada.

- Cuando la versión del protocolo del grupo de destino es HTTP2, las comprobaciones de estado no están habilitadas de forma predeterminada. Sin embargo, puede habilitar las comprobaciones de estado y configurar manualmente la versión del protocolo en HTTP1 o HTTP2.
- La comprobación de estado no admite las versiones del protocolo gRPC para grupos de destino. Sin embargo, si habilita las comprobaciones de estado, debe especificar la versión del protocolo de comprobación de estado como HTTP1 o HTTP2.
- Las comprobaciones de estado no son compatibles con los grupos de destino de Lambda.
- Las comprobaciones de estado no son compatibles con los grupos de destino del equilibrador de carga de aplicación. Sin embargo, puede habilitar las comprobaciones de estado de los destinos de su equilibrador de carga de aplicación mediante Elastic Load Balancing. Para obtener más información, consulte las comprobaciones de estado de los grupos destinatarios en la Guía del usuario de los balanceadores de carga de aplicaciones.

Configuración de comprobación de estado

Puede configurar las comprobaciones de estado de los destinos de un grupo de destino según se indica en la siguiente tabla. Los nombres de configuración que se utilizan en la tabla son los que se utilizan en la API. El servicio envía una solicitud de comprobación de estado a cada destino registrado cada HealthCheckIntervalSecondssegundos utilizando el protocolo, el puerto y la ruta de ping especificados. Cada solicitud de comprobación de estado es independiente y el resultado dura todo el intervalo. El tiempo que tarda el destino en responder no afecta al intervalo de la siguiente solicitud de comprobación de estado. Si las comprobaciones de estado superan el umbral de los errores UnhealthyThresholdCountconsecutivos, el servicio inhabilita el destino. Cuando las comprobaciones de estado superan el umbral de los éxitos HealthyThresholdCountconsecutivos, el servicio vuelve a poner el destino en servicio.

Opción	Descripción
HealthCheckProtocol	Protocolo que el servicio utiliza al realizar comprobaciones de estado en los destinos. Los posibles protocolos son HTTP y HTTPS. El valor predeterminado es el protocolo HTTP.
HealthCheckPort	Puerto que el servicio utiliza al realizar comprobaciones de estado en los destinos. El valor predeterminado es el puerto en el que

Opción	Descripción
	cada destino recibe el tráfico procedente del servicio.
HealthCheckPath	El destino para las comprobaciones de estado en los destinos. Si la versión del protocolo es HTTP1 o HTTP2, especifique un URI válido (/path? consulta). El valor predeterminado es /.
HealthCheckTimeoutSeconds	Cantidad de tiempo, en segundos, durante la cual ninguna respuesta de un destino significa una comprobación de estado fallida. El rango va de 1 a 120 segundos. Si el tipo de destino es `INSTANCE` o `IP`, el valor predeterminado es 5 segundos. Especifique 0 para restablecer esta configuración a su valor predeterminado.
HealthCheckIntervalSeconds	Cantidad aproximada de tiempo, en segundos, que transcurre entre comprobaciones de estado de un destino individual. El rango va de 5 a 300 segundos. Si el tipo de destino es `INSTANCE` o `IP`, el valor predeterminado es 30 segundos. Especifique 0 para restablecer esta configuración a su valor predeterminado.
HealthyThresholdCount	Número de comprobaciones de estado consecutivas exitosas que deben superarse para considerar que un destino está en buen estado. El rango va de 2 a 10. El valor predeterminado es 5. Especifique 0 para restablecer esta configuración a su valor predeterminado.

Opción	Descripción
UnhealthyThresholdCount	Número de comprobaciones de estado consecutivas erróneas para que se considere que el estado de la instancia no es correcto. El rango va de 2 a 10. El valor predeterminado es 2. Especifique 0 para restablecer esta configura ción a su valor predeterminado.
Matcher	Códigos que se deben utilizar al comprobar si se ha recibido una respuesta exitosa de un destino. En la consola, se llaman códigos de éxito. Si la versión del protocolo es HTTP1 o HTTP2, los valores posibles oscilan entre 200 y 499. Puede especificar varios valores (por ejemplo, “200,202”) o un intervalo de valores (por ejemplo, “200-299”). El valor predeterminado es 200. La versión del protocolo de comprobación de estado para gRPC no es compatible actualmen te. Sin embargo, si la versión del protocolo de su grupo de destino es gRPC, puede especific ar HTTP1 o las versiones de HTTP2 protocolo en la configuración de comprobación de estado.

Comprobación del estado de los destinos

Puede comprobar el estado de los destinos registrados en los grupos de destino.

Para comprobar el estado de los destinos desde la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Grupos de destino.

3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña de Destinos, la columna de Estado indica el estado de cada destino. Si el estado es un valor distinto de `Healthy`, la columna Detalles del estado contiene más información.

Para comprobar la salud de los destinos con la AWS CLI

Use el comando list-targets. El resultado de este comando contiene el estado del destino. Si el estado es cualquier valor distinto de `Healthy`, la salida también incluye un código de motivo.

Para recibir notificaciones por correo electrónico sobre destinos en mal estado

Utilice CloudWatch alarmas para iniciar una función de Lambda y enviar detalles sobre los destinos en mal estado.

Cómo modificar la configuración de comprobación de estado

Puede modificar la configuración de comprobación de estado del grupo de destino en cualquier momento.

Cómo modificar la configuración de comprobación de estado mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Grupos de destino.
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Comprobaciones de estado, en la sección Configuración de comprobación de estado, elija Editar.
5. Modifique la configuración de comprobación de estado según sea necesario.
6. Seleccione Save changes (Guardar cambios).

Cómo modificar la configuración de comprobación de estado mediante la AWS CLI

Utilice el comando update-target-group.

Configuración de enrutamiento

De forma predeterminada, un servicio dirige las solicitudes a sus destinos mediante el protocolo y el número de puerto especificados al crear el grupo de destino. Si lo prefiere, puede anular el puerto utilizado para dirigir el tráfico a un destino al registrarlo en el grupo de destino.

Los grupos de destino admiten los siguientes protocolos y puertos:

- Protocolos: HTTP, HTTPS, TCP
- Puertos: 1-65535

Si un grupo de destino se configura con el protocolo HTTPS o utiliza comprobaciones de estado HTTPS, las conexiones TLS a los destinos utilizarán la política de seguridad del oyente. VPC Lattice establece conexiones TLS con los destinos mediante certificados que instala en los destinos. VPC Lattice no valida estos certificados. Por lo tanto, puede utilizar certificados autofirmados o certificados que hayan caducado. El tráfico entre VPC Lattice y los destinos se autentica en el nivel de paquete, por lo que no corre el riesgo de sufrir man-in-the-middle ataques o suplantación, incluso aunque los certificados de los destinos no sean válidos.

Los grupos de destino TCP solo son compatibles con los dispositivos de escucha TLS.

Algoritmo de enrutamiento

De forma predeterminada, el algoritmo de enrutamiento de turnos rotativos se utiliza para dirigir las solicitudes al grupo de destino.

Cuando el servicio de VPC Lattice recibe una solicitud, utiliza el siguiente proceso:

1. Evalúa las reglas del oyente en orden de prioridad para determinar qué regla se va a aplicar.
2. Selecciona un destino del grupo de destino para la acción de regla mediante el uso del algoritmo de turnos rotativos predeterminado. El enrutamiento se lleva a cabo de manera independiente para cada grupo de destino, aunque un destino se haya registrado en varios grupos de destino.

Si un grupo de destino contiene únicamente destinos en mal estado, las solicitudes se envían a todos los destinos, independientemente de su estado. Esto significa que, si todos los destinos no superan las comprobaciones de estado al mismo tiempo, se produce un error al abrir el servicio de VPC Lattice. El efecto de la apertura por error es permitir que el tráfico llegue a todos los destinos, independientemente de su estado, según el algoritmo de turnos rotativos.

Tipo de destino

Al crear un grupo de destino, debe especificar su tipo de destino, que determina el tipo de destino que especifica al registrar los destinos en este grupo de destino. Después de que crea un grupo de destino, no puede cambiar su tipo de destino.

Los tipos de destinos posibles son los siguientes:

`INSTANCE`

Los destinos se especifican por ID de instancia.

`IP`

Los destinos son direcciones IP.

`LAMBDA`

El destino es una función de Lambda.

`ALB`

El destino es un equilibrador de carga de aplicación.

Consideraciones

- Si el tipo de destino es `IP`, debe especificar las direcciones IP de las subredes de la VPC para el grupo de destino. Si necesita registrar direcciones IP ajenas a esta VPC, cree un tipo de grupo de destino `ALB` y registre las direcciones IP con el equilibrador de carga de aplicación.
- Cuando el tipo de destino es `IP`, no puede registrar puntos de conexión de VPC ni direcciones IP enrutables públicamente.
- Si el tipo de destino es `LAMBDA`, puede registrar una única función de Lambda. Cuando el servicio recibe una solicitud para la función de Lambda, invoca la función de Lambda. Si desea registrar varias funciones de Lambda en un servicio, debe utilizar varios grupos de destino.
- Si el tipo de destino es`ALB`, puede registrar un único Application Load Balancer interno como destino de hasta dos servicios de VPC Lattice. Para ello, registre el equilibrador de carga de aplicación con dos grupos de destino distintos, utilizados por dos servicios de VPC Lattice diferentes. Además, el equilibrador de carga de aplicación específico debe tener al menos un oyente cuyo puerto coincida con el puerto de grupo de destino.
- Puede registrar automáticamente las tareas de ECS en un grupo de destino de VPC Lattice en el momento del lanzamiento. El grupo de destino debe tener el tipo de destino `IP`. Para obtener

más información, consulte Uso de VPC Lattice con sus servicios de Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.

También puede registrar el equilibrador de carga de aplicación para su servicio de Amazon ECS en un grupo de destino de VPC Lattice de tipo VPC Lattice. `ALB` Para obtener más información, consulte Uso del equilibrio de carga para distribuir el tráfico del servicio Amazon ECS en la Guía para desarrolladores de Amazon Elastic Container Service.

- Para registrar un pod EKS como destino, utilice el controlador de AWS Gateway API, que obtiene las direcciones IP del servicio de Kubernetes.
- Si el protocolo de grupo de destino es TCP, los únicos tipos de destino compatibles son `INSTANCE` y`IP`.

Tipo de dirección IP

Al crear un grupo de destino con un tipo de destino de `IP`, puede especificar un tipo de dirección IP para el grupo de destino. Esto especifica qué tipo de direcciones usa el equilibrador de carga para enviar solicitudes y comprobaciones de estado a los destinos. Los valores posibles son `IPv4` y `IPv6`. El valor predeterminado es `IPV4`.

Consideraciones

- Si crea un grupo de destino con un tipo de dirección IP de`IPv6`, la VPC que especifique para el grupo de destino debe tener un rango de IPv6 direcciones.
- Las direcciones IP que registre en un grupo de destino deben coincidir con el tipo de dirección IP del grupo de destino. Por ejemplo, no puede registrar una IPv6 dirección en un grupo de destino si su tipo de dirección IP es`IPv4`.
- Las direcciones IP que registre en un grupo de destino deben estar dentro del rango de direcciones IP de la VPC que especificó para el grupo de destino.

Destinos HTTP en VPC Lattice

Las solicitudes y respuestas HTTP utilizan campos de encabezado para enviar información sobre los mensajes HTTP. Los encabezados HTTP se añaden automáticamente. Los campos de encabezado son pares nombre-valor separados por signos de dos puntos, separados a su vez por un retorno de carro (CR) y un salto de línea (LF). Un conjunto estándar de campos de encabezado HTTP se define en RFC 2616, Encabezados de mensaje. También hay encabezados HTTP no estándar disponibles

que se agregan automáticamente y que se suelen utilizar en las aplicaciones. Por ejemplo, hay encabezados HTTP no estándar con el prefijo `x-forwarded`.

Encabezados x-forwarded

Amazon VPC Lattice añade los siguientes encabezados `x-forwarded`:

`x-forwarded-for`

La dirección IP de origen.

`x-forwarded-for-port`

El puerto de destino.

`x-forwarded-for-proto`

El protocolo de conexión (`http` | `https`).

Encabezados de identidad del intermediario

Amazon VPC Lattice añade los siguientes encabezados de identidad del intermediario:

`x-amzn-lattice-identity`

La información de identidad. Los siguientes campos están presentes si la autenticación de AWS se realiza con éxito.

- `Principal`: la entidad principal autenticada.
- `PrincipalOrgID`: el ID de la organización para la entidad principal autenticada.
- `SessionName`: el nombre de sesión autenticada.

Los siguientes campos están presentes si se utilizan las credenciales de Roles Anywhere y la autenticación se realiza con éxito.

- `X509Issuer/OU`: el emisor (OU).
- `X509SAN/DNS`: el nombre alternativo del sujeto (DNS).
- `X509SAN/NameCN`: el nombre alternativo del emisor (nombre/CN).
- `X509SAN/URI`: el nombre alternativo del sujeto (URI).
- `X509Subject/CN`: el nombre del sujeto (CN).

`x-amzn-lattice-network`

La VPC. El formato es el siguiente.

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

`x-amzn-lattice-target`

El destino. El formato es el siguiente.

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

Para obtener información sobre el recurso de ARNs VPC Lattice, consulte Tipos de recursos definidos por Amazon VPC Lattice.

Los encabezados de identidad de las personas que llaman no se pueden falsificar. VPC Lattice elimina estos encabezados de las solicitudes entrantes.

Funciones de Lambda como destinos en VPC Lattice

Puede registrar sus funciones de Lambda como destinos con un grupo de destino de VPC Lattice y configurar una regla del oyente para reenviar las solicitudes al grupo de destino de la función de Lambda. Cuando el servicio reenvía la solicitud a un grupo de destino con una función de Lambda como destino, invoca la función de Lambda y pasa el contenido de la solicitud a la función de Lambda, en formato JSON.

Limitaciones

- La función de Lambda y el grupo de destino deben estar en la misma cuenta y en la misma región.
- El tamaño máximo del cuerpo de la solicitud que puede enviar a una función de Lambda es de 6 MB.
- El tamaño máximo del JSON de respuesta que la función de Lambda puede enviar es de 6 MB.
- El protocolo debe ser HTTP o HTTPS.

Preparación de la función de Lambda

Se aplican las siguientes recomendaciones si está utilizando su función de Lambda con un servicio de VPC Lattice.

Permisos para invocar la función de Lambda

Cuando crea el grupo de destino y registra la función de Lambda mediante la AWS Management Console o la, AWS CLI VPC Lattice añade los permisos necesarios a la política de su función de Lambda en su nombre.

También puede añadir permisos por su cuenta mediante la siguiente llamada a la API:

```
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
```

Control de versiones de función de Lambda

Puede registrar una sola función de Lambda por grupo de destino. Para asegurarse de que puede cambiar la función de Lambda y de que el servicio de VPC Lattice siempre invoque la versión actual de la función de Lambda, cree un alias de función e incluya el alias en el ARN de la función cuando registre la función de Lambda en el servicio de VPC Lattice. Para obtener más información, consulte Versiones de funciones de Lambda y Creación de un alias para una función de Lambda en la Guía para desarrolladores.AWS Lambda

Creación de un grupo de destino para la función de Lambda

Cree el grupo de destino que se va a utilizar para el enrutamiento de solicitudes. Si el contenido de la solicitud coincide con una regla del oyente con una acción para reenviarlo a este grupo de destino, el servicio de VPC Lattice invoca la función de Lambda registrada.

Cómo crear un grupo de destino y registrar la función de Lambda mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Grupos de destino.
3. Elija Crear grupo de destino.
4. En Elegir un tipo de destino, seleccione Función de Lambda.
5. En Nombre del grupo de destino, escriba el nombre del grupo de destino.
6. En Versión de estructura de eventos de Lambda, elija una versión. Para obtener más información, consulte the section called “Recepción de eventos del servicio de VPC Lattice”.

7. (Opcional) Para agregar etiquetas, expanda Etiquetas, elija Agregar nueva etiqueta e ingrese la clave y el valor de la etiqueta.
8. Elija Siguiente.
9. En Función de Lambda, realice alguna de las siguientes acciones:
   - Seleccione una función de Lambda existente.
   - Cree una nueva función de Lambda y selecciónela.
   - Registre la función de Lambda más adelante.
10. Elija Crear grupo de destino.

Cómo crear un grupo de destino y registrar la función de Lambda mediante la AWS CLI

Utilice los comandos create-target-groupy register-targets.

Recepción de eventos del servicio de VPC Lattice

El servicio de VPC Lattice admite la invocación de Lambda de solicitudes a través de HTTP y HTTPS. El servicio envía un evento en formato JSON y agrega el encabezado `X-Forwarded-For` a cada solicitud.

Codificación en Base64

El servicio Base64 codifica el cuerpo si el encabezado `content-encoding` está presente y el tipo de contenido no es uno de los siguientes:

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

Si el encabezado `content-encoding` no está presente, la codificación en Base64 depende del tipo de contenido. Para los tipos de contenido anteriores, el servicio envía el cuerpo tal cual, sin la codificación en Base64.

Formato de estructura de evento

Al crear o actualizar un tipo de grupo de destino `LAMBDA`, puede especificar la versión de la estructura de eventos que recibe la función de Lambda. Las versiones posibles son `V1` y `V2`.

Example Ejemplo de evento: 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

El cuerpo de la solicitud. Está presente únicamente si el protocolo es HTTP, HTTPS o gRPC.

`headers`

El encabezado HTTP de la solicitud. Está presente únicamente si el protocolo es HTTP, HTTPS o gRPC.

`identity`

La información de identidad. A continuación se indican los posibles campos.

- `principal`: la entidad principal autenticada. Está presente solo si la AWS autenticación de se realiza con éxito.
- `principalOrgID`: el ID de la organización para la entidad principal autenticada. Está presente solo si la AWS autenticación de se realiza con éxito.
- `sessionName`: el nombre de sesión autenticada. Está presente solo si la AWS autenticación de se realiza con éxito.
- `sourceVpcArn`: el ARN de la VPC en donde se originó la solicitud. Está presente solo si se puede identificar la VPC de origen.
- `type`— El valor corresponde a `AWS_IAM` si se utiliza una política de AWS autenticación y la autenticación se realiza correctamente.

Si se utilizan las credenciales de Roles Anywhere y la autenticación se realiza con éxito, los siguientes campos son posibles.

- `x509IssuerOu`: el emisor (OU).
- `x509SanDns`: el nombre alternativo del sujeto (DNS).
- `x509SanNameCn`: el nombre alternativo del emisor (nombre/CN).
- `x509SanUri`: el nombre alternativo del sujeto (URI).
- `x509SubjectCn`: el nombre del sujeto (CN).

`isBase64Encoded`

Indica si el cuerpo tenía codificación en Base64. Está presente solo si el protocolo es HTTP, HTTPS o gRPC y el cuerpo de la solicitud aún no es una cadena.

`method`

El método HTTP de la solicitud. Está presente únicamente si el protocolo es HTTP, HTTPS o gRPC.

`path`

La ruta de la solicitud. Está presente únicamente si el protocolo es HTTP, HTTPS o gRPC.

`queryStringParameters`

Los parámetros de cadenas de consulta HTTP. Está presente únicamente si el protocolo es HTTP, HTTPS o gRPC.

`serviceArn`

El ARN del servicio que recibe la solicitud.

`serviceNetworkArn`

El ARN de la red de servicios que entrega la solicitud.

`targetGroupArn`

El ARN del grupo de destino que recibe la solicitud.

`timeEpoch`

El tiempo, en microsegundos.

Example Ejemplo de evento: 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
}
```

Respuesta al servicio de VPC Lattice

La respuesta de la función de Lambda debe incluir el estado de codificación en Base64, el código de estado y los encabezados. Puede omitir el cuerpo.

Para incluir contenido binario en el cuerpo de la respuesta, debe codificar en Base64 el contenido y establecer `isBase64Encoded` en `true`. El servicio descodifica el contenido para recuperar el contenido binario y lo envía al cliente en el cuerpo de la respuesta HTTP.

El servicio de VPC Lattice no respeta hop-by-hop los encabezados, como o. `Connection` `Transfer-Encoding` Puede omitir el encabezado `Content-Length` porque el servicio lo procesa antes de enviar las respuestas a los clientes.

A continuación, se muestra un ejemplo de la respuesta de una función de Lambda:

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

Encabezados de varios valores

VPC Lattice admite solicitudes de un cliente o las respuestas de una función de Lambda que contienen encabezados con varios valores o contienen el mismo encabezado varias veces. VPC Lattice pasa todos los valores a los destinos.

En el siguiente ejemplo, hay dos encabezados nombrados header1 con valores diferentes.

```
header1 = value1
header1 = value2
```

Con una estructura de eventos V2, VPC Lattice envía los valores de una lista. Por ejemplo:

```
"header1": ["value1", "value2"]
```

Con una estructura de eventos V1, VPC Lattice combina los valores en una sola cadena. Por ejemplo:

```
"header1": "value1, value2"
```

Normalizar parámetros de cadena de cadena de cadena de parámetros

VPC Lattice admite parámetros de consulta con varios valores para la misma clave.

En el siguiente ejemplo, hay dos parámetros nombrados QS1 con valores diferentes.

```
http://www.example.com?&QS1=value1&QS1=value2
```

Con una estructura de eventos V2, VPC Lattice envía los valores de una lista. Por ejemplo:

```
"QS1": ["value1", "value2"]
```

Con una estructura de eventos V1, VPC Lattice usa el último valor pasado. Por ejemplo:

```
"QS1": "value2"
```

Anulación del registro de la función de Lambda

Si ya no necesita enviar tráfico a la función de Lambda, puede anular su registro. Después de anular el registro de una función de Lambda, las solicitudes en tránsito producirán errores HTTP 5XX.

Para sustituir una función de Lambda, le recomendamos que cree un nuevo grupo de destino, registre la nueva función en el nuevo grupo de destino y actualice las reglas del oyente para que utilicen el nuevo grupo de destino en lugar del existente.

Cómo anular el registro de la función de Lambda mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Grupos de destino.
3. Elija el nombre del grupo de destino para mostrar sus detalles.
4. En la pestaña Destinos, elija Anular registro.
5. Cuando se le pida confirmación, ingrese **`confirm`** y luego elija Anular registro.

Para anular el registro de la función de Lambda mediante la AWS CLI

Use el comando deregister-targets.

Equilibradores de carga de aplicación como destinos en VPC Lattice

Puede crear un grupo de destino de VPC Lattice, registrar un único equilibrador de carga de aplicación interno como destino y configurar su servicio de VPC Lattice para reenviar el tráfico a este grupo de destino. En este escenario, el equilibrador de carga de aplicación asume la decisión de enrutamiento en cuanto llega el tráfico. Esta configuración le permite utilizar la característica

de enrutamiento de capa 7 basada en solicitudes del equilibrador de carga de aplicación en combinación con las funciones compatibles con VPC Lattice, como la autenticación y la autorización de IAM y la conectividad entre las cuentas. VPCs

Limitaciones

- Puede registrar un único equilibrador de carga de aplicación interno como destino en un grupo de destino de VPC Lattice de tipo `ALB`.
- Puede registrar un equilibrador de carga de aplicación como destino de hasta dos grupos de destino de VPC Lattice, utilizados por dos servicios de VPC Lattice diferentes.
- VPC Lattice no proporciona comprobaciones de estado para un grupo de destino de tipo `ALB`. Sin embargo, puede configurar las comprobaciones de estado de forma independiente en el nivel del equilibrador de carga para los destinos en Elastic Load Balancing. Para obtener más información, consulte las comprobaciones de estado de los grupos destinatarios en la Guía del usuario de los balanceadores de carga de aplicaciones

Requisitos previos

Cree un equilibrador de carga de aplicación para registrarlo como destino en su grupo de destino de VPC Lattice. El equilibrador de carga debe cumplir los siguientes criterios:

- El esquema del equilibrador de carga es interno.
- El equilibrador de carga de aplicación debe estar en la misma cuenta que el grupo de destino de VPC Lattice y debe estar en estado activo.
- El equilibrador de carga de aplicación debe estar en la misma VPC que el grupo de destino de VPC Lattice.
- Puede usar oyentes HTTPS en el equilibrador de carga de aplicación para finalizar la TLS, pero solo si el servicio de VPC Lattice usa el mismo certificado SSL/TLS que el equilibrador de carga.
- Para conservar el IP de cliente del servicio de VPC Lattice en el encabezado de solicitud `X-Forwarded-For`, debe establecer el atributo del equilibrador de carga de aplicación `routing.http.xff_header_processing.mode` a `Preserve`. Si el valor es `Preserve`, el equilibrador de carga conserva el encabezado `X-Forwarded-For` en la solicitud HTTP y lo envía a los destinos sin ningún cambio.

Para obtener más información, consulte Crear un Equilibrador de carga de aplicación en la Guía del usuario para Equilibradores de carga de aplicación.

Paso 1: crear un grupo de destino de tipo ALB

Utilice el siguiente procedimiento para crear el grupo de destino. Tenga en cuenta que VPC Lattice no admite comprobaciones de estado para ALB los grupos de destino. Sin embargo, puede configurar comprobaciones de estado para los grupos de destino de su equilibrador de carga de aplicación. Para obtener más información, consulte las comprobaciones de estado de los grupos destinatarios en la Guía del usuario de los balanceadores de carga de aplicaciones.

Cómo crear el grupo de destino

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Grupos de destino.
3. Elija Crear grupo de destino.
4. En la página Especificar detalles del grupo de destino, en Configuración básica, elija Equilibrador de carga de aplicación como tipo de destino.
5. En Nombre del grupo de destino, escriba el nombre del grupo de destino.
6. En Protocolo, elija **HTTP** o **HTTPS**. El protocolo del grupo de destino debe coincidir con el protocolo del oyente de su equilibrador de carga de aplicación interno.
7. En Puerto, especifique el puerto de su grupo de destino. Este puerto debe coincidir con el puerto del oyente de su equilibrador de carga de aplicación interno. También puede añadir un puerto del oyente en el equilibrador de carga de aplicación interno para que coincida con el puerto de grupo de destino que especifique aquí.
8. En VPC, seleccione la misma nube privada virtual (VPC) que seleccionó al crear el equilibrador de carga de aplicación interno. Debe ser la VPC que contiene los recursos de VPC Lattice.
9. En Versión del protocolo, elija la versión de protocolo que admita su equilibrador de carga de aplicación.
10. (Opcional) Agregue las etiquetas necesarias.
11. Elija Siguiente.

Paso 2: registrar el equilibrador de carga de aplicación como destino

Puede registrar el equilibrador de carga como destino ahora o más adelante.

Para registrar un equilibrador de carga de aplicación como destino

1. Elija Registrar ahora.

2. En Equilibrador de carga de aplicación, elija su equilibrador de carga de aplicación interno.
3. En Puerto, deje el puerto predeterminado o especifique otro. Este puerto debe coincidir con un puerto de oyente existente en su equilibrador de carga de aplicación. Si continúa sin un puerto coincidente, el tráfico no llegará a su equilibrador de carga de aplicación.
4. Elija Crear grupo de destino.

Versión del protocolo

De forma predeterminada, los servicios envían las solicitudes a destinos mediante HTTP/1.1. Puede usar la versión del protocolo para enviar solicitudes a los destinos mediante HTTP/2 o gRPC.

En la siguiente tabla se resumen el resultado de las combinaciones del protocolo de solicitud y la versión del protocolo de grupo de destino.

Protocolo de solicitud	Versión del protocolo	Resultado
HTTP/1.1	HTTP/1.1	Success
HTTP/2	HTTP/1.1	Success
gRPC	HTTP/1.1	Error
HTTP/1.1	HTTP/2	Error
HTTP/2	HTTP/2	Success
gRPC	HTTP/2	Correcto si los destinos respaldan el gRPC
HTTP/1.1	gRPC	Error
HTTP/2	gRPC	Correcto si una solicitud POST
gRPC	gRPC	Success

Consideraciones para la versión del protocolo gRPC

- El único protocolo de oyente compatible es HTTPS.

- Solo se admiten los tipos de destino `INSTANCE` y `IP`.
- El servicio analiza las solicitudes de gRPC y enruta las llamadas de gRPC a los grupos de destino apropiados en función del paquete, el servicio y el método.
- No podrá utilizar las funciones de Lambda como destinos.

Consideraciones para la versión del protocolo HTTP/2

- El único protocolo de oyente compatible es HTTPS. Puede elegir HTTP o HTTPS como protocolo del grupo de destino.
- Las únicas reglas de oyente admitidas son la respuesta directa y la respuesta fija.
- Solo se admiten los tipos de destino `INSTANCE` y `IP`.
- El servicio admite la transmisión desde los clientes. El servicio no admite la transmisión a los destinos.

Etiquetas para su grupo de destino de VPC Lattice

Las etiquetas lo ayudan a clasificar los grupos de destino de diversas maneras, por ejemplo, según su finalidad, propietario o entorno.

Puede agregar varias etiquetas a cada grupo de destino. Las claves de las etiquetas deben ser únicas en cada grupo de destino. Si agrega una etiqueta con una clave que ya está asociada al grupo de destino, se actualizará el valor de esa etiqueta.

Cuando ya no necesite una etiqueta, puede eliminarla.

Restricciones

- Número máximo de etiquetas por recurso: 50
- Longitud máxima de la clave: 127 caracteres Unicode
- Longitud máxima del valor: 255 caracteres Unicode
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas. Los caracteres permitidos son letras, espacios y números representables en UTF-8, además de los siguientes caracteres especiales: + - = . _ : / @. No utilice espacios iniciales ni finales.
- No utilice el `aws:` prefijo en los nombres o valores de las etiquetas, porque está reservado para AWS uso de. Los nombres y valores de etiquetas que tienen este prefijo no se pueden editar ni eliminar. Las etiquetas que tengan este prefijo no cuentan para el límite de etiquetas por recurso.

Para actualizar las etiquetas de un grupo de destino desde la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Grupos de destino.
3. Seleccione el nombre del grupo de destino para abrir su página de detalles.
4. Elija la pestaña Etiquetas.
5. Para agregar una etiqueta, elija Agregar etiquetas e ingrese la clave y el valor de la etiqueta. Para agregar otra etiqueta, elija Agregar nueva etiqueta. Cuando haya terminado de añadir etiquetas, elija Guardar cambios.
6. Para eliminar una etiqueta, active la casilla de verificación de la etiqueta y elija Eliminar. Cuando le pidan confirmación, escriba **`confirm`** y elija Eliminar.

Para actualizar las etiquetas de un grupo de destino mediante la AWS CLI

Utilice los comandos tag-resource y untag-resource.

Para eliminar un grupo de destino de VPC Lattice

Puede eliminar un grupo de destino si las acciones de las reglas de oyente no hacen referencia a él. La eliminación de un grupo de destino no afecta a los destinos registrados en él. Si ya no necesita una EC2 instancia registrada, puede detenerla o finalizarla.

Para eliminar un grupo de destino desde la consola

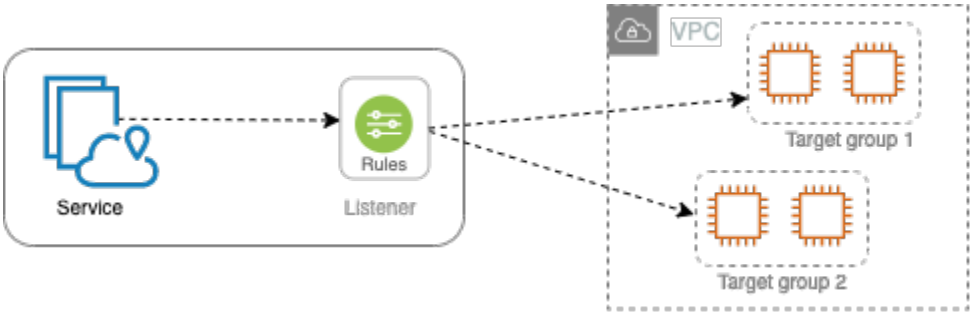
1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Grupos de destino.
3. Seleccione la casilla de verificación para el grupo de destino y, a continuación, elija Acciones, Eliminar.
4. Cuando le pidan confirmación, escriba **`confirm`** y elija Eliminar.

Para eliminar un grupo de destino mediante la AWS CLI

Utilice el comando delete-target-group.

Oyentes para su servicio VPC Lattice

Antes de comenzar a utilizar su servicio VPC Lattice, debe agregar un oyente. Un oyente es un proceso que comprueba las solicitudes de conexión utilizando el protocolo y el puerto configurados. Las reglas que defina para un oyente determinan cómo el servicio va a direccionar las solicitudes hacia sus destinos registrados.



Contenido

Configuración del oyente

Los oyentes son compatibles con los siguientes protocolos y puertos:

- Protocolos: HTTP, HTTPS, TLS
- Puertos: 1-65535

Si el protocolo del oyente es HTTPS, VPC Lattice aprovisionará y administrará un certificado TLS asociado al FQDN generado por VPC Lattice. VPC Lattice utiliza TLS en HTTP/1.1 y HTTP/2. Al configurar un servicio con un oyente HTTPS, VPC Lattice determinará automáticamente el protocolo HTTP a través de la negociación del protocolo de la capa de aplicación (ALPN). Si no hay ALPN,

VPC Lattice utiliza HTTP/1.1 de forma predeterminada. Para obtener más información, consulte Oyentes HTTPS.

VPC Lattice puede ser oyente en HTTP, HTTPS, HTTP/1.1 y HTTP/2 y comunicarse con los destinatarios a través de cualquiera de estos protocolos y versiones. No es necesario que los protocolos del oyente y del grupo de destino coincidan. VPC Lattice administra todo el proceso de actualización y degradación entre protocolos y versiones. Para obtener más información, consulte Versión del protocolo.

Puede crear un agente de escucha de TLS para garantizar que su aplicación descifre el tráfico cifrado en lugar de VPC Lattice. Para obtener más información, consulte Oyentes de TLS.

VPC Lattice no es compatible. WebSockets

Oyentes HTTP para servicios de VPC Lattice

Un oyente es un proceso que verifica solicitudes de conexión. Puede definir un oyente cuando crea su servicio VPC Lattice. Puede agregar oyentes a su servicio en todo momento.

La información en esta página lo ayuda a crear un oyente HTTP para su servicio. Para obtener información sobre la creación de oyentes que utilicen otros protocolos, consulte y. Oyentes HTTPS Oyentes de TLS

Requisitos previos

- Para añadir una acción de reenvío a la regla predeterminada del oyente, debe especificar un grupo de destino de VPC Lattice disponible. Para obtener más información, consulte Creación de un grupo de destino de VPC Lattice.
- Puede especificar el mismo grupo de destino en más de un oyente, pero todos los oyentes deben pertenecer al mismo servicio. Para utilizar un grupo de destino con un servicio de VPC Lattice, debe asegurarse de que ningún oyente lo utilice para otro servicio de VPC Lattice.

Adición de un oyente HTTP

Puede agregar oyentes y reglas a su servicio en todo momento. Usted configura un oyente con un protocolo y un puerto para las conexiones de clientes al servicio, y un grupo de destinos de VPC Lattice para la regla predeterminada del oyente. Para obtener más información, consulte Configuración del oyente.

Cómo agregar un oyente HTTPS utilizando la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Servicios.
3. Seleccione el nombre del servicio para abrir la página de detalles.
4. En la pestaña Enrutamiento, elija Agregar oyente.
5. Para Nombre del oyente, puede proporcionar un nombre personalizado o usar el protocolo y el puerto del oyente como el nombre del oyente. El nombre personalizado que indique puede tener un máximo de 63 caracteres y debe ser único para cada servicio que tenga en su cuenta. Los caracteres válidos son a-z, 0-9 y guiones (-). No puede usar un guion como primer o último carácter, ni tampoco seguido de otro guion. No puede cambiar el nombre después de crearlo.
6. En Protocolo: puerto, elija HTTP e ingrese un número de puerto.
7. Como Acción predeterminada, elija el grupo de destino de VPC Lattice que recibirá el tráfico y la ponderación que quiera asignarle a este grupo. El peso que asigne a un grupo de destino establece su prioridad para recibir tráfico. Por ejemplo, si dos grupos de destino tienen la misma ponderación, cada grupo recibe la mitad del tráfico. Si indicó un solo grupo de destino, el 100 por ciento del tráfico se enviará a ese grupo.

   Si lo desea, puede agregar otro grupo de destino para la acción predeterminada. Seleccione Añadir acción y, a continuación, elija un grupo de destino e indique su ponderación.
8. (Opcional) Para añadir otra regla, elija Añadir regla y, a continuación, introduzca un nombre, una prioridad, una condición y una acción para la regla.

   Puede asignar a cada regla un número de prioridad entre 1 y 100. Un oyente no puede tener varias reglas con la misma prioridad. Las reglas se evalúan por orden de prioridad, desde el valor más bajo hasta el valor más alto. La regla predeterminada se evalúa en último lugar. Para obtener más información, consulte Reglas del oyente.
9. (Opcional) Para agregar etiquetas, diríjase a Etiquetas del oyente, elija Agregar nueva etiqueta e ingrese la clave y el valor de la etiqueta.
10. Revise su configuración y luego elija Añadir.

Para agregar un oyente HTTPS mediante la AWS CLI

Utilice el comando create-listener para crear un oyente con una regla predeterminada y el comando create-rule para crear reglas adicionales para el oyente.

Oyentes HTTPS para servicios de VPC Lattice

Un oyente es un proceso que verifica solicitudes de conexión. Al crear el servicio, se establece un oyente. Puede añadir oyentes a su servicio en VPC Lattice en todo momento.

Puede crear un oyente HTTPS que utilice la versión 1.2 o la versión 1.3 de TLS para finalizar las conexiones HTTPS con VPC Lattice de inmediato. VPC Lattice aprovisionará y administrará un certificado TLS asociado con el nombre de dominio completo (FQDN) generado por VPC Lattice. VPC Lattice es compatible con TLS en HTTP/1.1 y HTTP/2. Cuando configura un servicio con un oyente HTTPS, VPC Lattice determinará automáticamente el protocolo HTTP a través de la negociación del protocolo de capa de aplicación (ALPN). Si no hay ALPN, VPC Lattice utiliza HTTP/1.1 de forma predeterminada.

VPC Lattice utiliza una arquitectura de varias tenencias, lo que significa que puede alojar varios servicios en el mismo punto de conexión. VPC Lattice utiliza TLS con indicación de nombre de servidor (SNI) para cada solicitud de cliente. No se admiten el saludo de cliente cifrado (ECH) ni la indicación de nombre de servidor cifrada (ESNI).

VPC Lattice puede ser oyente en HTTP, HTTPS, HTTP/1.1 y HTTP/2 y comunicarse con los destinatarios a través de cualquiera de estos protocolos y versiones. No es necesario que estas configuraciones de oyente y grupo de destinos coincidan. VPC Lattice administra todo el proceso de actualización y degradación entre protocolos y versiones. Para obtener más información, consulte Versión del protocolo.

Para asegurarte de que tu aplicación descifra el tráfico, crea un detector de TLS en su lugar. Con la transferencia TLS, VPC Lattice no termina TLS. Para obtener más información, consulte Oyentes de TLS.

Contenido

Política de seguridad

VPC Lattice utiliza una política de seguridad que es una combinación de un protocolo TLSv1 .2 y una lista de cifrados SSL/TLS. El protocolo establece una conexión segura entre un cliente y un servidor y ayuda a garantizar que todos los datos pasados entre el cliente y su servicio en VPC Lattice sean

privados. Un cifrado es un algoritmo de cifrado que usa claves de cifrado para crear un mensaje codificado. Los protocolos usan diversos cifrados para cifrar los datos. Durante el proceso de negociación de conexiones, el cliente y VPC Lattice presentan una lista con los cifrados y protocolos que admite cada uno por orden de preferencia. De forma predeterminada, el primer cifrado que se va a seleccionar para la conexión segura será el primero de la lista del servidor que coincida con uno de los cifrados del cliente.

VPC Lattice utiliza los siguientes cifrados TLS 1.2 SSL/TLS en este orden de preferencia:

- `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`

VPC Lattice también utiliza los siguientes cifrados TLS 1.3 SSL/TLS en este orden de preferencia:

- `TLS_AES_128_GCM_SHA256`
- `TLS_AES_256_GCM_SHA384`
- `TLS_CHACHA20_POLY1305_SHA256`

Política de ALPN

La negociación de protocolo de capa de aplicación (ALPN) es una extensión TLS que se envía en los mensajes de saludo iniciales de TLS. ALPN permite a la capa de aplicación negociar qué protocolos deben utilizarse a través de una conexión segura, como HTTP/1 y HTTP/2.

Cuando el cliente inicia una conexión de ALPN, el servicio VPC Lattice compara la lista de preferencias de ALPN del cliente con su política de ALPN. Si el cliente admite un protocolo de la política de ALPN, el servicio VPC Lattice establece la conexión según la lista de preferencias de la política de ALPN. De lo contrario, el servicio no utiliza ALPN.

VPC Lattice es compatible con la siguiente política de ALPN:

`HTTP2Preferred`

Se prefiere HTTP/2 sobre HTTP/1.1. La lista de preferencias de ALPN es h2, http/1.1.

Adición de un oyente HTTPS

Un oyente se configura con un protocolo y un puerto para las conexiones entre los clientes y el servicio, y también con un grupo de destino para la regla predeterminada del oyente. Para obtener más información, consulte Configuración del oyente.

Requisitos previos

- Para añadir una acción de reenvío a la regla predeterminada del oyente, debe especificar un grupo de destino de VPC Lattice disponible. Para obtener más información, consulte Creación de un grupo de destino de VPC Lattice.
- Puede especificar el mismo grupo de destino en varios oyentes, pero estos oyentes deben pertenecer al mismo servicio de VPC Lattice. Para utilizar un grupo de destino con un servicio de VPC Lattice, debe asegurarse de que ningún oyente lo utilice para otro servicio de VPC Lattice.
- Puede utilizar el certificado que proporciona VPC Lattice o importar su propio certificado a. AWS Certificate Manager Para obtener más información, consulte the section called “BYOC”.

Cómo agregar un oyente HTTPS mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Servicios.
3. Seleccione el nombre del servicio para abrir la página de detalles.
4. En la pestaña Enrutamiento, elija Agregar oyente.
5. Para Nombre del oyente, puede proporcionar un nombre personalizado o usar el protocolo y el puerto del oyente como el nombre del oyente. El nombre personalizado que especifique puede tener hasta 63 caracteres y debe ser único para cada servicio de su cuenta. Los caracteres válidos son a-z, 0-9 y guiones (-). No puede usar un guion como primer o último carácter, ni inmediatamente después de otro guion. No puede cambiar el nombre de un oyente después de crearlo.
6. En Protocolo: puerto, elija HTTPS e ingrese un número de puerto.
7. Como Acción predeterminada, elija el grupo de destino de VPC Lattice que recibirá el tráfico y la ponderación que quiera asignarle a este grupo. El peso que asigne a un grupo de destino

establece su prioridad para recibir tráfico. Por ejemplo, si dos grupos de destino tienen la misma ponderación, cada grupo recibe la mitad del tráfico. Si indicó un solo grupo de destino, el 100 por ciento del tráfico se enviará a ese grupo.

Si lo desea, puede agregar otro grupo de destino para la acción predeterminada. Seleccione Añadir acción y, a continuación, elija un grupo de destino e indique su ponderación.

8. (Opcional) Para añadir otra regla, elija Añadir regla y, a continuación, introduzca un nombre, una prioridad, una condición y una acción para la regla.

   Puede asignar a cada regla un número de prioridad entre 1 y 100. Un oyente no puede tener varias reglas con la misma prioridad. Las reglas se evalúan por orden de prioridad, desde el valor más bajo hasta el valor más alto. La regla predeterminada se evalúa en último lugar. Para obtener más información, consulte Reglas del oyente.

9. (Opcional) Para agregar etiquetas, diríjase a Etiquetas del oyente, elija Agregar nueva etiqueta e ingrese la clave y el valor de la etiqueta.

10. Para la configuración del certificado del oyente HTTPS, si no indicó un nombre de dominio personalizado al crear el servicio, VPC Lattice genera un certificado TLS automático para proteger el tráfico que fluye a través del oyente.

    Si creó el servicio con un nombre de dominio personalizado, pero no especificó un certificado compatible, puede hacerlo ahora mediante la elección del Certificado SSL/TLS personalizado. De lo contrario, el certificado que indicó al crear el servicio ya está elegido.

11. Verifique su configuración y luego elija Añadir.

Para agregar un oyente HTTPS mediante la AWS CLI

Utilice el comando create-listener para crear un oyente con una regla predeterminada y el comando create-rule para crear reglas adicionales para el oyente.

Oyentes TLS para servicios de VPC Lattice

Un oyente es un proceso que verifica solicitudes de conexión. Puede definir un oyente cuando crea su servicio VPC Lattice. Puede agregar oyentes a su servicio en todo momento.

Puede crear un agente de escucha de TLS para que VPC Lattice transmita el tráfico cifrado a sus aplicaciones sin descifrarlo.

Si prefiere que VPC Lattice descifre el tráfico cifrado y envíe el tráfico no cifrado a sus aplicaciones, cree un agente de escucha HTTPS en su lugar. Para obtener más información, consulte Oyentes HTTPS.

Consideraciones

Las siguientes consideraciones se aplican a los oyentes TLS:

- El servicio VPC Lattice debe tener un nombre de dominio personalizado. El nombre de dominio personalizado del servicio se utiliza como coincidencia con la indicación del nombre del servicio (SNI). Si especificó un certificado al crear el servicio, no se utilizará.
- La única regla permitida para un agente de escucha de TLS es la regla predeterminada.
- La acción predeterminada para un agente de escucha de TLS debe ser una acción de reenvío a un grupo objetivo de TCP.
- De forma predeterminada, las comprobaciones de estado están deshabilitadas para los grupos objetivo de TCP. Si habilita las comprobaciones de estado para un grupo objetivo de TCP, debe especificar un protocolo y una versión del protocolo.
- Los oyentes de TLS enrutan las solicitudes mediante el campo SNI del mensaje de saludo al cliente. Puede usar certificados comodín y SAN en sus destinos si la condición de coincidencia coincide exactamente con la del saludo del cliente.
- Como todo el tráfico permanece cifrado desde el cliente hasta el destino, VPC Lattice no puede leer los encabezados HTTP ni puede insertarlos ni eliminarlos. Por lo tanto, con un detector de TLS, existen las siguientes limitaciones:
  - La duración de la conexión está limitada a 10 minutos
  - Las políticas de autenticación se limitan a los directores anónimos
  - No se admiten los objetivos Lambda
- No se admite Encrypted Client Hello (ECH).
- No se admite la indicación de nombre de servidor cifrada (ESNI).

Agregación de un oyente TLS

Un oyente se configura con un protocolo y un puerto para las conexiones entre los clientes y el servicio, y también con un grupo de destino para la regla predeterminada del oyente. Para obtener más información, consulte Configuración del oyente.

Para agregar un oyente TLS mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Servicios.
3. Seleccione el nombre del servicio para abrir la página de detalles.
4. En la pestaña Enrutamiento, elija Agregar oyente.
5. Para Nombre del oyente, puede proporcionar un nombre personalizado o usar el protocolo y el puerto del oyente como el nombre del oyente. El nombre personalizado que especifique puede tener hasta 63 caracteres y debe ser único para cada servicio de su cuenta. Los caracteres válidos son a-z, 0-9 y guiones (-). No puede usar un guion como primer o último carácter, ni inmediatamente después de otro guion. No puede cambiar el nombre de un oyente después de crearlo.
6. En Protocol, elija TLS. En Puerto, introduzca un número de puerto.
7. En Reenviar al grupo de destino, elija un grupo de destino de VPC Lattice que utilice el protocolo TCP para recibir el tráfico y elija el peso que desee asignar a este grupo de destino. Si lo desea, puede añadir otro grupo de destino. Seleccione Añadir grupo de destino y, a continuación, elija un grupo de destino e introduzca su ponderación.
8. (Opcional) Para agregar etiquetas, diríjase a Etiquetas del oyente, elija Agregar nueva etiqueta e ingrese la clave y el valor de la etiqueta.
9. Revise su configuración y luego elija Añadir.

Para añadir un agente de escucha de TLS mediante el AWS CLI

Utilice el comando create-listener para crear un oyente con una regla predeterminada. Especifique el protocolo TLS_PASSTHROUGH.

Reglas del oyente para su servicio de VPC Lattice

Cada oyente tiene una regla predeterminada y reglas adicionales que puede definir. Cada regla consta de una prioridad, una o más acciones y una o más condiciones. Puede agregar y editar reglas en cualquier momento.

Contenido

Reglas predeterminadas

Cuando crea un oyente, define acciones para la regla predeterminada. Las reglas predeterminadas no pueden tener condiciones. Si no se cumplen las condiciones de ninguna de las reglas del oyente, se realiza la acción de la regla predeterminada.

Prioridad de las reglas

Cada regla tiene una prioridad. Las reglas se evalúan por orden de prioridad, desde el valor más bajo hasta el valor más alto. La regla predeterminada se evalúa en último lugar. Puede cambiar la prioridad de una regla no predeterminada en cualquier momento. No puede cambiar la prioridad de la regla predeterminada.

Acción de regla

Los oyentes de los servicios de VPC Lattice son compatibles con acciones de reenvío y acciones de respuestas fijas.

Acciones de reenvío

Puede utilizar acciones `forward` para direccionar solicitudes a uno o más grupos de destino de VPC Lattice. Si especifica varios grupos de destino para una acción `forward`, debe especificar una ponderación para cada grupo de destino. Cada ponderación de grupo de destino es un valor de 0 a 999. Las solicitudes que coinciden con una regla del oyente con los grupos de destino ponderados se distribuyen a estos grupos de destino en función de sus ponderaciones. Por ejemplo, si especifica dos grupos de destino, cada uno con una ponderación de 10, cada grupo de destino recibe la mitad de las solicitudes. Si especifica dos grupos de destino, uno con una ponderación de 10 y el otro con una ponderación de 20, el grupo de destino con una ponderación de 20 recibe el doble de solicitudes que el otro grupo de destino.

Acciones de respuesta fija

Puede utilizar acciones `fixed-response` para omitir las solicitudes del cliente y devolver una respuesta HTTP personalizada. Puede utilizar esta acción para devolver un código de respuesta 404 o 500.

Example Ejemplo de acción de respuesta fija para la AWS CLI

Puede especificar una acción al crear o actualizar una regla. La siguiente acción envía una respuesta fija con el código de estado especificado.

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

Condiciones de las reglas

Cada condición de regla tiene un tipo e información de configuración. Cuando se cumplen las condiciones de una regla, se llevan a cabo sus acciones.

Los siguientes son los criterios de coincidencia compatibles para una regla:

Coincidencia de encabezados

El enrutamiento está basado en los encabezados HTTP de cada solicitud. Puede utilizar las condiciones de encabezado HTTP para configurar reglas que dirijan solicitudes basadas en los encabezados HTTP para la solicitud. Puede especificar los nombres de campos de encabezado HTTP estándar o personalizados. El nombre del encabezado y la evaluación de coincidencia no distinguen entre mayúsculas y minúsculas. Puede cambiar esta configuración mediante la activación de la distinción entre mayúsculas y minúsculas. Los caracteres comodín no se admiten en el nombre del encabezado. Al hacer coincidir el encabezado, se admiten las coincidencias de prefijo, exactas y de contenido.

Coincidencia de métodos

El enrutamiento se basa en el método de solicitud HTTP de cada solicitud.

Puede utilizar las condiciones de método de solicitud HTTP para configurar reglas que dirijan solicitudes basadas en el método de solicitud HTTP de la solicitud. Puede especificar métodos

HTTP estándar o personalizados. La coincidencia distingue entre mayúsculas y minúsculas. El nombre del método debe ser una coincidencia exacta. No se admiten caracteres comodín.

Coincidencia de ruta

El enrutamiento se basa en hacer coincidir los patrones de ruta en la solicitud URLs.

Puede utilizar condiciones de ruta para definir reglas que enrutan solicitudes en función de la URL de la solicitud. No se admiten caracteres comodín. La coincidencia exacta y de prefijo en la ruta son compatibles.

Adición de una regla

Puede agregar una regla del oyente en todo momento.

Cómo agregar una regla de oyente a través de la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Servicios.
3. Seleccione el nombre del servicio para abrir la página de detalles.
4. En la pestaña Enrutamiento, elija Editar oyente.
5. Expanda las Reglas de oyente y elija Añadir regla.
6. En Nombre de la regla, ingrese el nombre de la regla.
7. Para Prioridad, introduzca una prioridad entre 1 y 100. Las reglas se evalúan por orden de prioridad, desde el valor más bajo hasta el valor más alto. La regla predeterminada se evalúa en último lugar.
8. En Condición, introduzca un patrón de ruta para la condición de coincidencia de ruta. El tamaño máximo de cada cadena es de 200 caracteres. Esta comparación no distingue entre mayúsculas y minúsculas. No se admiten caracteres comodín.

   Para agregar una condición de regla de coincidencia de encabezado o método, utilice la AWS CLI o un AWS SDK.
9. Para Acción, elija un grupo de destino de VPC Lattice.
10. Seleccione Save changes (Guardar cambios).

Para añadir una regla mediante el AWS CLI

Utilice el comando create-rule.

Actualización de una regla

Puede actualizar una regla del oyente en cualquier momento. Puede modificar su prioridad, condición, grupo de destino y ponderación de cada grupo de destino. No puede modificar el nombre de la regla.

Cómo actualizar una regla del oyente a través de la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Servicios.
3. Seleccione el nombre del servicio para abrir la página de detalles.
4. En la pestaña Enrutamiento, elija Editar oyente.
5. Modifique las prioridades, condiciones y acciones de la regla según sea necesario.
6. Revise las actualizaciones y seleccione Guardar cambios.

Cómo actualizar una regla mediante la AWS CLI

Utilice el comando update-rule.

Eliminar una regla

Puede eliminar las reglas no predeterminadas de un oyente en cualquier momento. No puede eliminar la regla predeterminada de un oyente. Cuando se elimina un oyente, se eliminan todas sus reglas.

Cómo eliminar un oyente a través de la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Servicios.
3. Seleccione el nombre del servicio para abrir la página de detalles.
4. En la pestaña Enrutamiento, elija Editar oyente.
5. Busque la regla y seleccione Eliminar.
6. Seleccione Save changes (Guardar cambios).

Para eliminar una regla mediante la AWS CLI

Utilice el comando delete-rule.

Elimine un oyente para su servicio VPC Lattice

Puede eliminar un oyente en cualquier momento. Cuando se elimina un oyente, se eliminan todas sus reglas de manera automática.

Cómo eliminar un oyente a través de la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Servicios.
3. Seleccione el nombre del servicio para abrir la página de detalles.
4. En la pestaña Enrutamiento, elija Agregar oyente.
5. Cuando le pidan confirmación, escriba **`confirm`** y elija Eliminar.

Para eliminar un oyente mediante la AWS CLI

Utilice el comando delete-listener.

Recursos de VPC en Amazon VPC Lattice

Puede compartir los recursos de VPC con otros equipos de su organización o con socios proveedores de software independientes (ISV) externos. Un recurso de VPC puede ser un recurso AWS nativo, como una base de datos de Amazon RDS, un nombre de dominio o una dirección IP. El recurso puede estar en tu VPC o en una red local y no es necesario que tenga un equilibrio de carga. Se utiliza AWS RAM para especificar los principales que pueden acceder al recurso. Usted crea una puerta de enlace de recursos a través de la cual se puede acceder a su recurso. También puede crear una configuración de recursos que represente el recurso o un grupo de recursos que desee compartir.

Los principales con los que comparte el recurso pueden acceder a estos recursos de forma privada mediante puntos de conexión de VPC. Pueden usar un punto de enlace de VPC de recursos para acceder a un recurso o agrupar varios recursos en una red de servicios de VPC Lattice y acceder a la red de servicios mediante un punto de enlace de VPC de red de servicio.

En las siguientes secciones, se explica cómo crear y administrar los recursos de VPC en VPC Lattice:

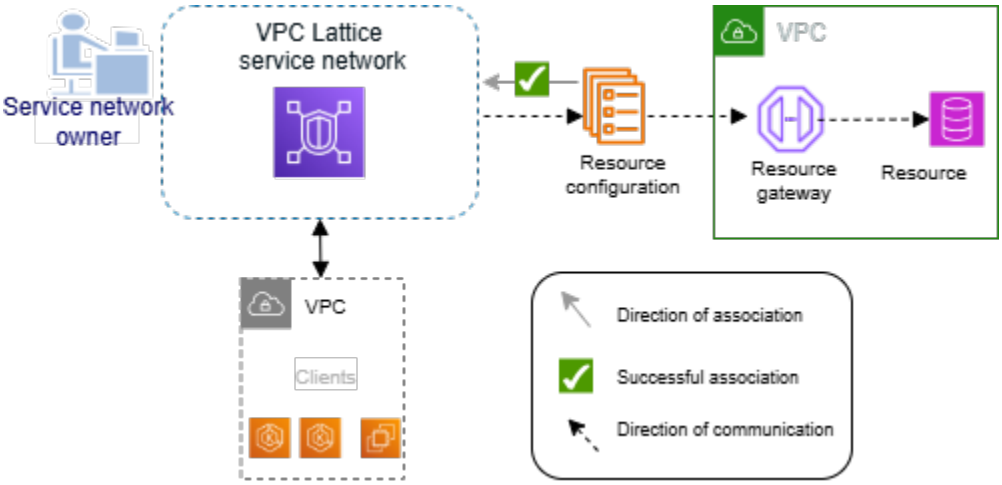
Temas

Pasarelas de recursos en VPC Lattice

Una puerta de enlace de recursos es el punto que recibe el tráfico hacia la VPC en la que reside un recurso. Abarca varias zonas de disponibilidad.

Una VPC debe tener una puerta de enlace de recursos si planea hacer que los recursos de la VPC sean accesibles desde otras cuentas o cuentas. VPCs Cada recurso que compartes está asociado a una puerta de enlace de recursos. Cuando los clientes de otras VPCs cuentas acceden a un recurso de su VPC, el recurso ve el tráfico que proviene localmente de la puerta de enlace de recursos de esa VPC. La dirección IP de origen del tráfico es la dirección IP de la puerta de enlace de recursos en una zona de disponibilidad. Se pueden adjuntar varias configuraciones de recursos, cada una con varios recursos, a una puerta de enlace de recursos.

El siguiente diagrama muestra cómo un cliente accede a un recurso a través de la puerta de enlace de recursos:



Contenido

Consideraciones

Las siguientes consideraciones se aplican a las pasarelas de recursos:

- Para que se pueda acceder a su recurso desde todas las zonas de disponibilidad, debe crear sus puertas de enlace de recursos para abarcar tantas zonas de disponibilidad como sea posible.
- Al menos una zona de disponibilidad del punto final de la VPC y la puerta de enlace de recursos deben superponerse.
- Una VPC puede tener un máximo de 100 puertas de enlace de recursos. Para obtener más información, consulte Cuotas para VPC Lattice.
- No puede crear una puerta de enlace de recursos en una subred compartida.

Grupos de seguridad

Puede adjuntar grupos de seguridad a una puerta de enlace de recursos. Las reglas de los grupos de seguridad para las puertas de enlace de recursos controlan el tráfico saliente desde la puerta de enlace de recursos a los recursos.

Reglas de salida recomendadas para el tráfico que fluye desde una puerta de enlace de recursos a un recurso de base de datos

Para que el tráfico fluya desde una puerta de enlace de recursos a un recurso, debe crear reglas de salida para los protocolos de escucha y los rangos de puertos aceptados por el recurso.

Destino	Protocolo	Intervalo de puertos	Comentario
CIDR range for resource	TCP	3306	Permite el tráfico desde la puerta de enlace de recursos a las bases de datos.

Tipos de direcciones IP

Una pasarela de recursos puede tener direcciones IPv4 de pila doble IPv6 o doble. El tipo de dirección IP de una puerta de enlace de recursos debe ser compatible con las subredes de la puerta de enlace de recursos y el tipo de dirección IP del recurso, tal y como se describe a continuación:

- IPv4— Asigne IPv4 direcciones a las interfaces de red de la puerta de enlace de recursos. Esta opción solo se admite si todas las subredes seleccionadas tienen rangos de IPv4 direcciones y el recurso también tiene una IPv4 dirección.
- IPv6— Asigne IPv6 direcciones a las interfaces de red de la puerta de enlace de recursos. Esta opción solo se admite si todas las subredes seleccionadas son IPv6 solo subredes y el recurso también tiene una IPv6 dirección.
- Dualstack: IPv4 asigne ambas IPv6 direcciones a las interfaces de red de la puerta de enlace de recursos. Esta opción solo se admite si todas las subredes seleccionadas tienen ambos rangos de IPv6 direcciones IPv4 y el recurso tiene una IPv4 dirección o. IPv6

El tipo de dirección IP de la puerta de enlace de recursos es independiente del tipo de dirección IP del cliente o del punto final de la VPC a través del cual se accede al recurso.

Cree una puerta de enlace de recursos en VPC Lattice

Utilice la consola para crear una puerta de enlace de recursos.

Requisito previo

Para crear una puerta de enlace de recursos, debe tener un bloque /28 disponible en una subred.

Para crear una puerta de enlace de recursos mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en Lattice, selecciona Resource Gateways. PrivateLink
3. Elija Crear puerta de enlace de recursos.
4. Introduzca un nombre que sea único en su AWS cuenta.
5. Elija el tipo de IP para la puerta de enlace de recursos.
6. Elija la VPC en la que se encuentra el recurso.
7. Elija hasta cinco grupos de seguridad para controlar el tráfico entrante desde la VPC a la red de servicio.
8. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
9. Elija Crear puerta de enlace de recursos.

Para crear una puerta de enlace de recursos mediante el AWS CLI

Utilice el comando create-resource-gateway.

Eliminar una puerta de enlace de recursos en VPC Lattice

Utilice la consola para eliminar una puerta de enlace de recursos.

Para eliminar una puerta de enlace de recursos mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en Lattice, selecciona Resource Gateways. PrivateLink
3. Seleccione la casilla de verificación de la pasarela de recursos que desee eliminar y elija Acciones, Eliminar. Cuando le pidan confirmación, escriba **`confirm`** y elija Eliminar.

Para eliminar una puerta de enlace de recursos mediante el AWS CLI

Utilice el comando delete-resource-gateway.

Configuraciones de recursos para recursos de VPC

Una configuración de recursos representa un recurso o un grupo de recursos que desea poner a disposición de los clientes de otras cuentas VPCs y cuentas. Al definir una configuración de recursos, puede permitir la conectividad de red unidireccional, segura y privada a los recursos de su VPC desde clientes de VPCs otras cuentas y. Una configuración de recursos está asociada a una puerta de enlace de recursos a través de la cual recibe tráfico. Para poder acceder a un recurso desde otra VPC, debe tener una configuración de recursos.

Contenido

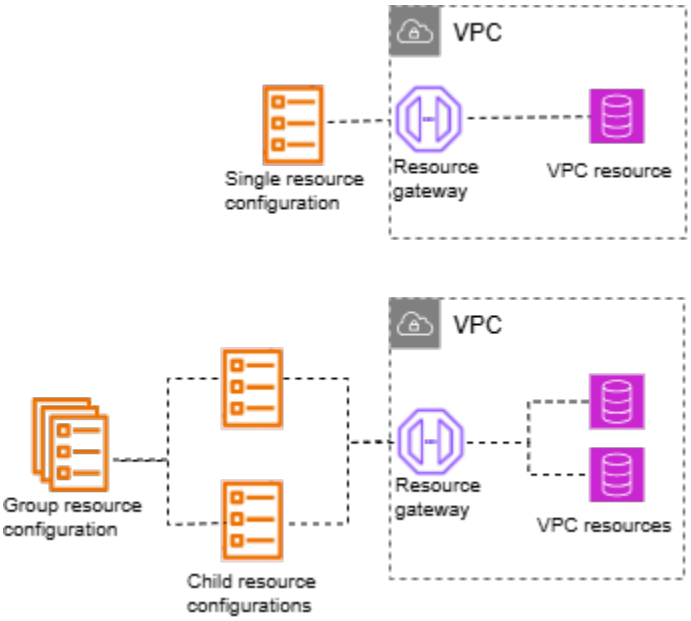
Tipos de configuraciones de recursos

Una configuración de recursos puede ser de varios tipos. Los distintos tipos ayudan a representar distintos tipos de recursos. Los tipos son:

- Configuración de un solo recurso: representa una dirección IP o un nombre de dominio. Se puede compartir de forma independiente.

- Configuración de recursos de grupo: es una colección de configuraciones de recursos secundarios. Se puede usar para representar un grupo de puntos finales de direcciones IP y DNS.
- Configuración de recursos secundarios: es miembro de una configuración de recursos de grupo. Representa una dirección IP o un nombre de dominio. No se puede compartir de forma independiente; solo se puede compartir como parte de un grupo. Se puede añadir y quitar de un grupo. Cuando se agrega, quienes pueden acceder al grupo pueden acceder automáticamente a él.
- Configuración de recursos del ARN: representa un tipo de recurso compatible aprovisionado por un servicio. AWS Cualquier relación grupo-hijo se gestiona automáticamente.

La siguiente imagen muestra una configuración de recursos individual, secundaria y grupal:



Pasarela de recursos

Una configuración de recursos está asociada a una puerta de enlace de recursos. Una puerta de enlace de recursos es un conjunto ENIs que sirve como punto de entrada a la VPC en la que se encuentra el recurso. Se pueden asociar varias configuraciones de recursos a la misma puerta de enlace de recursos. Cuando los clientes de otras VPCs cuentas acceden a un recurso de su VPC, el recurso ve el tráfico que proviene localmente de las direcciones IP de la puerta de enlace de recursos en esa VPC.

Definición de recursos

En la configuración del recurso, identifique el recurso de una de las siguientes maneras:

- Mediante un nombre de recurso de Amazon (ARN): los tipos de recursos admitidos que aprovisionan los AWS servicios se pueden identificar por su ARN. Solo se admiten las bases de datos de Amazon RDS. No puede crear una configuración de recursos para un clúster de acceso público.
- Por destino de nombre de dominio: puedes usar cualquier nombre de dominio que se pueda resolver públicamente. Si el nombre de dominio apunta a una IP que está fuera de la VPC, debe tener una puerta de enlace NAT en la VPC.
- Mediante una dirección IP: Para ello IPv4, especifique una IP privada de los siguientes rangos: 10.0.0.0/8, 100.64.0.0/10, 172.16.0.0/12, 192.168.0.0/16. Para IPv6, especifique una IP de la VPC. IPs No se admiten las públicas.

Protocolo

Al crear una configuración de recursos, puede definir los protocolos que admitirá el recurso. Actualmente, solo se admite el protocolo TCP.

Intervalos de puertos

Al crear una configuración de recursos, puede definir los puertos en los que aceptará las solicitudes. No se permitirá el acceso del cliente a otros puertos.

Acceso a recursos de

Los consumidores pueden acceder a las configuraciones de recursos directamente desde su VPC mediante un punto final de VPC o a través de una red de servicios. Como consumidor, puede habilitar el acceso desde su VPC a una configuración de recursos que esté en su cuenta o que se haya compartido con usted desde otra cuenta a través de ella. AWS RAM

- Acceder directamente a una configuración de recursos

  Puede crear un punto de enlace de AWS PrivateLink VPC de tipo recurso (punto de enlace de recurso) en su VPC para acceder a una configuración de recursos de forma privada desde su VPC. Para obtener más información sobre cómo crear un punto final de recursos, consulte Acceder a los recursos de VPC en la guía del AWS PrivateLink usuario.
- Acceder a una configuración de recursos a través de una red de servicios

Puede asociar una configuración de recursos a una red de servicio y conectar su VPC a la red de servicio. Puede conectar la VPC a la red de servicio mediante una asociación o mediante un punto final de VPC de la AWS PrivateLink red de servicio.

Para obtener más información sobre las asociaciones de redes de servicios, consulte Administrar las asociaciones de una red de servicios de VPC Lattice.

Para obtener más información sobre los puntos finales de VPC de la red de servicio, consulte Acceder a las redes de servicio en la guía del AWS PrivateLink usuario.

Cuando el DNS privado está habilitado para su VPC, no puede crear un extremo de recurso y un extremo de red de servicio para la misma configuración de recursos.

Asociación con el tipo de red de servicio

Al compartir una configuración de recursos con una cuenta de consumidor, por ejemplo, la cuenta B, la cuenta B puede acceder a la configuración de recursos directamente a través AWS RAM de un punto final de VPC de recursos o a través de una red de servicios.

Para acceder a una configuración de recursos a través de una red de servicios, la cuenta B tendría que asociar la configuración de recursos a una red de servicios. Las redes de servicios se pueden compartir entre cuentas. Por lo tanto, la cuenta B puede compartir su red de servicios (a la que está asociada la configuración de recursos) con la cuenta C, lo que permite acceder al recurso desde la cuenta C.

Para evitar este uso compartido transitivo, puedes especificar que tu configuración de recursos no se pueda añadir a las redes de servicios que se puedan compartir entre cuentas. Si lo especificas, la cuenta B no podrá agregar tu configuración de recursos a las redes de servicio compartidas o que se puedan compartir con otra cuenta en el futuro.

Tipos de redes de servicio

Al compartir una configuración de recursos con otra cuenta, por ejemplo, la Cuenta B, la Cuenta B puede acceder a AWS RAM los recursos especificados en la configuración de recursos de una de estas tres maneras:

- Uso de un punto final de VPC de tipo recurso (punto final de VPC de recurso).
- Uso de un punto final de VPC de tipo red de servicio (punto final de VPC de red de servicio).

- Uso de una asociación de VPC de red de servicio.

  Cuando se utiliza una asociación de red de servicio, a cada recurso se le asigna una IP por subred del bloque 129.224.0.0/17, que es propia y no se puede enrutar. AWS Esto se suma a la lista de prefijos administrados que VPC Lattice usa para enrutar el tráfico a los servicios a través de la red VPC Lattice. Ambos IPs se actualizan en la tabla de enrutamiento de la VPC.

Para el punto final de la VPC de la red de servicio y la asociación de VPC de la red de servicio, la configuración de recursos tendría que estar asociada a una red de servicio en la cuenta B. Las redes de servicio se pueden compartir entre cuentas. Por lo tanto, la cuenta B puede compartir su red de servicios (que contiene la configuración de recursos) con la cuenta C, lo que permite acceder al recurso desde la cuenta C. Para evitar que se comparta de forma transitiva, puedes impedir que tu configuración de recursos se añada a las redes de servicio que se pueden compartir entre cuentas. Si no lo permites, la cuenta B no podrá añadir tu configuración de recursos a una red de servicios que esté compartida o que pueda compartirse con otra cuenta.

Compartir configuraciones de recursos mediante AWS RAM

Las configuraciones de recursos están integradas con AWS Resource Access Manager. Puede compartir su configuración de recursos con otra cuenta a través de AWS RAM. Cuando compartes una configuración de recursos con una AWS cuenta, los clientes de esa cuenta pueden acceder al recurso de forma privada. Puede compartir una configuración de recursos mediante un recurso compartido en AWS RAM.

Utilice la AWS RAM consola para ver los recursos compartidos a los que se le ha agregado, los recursos compartidos a los que puede acceder y las AWS cuentas que han compartido recursos con usted. Para obtener más información, consulte los recursos que compartimos con usted en la Guía del AWS RAM usuario.

Para acceder a un recurso desde otra VPC de la misma cuenta que la configuración de recursos, no es necesario compartir la configuración de recursos a través de ella. AWS RAM

Monitorización

Puede habilitar los registros de supervisión en la configuración de sus recursos. Puede elegir un destino al que enviar los registros.

Crear una configuración de recursos en VPC Lattice

Utilice la consola para crear una configuración de recursos.

Para crear una configuración de recursos mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en Lattice PrivateLink y Lattice, elija Configuraciones de recursos.
3. Seleccione Crear configuración de recursos.
4. Introduzca un nombre que sea único en su AWS cuenta. No puede cambiar este nombre una vez creada la configuración de recursos.
5. En Tipo de configuración, elija Recurso para un recurso individual o secundario o Grupo de recursos para un grupo de recursos secundarios.
6. Elija una pasarela de recursos que haya creado anteriormente o cree una ahora.
7. Elija el identificador del recurso que desea que represente esta configuración de recursos.
8. Elija los rangos de puertos a través de los cuales desea compartir el recurso.
9. En Configuración de asociación, especifique si esta configuración de recursos se puede asociar a redes de servicios que se puedan compartir.
10. En la configuración de recursos compartidos, elija los recursos compartidos que identifiquen a los principales que pueden acceder a este recurso.
11. (Opcional) Para la supervisión, habilite los registros de acceso a los recursos y el destino de entrega si desea supervisar las solicitudes y las respuestas desde y hacia la configuración de recursos.
12. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
13. Seleccione Crear configuración de recursos.

Para crear una configuración de recursos mediante el AWS CLI

Utilice el comando create-resource-configuration.

Gestione las asociaciones para una configuración de recursos de VPC Lattice

Las cuentas de consumidor con las que comparte una configuración de recursos y los clientes de su cuenta pueden acceder a la configuración de recursos directamente mediante un punto de enlace de VPC de tipo recurso o a través de un punto de enlace de VPC de tipo service-network. Como resultado, la configuración de sus recursos tendrá asociaciones de puntos finales y asociaciones de redes de servicios.

Administre las asociaciones de redes de servicios

Cree o elimine una asociación de redes de servicios.

> **Note**
>
> Si recibe un mensaje de acceso denegado al crear la asociación entre la red de servicio y la configuración de los recursos, compruebe la versión de su AWS RAM política y asegúrese de que sea la versión 2. Para obtener más información, consulte la guía del AWS RAM usuario.

Para administrar una asociación de red de servicios mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en Lattice, selecciona PrivateLink Configuraciones de recursos.
3. Seleccione el nombre de la configuración de recursos para abrir su página de detalles.
4. Seleccione la pestaña Asociaciones de redes de servicios.
5. Elija Crear asociaciones.
6. Seleccione una red de servicios en Red de servicios de VPC Lattice. Para crear una red de servicios, elija Crear una red de VPC Lattice.
7. (Opcional) Para agregar una etiqueta, expanda Etiquetas de asociación de servicios, elija Agregar etiqueta nueva e ingrese una clave y un valor de etiqueta.
8. Seleccione Save changes (Guardar cambios).
9. Para eliminar una asociación, active la casilla de verificación de la asociación y, a continuación, elija Acciones, Eliminar. Cuando le pidan confirmación, escriba **`confirm`** y elija Eliminar.

Para crear una asociación de red de servicios mediante el AWS CLI

Utilice el comando create-service-network-resource-association.

Para eliminar una asociación de red de servicios mediante el AWS CLI

Utilice el comando delete-service-network-resource-association.

Gestione las asociaciones de puntos finales de VPC

Gestione una asociación de puntos finales de VPC.

Para administrar una asociación de puntos de conexión de VPC mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en PrivateLink y Lattice, selecciona Configuraciones de recursos.
3. Seleccione el nombre de la configuración de recursos para abrir su página de detalles.
4. Seleccione la pestaña Asociaciones de terminales.
5. Seleccione el ID de la asociación para abrir su página de detalles. Desde aquí, puede modificar o eliminar la asociación.
6. Para crear una nueva asociación de puntos de conexión, vaya a PrivateLink Lattice en el panel de navegación izquierdo y seleccione Puntos de conexión.
7. Seleccione Crear puntos de enlace.
8. Seleccione la configuración de recursos que desee conectar a la VPC.
9. Seleccione la VPC, las subredes y los grupos de seguridad.
10. (Opcional) Para etiquetar su punto final de VPC, elija Añadir nueva etiqueta e introduzca una clave de etiqueta y un valor de etiqueta.
11. Elija Crear punto de conexión.

Para crear una asociación de puntos de conexión de VPC mediante el AWS CLI

Utilice el comando create-vpc-endpoint.

Para eliminar una asociación de puntos de conexión de VPC mediante el AWS CLI

Utilice el comando delete-vpc-endpoint.

Comparta sus entidades de VPC Lattice

Amazon VPC Lattice se integra con AWS Resource Access Manager (AWS RAM) para permitir el uso compartido de servicios, configuraciones de recursos y redes de servicios. AWS RAM es un servicio que le permite compartir algunas entidades de VPC Lattice con otras Cuentas de AWS o a través de ellas. AWS Organizations Con AWS RAM, compartes entidades de tu propiedad mediante la creación de un recurso compartido. Un recurso compartido especifica las entidades que se van a compartir y los consumidores con los que se van a compartir. Los consumidores pueden incluir lo siguiente:

- Cuentas de AWS Específico dentro o fuera de su organización AWS Organizations.
- Una unidad organizativa dentro de la organización en AWS Organizations.
- Toda una organización en AWS Organizations.

Para obtener más información al respecto AWS RAM, consulte la Guía AWS RAM del usuario.

Contenido

Requisitos previos para compartir entidades de VPC Lattice

- Para compartir una entidad, debe ser su propietario. Cuenta de AWS Esto significa que la entidad debe estar asignada o aprovisionada en tu cuenta. No puedes compartir una entidad que se haya compartido contigo.
- Para compartir una entidad con tu organización o unidad organizativa AWS Organizations, debes habilitar la opción de compartir con AWS Organizations. Para obtener más información, consulte Habilitar el uso compartido de recursos dentro de AWS Organizations en la Guía del usuario de AWS RAM .

Comparta entidades de VPC Lattice

Para compartir una entidad, comience por crear un recurso compartido utilizando AWS Resource Access Manager. Un recurso compartido especifica las entidades que se van a compartir, los consumidores con los que se comparten y las acciones que pueden realizar los directores.

Cuando compartes una entidad de VPC Lattice de la que eres propietario con otra Cuentas de AWS, permites que esas cuentas asocien sus entidades a las entidades de tu cuenta. Al crear una asociación contra una entidad compartida, generamos un nombre de recurso de Amazon (ARN) en la cuenta del propietario de la entidad y en la cuenta que creó la asociación. Por lo tanto, tanto el propietario de la entidad como la cuenta que creó la asociación pueden eliminarla.

Si forma parte de una organización AWS Organizations y está habilitado el uso compartido dentro de su organización, los consumidores de su organización tienen acceso automático a la entidad compartida. De lo contrario, los consumidores reciben una invitación para unirse al recurso compartido y se les concede acceso a la entidad compartida tras aceptar la invitación.

Consideraciones

- Puede compartir tres tipos de entidades de VPC Lattice: redes de servicio, servicios y configuraciones de recursos.
- Puede compartir sus entidades de VPC Lattice con cualquiera. Cuenta de AWS
- No puede compartir sus entidades de VPC Lattice con usuarios y roles de IAM individuales.
- VPC Lattice admite permisos administrados por el cliente para servicios, configuraciones de recursos y redes de servicios.

Para compartir una entidad de su propiedad mediante la consola VPC Lattice

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, selecciona Servicios, Redes de servicios o Configuraciones de recursos.
3. Elija el nombre de la entidad para abrir su página de detalles y, a continuación, seleccione Compartir servicio, Compartir red de servicios o Compartir configuración de recursos en la pestaña Compartir.
4. Elija los AWS RAM recursos compartidos en Recursos compartidos. Para crear un recurso compartido, elija Crear un recurso compartido en la consola RAM.

5. Elija Compartir servicio, Compartir red de servicios o Compartir configuración de recursos.

Para compartir una entidad de tu propiedad mediante la AWS RAM consola

Utilice el procedimiento que se describe en Crear un recurso de uso compartido en la Guía del usuario de AWS RAM .

Para compartir una entidad de tu propiedad mediante el AWS CLI

Utilice el comando associate-resource-share.

Dejar de compartir entidades de VPC Lattice

Para dejar de compartir una entidad de VPC Lattice de su propiedad, debe eliminarla del recurso compartido. Las asociaciones existentes persisten después de dejar de compartir la entidad. No se permiten nuevas asociaciones a una entidad previamente compartida. Cuando el propietario de la entidad o el propietario de la asociación eliminan una asociación, esta se elimina de ambas cuentas. Si el propietario de una cuenta quiere dejar un recurso compartido, debe pedirle al propietario del recurso compartido que elimine su cuenta de la lista de cuentas con las que se compartió este recurso.

Para dejar de compartir una entidad de su propiedad mediante la consola VPC Lattice

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, selecciona Servicios, Redes de servicios o Configuraciones de recursos.
3. Elija el nombre de la entidad para abrir su página de detalles.
4. En la pestaña Compartir, seleccione la casilla de verificación del recurso compartido y, a continuación, elija Eliminar.

Para dejar de compartir una entidad de tu propiedad mediante la AWS RAM consola

Consulte Actualización de un recurso de uso compartido en la Guía del usuario de AWS RAM .

Para dejar de compartir una entidad de tu propiedad mediante el AWS CLI

Utilice el comando disassociate-resource-share.

Responsabilidades y permisos

Cuando se utilizan entidades de VPC Lattice compartidas, se aplican las siguientes responsabilidades y permisos.

Propietarios de entidades

- El propietario de la red de servicio no puede modificar un servicio que haya creado un consumidor.
- El propietario de la red de servicio no puede eliminar un servicio que haya creado un consumidor.
- El propietario de la red de servicio puede describir todas las asociaciones de servicio para la red de servicios.
- El propietario de la red de servicio puede desasociar cualquier servicio asociado a la red de servicios, independientemente de quién haya creado la asociación.
- El propietario de la red de servicio puede describir todas las asociaciones VPC para la red de servicio.
- El propietario de la red de servicio puede desasociar cualquier VPC que un consumidor asocie a la red de servicio.
- El propietario de la red de servicio puede describir todas las asociaciones de configuración de recursos de la red de servicio.
- El propietario de la red de servicio puede desasociar cualquier configuración de recursos asociada a la red de servicio, independientemente de quién haya creado la asociación.
- El propietario de la red de servicio puede describir todas las asociaciones de puntos finales de la red de servicio.
- El propietario de la red de servicio puede desasociar cualquier punto final asociado a la red de servicio, independientemente de quién haya creado la asociación.
- El propietario del servicio puede describir todas las asociaciones de la red de servicios con el servicio.
- El propietario del servicio puede desasociar un servicio de cualquier red de servicios a la que esté asociado.
- El propietario de la configuración de recursos puede describir todas las asociaciones de red con la configuración de recursos.
- El propietario de la configuración de recursos puede desasociar una configuración de recursos de cualquier red de servicios a la que esté asociada.

- El propietario del punto final de la VPC puede describir la red de servicio a la que está asociado.
- El propietario del punto final de la VPC puede disociar un punto final de la red de servicio.
- Solo la cuenta que creó una asociación puede actualizar la asociación entre la red de servicios y la VPC.

Consumidores de entidades

- El consumidor no puede eliminar una configuración de servicio o recurso que no haya creado.
- El consumidor solo puede disociar los servicios o las configuraciones de recursos que asoció a una red de servicios.
- El consumidor y el propietario de la red pueden describir todas las asociaciones entre una red de servicio y una configuración de servicio o recurso.
- El consumidor no puede recuperar la información de servicio de un servicio ni la información de configuración de recursos de una configuración de recursos que no sea de su propiedad.
- El consumidor puede describir todas las asociaciones de servicios y configuraciones de recursos con una red de servicios compartidos.
- El consumidor puede asociar un servicio o una configuración de recursos a una red de servicios compartidos.
- El consumidor puede ver todas las asociaciones VPC con una red de servicios compartidos.
- El consumidor puede asociar una VPC a una red de servicios compartidos.
- El consumidor solo puede disociar lo VPCs que asoció a una red de servicios.
- El consumidor puede crear un punto final de VPC de red de servicios para conectar su VPC a una red de servicios compartidos.
- El consumidor solo puede eliminar el punto final de la VPC de la red de servicio que creó para conectar su VPC a una red de servicios compartidos.
- El consumidor de un servicio compartido no puede asociar un servicio a una red de servicios que no le pertenecen.
- El consumidor de una red de servicios compartidos no puede asociar una VPC o un servicio que no le pertenece.
- El consumidor de una configuración de recursos compartidos no puede asociar una configuración de recursos a una red de servicios que no sea de su propiedad.
- El consumidor de una red de servicios compartidos no puede asociar una VPC o una configuración de servicio o recurso que no sea de su propiedad.

- El consumidor puede describir un servicio, una red de servicios o una configuración de recursos que comparta con él.
- El consumidor no puede asociar dos entidades si ambas se comparten con ellas.

Eventos entre cuentas

Cuando los propietarios de las entidades y los consumidores realizan acciones en una entidad compartida, esas acciones se registran como eventos multicuentas en AWS CloudTrail.

`CreateServiceNetworkResourceAssociationBySharee`

Se envía al propietario de la entidad cuando un consumidor de la entidad llama CreateServiceNetworkResourceAssociation a una entidad compartida. Si la persona que llama es propietaria de la configuración de recursos, el evento se envía al propietario de la red de servicio. Si la persona que llama es propietaria de la red de servicio, el evento se envía al propietario de la configuración de recursos.

`CreateServiceNetworkServiceAssociationBySharee`

Se envía al propietario de la entidad cuando un consumidor de la entidad llama CreateServiceNetworkServiceAssociationa una entidad compartida. Si la persona que llama es propietaria del servicio, el evento se envía al propietario de la red de servicios. Si la persona que llama es propietaria de la red de servicio, el evento se envía al propietario del servicio.

`CreateServiceNetworkVpcAssociationBySharee`

Se envía al propietario de la entidad cuando un consumidor de la entidad llama CreateServiceNetworkVpcAssociationa través de una red de servicios compartidos.

`DeleteServiceNetworkResourceAssociationByOwner`

Se envía al propietario de la asociación cuando el propietario de la entidad llama DeleteServiceNetworkResourceAssociation a una entidad compartida. Si la persona que llama es propietaria de la configuración de recursos, el evento se envía al propietario de la asociación de la red de servicios. Si la persona que llama es propietaria de la red de servicio, el evento se envía al propietario de la asociación de recursos.

`DeleteServiceNetworkResourceAssociationBySharee`

Se envía al propietario de la entidad cuando un consumidor de la entidad llama DeleteServiceNetworkResourceAssociation a una entidad compartida. Si la persona que llama es

propietaria de la configuración de recursos, el evento se envía al propietario de la red de servicio. Si la persona que llama es propietaria de la red de servicio, el evento se envía al propietario de la configuración de recursos.

`DeleteServiceNetworkServiceAssociationByOwner`

Se envía al propietario de la asociación cuando el propietario de la entidad llama DeleteServiceNetworkServiceAssociationa una entidad compartida. Si la persona que llama es propietaria del servicio, el evento se envía al propietario de la asociación de redes de servicios. Si la persona que llama es propietaria de la red de servicios, el evento se envía al propietario de la asociación de servicios.

`DeleteServiceNetworkServiceAssociationBySharee`

Se envía al propietario de la entidad cuando un consumidor de la entidad llama DeleteServiceNetworkServiceAssociationa una entidad compartida. Si la persona que llama es propietaria del servicio, el evento se envía al propietario de la red de servicios. Si la persona que llama es propietaria de la red de servicio, el evento se envía al propietario del servicio.

`DeleteServiceNetworkVpcAssociationByOwner`

Se envía al propietario de la asociación cuando el propietario de la entidad llama DeleteServiceNetworkVpcAssociationa través de una red de servicios compartidos.

`DeleteServiceNetworkVpcAssociationBySharee`

Se envía al propietario de la entidad cuando un consumidor de la entidad llama DeleteServiceNetworkVpcAssociationa través de una red de servicios compartidos.

`GetServiceBySharee`

Se envía al propietario de la entidad cuando un consumidor de la entidad llama GetServicecon un servicio compartido.

`GetServiceNetworkBySharee`

Se envía al propietario de la entidad cuando un consumidor de la entidad llama GetServiceNetworka través de una red de servicios compartidos.

`GetServiceNetworkResourceAssociationBySharee`

Se envía al propietario de la entidad cuando un consumidor de la entidad llama GetServiceNetworkResourceAssociation a una entidad compartida. Si la persona que llama es propietaria de la configuración de recursos, el evento se envía al propietario de la red de servicio.

Si la persona que llama es propietaria de la red de servicio, el evento se envía al propietario de la configuración de recursos.

`GetServiceNetworkServiceAssociationBySharee`

Se envía al propietario de la entidad cuando un consumidor de la entidad llama GetServiceNetworkServiceAssociationa una entidad compartida. Si la persona que llama es propietaria del servicio, el evento se envía al propietario de la red de servicios. Si la persona que llama es propietaria de la red de servicio, el evento se envía al propietario del servicio.

`GetServiceNetworkVpcAssociationBySharee`

Se envía al propietario de la entidad cuando un consumidor de la entidad llama GetServiceNetworkVpcAssociationa través de una red de servicios compartidos.

A continuación, se ve un ejemplo de una entrada para el evento `CreateServiceNetworkServiceAssociationBySharee`.


```
{
    "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"
}
```

Celosía de VPC para Oracle Database@AWS

VPC Lattice potencia las integraciones de servicios AWS gestionados para Oracle Database@AWS(ODB) y le proporciona una conectividad simplificada entre la red ODB y las instalaciones. AWS VPCs Para respaldar esta conectividad, VPC Lattice aprovisiona las siguientes entidades en su nombre:

Red de servicio predeterminada

La red de servicio predeterminada usa la convención de nomenclatura `default-odb-network-randomHash`

Punto final de la red de servicio predeterminado

No hay ningún nombre para este AWS recurso.

Pasarela de recursos

La pasarela de recursos utiliza la convención de nomenclatura `default-odb-network-randomHash`

VPC Lattice admite las integraciones de servicios AWS gestionados, denominadas integraciones gestionadas, en su red ODB. De forma predeterminada, está activado Managed Backup to Amazon S3 de Oracle Cloud Infrastructure (OCI). Puede optar por habilitar el acceso autogestionado a Amazon S3 y Zero-ETL.

Una vez que haya creado su red ODB, podrá ver los recursos aprovisionados mediante la tecla o. AWS Management Console AWS CLI El siguiente comando de ejemplo muestra las integraciones administradas predeterminadas de la red ODB y cualquier otro recurso que pueda tener para esta red de servicios:

```
aws vpc-lattice list-service-network-resource-associations \
        --service-network-identifier default-odb-network-randomHash
```

Consideraciones

Las siguientes consideraciones se aplican a VPC Lattice para: Oracle Database@AWS

- No puedes eliminar la red de servicios predeterminada, el punto final de la red de servicios, la puerta de enlace de recursos ni ninguna integración gestionada por ODB proporcionada por

VPC Lattice. Para eliminar estas entidades, elimina tu red ODB o desactiva las integraciones gestionadas.

- Los clientes solo pueden acceder a las integraciones administradas en la red ODB. Los clientes que se encuentran fuera de la red ODB, como la suya VPCs, no pueden usar estas integraciones administradas para acceder a S3 o Zero-ETL.
- No puedes conectarte a ninguna de las integraciones gestionadas fuera de la red ODB aprovisionada por VPC Lattice.
- Todo el tráfico a Amazon S3 pasa por el punto de conexión de la red de servicio predeterminado y se aplican los cargos de procesamiento estándar por el acceso a los recursos. Todo el tráfico sin ETL pasa por la pasarela de recursos y se aplican los cargos estándar de procesamiento de datos por los recursos que usted comparte. Para obtener más información, consulte los precios de VPC Lattice.
- No se cobran cargos por hora para las integraciones Oracle Database@AWS gestionadas.
- Puede gestionar los recursos aprovisionados por VPC Lattice como cualquier otra red de servicios. Puede compartir la red de servicios predeterminada con otras Cuentas de AWS organizaciones y agregar nuevos puntos finales, asociaciones de VPC, servicios y recursos de VPC Lattice a la red predeterminada.
- Se requieren los siguientes permisos para que VPC Lattice aprovisione recursos: Oracle Database@AWS

  JSON

```
{
 "Version": "2012-10-17",
 "Statement": [
     {
         "Sid": "AllowODBEC2andLatticeActions",
         "Action": [
             "ec2:DescribeVpcs",
             "ec2:CreateTags",
             "ec2:DescribeAvailabilityZones",
             "ec2:CreateOdbNetworkPeering",
             "ec2:DeleteOdbNetworkPeering",
             "ec2:ModifyOdbNetworkPeering",
             "ec2:DescribeVpcEndpointAssociations",
             "ec2:CreateVpcEndpoint",
             "ec2:DeleteVpcEndpoints",
             "ec2:DescribeVpcEndpoints",
             "vpc-lattice:CreateServiceNetwork",
```

```
                "vpc-lattice:DeleteServiceNetwork",
                "vpc-lattice:GetServiceNetwork",
                "vpc-lattice:CreateServiceNetworkResourceAssociation",
                "vpc-lattice:DeleteServiceNetworkResourceAssociation",
                "vpc-lattice:GetServiceNetworkResourceAssociation",
                "vpc-lattice:CreateResourceGateway",
                "vpc-lattice:DeleteResourceGateway",
                "vpc-lattice:GetResourceGateway",
                "vpc-lattice:CreateServiceNetworkVpcEndpointAssociation"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
    "Sid": "AllowSLRActionsForLattice",
    "Effect": "Allow",
    "Action": [
     "iam:CreateServiceLinkedRole"
    ],
    "Resource": "*",
     "Condition": {
      "StringEquals": {
       "iam:AWSServiceName": [
        "vpc-lattice.amazonaws.com"
       ]
      }
     }
   }
    ]
}
```

Para usar VPC Lattice, le recomendamos que esté familiarizado con las redes de servicios Oracle Database@AWS, las asociaciones de redes de servicios y las puertas de enlace de recursos de VPC Lattice.

Temas

- the section called “Backup gestionado de Oracle Cloud Infrastructure (OCI) en Amazon S3”
- the section called “Acceso a Amazon S3”
- the section called “ETL cero para Amazon Redshift”
- the section called “Acceda a entidades de VPC Lattice y compártalas”

Backup gestionado de Oracle Cloud Infrastructure (OCI) en Amazon S3

Al crear una Oracle Database@AWS base de datos, VPC Lattice crea una configuración de recursos llamada. `odb-managed-s3-backup-access` Esta configuración de recursos representa una copia de seguridad gestionada por OCI de sus bases de datos en Amazon S3 y solo permite la conectividad con los buckets de Amazon S3 propiedad de OCI. El tráfico entre la red ODB y S3 nunca sale de la red Amazon.

Acceso a Amazon S3

Además del OCI Managed Backup to Amazon S3, puede crear una integración gestionada que permita el acceso a Amazon S3 desde la red ODB. Al modificar la Oracle Database@AWS red para habilitar la integración gestionada de Amazon S3 Access, VPC Lattice aprovisiona una configuración de recursos denominada `odb-s3-access` en la red de servicio predeterminada. Puede utilizar esta integración para acceder a Amazon S3 para sus propias necesidades, incluidas las copias de seguridad o restauraciones autogestionadas. Puede establecer el control perimetral proporcionando una política de autenticación.

Consideraciones

Las siguientes son consideraciones para la integración gestionada de Amazon S3 Access:

- Solo puede crear una integración gestionada de Amazon S3 Access para la red ODB.
- Esta integración gestionada permite el acceso a Amazon S3 únicamente desde la red ODB y no desde otras asociaciones de VPC o puntos de enlace de la red de servicios de la red de servicios predeterminada.
- No puede acceder a los buckets de S3 en distintas regiones. AWS

Habilite la integración gestionada de Amazon S3 Access

Utilice el siguiente comando para habilitar la integración gestionada de Amazon S3 Access:

```
aws odb update-odb-network \
  --odb-network-id odb-network-id \
  --s3-access ENABLED
```

Proteja el acceso con una política de autenticación

Puede proteger el acceso a los buckets de S3 definiendo una política de autenticación mediante la API de ODB. El siguiente ejemplo de política otorga acceso a buckets de S3 específicos que son propiedad de una organización específica.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "Policy1515115909152",
  "Statement": [
    {
      "Sid": "GrantAccessToMyOrgS3",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::awsexamplebucket1",
        "arn:aws:s3:::awsexamplebucket1/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceOrgID": "o-abcd1234"
        }
      }
    }
  ]
}
```

> **Note**
>
> Las claves de `aws:VpcSourceIp` condición `aws:SourceVpcaws:SourceVpce`, y no son compatibles con las políticas de bucket de S3 cuando se utilizan integraciones gestionadas por ODB.

ETL cero para Amazon Redshift

Puede usar la red de servicios proporcionada por VPC Lattice para habilitar Zero-ETL. Esta integración gestionada conecta las bases de datos de la red ODB a Amazon Redshift para ayudar a analizar los datos de distintas bases de datos. Puede iniciar la configuración sin ETL mediante la AWS Glue integración APIs y utilizar la ODB APIs para activar la integración gestionada y configurar la ruta de red. Para obtener más información, consulte Integración sin ETL con Amazon Redshift.

Consideraciones

Las siguientes son consideraciones para la integración gestionada sin ETL:

- Si habilita la integración gestionada sin ETL, solo podrá usar sin ETL para acceder a las instancias de su red ODB. Otros servicios y recursos asociados a su red de servicios están aislados del ETL cero.

Acceda a entidades de VPC Lattice y compártalas

También puede conectar su red ODB a servicios, recursos y otros clientes VPCs mediante VPC Lattice. Estas opciones de conectividad se alimentan a través de la red de servicio predeterminada, la puerta de enlace de recursos y el punto final de la red de servicios proporcionados por VPC Lattice.

Acceda a los servicios y recursos de VPC Lattice

Para acceder a otras entidades, asocie los servicios o recursos que le pertenezcan o que compartan con usted a la red de servicios predeterminada. Los clientes de la red ODB pueden acceder a los servicios o recursos a través del punto final de la red de servicios predeterminado.

Consideraciones

Las siguientes son consideraciones para conectarse a otras entidades de VPC Lattice:

- Puede añadir nuevos puntos de conexión de red de servicios, asociaciones de VPC, recursos y servicios de VPC Lattice a la red de servicios, pero no puede modificar los recursos aprovisionados por VPC Lattice en nombre de la red ODB. Estos deben Oracle Database@AWS APIs gestionarse a través de.

Comparta su red ODB a través de VPC Lattice

Puede compartir los recursos de su red ODB con clientes de otras VPCs cuentas o locales. Para empezar, cree una configuración de recursos para los recursos que desee compartir. Las configuraciones de recursos deben usar la puerta de enlace de recursos predeterminada para la red ODB. A continuación, puede asociar los recursos a la red de servicios predeterminada.

Los clientes de otra red de servicios VPCs o con los Cuentas de AWS que hayas compartido tu red pueden acceder a estos recursos a través de sus propios puntos finales de red de servicios o asociaciones de VPC. Para obtener más información, consulte the section called “Gestión de asociaciones”.

Consideraciones

Las siguientes son consideraciones para compartir su red ODB:

- Recomendamos compartir únicamente las instancias de red ODB como recursos basados en IP.
- VPC Lattice no admite el DNS de escucha del nombre de acceso de cliente único (SCAN) de OCI.

Seguridad en Amazon VPC Lattice

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los AWS servicios en la. Nube de AWS AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los AWS programas de de . Para obtener más información sobre los programas de conformidad que se aplican a Amazon VPC Lattice, consulte AWS Servicios dentro del alcance por programa de conformidad AWS Servicios dentro del alcance por programa .
- Seguridad en la nube: usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza VPC Lattice. En los siguientes temas, se le mostrará cómo configurar VPC Lattice para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger su servicio VPC Lattice, las redes de servicios y las configuraciones de recursos.

Contenido

Gestione el acceso a los servicios de VPC Lattice

VPC Lattice es seguro de forma predeterminada porque debe ser explícito en cuanto a los servicios y configuraciones de recursos a los que se debe proporcionar acceso y con cuáles. VPCs Puede acceder a los servicios a través de una asociación de VPC o un punto final de VPC de tipo red de servicio. En escenarios con varias cuentas, puede utilizarlos AWS Resource Access Managerpara compartir servicios, configuraciones de recursos y redes de servicios entre cuentas.

VPC Lattice proporciona un marco que le permite implementar una estrategia defense-in-depth en varias capas de la red.

- Primera capa: asociación del servicio, el recurso, la VPC y el punto final de la VPC con una red de servicio. Una VPC puede conectarse a una red de servicio mediante una asociación o mediante un punto final de VPC. Si una VPC no está conectada a una red de servicio, los clientes de la VPC no pueden acceder a las configuraciones de servicios y recursos asociadas a la red de servicios.
- Segundo nivel: protecciones de seguridad opcionales a nivel de red para la red de servicio, como los grupos de seguridad y la red. ACLs Al usarlos, puede permitir el acceso a grupos específicos de clientes en una VPC en lugar de a todos los clientes de la VPC.
- Tercera capa: política de autenticación opcional de VPC Lattice. Puede aplicar una política de autenticación a redes de servicio y a servicios individuales. ry streamPor lo general, el administrador de la red o de la nube es quien gestiona la política de autenticación de la red de servicio e implementa una autorización básica. Por ejemplo, al permitir solo solicitudes autenticadas de una organización específica en AWS Organizations. En el caso de una política de autenticación a nivel de servicio, normalmente el propietario del servicio establece controles exhaustivos, que pueden ser más restrictivos que la autorización básica que se aplica a nivel de la red de servicio.

> **Note**
>
> La política de autenticación de la red de servicios no se aplica a las configuraciones de recursos de la red de servicios.

Métodos de control de acceso

- Políticas de autenticación
- Grupos de seguridad

- Red ACLs

Controle el acceso a los servicios de VPC Lattice mediante políticas de autenticación

Las políticas de autenticación de VPC Lattice son documentos de políticas de IAM que se adjuntan a las redes de servicios o servicios para controlar si una entidad principal específica tiene acceso a un grupo de servicios o a un servicio específico. Puede adjuntar una política de autenticación a cada red de servicio o servicio cuyo acceso quiera controlar.

> **Note**
>
> La política de autenticación de la red de servicios no se aplica a las configuraciones de recursos de la red de servicios.

Las políticas de autenticación difieren de las políticas basadas en entidades de IAM. Las políticas basadas en identidad de IAM se asocian a usuarios, grupos o roles de IAM y definen qué acciones pueden realizar esas identidades y en qué recursos. Las políticas de autenticación están asociadas a los servicios y a las redes de servicios. Para que la autorización funcione, tanto las políticas de autenticación como las políticas basadas en identidades deben incluir instrucciones de autorización explícitas. Para obtener más información, consulte Cómo funciona la autorización.

Puede usar la consola AWS CLI y para ver, agregar, actualizar o eliminar las políticas de autenticación en los servicios y las redes de servicios. Cuando agregas, actualizas o eliminas una política de autenticación, es posible que tarde unos minutos en estar lista. Cuando utilices AWS CLI, asegúrate de que te encuentras en la región correcta. Puede cambiar la región predeterminada de su perfil o utilizar el `--region` parámetro con el comando.

Contenido

Para empezar a utilizar las políticas de autenticación, siga el procedimiento para crear una política de autenticación que se aplique a una red de servicios. Para obtener permisos más restrictivos que no quieran que se apliquen a otros servicios, puede optar por establecer políticas de autenticación en servicios individuales.

Administración del acceso a una red de servicios con políticas de autenticación

Las siguientes AWS CLI tareas muestran cómo administrar el acceso a una red de servicios mediante políticas de autenticación. Para obtener instrucciones sobre cómo utilizar la consola, consulte Redes de servicios en VPC Lattice.

Tareas

- Cómo agregar una política de autenticación a una red de servicios
- Cambio del tipo de autenticación de una red de servicios
- Eliminación de una política de autenticación de una red de servicios

Cómo agregar una política de autenticación a una red de servicios

Siga los pasos de esta sección para utilizarlos AWS CLI para:

- Habilite el control de acceso de una red de servicios mediante IAM.
- Agregue una política de autenticación a la red de servicios. Si no agrega una política de autenticación, todo el tráfico recibirá un error de acceso denegado.

Para habilitar el control de acceso y agregar una política de autenticación a una nueva red de servicios

1. Para habilitar el control de acceso de una red de servicios para que pueda usar una política de autenticación, utilice el comando create-service-network con la opción `--auth-type` y un valor de `AWS_IAM`.

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

   Si se ejecuta correctamente, el comando devolverá información similar a la siguiente.

   ```
   {
      "arn": "arn",
   ```

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

2. Use el comando put-auth-policy y especifique el ID de la red de servicios a la que desea agregar la política de autenticación y la política de autenticación que desea agregar.

   Por ejemplo, utilice el siguiente comando para crear una política de autenticación para la red de servicios con el ID *sn-0123456789abcdef0*.

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

   Use JSON para crear una definición de política. Para obtener más información, consulte Elementos comunes de una política de autenticación.

   Si se ejecuta correctamente, el comando devolverá información similar a la siguiente.

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

Cómo habilitar el control de acceso y añadir una política de autenticación a una red de servicios existente

1. Para habilitar el control de acceso de una red de servicios para que pueda usar una política de autenticación, utilice el comando update-service-network con la opción `--auth-type` y un valor de `AWS_IAM`.

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

   Si se ejecuta correctamente, el comando devolverá información similar a la siguiente.

   ```
   {
      "arn": "arn",
      "authType": "AWS_IAM",
   ```

```
   "id": "sn-0123456789abcdef0",
   "name": "Name"
}
```

2. Use el comando put-auth-policy y especifique el ID de la red de servicios a la que desea agregar la política de autenticación y la política de autenticación que desea agregar.

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

Use JSON para crear una definición de política. Para obtener más información, consulte Elementos comunes de una política de autenticación.

Si se ejecuta correctamente, el comando devolverá información similar a la siguiente.

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

Cambio del tipo de autenticación de una red de servicios

Cómo deshabilitar la política de autenticación de una red de servicios

Utilice el comando update-service-network con la opción `--auth-type` y un valor de `NONE`.

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

Si necesita volver a habilitar la política de autenticación más adelante, ejecute este comando con el `AWS_IAM` especificado para la opción `--auth-type`.

Eliminación de una política de autenticación de una red de servicios

Cómo eliminar una política de autenticación de una red de servicios

Utilice el comando delete-auth-policy.

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

La solicitud falla si elimina una política de autenticación antes de cambiar el tipo de autenticación de una red de servicios a `NONE`.

Administración del acceso a un servicio con políticas de autenticación

Las siguientes AWS CLI tareas muestran cómo administrar el acceso a un servicio mediante políticas de autenticación. Para obtener instrucciones sobre cómo utilizar la consola, consulte Servicios en VPC Lattice.

Tareas

- Adición de una política de autenticación a un servicio
- Cambio de un tipo de autenticación de servicio
- Eliminación de una política de autenticación de un servicio

Adición de una política de autenticación a un servicio

Siga estos pasos para utilizarlos AWS CLI para:

- Habilite el control de acceso de un servicio mediante IAM.
- Agregue una política de autenticación al servicio. Si no agrega una política de autenticación, todo el tráfico recibirá un error de acceso denegado.

Cómo habilitar el control de acceso y agregar una política de autenticación a un nuevo servicio

1. Para habilitar el control de acceso de un servicio para que pueda usar una política de autenticación, utilice el comando create-service con la opción `--auth-type` y un valor de `AWS_IAM`.

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

   Si se ejecuta correctamente, el comando devolverá información similar a la siguiente.

   ```
   {
      "arn": "arn",
      "authType": "AWS_IAM",
      "dnsEntry": {
         ...
      },
   ```

```
   "id": "svc-0123456789abcdef0",
   "name": "Name",
   "status": "CREATE_IN_PROGRESS"
}
```

2. Use el comando put-auth-policy y especifique el ID del servicio al que desea agregar la política de autenticación y la política de autenticación que desea agregar.

   Por ejemplo, usa el siguiente comando para crear una política de autenticación para el servicio con el ID*svc-0123456789abcdef0*.

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

   Use JSON para crear una definición de política. Para obtener más información, consulte Elementos comunes de una política de autenticación.

   Si se ejecuta correctamente, el comando devolverá información similar a la siguiente.

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

Cómo habilitar el control de acceso y añadir una política de autenticación a un servicio existente

1. Para habilitar el control de acceso de un servicio para que pueda usar una política de autenticación, utilice el comando update-service con la opción `--auth-type` y un valor de `AWS_IAM`.

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

   Si se ejecuta correctamente, el comando devolverá información similar a la siguiente.

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

```
}
```

2. Use el comando put-auth-policy y especifique el ID del servicio al que desea agregar la política de autenticación y la política de autenticación que desea agregar.

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

Use JSON para crear una definición de política. Para obtener más información, consulte Elementos comunes de una política de autenticación.

Si se ejecuta correctamente, el comando devolverá información similar a la siguiente.

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

Cambio de un tipo de autenticación de servicio

Cómo deshabilitar la política de autenticación de un servicio

Utilice el comando update-service con la opción `--auth-type` y un valor de `NONE`.

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

Si necesita volver a habilitar la política de autenticación más adelante, ejecute este comando con el `AWS_IAM` especificado para la opción `--auth-type`.

Eliminación de una política de autenticación de un servicio

Cómo eliminar una política de autenticación de un servicio

Utilice el comando delete-auth-policy.

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

La solicitud falla si elimina una política de autenticación antes de cambiar el tipo de autenticación del servicio a `NONE`.

Si habilita políticas de autenticación que requieren solicitudes autenticadas para un servicio, todas las solicitudes para ese servicio deben contener una firma de solicitud válida que se calcule con Signature Version 4 (SigV4). Para obtener más información, consulte SIGv4 solicitudes autenticadas para Amazon VPC Lattice.

Elementos comunes de una política de autenticación

Las políticas de autenticación de VPC Lattice se especifican utilizando la misma sintaxis que para las políticas de IAM. Para obtener más información, consulte Políticas basadas en identidad y políticas basadas en recursos en la Guía del usuario de IAM.

Una política de autenticación contiene los siguientes elementos:

- Entidad principal: la persona o la aplicación con permiso de acceso a las acciones y los recursos en la instrucción. En una política de autenticación, la entidad principal es la entidad de IAM que recibe este permiso. La entidad principal se autentica como entidad de IAM para realizar solicitudes a un recurso o grupo de recursos específico, como en el caso de los servicios de una red de servicios.

  Debe especificar una entidad principal en una política basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o servicios. AWS Para obtener más información, consulte Elementos de la política de JSON de AWS : entidad principal en la Guía del usuario de IAM.
- Efecto: el efecto cuando la entidad principal específica solicita la acción específica. Puede ser `Allow` o `Deny`. De forma predeterminada, cuando se habilita el control de acceso de un servicio o una red de servicios mediante IAM, las entidades principales no tienen permisos para realizar solicitudes al servicio o a la red de servicios.
- Acciones: la acción específica de la API para la que se concede o deniega el permiso. VPC Lattice admite acciones que usan el prefijo. `vpc-lattice-svcs` Para obtener más información, consulte las acciones definidas por Amazon VPC Lattice Services en la Referencia de autorización de servicios.
- Recursos: los servicios que se ven afectados por la acción.
- Condición: las condiciones son opcionales. Puede utilizarlas para controlar cuándo entra en vigor su política. Para obtener más información, consulte Claves de condición de los servicios de Amazon VPC Lattice en la Referencia de autorización de servicios.

Al crear y administrar las políticas de autenticación, es posible que quiera usar el generador de políticas de IAM.

Requisito

La política de JSON no debe contener líneas nuevas o líneas en blanco.

Formato de recurso para políticas de autenticación

Puede restringir el acceso a recursos específicos al crear una política de autenticación que utilice un esquema coincidente con un patrón `<serviceARN>/<path>` y codificar el elemento `Resource`, como se muestra en los siguientes ejemplos.

Protocolo	Ejemplos
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/*"`

Utilice el siguiente formato de nombre de recurso de Amazon (ARN) para `<serviceARN>`:

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

Por ejemplo:

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

Claves de condición que se pueden utilizar en políticas de autenticación

El acceso puede controlarse aún más mediante las claves de condición en el elemento Condición de las políticas de autenticación. Estas claves de condición están presentes para su evaluación en función del protocolo y de si la solicitud está firmada con Signature Version 4 (SigV4) o es anónima. Las claves de condición distinguen entre mayúsculas y minúsculas.

AWS proporciona claves de condición globales que puede usar para controlar el acceso, como `aws:PrincipalOrgID` y `aws:SourceIp`. Para ver una lista de las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

En la siguiente tabla se enumeran las claves de condición de VPC Lattice. Para obtener más información, consulte Claves de condición de los servicios de Amazon VPC Lattice en la Referencia de autorización de servicios.

Claves de condición	Descripción	Ejemplo	Disponibilidad para usuarios anónimos (no autenticados)	Disponibilidad para gRPC
`vpc-lattice-svcs:Port`	Filtra el acceso por el puerto de servicio al que se realiza la solicitud	80	Sí	Sí
`vpc-lattice-svcs:RequestMethod`	Filtra el acceso por el método de la solicitud	GET	Sí	PUBLICAR siempre
`vpc-lattice-svcs:RequestHeader/` *`header-name`* `:` *`value`*	Filtra el acceso por un par de nombre-valor de encabezado en	content-type: application/json	Sí	Sí

Claves de condición	Descripción	Ejemplo	Disponibilidad para usuarios anónimos (no autenticados)	Disponibilidad para gRPC
	los encabezados de la solicitud			
`vpc-lattice-svcs:RequestQueryString/` *`key-name`*`: `*`value`*	Filtra el acceso por los pares de clave-valor de la cadena de consulta en la URL de la solicitud	quux: [corge, grault]	Sí	No
`vpc-lattice-svcs:ServiceNetworkArn`	Filtra el acceso por el ARN de la red de servicios del servicio que recibe la solicitud	arn:aws:vpc-lattice:us-west-2:123456789012:servicenetwork/sn-0123456789abcdef0	Sí	Sí
`vpc-lattice-svcs:ServiceArn`	Filtra el acceso por el ARN del servicio que recibe la solicitud	arn:aws:vpc-lattice:us-west-2:123456789012:service/svc-0123456789abcdef0	Sí	Sí
`vpc-lattice-svcs:SourceVpc`	Filtra el acceso por la VPC desde la que se realiza la solicitud	vpc-1a2b3c4d	Sí	Sí

Claves de condición	Descripción	Ejemplo	Disponibilidad para usuarios anónimos (no autenticados)	Disponibilidad para gRPC
`vpc-lattice-svcs:SourceVpcOwnerAccount`	Filtra el acceso por la cuenta propietaria de la VPC desde la que se realiza la solicitud	123456789012	Sí	Sí

Entidades principales anónimas (no autenticadas)

Los directores anónimos son personas que llaman y no firman sus AWS solicitudes con la versión 4 de la firma (SigV4) y se encuentran dentro de una VPC que está conectada a la red de servicio. Las entidades principales anónimas pueden realizar solicitudes no autenticadas a los servicios de la red de servicios si una política de autenticación así lo permite.

Ejemplo de políticas de autenticación

Los siguientes son ejemplos de políticas de autenticación que requieren que las solicitudes las realicen las entidades principales autenticadas.

Todos los ejemplos utilizan la `us-west-2` región y contienen una cuenta ficticia. IDs

Ejemplo 1: restringir el acceso a los servicios por parte de una organización específica AWS

El siguiente ejemplo de política de autenticación concede permisos a cualquier solicitud autenticada para acceder a cualquier servicio de la red de servicios a la que se aplique la política. Sin embargo, la solicitud debe provenir de los directores que pertenezcan a la AWS organización especificada en la condición.

JSON

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

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

Ejemplo 2: restringir el acceso a un servicio por un rol de IAM específico

El siguiente ejemplo de política de autenticación concede permisos a cualquier solicitud autenticada que utilice el rol de IAM `rates-client` para realizar solicitudes HTTP GET en el servicio especificado en el elemento `Resource`. El recurso del elemento `Resource` es el mismo que el servicio al que está asociada la política.

JSON

```
{
   "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"
            }
         }
      }
   ]
}
```

Ejemplo 3: Restringir el acceso a los servicios por parte de las entidades principales autenticadas en una VPC específica

El siguiente ejemplo de política de autenticación solo permite solicitudes autenticadas de las entidades principales de la VPC cuyo ID de VPC sea *vpc-1a2b3c4d*.

JSON

```
{
   "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"
            }
         }
      }
   ]
}
```

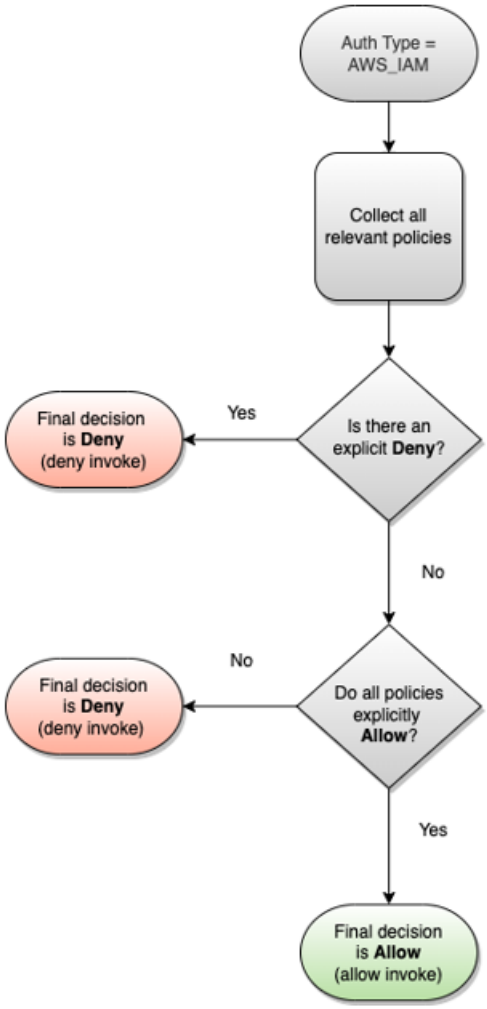
Cómo funciona la autorización

Cuando un servicio de VPC Lattice recibe una solicitud, el código de AWS cumplimiento evalúa todas las políticas de permisos relevantes en conjunto para determinar si se debe autorizar o denegar la solicitud. Evalúa todas las políticas basadas en identidad de IAM y las políticas de autenticación que se aplican en el contexto de la solicitud durante la autorización. De forma predeterminada, todas las solicitudes se deniegan de manera implícita si el tipo de autenticación es `AWS_IAM`. Un permiso explícito de todas las políticas relevantes anula el valor predeterminado.

La autorización incluye:

- Recopilar todas las políticas basadas en identidad de IAM y las políticas de autenticación relevantes.
- Evaluación del conjunto de políticas resultante:
  - Verificar que el solicitante (como un rol o usuario de IAM) cuente con los permisos para realizar la operación desde la cuenta a la que pertenece el solicitante. Si no hay una declaración de autorización explícita, AWS no autoriza la solicitud.
  - Verificar que la solicitud esté permitida por la política de autenticación de la red de servicios. Si una política de autenticación está habilitada, pero no hay una declaración de autorización explícita, AWS no autoriza la solicitud. Si hay una instrucción de autorización explícita o el tipo de autenticación es `NONE`, el código continúa.
  - Verificar que la solicitud esté permitida por la política de autenticación del servicio. Si una política de autenticación está habilitada, pero no hay una declaración de autorización explícita, AWS no autoriza la solicitud. Si hay una instrucción de autorización explícita o si el tipo de autenticación es `NONE`, entonces el código de aplicación devuelve una decisión final de Permitir.
  - Una denegación explícita en cualquier política invalida cualquier permiso concedido.

En el diagrama se muestra el flujo de trabajo de la autorización. Cuando se realiza una solicitud, las políticas relevantes permiten o deniegan el acceso de la solicitud a un servicio determinado.



Control del tráfico en VPC Lattice mediante grupos de seguridad

AWS los grupos de seguridad actúan como firewalls virtuales y controlan el tráfico de red hacia y desde las entidades a las que están asociados. Con VPC Lattice, puede crear grupos de seguridad y asignarlos a la asociación de VPC que conecta una VPC a una red de servicio para aplicar protecciones de seguridad adicionales a nivel de red para su red de servicio. Si conecta una VPC a una red de servicio mediante un punto de enlace de VPC, también puede asignar grupos de seguridad al punto de enlace de la VPC. Del mismo modo, puede asignar grupos de seguridad a las puertas de enlace de recursos que cree para permitir el acceso a los recursos de su VPC.

Contenido

Lista de prefijos administrada

VPC Lattice proporciona listas de prefijos gestionadas que incluyen las direcciones IP que se utilizan para enrutar el tráfico a través de la red de VPC Lattice cuando se utiliza una asociación de red de servicio para conectar la VPC a una red de servicio mediante una asociación de VPC. Se trata de enlaces privados y locales o públicos no enrutables. IPs IPs IPs

Puede hacer referencia a las listas de prefijos administradas por VPC Lattice en las reglas de grupo de seguridad. Esto permite que el tráfico fluya desde los clientes, a través de la red de servicios de VPC Lattice y hacia los destinos del servicio de VPC Lattice.

Por ejemplo, supongamos que tiene una EC2 instancia registrada como destino en la región EE.UU. Oeste (Oregón) (). `us-west-2` Puede añadir una regla al grupo de seguridad de la instancia que permita el acceso HTTPS entrante desde la lista de prefijos administrada de VPC Lattice, de modo que el tráfico de VPC Lattice de esta región pueda llegar a la instancia. Si elimina todas las demás reglas entrantes del grupo de seguridad, podrá evitar que cualquier tráfico que no sea de VPC Lattice llegue a la instancia.

Los nombres de las listas de prefijos administradas para VPC Lattice son los siguientes:

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

Para obtener más información, consulte Listas de prefijos administradas de AWS en la Guía del usuario de Amazon VPC.

Clientes para Windows y macOS

Las direcciones de las listas de prefijos de VPC Lattice son direcciones locales de enlace y direcciones públicas no enrutables. Si se conecta a VPC Lattice desde estos clientes, debe actualizar sus configuraciones para que reenvíe las direcciones IP de la lista de prefijos administrados a la dirección IP principal del cliente. El siguiente es un ejemplo de comando que actualiza la configuración del cliente de Windows, donde 169.254.171.0 se encuentra una de las direcciones de la lista de prefijos administrados.

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

A continuación, se muestra un comando de ejemplo que actualiza la configuración del cliente macOS, donde 169.254.171.0 se encuentra una de las direcciones de la lista de prefijos administrados.

```
sudo route -n add -net 169.254.171.0 primary-ip-address 255.255.255.0
```

Para evitar crear una ruta estática, le recomendamos que utilice un punto final de red de servicio en una VPC para establecer la conectividad. Para obtener más información, consulte the section called “Gestione las asociaciones de puntos finales de VPC”.

Reglas del grupo de seguridad

El uso de VPC Lattice con o sin grupos de seguridad no afectará a la configuración de los grupos de seguridad de VPC existentes. Sin embargo, puede agregar sus propios grupos de seguridad en cualquier momento.

Consideraciones clave

- Las reglas de los grupos de seguridad para los clientes controlan el tráfico saliente a VPC Lattice.
- Las reglas de los grupos de seguridad para los objetivos controlan el tráfico entrante desde VPC Lattice hacia los objetivos, incluido el tráfico de comprobación de estado.
- Las reglas del grupo de seguridad para la asociación entre la red de servicios y la VPC controlan qué clientes pueden acceder a la red de servicios de VPC Lattice.
- Las reglas del grupo de seguridad para la puerta de enlace de recursos controlan el tráfico saliente desde la puerta de enlace de recursos a los recursos.

Reglas de salida recomendadas para el tráfico que fluye desde la puerta de enlace de recursos a un recurso de base de datos

Para que el tráfico fluya desde la puerta de enlace de recursos a los recursos, debe crear reglas de salida para los puertos abiertos y protocolos de escucha aceptados para los recursos.

Destino	Protocolo	Intervalo de puertos	Comentario
CIDR range for resource	*TCP*	*3306*	Permita el tráfico desde la pasarela de recursos a las bases de datos

Reglas de entrada recomendadas para redes de servicios y asociaciones de VPC

Para que el tráfico fluya del cliente VPCs a los servicios asociados a la red de servicios, debe crear reglas de entrada para los puertos de escucha y los protocolos de escucha de los servicios.

Origen	Protocolo	Intervalo de puertos	Comentario
VPC CIDR	*listener*	*listener*	Permitir el tráfico de los clientes a VPC Lattice

Reglas de salida recomendadas para el tráfico que fluye desde las instancias de clientes hasta VPC Lattice

De forma predeterminada, los grupos de seguridad permiten el tráfico de salida. Sin embargo, si tiene reglas de salida personalizadas, debe permitir el tráfico saliente al prefijo de VPC Lattice para los puertos y protocolos de escucha, de modo que las instancias cliente puedan conectarse a todos los servicios asociados a la red de servicios de VPC Lattice. Puede permitir este tráfico haciendo referencia al ID de la lista de prefijos de VPC Lattice.

Destino	Protocolo	Intervalo de puertos	Comentario
ID of the VPC Lattice prefix list	*listener*	*listener*	Permitir el tráfico de los clientes a VPC Lattice

Reglas de entrada recomendadas para el tráfico que fluye desde VPC Lattice hasta las instancias de destino

No puede usar el grupo de seguridad del cliente como fuente para los grupos de seguridad de su destino, ya que el tráfico fluye desde VPC Lattice. Puede hacer referencia al ID de la lista de prefijos de VPC Lattice.

Origen	Protocolo	Intervalo de puertos	Comentario
ID of the VPC Lattice prefix list	*target*	*target*	Permita el tráfico de VPC Lattice a los objetivos
ID of the VPC Lattice prefix list	*health check*	*health check*	Permita comprobar el estado del tráfico desde VPC Lattice a los objetivos

Administración de grupos de seguridad para una asociación de VPC

Puede usarlo AWS CLI para ver, agregar o actualizar los grupos de seguridad de la VPC a la asociación de redes de servicio. Cuando utilice la AWS CLI, recuerde que sus comandos se ejecutan en la Región de AWS configuración de su perfil. Si desea ejecutar los comandos en otra región, cambie la región predeterminada de su perfil o utilice el parámetro `--region` con el comando.

Antes de empezar, confirme que ha creado el grupo de seguridad en la misma VPC que la VPC que quiere añadir a la red de servicios. Para obtener más información, consulte Controle el tráfico a sus recursos mediante grupos de seguridad en la Guía del usuario de Amazon VPC

Cómo agregar un grupo de seguridad al crear una asociación de VPC mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en VPC Lattice, elija Redes de servicios.
3. Seleccione el nombre de la red de servicios para abrir la página de detalles.
4. En la pestaña Asociaciones de VPC, elija Crear asociaciones de VPC y, a continuación, elija Agregar asociación de VPC.
5. Seleccione una VPC y hasta cinco grupos de seguridad.
6. Seleccione Save changes (Guardar cambios).

Cómo actualizar o agregar grupos de seguridad a una asociación de VPC existente mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.

2. En el panel de navegación, en VPC Lattice, elija Redes de servicios.
3. Seleccione el nombre de la red de servicios para abrir la página de detalles.
4. En la pestaña Asociaciones de VPC, seleccione la casilla de verificación de la asociación y, a continuación, elija Acciones, Editar grupos de seguridad.
5. Añada y elimine grupos de seguridad según sea necesario.
6. Seleccione Save changes (Guardar cambios).

Para agregar un grupo de seguridad al crear una asociación de VPC mediante el AWS CLI

Use el comando create-service-network-vpc-association, que especifica el ID de la VPC para la asociación de VPC y el ID de los grupos de seguridad que se van a agregar.

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

Si se ejecuta correctamente, el comando devolverá información similar a la siguiente.

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

Para agregar o actualizar grupos de seguridad a una asociación de VPC existente mediante la AWS CLI

Utilice el comando update-service-network-vpc-association, que especifica el ID de la red de servicio y el de los grupos IDs de seguridad. Estos grupos de seguridad anulan cualquier grupo de seguridad asociado con anterioridad. Defina al menos un grupo de seguridad al actualizar la lista.

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

> **Warning**
>
> No puede eliminar todos los grupos de seguridad. En cambio, primero debe eliminar la asociación de VPC y, a continuación, volver a crear la asociación de VPC sin ningún grupo de seguridad. Tenga cuidado al eliminar la asociación de VPC. Esto impide que el tráfico llegue a los servicios que se encuentran en esa red de servicios.

Controle el tráfico a VPC Lattice mediante la red ACLs

Una lista de control de acceso (ACL) de red permite o deniega el tráfico entrante o saliente específico en el nivel de subred. La ACL de red predeterminada permite el tráfico de entrada y de salida. Puede crear una red personalizada ACLs para sus subredes a fin de proporcionar un nivel de seguridad adicional. Para obtener más información, consulte Red ACLs en la Guía del usuario de Amazon VPC.

Contenido

Red ACLs para las subredes de sus clientes

La red ACLs para las subredes de los clientes debe permitir el tráfico entre los clientes y VPC Lattice. Puede obtener los rangos de direcciones IP permitidos en la lista de prefijos administrados de VPC Lattice.

A continuación, se muestra un ejemplo de regla de entrada.

Origen	Protocolo	Intervalo de puertos	Comentario
vpc_lattice_cidr_block	TCP	1025-65535	Permiso de tráfico desde VPC Lattice hacia los clientes

A continuación, se muestra un ejemplo de una regla de salida.

Destino	Protocolo	Intervalo de puertos	Comentario
vpc_lattice_cidr_block	*listener*	*listener*	Permitir el tráfico de los clientes a VPC Lattice

Red ACLs para sus subredes de destino

La red ACLs para las subredes de destino debe permitir el tráfico entre los destinos y VPC Lattice tanto en el puerto de destino como en el puerto de comprobación de estado. Puede obtener los rangos de direcciones IP permitidos en la lista de prefijos administrados de VPC Lattice.

A continuación, se muestra un ejemplo de regla de entrada.

Origen	Protocolo	Intervalo de puertos	Comentario
vpc_lattice_cidr_block	*target*	*target*	Permita el tráfico de VPC Lattice a los objetivos
vpc_lattice_cidr_block	*health check*	*health check*	Permita comprobar el estado del tráfico desde VPC Lattice a los objetivos

A continuación, se muestra un ejemplo de una regla de salida.

Destino	Protocolo	Intervalo de puertos	Comentario
vpc_lattice_cidr_block	*target*	1024-65535	Permiso de tráfico desde los destinos hacia VPC Lattice
vpc_lattice_cidr_block	*health check*	1024-65535	Permiso de comprobación de estado del tráfico

Destino	Protocolo	Intervalo de puertos	Comentario
			desde los destinos hasta VPC Lattice

SIGv4 solicitudes autenticadas para Amazon VPC Lattice

VPC Lattice utiliza la versión de firma 4 (SIGv4) o la versión de firma 4A (SIGv4A) para la autenticación del cliente. Para obtener más información, consulte la versión 4 de AWS Signature para ver las solicitudes de API en la Guía del usuario de IAM.

Consideraciones

- VPC Lattice intenta autenticar cualquier solicitud firmada con o A. SIGv4 SIGv4 La solicitud falla sin autenticación.
- VPC Lattice no admite la firma de cargas. Debe enviar un encabezado `x-amz-content-sha256` con el valor establecido en `"UNSIGNED-PAYLOAD"`.

Ejemplos

- Python
- Java
- Node.js
- Golang
- Golang - GRPC

Python

En este ejemplo, se envían las solicitudes firmadas a través de una conexión segura a un servicio registrado en la red. Si prefiere utilizar solicitudes, el paquete botocore simplifica el proceso de autenticación, pero no es obligatorio. Para obtener más información, consulte Credenciales en la documentación de Boto3.

Para instalar los `awscrt` paquetes `botocore` y, utilice el siguiente comando. Para obtener más información, consulte AWS CRT Python.

```
pip install botocore awscrt
```

Si ejecuta la aplicación cliente en Lambda, instale los módulos necesarios mediante capas Lambda o inclúyalos en su paquete de implementación.

En el siguiente ejemplo, sustituya los valores de los marcadores de posición por sus propios valores.

SIGv4

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

if __name__ == '__main__':
    session = botocore.session.Session()
    signer = crt.auth.CrtSigV4Auth(session.get_credentials(), 'vpc-lattice-svcs',
 'us-west-2')
    endpoint = 'https://data-svc-022f67d3a42.1234abc.vpc-lattice-svcs.us-
west-2.on.aws'
    data = "some-data-here"
    headers = {'Content-Type': 'application/json', 'x-amz-content-sha256':
 'UNSIGNED-PAYLOAD'}
    request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)
    request.context["payload_signing_enabled"] = False
    signer.add_auth(request)

    prepped = request.prepare()

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

SIGv4A

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

if __name__ == '__main__':
    session = botocore.session.Session()
    signer = crt.auth.CrtSigV4AsymAuth(session.get_credentials(), 'vpc-lattice-
svcs', '*')
    endpoint = 'https://data-svc-022f67d3a42.1234abc.vpc-lattice-svcs.us-
west-2.on.aws'
```

```
    data = "some-data-here"
    headers = {'Content-Type': 'application/json', 'x-amz-content-sha256':
 'UNSIGNED-PAYLOAD'}
    request = AWSRequest(method='POST', url=endpoint, data=data, headers=headers)
    request.context["payload_signing_enabled"] = False
    signer.add_auth(request)

    prepped = request.prepare()

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

Java

En este ejemplo, se muestra cómo se puede realizar la firma de solicitudes mediante interceptores personalizados. Utiliza la clase de proveedor de credenciales predeterminada desde AWS SDK for Java 2.x, que obtiene las credenciales correctas para usted. Si prefiere utilizar un proveedor de credenciales específico, puede seleccionar uno de AWS SDK for Java 2.x. Solo AWS SDK para Java permite cargas útiles sin firmar a través de HTTPS. Sin embargo, puede ampliar el firmante para que admita cargas no firmadas a través de HTTP.

SIGv4

```
package com.example;

import software.amazon.awssdk.http.auth.aws.signer.AwsV4HttpSigner;
import software.amazon.awssdk.http.auth.spi.signer.SignedRequest;

import software.amazon.awssdk.http.SdkHttpMethod;
import software.amazon.awssdk.http.SdkHttpClient;
import software.amazon.awssdk.identity.spi.AwsCredentialsIdentity;
import software.amazon.awssdk.http.SdkHttpRequest;
import software.amazon.awssdk.http.apache.ApacheHttpClient;
import software.amazon.awssdk.http.HttpExecuteRequest;
import software.amazon.awssdk.http.HttpExecuteResponse;
import java.io.IOException;
import java.net.URI;

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

public class sigv4 {
```

```
    public static void main(String[] args) {
        AwsV4HttpSigner signer = AwsV4HttpSigner.create();

        AwsCredentialsIdentity credentials =
 DefaultCredentialsProvider.create().resolveCredentials();

        if (args.length < 2) {
            System.out.println("Usage: sample <url> <region>");
            System.exit(1);
        }
        // Create the HTTP request to be signed
        var url = args[0];
        SdkHttpRequest httpRequest = SdkHttpRequest.builder()
                .uri(URI.create(url))
                .method(SdkHttpMethod.GET)
                .build();

        SignedRequest signedRequest = signer.sign(r -> r.identity(credentials)
                .request(httpRequest)
                .putProperty(AwsV4HttpSigner.SERVICE_SIGNING_NAME, "vpc-lattice-
svcs")
                .putProperty(AwsV4HttpSigner.PAYLOAD_SIGNING_ENABLED, false)
                .putProperty(AwsV4HttpSigner.REGION_NAME, args[1]));

        System.out.println("[*] Raw request headers:");
        signedRequest.request().headers().forEach((key, values) -> {
            values.forEach(value -> System.out.println("  " + key + ": " + value));
        });

        try (SdkHttpClient httpClient = ApacheHttpClient.create()) {
            HttpExecuteRequest httpExecuteRequest = HttpExecuteRequest.builder()
                    .request(signedRequest.request())
                    .contentStreamProvider(signedRequest.payload().orElse(null))
                    .build();

            System.out.println("[*] Sending request to: " + url);

            HttpExecuteResponse httpResponse =
 httpClient.prepareRequest(httpExecuteRequest).call();

            System.out.println("[*] Request sent");
```

```
            System.out.println("[*] Response status code: " +
 httpResponse.httpResponse().statusCode());
            // Read and print the response body
            httpResponse.responseBody().ifPresent(inputStream -> {
                try {
                    String responseBody = new String(inputStream.readAllBytes());
                    System.out.println("[*] Response body: " + responseBody);
                } catch (IOException e) {
                    System.err.println("[*] Failed to read response body");
                    e.printStackTrace();
                } finally {
                    try {
                        inputStream.close();
                    } catch (IOException e) {
                        System.err.println("[*] Failed to close input stream");
                        e.printStackTrace();
                    }
                }
            });
        } catch (IOException e) {
            System.err.println("[*] HTTP Request Failed.");
            e.printStackTrace();
        }

    }
}
```

SIGv4A

Este ejemplo requiere una dependencia adicional de. `software.amazon.awssdk:http-auth-aws-crt`

```
package com.example;


import software.amazon.awssdk.http.auth.aws.signer.AwsV4aHttpSigner;
import software.amazon.awssdk.http.auth.aws.signer.RegionSet;
import software.amazon.awssdk.http.auth.spi.signer.SignedRequest;

import software.amazon.awssdk.http.SdkHttpMethod;
import software.amazon.awssdk.http.SdkHttpClient;
import software.amazon.awssdk.identity.spi.AwsCredentialsIdentity;
import software.amazon.awssdk.http.SdkHttpRequest;
```

```
import software.amazon.awssdk.http.apache.ApacheHttpClient;
import software.amazon.awssdk.http.HttpExecuteRequest;
import software.amazon.awssdk.http.HttpExecuteResponse;
import java.io.IOException;
import java.net.URI;
import java.util.Arrays;

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

public class sigv4a {

    public static void main(String[] args) {
        AwsV4aHttpSigner signer = AwsV4aHttpSigner.create();

        AwsCredentialsIdentity credentials =
 DefaultCredentialsProvider.create().resolveCredentials();

        if (args.length < 2) {
            System.out.println("Usage: sample <url> <regionset>");
            System.exit(1);
        }
        // Create the HTTP request to be signed
        var url = args[0];
        SdkHttpRequest httpRequest = SdkHttpRequest.builder()
                .uri(URI.create(url))
                .method(SdkHttpMethod.GET)
                .build();

        SignedRequest signedRequest = signer.sign(r -> r.identity(credentials)
                .request(httpRequest)
                .putProperty(AwsV4aHttpSigner.SERVICE_SIGNING_NAME, "vpc-lattice-
svcs")
                .putProperty(AwsV4aHttpSigner.PAYLOAD_SIGNING_ENABLED, false)
                .putProperty(AwsV4aHttpSigner.REGION_SET,
 RegionSet.create(String.join(" ",Arrays.copyOfRange(args, 1, args.length)))));

        System.out.println("[*] Raw request headers:");
        signedRequest.request().headers().forEach((key, values) -> {
            values.forEach(value -> System.out.println("  " + key + ": " + value));
        });

        try (SdkHttpClient httpClient = ApacheHttpClient.create()) {
            HttpExecuteRequest httpExecuteRequest = HttpExecuteRequest.builder()
                    .request(signedRequest.request())
```

```
                    .contentStreamProvider(signedRequest.payload().orElse(null))
                    .build();

            System.out.println("[*] Sending request to: " + url);

            HttpExecuteResponse httpResponse =
 httpClient.prepareRequest(httpExecuteRequest).call();

            System.out.println("[*] Request sent");

            System.out.println("[*] Response status code: " +
 httpResponse.httpResponse().statusCode());
            // Read and print the response body
            httpResponse.responseBody().ifPresent(inputStream -> {
                try {
                    String responseBody = new String(inputStream.readAllBytes());
                    System.out.println("[*] Response body: " + responseBody);
                } catch (IOException e) {
                    System.err.println("[*] Failed to read response body");
                    e.printStackTrace();
                } finally {
                    try {
                        inputStream.close();
                    } catch (IOException e) {
                        System.err.println("[*] Failed to close input stream");
                        e.printStackTrace();
                    }
                }
            });
        } catch (IOException e) {
            System.err.println("[*] HTTP Request Failed.");
            e.printStackTrace();
        }
    }
}
```

Node.js

En este ejemplo, se utilizan los enlaces aws-crt NodeJS para enviar una solicitud firmada mediante HTTPS.

Para instalar el paquete `aws-crt`, use el siguiente comando.

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

Si la variable de entorno `AWS_REGION` existe, en el ejemplo se utiliza la región especificada por `AWS_REGION`. La región predeterminada es `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', algorithm).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: new URL(process.argv[2]).pathname,
      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', algorithm).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: new URL(process.argv[2]).pathname,
      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()
  }
)
```

Golang

En este ejemplo, se utilizan los generadores de código Smithy para Go y el AWS SDK para el lenguaje de programación Go para gestionar las solicitudes de firma de solicitudes. El ejemplo requiere una versión de Go 1.21 o superior.

SIGv4

```
package main

import (
        "context"
        "flag"
        "fmt"
        "io"
        "log"
        "net/http"
        "net/http/httputil"
        "os"
        "strings"

        "github.com/aws/aws-sdk-go-v2/aws"
        "github.com/aws/aws-sdk-go-v2/config"
        "github.com/aws/smithy-go/aws-http-auth/credentials"
        "github.com/aws/smithy-go/aws-http-auth/sigv4"
        v4 "github.com/aws/smithy-go/aws-http-auth/v4"
)

type nopCloser struct {
        io.ReadSeeker
}

func (nopCloser) Close() error {
        return nil
}

type stringFlag struct {
        set   bool
        value string
}



        flag.PrintDefaults()
```

```
        os.Exit(1)
}

func main() {
        flag.Parse()
        if !url.set || !region.set {
                Usage()
        }

        cfg, err := config.LoadDefaultConfig(context.TODO(),
 config.WithClientLogMode(aws.LogSigning))
        if err != nil {
                log.Fatalf("failed to load SDK configuration, %v", err)
        }

        if len(os.Args) < 2 {
                log.Fatalf("Usage: go run main.go  <url>")
        }

        // Retrieve credentials from an SDK source, such as the instance profile
        sdkCreds, err := cfg.Credentials.Retrieve(context.TODO())
        if err != nil {
                log.Fatalf("Unable to retrieve credentials from SDK, %v", err)
        }

        creds := credentials.Credentials{
                AccessKeyID:     sdkCreds.AccessKeyID,
                SecretAccessKey: sdkCreds.SecretAccessKey,
                SessionToken:    sdkCreds.SessionToken,
        }

        // Add a payload body, which will not be part of the signature calculation
        body := nopCloser{strings.NewReader(`Example payload body`)}

        req, _ := http.NewRequest(http.MethodPost, url.value, body)

        // Create a sigv4a signer with specific options
        signer := sigv4.New(func(o *v4.SignerOptions) {
                o.DisableDoublePathEscape = true
                // This will add the UNSIGNED-PAYLOAD sha256 header
                o.AddPayloadHashHeader = true
                o.DisableImplicitPayloadHashing = true
        })
```

```
        // Perform the signing on req, using the credentials we retrieved from the
 SDK
        err = signer.SignRequest(&sigv4.SignRequestInput{
                Request:     req,
                Credentials: creds,
                Service:     "vpc-lattice-svcs",
                Region: region.String(),
        })

        if err != nil {
                log.Fatalf("%s", err)
        }

        res, err := httputil.DumpRequest(req, true)

        if err != nil {
                log.Fatalf("%s", err)
        }

        log.Printf("[*] Raw request\n%s\n", string(res))

        log.Printf("[*] Sending request to %s\n", url.value)

        resp, err := http.DefaultClient.Do(req)
        if err != nil {
                log.Fatalf("%s", err)
        }

        log.Printf("[*] Request sent\n")

        log.Printf("[*] Response status code: %d\n", resp.StatusCode)

        respBody, err := io.ReadAll(resp.Body)
        if err != nil {
                log.Fatalf("%s", err)
        }

        log.Printf("[*] Response body: \n%s\n", respBody)
}
```

SIGv4A

```
package main
```

```
import (
        "context"
        "flag"
        "fmt"
        "io"
        "log"
        "net/http"
        "net/http/httputil"
        "os"
        "strings"

        "github.com/aws/aws-sdk-go-v2/aws"
        "github.com/aws/aws-sdk-go-v2/config"
        "github.com/aws/smithy-go/aws-http-auth/credentials"
        "github.com/aws/smithy-go/aws-http-auth/sigv4a"
        v4 "github.com/aws/smithy-go/aws-http-auth/v4"
)

type nopCloser struct {
        io.ReadSeeker
}

func (nopCloser) Close() error {
        return nil
}

type stringFlag struct {

func main() {
        flag.Parse()
        if !url.set || !regionSet.set {
                Usage()
        }

        cfg, err := config.LoadDefaultConfig(context.TODO(),
 config.WithClientLogMode(aws.LogSigning))
        if err != nil {
                log.Fatalf("failed to load SDK configuration, %v", err)
        }

        if len(os.Args) < 2 {
                log.Fatalf("Usage: go run main.go <url>")
        }
```

```
        // Retrieve credentials from an SDK source, such as the instance profile
        sdkCreds, err := cfg.Credentials.Retrieve(context.TODO())
        if err != nil {
                log.Fatalf("Unable to retrieve credentials from SDK, %v", err)
        }

        creds := credentials.Credentials{
                AccessKeyID:     sdkCreds.AccessKeyID,
                SecretAccessKey: sdkCreds.SecretAccessKey,
                SessionToken:    sdkCreds.SessionToken,
        }

        // Add a payload body, which will not be part of the signature calculation
        body := nopCloser{strings.NewReader(`Example payload body`)}

        req, _ := http.NewRequest(http.MethodPost, url.value, body)

        // Create a sigv4a signer with specific options
        signer := sigv4a.New(func(o *v4.SignerOptions) {
                o.DisableDoublePathEscape = true
                // This will add the UNSIGNED-PAYLOAD sha256 header
                o.AddPayloadHashHeader = true
                o.DisableImplicitPayloadHashing = true
        })

        // Create a slice out of the provided regionset
        rs := strings.Split(regionSet.value, ",")

        // Perform the signing on req, using the credentials we retrieved from the
SDK
        err = signer.SignRequest(&sigv4a.SignRequestInput{
                Request:     req,
                Credentials: creds,
                Service:     "vpc-lattice-svcs",
                RegionSet: rs,
        })

        if err != nil {
                log.Fatalf("%s", err)
        }

        res, err := httputil.DumpRequest(req, true)
```

```
        if err != nil {
                log.Fatalf("%s", err)
        }

        log.Printf("[*] Raw request\n%s\n", string(res))

        log.Printf("[*] Sending request to %s\n", url.value)

        resp, err := http.DefaultClient.Do(req)
        if err != nil {
                log.Fatalf("%s", err)
        }

        log.Printf("[*] Request sent\n")

        log.Printf("[*] Response status code: %d\n", resp.StatusCode)

        respBody, err := io.ReadAll(resp.Body)
        if err != nil {
                log.Fatalf("%s", err)
        }

        log.Printf("[*] Response body: \n%s\n", respBody)
}
```

Golang - GRPC

En este ejemplo, se utiliza el AWS SDK del lenguaje de programación Go para gestionar la firma de solicitudes de GRPC. Esto se puede usar con el servidor echo del repositorio de códigos de muestra del GRPC.

```
package main

import (
    "context"
    "crypto/tls"
    "crypto/x509"

    "flag"
    "fmt"
    "log"
    "net/http"
```

```
    "net/url"
    "strings"
    "time"

    "google.golang.org/grpc"
    "google.golang.org/grpc/credentials"

    "github.com/aws/aws-sdk-go-v2/aws"
    v4 "github.com/aws/aws-sdk-go-v2/aws/signer/v4"
    "github.com/aws/aws-sdk-go-v2/config"

    ecpb "google.golang.org/grpc/examples/features/proto/echo"
)

const (
    headerContentSha    = "x-amz-content-sha256"
    headerSecurityToken = "x-amz-security-token"
    headerDate          = "x-amz-date"
    headerAuthorization = "authorization"
    unsignedPayload     = "UNSIGNED-PAYLOAD"
)

type SigV4GrpcSigner struct {
    service      string
    region       string
    credProvider aws.CredentialsProvider
    signer       *v4.Signer
}

func NewSigV4GrpcSigner(service string, region string, credProvider
 aws.CredentialsProvider) *SigV4GrpcSigner {
    signer := v4.NewSigner()
    return &SigV4GrpcSigner{
        service:      service,
        region:       region,
        credProvider: credProvider,
        signer:       signer,
    }
}

func (s *SigV4GrpcSigner) GetRequestMetadata(ctx context.Context, uri ...string)
 (map[string]string, error) {
    ri, _ := credentials.RequestInfoFromContext(ctx)
    creds, err := s.credProvider.Retrieve(ctx)
```

```
    if err != nil {
        return nil, fmt.Errorf("failed to load credentials: %w", err)
    }

    // The URI we get here is scheme://authority/service/ - for siging we want to
include the RPC name
    // But RequestInfoFromContext only has the combined /service/rpc-name - so read the
URI, and
    // replace the Path with what we get from RequestInfo.
    parsed, err := url.Parse(uri[0])
    if err != nil {
        return nil, err
    }
    parsed.Path = ri.Method

    // Build a request for the signer.
    bodyReader := strings.NewReader("")
    req, err := http.NewRequest("POST", uri[0], bodyReader)
    if err != nil {
        return nil, err
    }
    date := time.Now()
    req.Header.Set(headerContentSha, unsignedPayload)
    req.Header.Set(headerDate, date.String())
    if creds.SessionToken != "" {
        req.Header.Set(headerSecurityToken, creds.SessionToken)
    }
    // The signer wants this as //authority/path
    // So get this by triming off the scheme and the colon before the first slash.
    req.URL.Opaque = strings.TrimPrefix(parsed.String(), parsed.Scheme+":")

    err = s.signer.SignHTTP(context.Background(), creds, req, unsignedPayload,
s.service, s.region, date)
    if err != nil {
        return nil, fmt.Errorf("failed to sign request: %w", err)
    }

    // Pull the relevant headers out of the signer, and return them to get
    // included in the request we make.
    reqHeaders := map[string]string{
        headerContentSha:    req.Header.Get(headerContentSha),
        headerDate:          req.Header.Get(headerDate),
        headerAuthorization: req.Header.Get(headerAuthorization),
    }
```

```
    if req.Header.Get(headerSecurityToken) != "" {
        reqHeaders[headerSecurityToken] = req.Header.Get(headerSecurityToken)
    }

    return reqHeaders, nil
}

func (c *SigV4GrpcSigner) RequireTransportSecurity() bool {
    return true
}

var addr = flag.String("addr", "some-lattice-service:443", "the address to connect to")
var region = flag.String("region", "us-west-2", "region")

func callUnaryEcho(client ecpb.EchoClient, message string) {
    ctx, cancel := context.WithTimeout(context.Background(), 10*time.Second)
    defer cancel()
    resp, err := client.UnaryEcho(ctx, &ecpb.EchoRequest{Message: message})
    if err != nil {
        log.Fatalf("client.UnaryEcho(_) = _, %v: ", err)
    }
    fmt.Println("UnaryEcho: ", resp.Message)
}

func main() {
    flag.Parse()
    cfg, err := config.LoadDefaultConfig(context.TODO(),
 config.WithClientLogMode(aws.LogSigning))
    if err != nil {
        log.Fatalf("failed to load SDK configuration, %v", err)
    }

    pool, _ := x509.SystemCertPool()
    tlsConfig := &tls.Config{
        RootCAs: pool,
    }

    authority, _, _ := strings.Cut(*addr, ":") // Remove the port from the addr
    opts := []grpc.DialOption{
        grpc.WithTransportCredentials(credentials.NewTLS(tlsConfig)),

        // Lattice needs both the Authority to be set (without a port), and the SigV4
 signer
        grpc.WithAuthority(authority),
```

```
        grpc.WithPerRPCCredentials(NewSigV4GrpcSigner("vpc-lattice-svcs", *region,
 cfg.Credentials)),
    }

    conn, err := grpc.Dial(*addr, opts...)

    if err != nil {
        log.Fatalf("did not connect: %v", err)
    }
    defer conn.Close()
    rgc := ecpb.NewEchoClient(conn)

    callUnaryEcho(rgc, "hello world")
}
```

Protección de datos en Amazon VPC Lattice

El modelo de se aplica a protección de datos en Amazon VPC Lattice. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los. Nube de AWS Es responsable de mantener el control sobre su contenido que se encuentra alojado en esta infraestructura. Este contenido incluye la configuración de seguridad y las tareas de administración para el Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de datos, consulte Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Cifrado en tránsito

VPC Lattice es un servicio totalmente gestionado que consta de un plano de control y un plano de datos. Cada plano tiene un propósito distinto en el servicio. El plano de control proporciona los recursos administrativos que APIs se utilizan para crear, leer/describir, actualizar, eliminar y enumerar los recursos (CRUDL) (por ejemplo, `CreateService` y). `UpdateService` Las comunicaciones con el plano de control de VPC Lattice están protegidas durante el tránsito mediante TLS. El plano de datos es la API Lattice Invoke de VPC, que proporciona la interconexión entre los servicios. TLS cifra las comunicaciones con el plano de datos de VPC Lattice cuando se utiliza HTTPS o TLS. El conjunto de cifrado y la versión del protocolo utilizan los valores predeterminados proporcionados por VPC Lattice y no son configurables. Para obtener más información, consulte Oyentes HTTPS para servicios de VPC Lattice.

Cifrado en reposo

De forma predeterminada, el cifrado de los datos en reposo ayuda a reducir la sobrecarga operativa y la complejidad que implica la protección de los datos confidenciales. Al mismo tiempo, le permite crear aplicaciones seguras que cumplen con los estrictos requisitos normativos y de conformidad del cifrado.

Contenido

Cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3)

Cuando se usa el cifrado del lado del servidor con claves administradas por Amazon S3 (SSE-S3), cada objeto se cifra con una clave exclusiva. Como medida de seguridad adicional, ciframos la propia clave con una clave raíz que cambiamos periódicamente. El cifrado del lado del servidor de Simple Storage Service (Amazon S3) utiliza uno de los cifrados de bloques más seguros disponibles, Advanced Encryption Standard de 256 bits (AES-256) GCM, para cifrar los datos. En el caso de los objetos cifrados antes de AES-GCM, AES-CBC sigue siendo compatible para descifrar esos objetos. Para obtener más información, consulte Uso de cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3).

Si habilita el cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (SSE-S3) para su bucket de S3 para los registros de acceso de VPC Lattice, ciframos automáticamente cada archivo de registro de acceso antes de que se almacene en su bucket de S3. Para obtener más información, consulte Registros enviados a Amazon S3 en la Guía del CloudWatch usuario de Amazon.

Cifrado del lado del servidor con AWS KMS claves almacenadas en AWS KMS (SSE-KMS)

El cifrado con AWS KMS claves del lado del servidor (SSE-KMS) es similar al SSE-S3, pero con ventajas y cargos adicionales por el uso de este servicio. Existen permisos independientes para la AWS KMS clave que proporcionan protección adicional contra el acceso no autorizado a sus objetos en Amazon S3. El SSE-KMS también le proporciona un registro de auditoría que muestra cuándo y AWS KMS quién utilizó su clave. Para obtener más información, consulte Uso del cifrado del lado del servidor con AWS Key Management Service (SSE-KMS).

Contenido

Cifrado y descifrado de la clave privada de su certificado

El certificado ACM y la clave privada se cifran mediante una clave KMS AWS administrada que tiene el alias aws/acm. Puede ver el ID de clave con este alias en la AWS KMS consola, en la sección de claves administradas.AWS

VPC Lattice no tiene acceso directo a los recursos de ACM. Utiliza AWS TLS Connection Manager para proteger y acceder a las claves privadas del certificado. Cuando usa su certificado ACM para crear un servicio de VPC Lattice, VPC Lattice asocia su certificado con TLS Connection Manager de AWS . Para ello, se crea una concesión en AWS KMS la clave AWS gestionada con el prefijo aws/acm. Una concesión es un instrumento de política que permite que TLS Connection Manager use claves KMS en operaciones criptográficas. La concesión le permite a la entidad principal beneficiaria (TLS Connection Manager) llamar a las operaciones de concesión especificadas en la clave KMS para descifrar la clave privada de su certificado. A continuación, TLS Connection Manager utiliza el certificado y la clave privada descifrada (texto sin formato) para establecer una conexión segura (sesión SSL/TLS) con los clientes de los servicios de VPC Lattice. Cuando el certificado se desvincula de un servicio de VPC Lattice, la concesión se retira.

Si desea eliminar el acceso a la clave KMS, le recomendamos que sustituya o elimine el certificado del servicio mediante el comando AWS Management Console o del`update-service`. AWS CLI

Contexto de cifrado para VPC Lattice

Un contexto de cifrado es un conjunto opcional de pares clave-valor que contienen información contextual sobre el uso que se puede dar a la clave privada. AWS KMS vincula el contexto de cifrado a los datos cifrados y lo utiliza como datos autenticados adicionales para respaldar el cifrado autenticado.

Cuando las claves TLS se utilizan con VPC Lattice y TLS Connection Manager, el nombre del servicio de VPC Lattice se incluye en el contexto de cifrado utilizado para cifrar la clave en reposo. Puede comprobar para qué servicio de VPC Lattice se utilizan su certificado y su clave privada consultando el contexto de cifrado en sus CloudTrail registros, como se muestra en la siguiente sección, o consultando la pestaña Recursos asociados de la consola de ACM.

Para descifrar los datos, se incluye el mismo contexto de cifrado en la solicitud. VPC Lattice utiliza el mismo contexto de cifrado en todas las operaciones criptográficas de AWS KMS, donde la clave es `aws:vpc-lattice:arn` y el valor es el nombre de recurso de Amazon (ARN) del servicio VPC Lattice.

El siguiente ejemplo muestra el contexto de cifrado en el resultado de una operación como `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"
}
```

Monitoreo de sus claves de cifrado para VPC Lattice

Cuando utilizas una clave AWS gestionada con tu servicio VPC Lattice, puedes utilizarla AWS CloudTrailpara realizar un seguimiento de las solicitudes a las que envía VPC Lattice. AWS KMS

CreateGrant

Cuando agrega su certificado ACM a un servicio de VPC Lattice, se envía una solicitud `CreateGrant` en su nombre para que TLS Connection Manager pueda descifrar la clave privada asociada a su certificado ACM.

Puede ver la **`CreateGrant`** operación como un evento en el Historial de eventos CloudTrail,. CreateGrant

A continuación se muestra un ejemplo de registro de eventos en el historial de CloudTrail eventos de la `CreateGrant` operación.

```
{
    "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"
}
```

En el `CreateGrant` ejemplo anterior, el beneficiario principal es TLS Connection Manager y el contexto de cifrado tiene el ARN del servicio VPC Lattice.

ListGrants

Puede usar su ID de clave KMS y el ID de su cuenta para llamar a la API de `ListGrants`. De este modo, obtendrá una lista de todas las concesiones para la clave KMS especificada. Para obtener más información, consulte ListGrants.

Utilice el siguiente `ListGrants` comando AWS CLI para ver los detalles de todas las concesiones.

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

A continuación, se muestra un ejemplo del resultado.

```
{
    "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"
                }
            }
        }
    ]
}
```

En el `ListGrants` ejemplo anterior, el beneficiario principal es TLS Connection Manager y el contexto de cifrado tiene el ARN del servicio VPC Lattice.

Decrypt

VPC Lattice utiliza TLS Connection Manager para llamar a la operación `Decrypt` para descifrar la clave privada con el fin de servir las conexiones TLS en el servicio VPC Lattice. Puede ver la **`Decrypt`** operación como un evento en el historial de eventos, Decrypt. CloudTrail

A continuación se muestra un ejemplo de registro de eventos en el historial de CloudTrail eventos de la `Decrypt` operación.

```
{
    "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"
}
```


Administración de identidades y accesos para Amazon VPC Lattice

En las siguientes secciones, se describe cómo se puede utilizar AWS Identity and Access Management (IAM) para proteger los recursos de VPC Lattice, controlando quién puede realizar las acciones de la API de VPC Lattice.

Temas

- Cómo funciona Amazon VPC Lattice con IAM
- Permisos de la API Amazon VPC Lattice
- Políticas basadas en identidad para Amazon VPC Lattice
- Uso de roles vinculados a servicios para Amazon VPC Lattice
- AWS políticas gestionadas para Amazon VPC Lattice

Cómo funciona Amazon VPC Lattice con IAM

Antes de utilizar IAM para administrar el acceso a VPC Lattice, conozca qué características de IAM se pueden utilizar con VPC Lattice.

Característica de IAM	Compatibilidad con VPC Lattice
Políticas basadas en identidades	Sí
Políticas basadas en recursos	Sí
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACLs	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Roles de servicio	No
Roles vinculados al servicio	Sí

Para obtener una visión general de cómo funcionan VPC Lattice y otros AWS servicios con la mayoría de las funciones de IAM, consulte los AWS servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidad para VPC Lattice

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica

al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Políticas basadas en recursos de VPC Lattice

Compatibilidad con las políticas basadas en recursos: sí

Las políticas basadas en recursos son documentos de políticas de JSON que se adjuntan a un recurso. AWS En AWS los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico de ese servicio. AWS Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos.

VPC Lattice admite políticas de autenticación, una política basada en recursos que le permite controlar el acceso a los servicios de su red de servicios. Para obtener más información, consulte Controle el acceso a los servicios de VPC Lattice mediante políticas de autenticación.

VPC Lattice también admite políticas de permisos basadas en recursos para su integración con AWS Resource Access Manager. Puede usar estas políticas basadas en recursos para conceder permisos para administrar la conectividad con otras AWS cuentas u organizaciones para los servicios, las configuraciones de recursos y las redes de servicios. Para obtener más información, consulte Comparta sus entidades de VPC Lattice.

Acciones de política para VPC Lattice

Compatibilidad con las acciones de políticas: sí

En una instrucción de política de IAM, puede especificar cualquier acción de API de cualquier servicio que sea compatible con IAM. Para VPC Lattice, use el siguiente prefijo con el nombre de la acción de API: `vpc-lattice:`. Por ejemplo, `vpc-lattice:CreateService`, `vpc-lattice:CreateTargetGroup` y `vpc-lattice:PutAuthPolicy`.

Para especificar varias acciones en una única instrucción, sepárelas con comas del siguiente modo:

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

También puede utilizar caracteres comodín para especificar varias acciones. Por ejemplo, puede especificar todas las acciones cuyos nombres comiencen con la palabra `Get` del siguiente modo:

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

Para ver una lista completa de las acciones de API de VPC Lattice, consulte Acciones definidas por Amazon VPC Lattice en la Referencia de autorización de servicios.

Recursos de políticas para VPC Lattice

Compatibilidad con los recursos de políticas: sí

En una instrucción de política de IAM, el elemento `Resource` especifica el objeto o los objetos que abarca la instrucción. En el caso de VPC Lattice, cada declaración de política de IAM se aplica a los recursos que especifique mediante su uso. ARNs

El formato del nombre de recurso de Amazon (ARN) específico depende del recurso. Cuando proporciones un ARN, reemplaza el *italicized* texto por la información específica del recurso.

- Suscripciones al registro de acceso:

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

- Oyentes:

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

- Puertas de enlace de recursos

```
"Resource": "arn:aws:vpc-lattice:region:account-id:resourcegateway/resource-gateway-id"
```

- Configuración de recursos

```
"Resource": "arn:aws:vpc-lattice:region:account-id:resourceconfiguration/resource-configuration-id"
```

- Reglas:

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

- Servicios:

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

- Redes de servicios:

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

- Asociaciones de servicios de redes de servicios:

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

- Asociaciones de configuración de recursos de red de servicios

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

- Asociaciones de VPC de redes de servicios:

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

- Grupos de destino:

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

Claves de condición de política para VPC Lattice

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios

valores para una sola clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Para ver una lista de las claves de estado de VPC Lattice, consulte Claves de condición de Amazon VPC Lattice en la Referencia de autorización de servicio.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para obtener información sobre las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Listas de control de acceso (ACLs) en VPC Lattice

Soporta ACLs: No

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Control de acceso basado en atributos (ABAC) con VPC Lattice

Admite ABAC (etiquetas en las políticas): sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con VPC Lattice

Compatibilidad con credenciales temporales: sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluidas las que Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio de un usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Roles de servicio para VPC Lattice

Compatible con roles de servicio: No

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de VPC Lattice. Edite los roles de servicio solo cuando VPC Lattice proporcione orientación para hacerlo.

Roles vinculados a servicios para VPC Lattice

Admite roles vinculados a servicios: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener información sobre cómo crear o administrar roles vinculados a servicios de VPC Lattice, consulte Uso de roles vinculados a servicios para Amazon VPC Lattice.

Permisos de la API Amazon VPC Lattice

Debe conceder a las identidades de IAM (tales como usuarios o roles) permisos para llamar a las acciones de la API de VPC Lattice que necesiten, tal y como se describe en Acciones de política para VPC Lattice. Además, para algunas acciones de VPC Lattice, debes conceder permiso a las identidades de IAM para invocar acciones específicas desde otras. AWS APIs

Permisos necesarios para la API

Cuando llame a las siguientes acciones de la API, debe conceder a los usuarios de IAM permiso para llamar a las acciones especificadas.

`CreateResourceConfiguration`

- `vpc-lattice:CreateResourceConfiguration`
- `ec2:DescribeSubnets`
- `rds:DescribeDBInstances`
- `rds:DescribeDBClusters`

`CreateResourceGateway`

- `vpc-lattice:CreateResourceGateway`

- ec2:AssignPrivateIpAddresses
- ec2:AssignIpv6Addresses
- ec2:CreateNetworkInterface
- ec2:CreateNetworkInterfacePermission
- ec2:DeleteNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets

DeleteResourceGateway

- vpc-lattice:DeleteResourceGateway
- ec2:DeleteNetworkInterface

UpdateResourceGateway

- vpc-lattice:UpdateResourceGateway
- ec2:AssignPrivateIpAddresses
- ec2:AssignIpv6Addresses
- ec2:UnassignPrivateIpAddresses
- ec2:CreateNetworkInterface
- ec2:CreateNetworkInterfacePermission
- ec2:DeleteNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:ModifyNetworkInterfaceAttribute

CreateServiceNetworkResourceAssociation

- vpc-lattice:CreateServiceNetworkResourceAssociation
- ec2:AssignIpv6Addresses
- ec2:CreateNetworkInterface
- ec2:CreateNetworkInterfacePermission
- ec2:DescribeNetworkInterfaces

`CreateServiceNetworkVpcAssociation`

- `vpc-lattice:CreateServiceNetworkVpcAssociation`
- `ec2:DescribeVpcs`
- `ec2:DescribeSecurityGroups` (Solo es necesario cuando se proporcionan grupos de seguridad)

`UpdateServiceNetworkVpcAssociation`

- `vpc-lattice:UpdateServiceNetworkVpcAssociation`
- `ec2:DescribeSecurityGroups` (Solo es necesario cuando se proporcionan grupos de seguridad)

`CreateTargetGroup`

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

`RegisterTargets`

- `vpc-lattice:RegisterTargets`
- `ec2:DescribeInstances` (Solo es necesario cuando `INSTANCE` es el tipo de grupo de destino)
- `ec2:DescribeVpcs` (Solo es necesario cuando `INSTANCE` o `IP` es el tipo de grupo de destino)
- `ec2:DescribeSubnets` (Solo es necesario cuando `INSTANCE` o `IP` es el tipo de grupo de destino)
- `lambda:GetFunction` (Solo es necesario cuando `LAMBDA` es el tipo de grupo de destino)
- `lambda:AddPermission` (Solo es necesario si el grupo de destino aún no tiene permiso para invocar la función de Lambda especificada)

`DeregisterTargets`

- `vpc-lattice:DeregisterTargets`

`CreateAccessLogSubscription`

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

`DeleteAccessLogSubscription`

- `vpc-lattice:DeleteAccessLogSubscription`

- `logs:DeleteLogDelivery`

`UpdateAccessLogSubscription`

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

Políticas basadas en identidad para Amazon VPC Lattice

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar los recursos de VPC Lattice. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la API. AWS Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puedes añadir las políticas de IAM a roles y los usuarios puedes asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por VPC Lattice, incluido el formato de cada uno de los ARNs tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon VPC Lattice en la Referencia de autorización de servicios.

Contenido

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidad determinan si alguien puede crear, acceder o eliminar los recursos de VPC Lattice de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las

políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.

- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Permisos necesarios adicionales para obtener acceso completo

Para utilizar otros AWS servicios con los que está integrado VPC Lattice y todo el conjunto de funciones de VPC Lattice, debe disponer de permisos adicionales específicos. Estos permisos

no están incluidos en la política administrada de `VPCLatticeFullAccess` debido al riesgo de escalada de privilegios suplente confuso.

Debe adjuntar la siguiente política a su rol y utilizarla junto con la política administrada de `VPCLatticeFullAccess`.

JSON

```
{
    "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*"
        }
    ]
}
```

Esta política ofrece los siguientes permisos adicionales:

- `iam:AttachRolePolicy`: permite asociar la política administrada especificada para el rol de IAM especificado.
- `iam:PutRolePolicy`: permite agregar o actualizar un documento de política insertado que está integrado en el rol de IAM especificado.
- `s3:PutBucketPolicy`: permite aplicar una política de bucket a un bucket de Amazon S3.
- `firehose:TagDeliveryStream`: permite actualizar o agregar etiquetas a los flujos de entrega de Firehose.

Ejemplos de políticas basadas en identidad de VPC Lattice

Temas

Ejemplo de política: administrar las asociaciones de VPC a una red de servicios

En el siguiente ejemplo se muestra una política que otorga a los usuarios con esta política el permiso para crear, actualizar y eliminar las asociaciones de VPC a una red de servicios, pero solo para la VPC y la red de servicios especificada en la condición. Para obtener más información acerca de cómo especificar claves de condición, consulte Claves de condición de política para VPC Lattice.

JSON

```
{
   "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"
            }
         }
      }
   ]
}
```

Ejemplo de política: crear asociaciones de servicios a una red de servicios

Si no utiliza claves de condición para controlar el acceso a los recursos de VPC Lattice, puede especificar los recursos ARNs del `Resource` elemento para controlar el acceso.

El siguiente ejemplo muestra una política que limita las asociaciones de servicios a una red de servicios que los usuarios con esta política puedan crear especificando el servicio y la red ARNs de servicios que se pueden utilizar con la acción de la `CreateServiceNetworkServiceAssociation` API. Para obtener más información sobre cómo especificar los valores de los ARN, consulte Recursos de políticas para VPC Lattice.

JSON

```
{
```

```
   "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"
         ]
      }
   ]
}
```

Ejemplo de política: añadir etiquetas a los recursos

En el siguiente ejemplo se muestra una política que otorga a los usuarios con esta política permiso para crear etiquetas en los recursos de VPC Lattice.

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "vpc-lattice:TagResource"
         ],
         "Resource": "arn:aws:vpc-lattice:us-west-2:123456789012:*/*"
      }
   ]
}
```

Ejemplo de política: crear un rol vinculado a un servicio

VPC Lattice requiere permisos para crear un rol vinculado a un servicio la primera vez que un usuario de VPC Lattice crea Cuenta de AWS recursos de VPC Lattice. Si el rol vinculado al servicio aún no existe, VPC Lattice lo crea en su cuenta. La función vinculada al servicio otorga permisos a VPC Lattice para que pueda llamar a otras personas en su nombre. Servicios de AWS Para obtener más información, consulte the section called “Cómo utilizar roles vinculados a servicios”.

Para que la creación automática de roles se realice correctamente, los usuarios deben disponer de permisos para la acción `iam:CreateServiceLinkedRole`.

```
"Action": "iam:CreateServiceLinkedRole"
```

En el siguiente ejemplo se muestra una política que concede a los usuarios con esta política permiso para crear un rol vinculado a servicios para VPC Lattice.

JSON

```
{
   "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"
            }
         }
      }
   ]
}
```

Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Uso de roles vinculados a servicios para Amazon VPC Lattice

Amazon VPC Lattice utiliza un rol vinculado a un servicio para los permisos que necesita para llamar a otros en su nombre. Servicios de AWS Para obtener más información, consulte Roles vinculados al servicio en la Guía del usuario de IAM.

VPC Lattice usa el rol vinculado al servicio denominado. AWSServiceRoleForVpcLattice

Permisos de roles vinculados a servicios de VPC Lattice

El rol vinculado a servicio de AWSServiceRoleForVpcLattice confía en el siguiente servicio para asumir el rol:

- `vpc-lattice.amazonaws.com`

La política de permisos de roles denominada AWSVpcLatticeServiceRolePolicy permite a VPC Lattice publicar CloudWatch métricas en el espacio de nombres. `AWS/VpcLattice` Para obtener más información, consulte la Referencia de políticas AWSVpcLatticeServiceRolePolicyadministradas AWS .

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte the section called “Ejemplo de política: crear un rol vinculado a un servicio”.

Crear un rol vinculado a un servicio para VPC Lattice

No necesita crear manualmente un rol vinculado a servicios. Cuando crea recursos de VPC Lattice en la AWS Management Console, la o la API AWS CLI AWS , VPC Lattice crea el rol vinculado al servicio por usted.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear recursos de VPC Lattice, VPC Lattice vuelve a crear el rol vinculado a servicios por usted.

Edición de un rol vinculado a un servicio para VPC Lattice

Puede editar la descripción del uso de IAM. AWSServiceRoleForVpcLattice Para obtener más información, consulte la Descripción sobre cómo editar un rol vinculado al servicio en la Guía del usuario de IAM.

Eliminar un rol vinculado a un servicio para VPC Lattice

Si ya no necesita usar Amazon VPC Lattice, le recomendamos que lo elimine. AWSServiceRoleForVpcLattice

Solo puede eliminar este rol vinculado a un servicio después de eliminar todos los recursos de VPC Lattice en su Cuenta de AWS.

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForVpcLatticeservicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Después de eliminar un rol vinculado a un servicio, VPC Lattice crea de nuevo el rol si se crean recursos de VPC Lattice en su Cuenta de AWS.

Regiones admitidas para los roles vinculados a servicios de VPC Lattice

VPC Lattice admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio esté disponible.

AWS políticas gestionadas para Amazon VPC Lattice

Una política AWS gestionada es una política independiente creada y administrada por. AWS AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

AWS política gestionada: VPCLattice FullAccess

Esta política proporciona acceso completo a Amazon VPC Lattice y acceso limitado a otros servicios dependientes. Incluye permisos para hacer lo siguiente:

- ACM: recupera el ARN del SSL/TLS certificado para los nombres de dominio personalizados.
- CloudWatch — Ver los registros de acceso y los datos de monitoreo.
- CloudWatch Registros: configure y envíe los registros de acceso a CloudWatch Logs.
- Amazon EC2 : configure las interfaces de red y recupere información sobre EC2 las instancias y VPCs. Se utiliza para crear configuraciones de recursos, pasarelas de recursos y grupos de objetivos, configurar asociaciones de entidades de VPC Lattice y registrar destinos.
- Elastic Load Balancing: recupere información sobre un equilibrador de carga de aplicación para registrarlo como destino.
- Firehose: recupera información sobre los flujos de entrega utilizados para almacenar los registros de acceso.
- Lambda: recupere información sobre una función de Lambda para registrarla como destino.
- Amazon RDS: recupere información sobre clústeres e instancias de RDS.
- Amazon S3: recupere información acerca de los buckets de S3 utilizados para almacenar registros de acceso.

Para ver los permisos de esta política, consulte VPCLatticeFullAccess en la Referencia de la política administrada de AWS .

Para utilizar otros AWS servicios con los que está integrado VPC Lattice y todo el conjunto de funciones de VPC Lattice, debe disponer de permisos adicionales específicos. Estos permisos no están incluidos en la política administrada `VPCLatticeFullAccess` debido al riesgo de escalada de privilegios suplente confuso. Para obtener más información, consulte Permisos necesarios adicionales para obtener acceso completo.

AWS política gestionada: VPCLattice ReadOnlyAccess

Esta política proporciona acceso de solo lectura a Amazon VPC Lattice y acceso limitado a otros servicios dependientes. Incluye permisos para hacer lo siguiente:

- ACM: recupera el ARN del SSL/TLS certificado para los nombres de dominio personalizados.
- CloudWatch — Ver los registros de acceso y los datos de monitoreo.

- CloudWatch Registros: consulte la información de entrega de registros para las suscripciones a los registros de acceso.
- Amazon EC2 : recupera información sobre EC2 las instancias y VPCs crea grupos de objetivos y registra los objetivos.
- Elastic Load Balancing: recupere información sobre un equilibrador de carga de aplicación.
- Firehose: recupera información sobre los flujos de entrega para acceder a la entrega de registros.
- Lambda: consulte información acerca de una función de Lambda.
- Amazon RDS: recupere información sobre clústeres e instancias de RDS.
- Amazon S3: recupere información sobre los buckets de S3 para la entrega de registros de acceso.

Para ver los permisos de esta política, consulte VPCLatticeReadOnlyAccess en la Referencia de la política administrada de AWS .

AWS política gestionada: VPCLattice ServicesInvokeAccess

Esta política proporciona acceso para invocar los servicios de Amazon VPC Lattice.

Para ver los permisos de esta política, consulte VPCLatticeServicesInvokeAccess en la Referencia de la política administrada de AWS .

AWS política gestionada: AWSVpc LatticeServiceRolePolicy

Esta política se adjunta a un rol vinculado a un servicio denominado AWSServiceRoleForVpcLatticepara permitir que VPC Lattice realice acciones en su nombre. No puede adjuntar esta política a sus entidades de IAM. Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon VPC Lattice.

Para ver los permisos de esta política, consulte AWSVpcLatticeServiceRolePolicy en la Referencia de la política administrada de AWS .

Actualizaciones de VPC Lattice a las políticas gestionadas AWS

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas para VPC Lattice desde que este servicio comenzó a realizar un seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS para consultar la Guía del usuario de VPC Lattice.

Cambio	Descripción	Fecha
VPCLatticeFullAccess	VPC Lattice añade permisos de solo lectura para describir los clústeres e instancias de Amazon RDS.	1 de diciembre de 2024
VPCLatticeReadOnlyAccess	VPC Lattice añade permisos de solo lectura para describir los clústeres e instancias de Amazon RDS.	1 de diciembre de 2024
AWSVpcLatticeServiceRolePolicy	VPC Lattice añade permisos para permitir que VPC Lattice cree una interfaz de red gestionada por el solicitante.	1 de diciembre de 2024
VPCLatticeFullAccess	VPC Lattice añade una nueva política para conceder permisos de acceso total a Amazon VPC Lattice y acceso limitado a otros servicios dependientes.	31 de marzo de 2023
VPCLatticeReadOnlyAccess	VPC Lattice añade una nueva política para conceder permisos de acceso de solo lectura a Amazon VPC Lattice y acceso limitado a otros servicios dependientes.	31 de marzo de 2023
VPCLatticeServicesInvokeAccess	VPC Lattice añade una nueva política para conceder acceso para invocar los servicios de Amazon VPC Lattice.	31 de marzo de 2023
AWSVpcLatticeServiceRolePolicy	VPC Lattice añade permisos a su función vinculada al servicio para permitir que VPC Lattice publique métricas en el espacio de nombres. CloudWatch `AWS/VpcLattice` La `AWSVpcLatticeServi`	5 de diciembre de 2022

Cambio	Descripción	Fecha
	`ceRolePolicy` política incluye el permiso para activar la acción de la API. CloudWatch PutMetricData Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon VPC Lattice.	
Inicio de seguimiento de cambios de VPC Lattice	VPC Lattice comenzó a realizar un seguimiento de los cambios en sus AWS políticas gestionadas.	5 de diciembre de 2022

Validación de la conformidad para Amazon VPC Lattice

Los auditores externos evalúan la seguridad y la conformidad de Amazon VPC Lattice como parte de varios AWS programas de conformidad.

Para saber si un programa de conformidad Servicio de AWS se encuentra dentro del ámbito de aplicación de programas de conformidad específicos, consulte Servicios de AWS Alcance por programa de conformidad Servicios de AWS y elija el programa de conformidad que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.

- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Acceda a Amazon VPC Lattice mediante puntos de enlace de interfaz ()AWS PrivateLink

Puede establecer una conexión privada entre la VPC y Amazon VPC Lattice mediante la creación de un punto de conexión de VPC de interfaz. Los puntos finales de la interfaz funcionan con una tecnología que le permite acceder de forma privada a VPC APIs Lattice sin una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión. AWS PrivateLink AWS Direct Connect Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con VPC Lattice. APIs

Cada punto de conexión de la interfaz está representado por una o más interfaces de red en las subredes.

Consideraciones para los puntos de conexión de VPC de interfaz

Antes de configurar un punto final de VPC de interfaz para VPC Lattice, asegúrese de revisar Access Servicios de AWS Through en la guía. AWS PrivateLinkAWS PrivateLink

VPC Lattice admite realizar llamadas a todas sus acciones de la API desde su VPC.

Creación de un punto de conexión de VPC de interfaz para VPC Lattice

Puede crear un punto de conexión de VPC para el servicio VPC Lattice mediante la consola de Amazon VPC o el (). AWS Command Line Interface AWS CLIPara obtener más información, consulte Crear un punto final de VPC de interfaz en la AWS PrivateLink Guía.

Cree un punto de conexión de VPC para VPC Lattice con el siguiente nombre de servicio:

`com.amazonaws.region.vpc-lattice`

Si habilita el DNS privado para el punto de conexión, puede realizar solicitudes de API a VPC Lattice usando su nombre de DNS predeterminado para la región, por ejemplo, `vpc-lattice.us-east-1.amazonaws.com`.

Resiliencia de Amazon VPC Lattice

La infraestructura AWS global se basa Regiones de AWS en zonas de disponibilidad.

Regiones de AWS proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia.

Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las zonas de disponibilidad Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global.AWS

Seguridad de infraestructura en Amazon VPC Lattice

Como servicio gestionado, Amazon VPC Lattice está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la

infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Las llamadas a la API AWS publicadas se utilizan para acceder a VPC Lattice a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Monitoreo de Amazon VPC Lattice

Utilice las características de esta sección para monitorear las redes de servicios, los servicios, los grupos de destino y las conexiones de VPC de su Amazon VPC Lattice.

Contenido

CloudWatch métricas de Amazon VPC Lattice

Amazon VPC Lattice envía los datos relacionados con sus grupos de destino y los servicios a Amazon CloudWatch y los procesa en métricas legibles casi en tiempo real. Estas métricas se mantienen durante 15 meses, de forma que pueda acceder a información histórica y disponer de una mejor perspectiva sobre el desempeño de su aplicación web o servicio. También puede establecer alarmas que observen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulte la Guía de CloudWatch usuario de Amazon.

Amazon VPC Lattice utiliza un rol de servicio en su AWS cuenta de para enviar métricas a Amazon. CloudWatch Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon VPC Lattice.

Contenido

Consulta de CloudWatch métricas de Amazon

Puede consultar las CloudWatch métricas de Amazon para sus grupos de destino y los servicios a través de la CloudWatch consola o la AWS CLI.

Para consultar las métricas desde la CloudWatch consola de

1. Abre la CloudWatch consola de Amazon en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Métricas.
3. Seleccione el espacio de nombres de `AWS/VpcLattice`.
4. (Opcional) Para ver una métrica en todas las dimensiones, ingrese su nombre en el campo de búsqueda.
5. (Opcional) Para filtrar por dimensión, seleccione una de las siguientes opciones:
   - Para mostrar solamente las métricas registradas para los grupos de destino, elija Grupos de destino. Para ver las métricas de un solo grupo de destino, escriba su nombre en el campo de búsqueda.
   - Para mostrar únicamente las métricas reportadas para sus servicios, elija Servicios. Para consultar las métricas de un solo servicio, escriba su nombre en el campo de búsqueda.

Para ver las métricas mediante el AWS CLI

Utilice el siguiente AWS CLI comando CloudWatch list-metrics para obtener una lista de las métricas disponibles:

```
aws cloudwatch list-metrics --namespace AWS/VpcLattice
```

Para obtener información acerca de las métricas y sus dimensiones, vea Métricas del grupo de destino y Métricas de servicios.

Métricas del grupo de destino

VPC Lattice almacena automáticamente las métricas relacionadas con los grupos de destino en el espacio de nombres Amazon `AWS/VpcLattice` Namespace. CloudWatch Para obtener más información acerca de los grupos de destino, vea Grupos de destino en VPC Lattice.

Dimensiones

Para filtrar las métricas de los grupos de destino, utilice las siguientes dimensiones:

- `AvailabilityZone`
- `TargetGroup`

Métrica	Descripción
`TotalConnectionCount`	Conexiones totales. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es `Sum`.
`ActiveConnectionCount`	Conexiones activas. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es `Sum`.
`ConnectionErrorCount`	Fallos totales de conexión. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico.

Métrica	Descripción
	Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es Sum.
HTTP1_ConnectionCount	Conexiones totales de HTTP/1.1. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es Sum.
HTTP2_ConnectionCount	Conexiones totales de HTTP/2. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es Sum.

Métrica	Descripción
`ConnectionTimeoutCount`	Límite de tiempo de espera para la conexión total. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es `Sum`.
`TotalReceivedConnectionBytes`	Total de bytes de conexión recibidos. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es `Sum`.

Métrica	Descripción
`TotalSentConnectionBytes`	Total de bytes de conexión enviados. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es `Sum`.
`TotalRequestCount`	Total de solicitudes. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es `Sum`.

Métrica	Descripción
`ActiveRequestCount`	Total de solicitudes activas. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es `Sum`.
`RequestTime`	Solicita el tiempo hasta el último byte en milisegundos. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • Las estadísticas más útiles son `Average` y `pNN.NN` (percentiles).

Métrica	Descripción
`HTTPCode_2XX_Count`, `HTTPCode_3XX_Count`, `HTTPCode_4XX_Count`, `HTTPCode_5XX_Count`	Códigos de respuesta de agregados HTTP. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es `Sum`.
`TLSConnectionErrorCount`	El total de errores de conexión TLS no incluye las verificaciones de certificados fallidas. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es `Sum`.

Métrica	Descripción
`TotalTLSConnection HandshakeCount`	Una conexión TLS totalmente exitosa. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es `Sum`.

Métricas de servicios

VPC Lattice almacena automáticamente las métricas relacionadas con los servicios en el espacio de nombres `AmazonAWS/VpcLattice`. CloudWatch Para obtener más información acerca de los servicios, consulte Servicios en VPC Lattice.

Dimensiones

Para filtrar las métricas de los grupos de destino, utilice las siguientes dimensiones:

- `AvailabilityZone`
- `Service`

Métrica	Descripción
`RequestTimeoutCount`	Número total de solicitudes en las que se agotó el tiempo de espera para recibir una respuesta.

Métrica	Descripción
	Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es `Sum`.
`TotalRequestCount`	Total de solicitudes. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es `Sum`.

Métrica	Descripción
`RequestTime`	Tiempo de solicitud en milisegundos. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • Las estadísticas más útiles son `Average` y `pNN.NN` (percentiles).
`HTTPCode_2XX_Count`, `HTTPCode_3XX_Count`, `HTTPCode_4XX_Count`, `HTTPCode_5XX_Count`	Códigos de respuesta de agregados HTTP. Criterios de presentación de informes • Siempre se informa (ya sea un valor equivalente o distinto a cero) desde el momento en el que el recurso recibe tráfico. Frecuencia de informes • Cada un minuto. Estadísticas • La estadística más conveniente es `Sum`.

Registros de acceso para Amazon VPC Lattice

Los registros de acceso recopilan información detallada sobre las configuraciones de recursos y servicios de VPC Lattice. Puede usar estos registros de acceso para analizar los

patrones de tráfico y controlar todos los servicios de la red. Para los servicios de VPC Lattice, publicamos `VpcLatticeAccessLogs` y para las configuraciones de recursos, publicamos las `VpcLatticeResourceAccessLogs` que deben configurarse por separado.

Los registros de acceso son opcionales y están deshabilitados de forma predeterminada. Después de habilitar los registros de acceso, puede deshabilitarlos en cualquier momento.

Precios

Los cargos se aplican cuando se publican los registros de acceso. Los registros que se publican de AWS forma nativa en su nombre se denominan registros vendidos. Para obtener más información sobre los precios de los registros vendidos, consulta los CloudWatch precios de Amazon, selecciona Logs y consulta los precios en Vended Logs.

Contenido

Permisos de IAM necesarios para habilitar los registros de acceso

Para habilitar los registros de acceso y enviarlos a sus destinos, debe tener las siguientes acciones en la política asociada al usuario, grupo o rol de IAM que está utilizando.

JSON

```
{
    "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": [
                "*"
            ]
        }
    ]
}
```

Para obtener más información, consulte Adición y eliminación de permisos de identidad de IAM en la Guía del usuario de AWS Identity and Access Management .

Una vez que haya actualizado la política asociada al usuario, grupo o rol de IAM que está utilizando, vaya a Habilitación de registros de acceso.

Destinos de registro de acceso

Puede enviar registros de acceso a los siguientes destinos.

Amazon CloudWatch Logs

- Por lo general, VPC Lattice entrega los registros a los registros en CloudWatch 2 minutos. Sin embargo, tenga en cuenta que el tiempo real de entrega de los registros se basa en el mayor esfuerzo y puede haber una demora adicional.
- Se crea automáticamente una política de recursos y se agrega al grupo de CloudWatch registros si el grupo de registros no tiene determinados permisos. Para obtener más información, consulta Registros enviados a CloudWatch Logs en la Guía del CloudWatch usuario de Amazon.
- Puede encontrar los registros de acceso que se envían en la CloudWatch sección Grupos de registros de la CloudWatch consola. Para obtener más información, consulta Ver los datos de registro enviados a CloudWatch Logs en la Guía del CloudWatch usuario de Amazon.

Amazon S3

- Normalmente, VPC Lattice le entrega los registros a Amazon S3 en un plazo de 6 minutos. Sin embargo, tenga en cuenta que el tiempo real de entrega de los registros se basa en el mayor esfuerzo y puede haber una demora adicional.
- Se creará una política de bucket automáticamente y se añadirá a su bucket de Amazon S3 si este no cuenta con ciertos permisos. Para obtener más información, consulte Registros enviados a Amazon S3 en la Guía del CloudWatch usuario de Amazon.
- Los registros de acceso que se envían a Amazon S3 utilizan la siguiente convención de nomenclatura:

```
[bucket]/[prefix]/AWSLogs/[accountId]/VpcLattice/AccessLogs/[region]/[YYYY/
MM/DD]/[resource-id]/[accountId]_VpcLatticeAccessLogs_[region]_[resource-
id]_YYYYMMDDTHHmmZ_[hash].json.gz
```

- VpcLatticeResourceAccessLogs que se envían a Amazon S3 utilizan la siguiente convención de nomenclatura:

```
[bucket]/[prefix]/AWSLogs/[accountId]/VpcLattice/ResourceAccessLogs/[region]/[YYYY/
MM/DD]/[resource-id]/[accountId]_VpcLatticeResourceAccessLogs_[region]_[resource-
id]_YYYYMMDDTHHmmZ_[hash].json.gz
```

Amazon Data Firehose

- Por lo general, VPC Lattice entrega los troncos a Firehose en 2 minutos. Sin embargo, tenga en cuenta que el tiempo real de entrega de los registros se basa en el mayor esfuerzo y puede haber una demora adicional.
- Se crea automáticamente una función vinculada al servicio que otorga permiso a VPC Lattice para enviar registros de acceso a Amazon Data Firehose. Para que la creación automática de roles se realice correctamente, los usuarios deben disponer de permisos para la acción `iam:CreateServiceLinkedRole`. Para obtener más información, consulta los registros enviados a Amazon Data Firehose en la Guía del CloudWatch usuario de Amazon.
- Para obtener más información sobre cómo ver los registros enviados a Amazon Data Firehose, consulte el Monitoreo de Amazon Kinesis Data Streams dentro de la Guía del desarrollador de Amazon Data Firehose .

Habilitación de registros de acceso

Complete el siguiente procedimiento para configurar los registros de acceso a fin de capturar y entregar los registros de acceso al destino que elija.

Contenido

Habilitación de registro de acceso desde la consola

Puede habilitar los registros de acceso para una red de servicios, un servicio o una configuración de recursos durante la creación. También puede habilitar los registros de acceso después de crear una configuración de red de servicio, servicio o recurso, tal como se describe en el siguiente procedimiento.

Creación de un servicio básico mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Seleccione la configuración de red, servicio o recurso de servicio.
3. Elija Acciones, Editar configuraciones de registro.
4. Active el conmutador de Registros de acceso.
5. Añada un destino de entrega para sus registros de acceso de la siguiente manera:
    - Seleccione Grupo de CloudWatch registros y elija un grupo de registros. Para crear un grupo de registros, elija Crear un grupo de registros en CloudWatch.
    - Seleccione Bucket de S3 e introduzca la ruta del bucket de S3, incluido cualquier prefijo. Para buscar sus buckets de S3, elija Explorar S3.
    - Seleccione Flujo de entrega de Kinesis Data Firehose y elija un flujo de entrega. Para crear un flujo de entrega, elija Crear un flujo de entrega en Kinesis.
6. Seleccione Save changes (Guardar cambios).

Habilitación de registros de acceso mediante la AWS CLI

Use el comando CLI create-access-log-subscriptionpara habilitar los registros de acceso para redes o servicios de servicio.

Contenidos del registro de acceso

En la siguiente tabla se describen los campos de una entrada de registro de acceso.

Campo	Descripción	Formato
`hostHeader`	El encabezado de autoridad de la solicitud.	cadena
`sslCipher`	El nombre OpenSSL del conjunto de cifrados que se utiliza para establecer la conexión TLS del cliente.	cadena
`serviceNetworkArn`	La red de servicios ARN.	arn:aws:vpc-lattice: :servicen etwork/ *region account id*
`resolvedUser`	El ARN del usuario cuando se habilita y se realiza la autenticación.	anulación | ARN | “Anónimo” | “Desconocido”
`authDeniedReason`	El motivo por el que se rechaza el acceso cuando la autenticación está habilitada.	anulación | “Servicio” | “Red” | “Identidad”
`requestMethod`	El encabezado del método de la solicitud.	cadena
`targetGroupArn`	El grupo de hosts de destino al que pertenece el host de destino.	cadena
`tlsVersion`	La versión de TLS.	TLSv*x*
`userAgent`	El encabezado del usuario-a gente.	cadena
`ServerNameIndication`	[Solo HTTPS] El valor establecido en el socket de la	cadena

Campo	Descripción	Formato
	conexión ssl para la indicación de nombre de servidor (SNI).	
`destinationVpcId`	El ID del VPC de destino.	vpc- *xxxxxxxx*
`sourceIpPort`	Dirección IP y el puerto del origen.	*ip*:*port*
`targetIpPort`	La dirección IP y el puerto de destino.	*ip*:*port*
`serviceArn`	El servicio ARN.	arn:aws:vpc-lattice: :service/ *region account id*
`sourceVpcId`	El ID del VPC de origen.	vpc- *xxxxxxxx*
`requestPath`	La ruta de la solicitud.	LatticePath?:*path*
`startTime`	La hora de inicio de la solicitud .	*YYYY*- *MM* - *DD* T *HHMM*: Z *SS*
`protocol`	El protocolo. Actualmente, HTTP/1.1 o HTTP/2.	cadena
`responseCode`	El código de respuesta HTTP. Solo se registra el código de respuesta de los encabezad os finales. Para obtener más información, consulte Solución de problemas en el registro de acceso.	entero
`bytesReceived`	Los bytes de cuerpo y encabezado recibidos.	entero
`bytesSent`	Los bytes de cuerpo y encabezado enviados.	entero

Campo	Descripción	Formato
`duration`	Duración total en milisegundos de la solicitud desde la hora de inicio hasta la salida del último byte.	entero
`requestToTargetDuration`	Duración total en milisegundos de la solicitud desde la hora de inicio hasta el envío a destino del último byte.	entero
`responseFromTargetDuration`	Duración total en milisegundos de la solicitud desde el primer byte leído desde el host de destino hasta el envío al cliente del último byte.	entero
`grpcResponseCode`	El código de respuesta gRPC. Para obtener más información, consulte los Códigos de estado y su uso en gRPC. Este campo solo se registra si el servicio es compatible con gRPC.	entero
`callerPrincipal`	La entidad principal autenticada.	cadena
`callerX509SubjectCN`	El nombre del sujeto (CN).	cadena
`callerX509IssuerOU`	El emisor (OU).	cadena
`callerX509SANNameCN`	La alternativa del emisor (nombre/CN).	cadena
`callerX509SANDNS`	El nombre alternativo del sujeto (DNS).	cadena

Campo	Descripción	Formato
`callerX509SANURI`	El nombre alternativo del sujeto (URI).	cadena
`sourceVpcArn`	El ARN de la VPC en donde se originó la solicitud.	arn:aws:ec2: ::vpc/ *region account id*

Ejemplo

A continuación, se muestra un ejemplo de entrada de registro.

```
{
    "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
}
```

Contenido del registro de acceso a los recursos

En la siguiente tabla se describen los campos de una entrada del registro de acceso a los recursos.

Campo	Descripción	Formato
`serviceNetworkArn`	La red de servicios ARN.	arn: *partition* vpc-latti ce: ::servicenetwork/ *region account id*
`serviceNetworkReso urceAssociationId`	El ID del recurso de la red de servicio.	*snra-xxx*
`vpcEndpointId`	El ID del punto final que se utilizó para acceder al recurso.	cadena
`sourceVpcArn`	El ARN de la VPC de origen o la VPC desde la que se inició la conexión.	cadena
`resourceConfigurat ionArn`	El ARN de la configuración de recursos a la que se accedió.	cadena
`protocol`	El protocolo utilizado para comunicarse con la configura ción de recursos. Actualmen te, solo se admite tcp.	cadena
`sourceIpPort`	La dirección IP y el puerto de la fuente que inició la conexión.	*ip*:*port*
`destinationIpPort`	La dirección IP y el puerto desde los que se inició la conexión. Será la IP de SN-E/ SN-A.	*ip*:*port*
`gatewayIpPort`	La dirección IP y el puerto utilizados por la puerta de	*ip*:*port*

Campo	Descripción	Formato
	enlace de recursos para acceder al recurso.	
`resourceIpPort`	La dirección IP y el puerto del recurso.	*ip*:*port*

Ejemplo

A continuación, se muestra un ejemplo de entrada de registro.

```
{
    "eventTimestamp": "2024-12-02T10:10:10.123Z",
    "serviceNetworkArn": "arn:aws:vpc-lattice:us-west-2:1234567890:servicenetwork/
sn-1a2b3c4d",
    "serviceNetworkResourceAssociationId": "snra-1a2b3c4d",
    "vpcEndpointId": "vpce-01a2b3c4d",
    "sourceVpcArn": "arn:aws:ec2:us-west-2:1234567890:vpc/vpc-01a2b3c4d",
    "resourceConfigurationArn": "arn:aws:vpc-lattice:us-
west-2:0987654321:resourceconfiguration/rcfg-01a2b3c4d",
    "protocol": "tcp",
    "sourceIpPort": "172.31.23.56:44076",
    "destinationIpPort": "172.31.31.226:80",
    "gatewayIpPort": "10.0.28.57:49288",
    "resourceIpPort": "10.0.18.190:80"
}
```

Solución de problemas en el registro de acceso

Esta sección contiene una explicación de los códigos de error HTTP que pueden aparecer en los registros de acceso.

Código de error	Causas posibles
HTTP 400: Solicitud errónea	• El cliente envió una solicitud incorrecta que no se ajusta a la especificación de HTTP. • El encabezado de la solicitud superó los 60 000 para todo el encabezado de la solicitud o los 100 encabezados.

Código de error	Causas posibles
	• El cliente cerró la conexión antes de enviar el cuerpo completo de la solicitud.
HTTP 403: Prohibido	Se configuró la autenticación del servicio, pero la solicitud entrante no está autenticada ni autorizada.
HTTP 404: servicio inexistente	Está intentando conectarse a un servicio que no existe o que no está registrado en la red de servicio correcta.
HTTP 500: Error interno del servidor	VPC Lattice ha detectado un error, por ejemplo, una falla al conectarse a los destinos.
HTTP 502: Bad Gateway	VPC Lattice ha detectado un error.

CloudTrail registros para Amazon VPC Lattice

Amazon VPC Lattice está integrado con AWS CloudTrailun servicio que proporciona un registro de las acciones realizadas por un usuario, rol o un. Servicio de AWS CloudTrail captura todas las llamadas a la API de VPC Lattice como eventos. Las llamadas capturadas incluyen llamadas desde la consola de VPC Lattice y llamadas de código a las operaciones de la API de VPC Lattice. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a VPC Lattice, la dirección IP desde la que se realizó la solicitud, cuándo se realizó y detalles adicionales.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó en nombre de un usuario de IAM Identity Center.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

CloudTrail está activa en tu cuenta Cuenta de AWS cuando creas la cuenta y tienes acceso automáticamente al historial de CloudTrail eventos. El historial de CloudTrail eventos proporciona un registro visible, consultable, descargable e inmutable de los últimos 90 días de eventos de gestión

registrados en un. Región de AWSPara obtener más información, consulte Uso del historial de CloudTrail eventos en la Guía del usuario.AWS CloudTrail La visualización del historial de eventos no conlleva ningún CloudTrail cargo.

Para tener un registro continuo de los eventos de Cuenta de AWS los últimos 90 días, crea un almacén de datos de eventos de senderos o CloudTraillagos.

CloudTrail senderos

Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Todos los senderos creados con él AWS Management Console son multirregionales. Puede crear un registro de seguimiento de una sola región o de varias regiones mediante la AWS CLI. Se recomienda crear un sendero multirregional, ya que puedes capturar toda la actividad de tu Regiones de AWS cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener más información acerca de los registros de seguimiento, consulte Creación de un registro de seguimiento para su Cuenta de AWS y Creación de un registro de seguimiento para una organización en la Guía del usuario de AWS CloudTrail .

Puede enviar una copia de sus eventos de administración en curso a su bucket de Amazon S3 sin coste alguno CloudTrail mediante la creación de una ruta; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

CloudTrail Almacenes de datos de eventos en Lake

CloudTrail Lake le permite ejecutar consultas basadas en SQL en sus eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato Apache ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información sobre CloudTrail Lake, consulte Cómo trabajar con AWS CloudTrail Lake en la Guía del AWS CloudTrail usuario.

CloudTrail Los almacenes de datos y las consultas sobre eventos de Lake conllevan costes. Cuando crea un almacén de datos de eventos, debe elegir la opción de precios que desee utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los

eventos, así como el período de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

Para controlar acciones adicionales, utilice los registros de acceso. Para obtener más información, consulte Registros de acceso.

Eventos de gestión de VPC Lattice en CloudTrail

Los eventos de administración proporcionan información sobre las operaciones de administración que se llevan a cabo en los recursos de su empresa. Cuenta de AWS Se denominan también operaciones del plano de control. De forma predeterminada, CloudTrail registra los eventos de administración.

Amazon VPC Lattice registra las operaciones del plano de control de VPC Lattice como eventos de administración. Para obtener una lista de las operaciones del plano de control de Amazon VPC Lattice en las que VPC Lattice inicia sesión, consulte CloudTrail la referencia de la API de Amazon VPC Lattice.

Ejemplos de eventos de VPC Lattice

Un evento representa una solicitud única de cualquier fuente e incluye información sobre la operación de API solicitada, la fecha y la hora de la operación, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que los eventos no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra un CloudTrail evento de la CreateServiceoperación.

```
{
  "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"
}
```

En el siguiente ejemplo, se muestra un CloudTrail evento de la DeleteServiceoperación.

```
{
  "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"
}
```


Para obtener información sobre el contenido de los CloudTrail registros, consulte el contenido de los CloudTrail registros en la Guía del AWS CloudTrail usuario.

Cuotas de Amazon VPC Lattice

Cuenta de AWS Tiene cuotas predeterminadas, anteriormente denominadas límites, para cada uno Servicio de AWS. A menos que se indique lo contrario, cada cuota es específica de la región. Puede solicitar aumentos para algunas cuotas, pero otras no se pueden aumentar.

Para ver las cuotas de VPC Lattice, abra la Consola de Service Quotas. En el panel de navegación, elija Servicios de AWS y seleccione VPC Lattice.

Para solicitar un aumento de cuota, consulte Solicitud de un aumento de cuota en la Guía de usuario de Service Quotas.

Cuenta de AWS Tiene las siguientes cuotas relacionadas con VPC Lattice.

Nombre	Valor predeterminado	Ajusta	Descripción
Tamaño de la política de autenticación	Cada región admitida: 10 kilobytes	No	Tamaño máximo de un archivo JSON en una política de autenticación.
Configuraciones de recursos secundarios por configuración de recursos de grupo	Cada región admitida: 40	Sí	El número máximo de configuraciones de recursos secundarios en una configuración de recursos de grupo. Para aumentar la capacidad y los límites adicionales, ponte en contacto con AWS Support.
Oyentes por servicio	Cada región admitida: 2	Sí	La cantidad máxima de oyentes que puede crear para un servicio. Para aumentar la capacidad y los límites adicionales, ponte en contacto con AWS Support.

Nombre	Valor predeterminado	Ajusta	Descripción
Configuraciones de recursos por red de servicio	Cada región admitida: 100	Sí	El número máximo de configuraciones de recursos asociadas a una red de servicios. Para aumentar la capacidad y los límites adicionales, ponte en contacto con AWS Support.
Configuraciones de recursos por AWS región	Cada región admitida: 500	Sí	El número máximo de configuraciones de recursos que puede tener una AWS cuenta por AWS región. Para aumentar la capacidad y los límites adicionales, ponte en contacto con AWS Support.
Puertas de enlace de recursos por VPC	Cada región admitida: 100	Sí	El número máximo de puertas de enlace de recursos en una VPC. Para aumentar la capacidad y los límites adicionales, ponte en contacto con AWS Support.

Nombre	Valor predeterminado	Ajusta	Descripción
Reglas por oyente	ca-central-1:10 Cada una de las demás regiones compatibles: 5	Sí	El número máximo de reglas que puede definir para el oyente de su servicio. Para aumentar la capacidad y los límites adicionales, ponte en contacto con AWS Support.
Grupos de seguridad por asociación	Cada región admitida: 5	No	Número máximo de grupos de seguridad que puede añadir a una asociación entre una VPC y una red de servicio.
Asociaciones de servicios por red de servicios	Cada región admitida: 500	Sí	Número máximo de servicios que puede asociar a una sola red de servicios. Para aumentar la capacidad y los límites adicionales, ponte en contacto con AWS Support.
Redes de servicios por región	Cada región admitida: 10	Sí	Número máximo de redes de servicios por región. Para aumentar la capacidad y los límites adicionales, ponte en contacto con AWS Support.

Nombre	Valor predeterminado	Ajusta	Descripción
Servicios por región	Cada región admitida: 500	Sí	El número máximo de servicios por región. Para aumentar la capacidad y los límites adicionales, ponte en contacto con AWS Support.
Grupos de destino por región	Cada región admitida: 500	Sí	El número máximo de grupos de destino por región. Para aumentar la capacidad y los límites adicionales, ponte en contacto con AWS Support.
Grupos de destino por servicio	ca-central-1:10 Cada una de las demás regiones compatibles: 5	Sí	Número máximo de grupos de destino que puede asociar a un servicio. Para aumentar la capacidad y los límites adicionales, ponte en contacto con AWS Support.
Destinos por grupo de destino	Cada región admitida: 1000	Sí	Número máximo de destinos que puede asociar a un solo grupo de destinos. Para aumentar la capacidad y los límites adicionales, ponte en contacto con AWS Support.

Nombre	Valor predeterminado	Ajusta	Descripción
Asociaciones de VPC por red de servicios	Cada región admitida: 500	Sí	La cantidad máxima VPCs que puede asociar a una sola red de servicio. Para aumentar la capacidad y los límites adicionales, ponte en contacto con AWS Support.
Puntos finales de VPC de tipo red de servicio por red de servicio	Cada región admitida: 50	Sí	El número máximo de puntos finales de la red de servicio asociados a una red de servicio. Para aumentar la capacidad y los límites adicionales, ponte en contacto con AWS Support.

Las siguientes zonas de disponibilidad no son compatibles con VPC Lattice:`use1-az3`,,,`usw1-az2`,`apne1-az3`, `apne2-az2euc1-az2`,`euw1-az4`. `cac1-az3` `ilc1-az2`

También aplican los siguientes límites.

Límite	Valor	Descripción
Ancho de banda por servicio por zona de disponibilidad	10 Gbps	El ancho de banda máximo asignado por servicio y por zona de disponibilidad.
Ancho de banda por puerta de enlace de recursos por zona de disponibilidad	100 Gbps	El ancho de banda máximo asignado por puerta de enlace de recursos por zona de disponibilidad.

Límite	Valor	Descripción
Unidad de transmisión máxima (MTU) por conexión	8500 bytes	El tamaño del paquete de datos más grande que puede aceptar un servicio.
Solicitudes por segundo por servicio y por zona de disponibilidad	10 000	En el caso de los servicios HTTP, este es el número máximo de solicitudes por segundo por servicio y por zona de disponibilidad.
Tiempo de inactividad de la conexión por conexión	1 minuto	El tiempo máximo que una conexión puede permanecer inactiva sin solicitudes activas (para HTTP y GRPC) o sin transferencia de datos activa (para TLS-PASSTHROUGH).
Duración máxima de la conexión por conexión	10 minutos	El tiempo máximo que puede estar abierta una conexión.
Red de servicio por VPC	1 red de servicio	Puede conectar una VPC a una sola red de servicio a través de una asociación. Para conectar una VPC a varias redes de servicio, puede utilizar puntos finales de VPC del tipo red de servicio.

Historial de documentos de la Guía del usuario de Amazon VPC Lattice

En la siguiente tabla se describen las versiones de la documentación de VPC Lattice.

Cambio	Descripción	Fecha
Se agregó VPC Lattice para Oracle Database@AWS	Lanzamiento de VPC Lattice. Oracle Database@AWS	26 de junio de 2025
Se agregó soporte de doble pila para los puntos finales de administración	VPC Lattice ahora admite puntos finales de doble pila (IPv4 y IPv6) para toda la administración de VPC Lattice. APIs	30 de abril de 2025
Comparta recursos y acceda a ellos	VPC Lattice ahora permite compartir y acceder a los recursos a través de los límites de la VPC y la cuenta. Esto incluye actualizaciones de las políticas y de las mismas VPCLatticeReadOnly Access. VPCLatticeFullAccess	1 de diciembre de 2024
Acceso directo a TLS	VPC Lattice ahora admite el paso directo de TLS, lo que le permite realizar la terminaci ón de TLS en su aplicación de autenticación. end-to-end	14 de mayo de 2024
Versión de la estructura de eventos Lambda	VPC Lattice ahora admite una nueva versión de la estructura de eventos de Lambda.	7 de septiembre de 2023
Support for shared VPCs	Los participantes pueden crear grupos de destino de VPC	5 de julio de 2023

	Lattice en una VPC compartid a.	
Versión de disponibilidad general	Versión de la Guía del usuario de VPC Lattice para disponibi lidad general (GA)	31 de marzo de 2023
VPC Lattice ahora informa de los cambios en sus políticas gestionadas AWS	Los cambios en las políticas administradas se indican en «Políticas AWS administr adas para VPC Lattice» en el capítulo «Seguridad».	29 de marzo de 2023
Compatibilidad con el tipo de destino Equilibrador de carga de aplicación	VPC Lattice ahora admite la creación de un grupo de destino de tipo Equilibrador de carga de aplicación.	29 de marzo de 2023
Compatibilidad con todos los tipos de instancias	VPC Lattice ahora es compatible con todos los tipos de instancias.	27 de marzo de 2023
IPv6 soporte	VPC Lattice ahora es compatible con ambos grupos de IPv4 destino IPv6 IP.	27 de marzo de 2023
HTTP2 versión de protocolo para controles de estado	Health checks ahora se admiten cuando la versión del protocolo del grupo objetivo es HTTP2.	27 de marzo de 2023
Acción de respuesta fija para las reglas de oyentes	Los oyentes de los servicios de VPC Lattice ahora admiten acciones de respuestas fijas además de acciones de reenvío.	27 de marzo de 2023

Compatibilidad con los nombres de dominio personalizados	Ahora puede configurar un nombre de dominio personalizado para su servicio de VPC Lattice	14 de febrero de 2023
Compatibilidad con BYOC (Traiga su propio certificado)	VPC Lattice admite el uso de su propio SSL/TLS certificado en ACM para nombres de dominio personalizados.	14 de febrero de 2023
VPC Lattice ahora informa una lista actualizada de tipos de instancias no compatibles	Se agregaron tres instancias adicionales a la lista de instancias no compatibles.	26 de enero de 2023
VPC Lattice ahora informa de los cambios en sus políticas gestionadas AWS	A partir del 5 de diciembre de 2022, los cambios en las políticas administradas se informan en el tema “Políticas administradas de AWS para VPC Lattice” en el capítulo “Seguridad”. El primer cambio de la lista es la adición de los permisos necesarios para CloudWatch la supervisión.	5 de diciembre de 2022
Versión inicial	Versión inicial de la Guía del usuario de VPC Lattice.	5 de diciembre de 2022

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.