AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

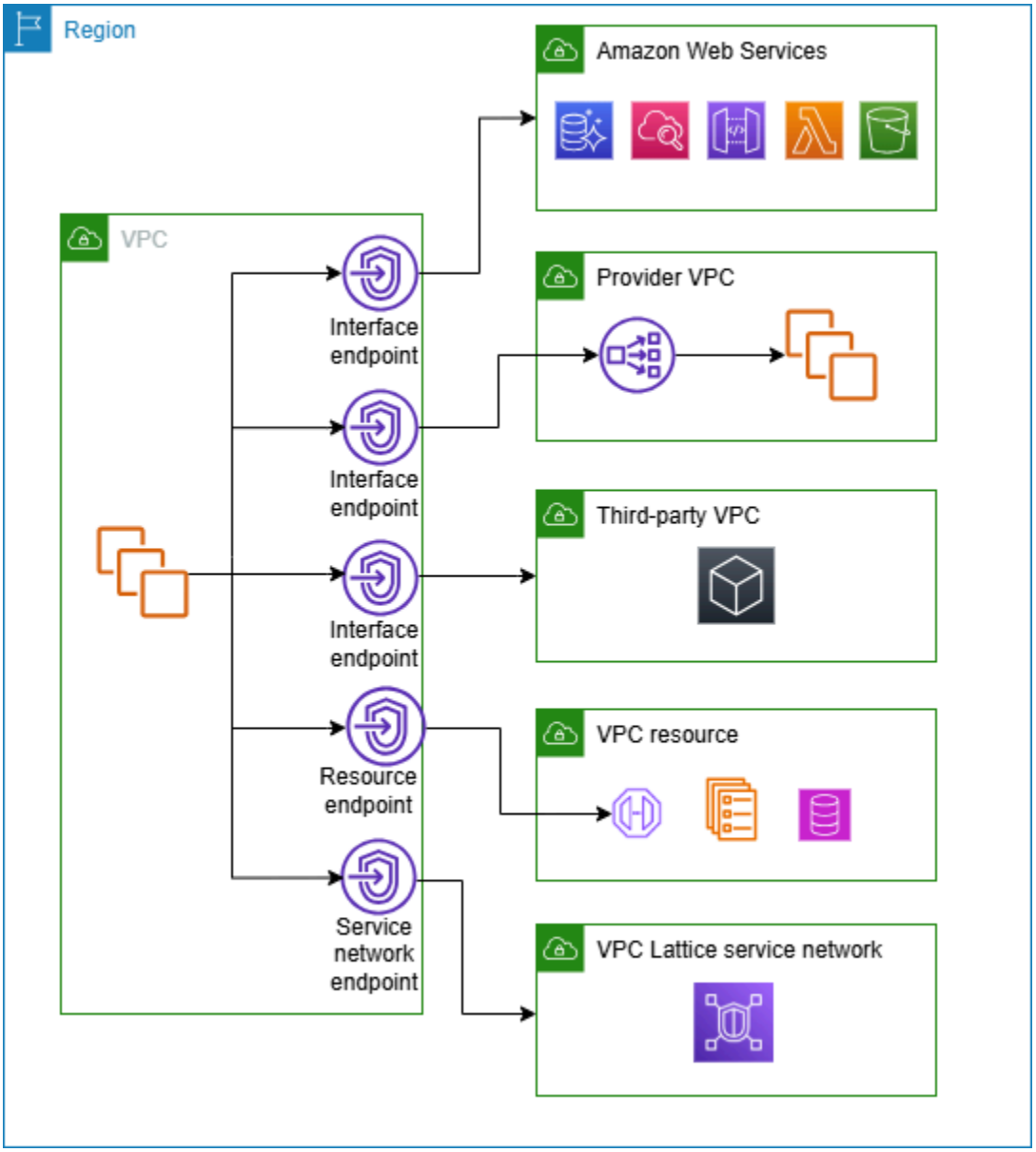
¿Qué es () AWS PrivateLink?

AWS PrivateLink es una tecnología escalable y de alta disponibilidad que puede usar para conectar de forma privada su VPC a servicios y recursos como si estuvieran en la VPC. No es necesario que utilice una puerta de enlace de Internet, un dispositivo NAT, una dirección IP pública, una conexión Direct Connect o una conexión AWS Site-to-Site VPN para comunicarse con el servicio o el recurso desde subredes privadas. Por lo tanto, controla los puntos de conexión, sitios y servicios de la API específicos a los que se puede acceder desde la VPC.

Casos de uso

Puede crear puntos de conexión de VPC para conectar clientes de la VPC a servicios y recursos que se integran con AWS PrivateLink. Puede crear su propio servicio de punto de conexión de VPC y permitir que otros clientes de AWS accedan al servicio. Para obtener más información, consulte the section called “Conceptos”.

En el siguiente diagrama, la VPC de la izquierda tiene varias instancias Amazon EC2 en una subred privada y cinco puntos de conexión de VPC: tres puntos de conexión de VPC de interfaz, un punto de conexión de VPC de recursos y un punto de conexión de VPC de red de servicios. El primer punto de conexión de VPC de interfaz se conecta a un servicio de AWS. El segundo punto de conexión de VPC de interfaz se conecta a un servicio alojado por otra cuenta de AWS (un servicio de punto de conexión de VPC). El tercer punto de conexión de VPC de interfaz se conecta a un servicio asociado de AWS Marketplace. El punto de conexión de VPC de recursos se conecta a una base de datos. El punto de conexión de VPC de red de servicios se conecta a una red de servicios.d



Más información

- Conceptos
- Acceso a Servicios de AWS
- Acceda a los productos SaaS
- Acceso a dispositivos virtuales
- Comparta sus servicios

Trabajo con puntos de enlace de la VPC

Puede crear, acceder y administrar puntos de enlace de la VPC mediante cualquiera de los siguientes procedimientos:

- Consola de administración de AWS: proporciona una interfaz web que se puede utilizar para obtener acceso a los recursos de AWS PrivateLink. Abra la consola de Amazon VPC y elija Puntos de conexión o Servicios de punto de conexión.
- AWS Command Line Interface (AWS CLI): proporciona comandos para un amplio conjunto de Servicios de AWS, incluido AWS PrivateLink. Para obtener más información sobre los comandos de AWS PrivateLink, consulte ec2 en la Referencia de comandos de la AWS CLI.
- CloudFormation: crea plantillas que describen tus recursos de AWS. Las plantillas se utilizan para aprovisionar y administrar estos recursos como una única unidad. Para obtener más información, consulte los recursos de AWS PrivateLink siguientes:
  - AWS::EC2::VPCEndpoint
  - AWS::EC2::VPCEndpointConnectionNotification
  - AWS::EC2::VPCEndpointService
  - AWS::EC2::VPCEndpointServicePermissions
  - AWS::ElasticLoadBalancingV2::LoadBalancer
- SDK de AWS: proporcionan API específicas del idioma. Los SDK se ocupan de muchos de los detalles de conexión, como el cálculo de firmas, la gestión de intentos de solicitud y la gestión de errores. Para obtener más información, consulte Herramientas para crear en AWS.
- API de consulta: proporciona acciones de API de nivel bajo a las que se llama mediante solicitudes HTTPS. El uso de la API de consulta es la forma más directa de acceder a Amazon VPC. Sin embargo, requiere que la aplicación gestione detalles de bajo nivel, como, por ejemplo, la generación del hash para firmar la solicitud y controlar errores. Para obtener más información, consulte Acciones de AWS PrivateLink en la Referencia de la API de Amazon EC2.

Precios

Para obtener información sobre los precios de los puntos de conexión de VPC, consulte Precios de AWS PrivateLink.

AWS PrivateLinkConceptos de

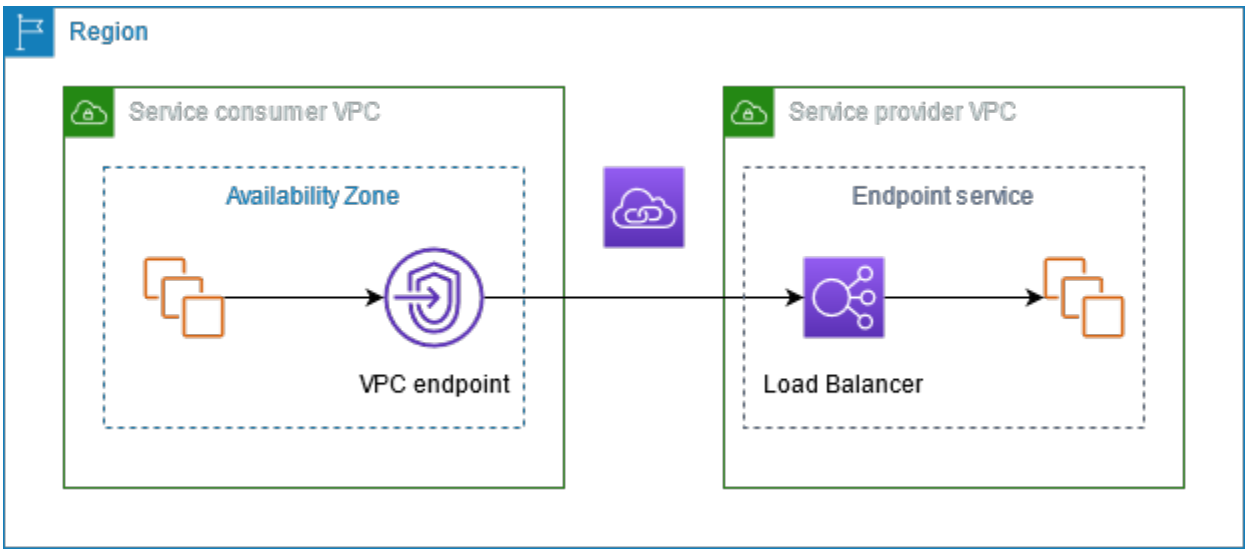
Puede utilizar Amazon VPC para definir una nube privada virtual (VPC), que es una red virtual aislada lógicamente. Puede permitir que los clientes de su VPC se conecten a destinos fuera de dicha VPC. Por ejemplo, agregue una puerta de enlace de Internet a la VPC para permitir el acceso a Internet o agregue una conexión de VPN para permitir el acceso a su red en las instalaciones. Como alternativa, utilice AWS PrivateLink para permitir que los clientes de su VPC se conecten a servicios y recursos de otras VPC mediante direcciones IP privadas, como si esos servicios y recursos estuvieran alojados directamente en su VPC.

Los siguientes conceptos son importantes y deben comprenderse cuando se comienza a utilizar AWS PrivateLink.

Contenido

Diagrama de arquitectura

El siguiente diagrama brinda información general de alto nivel sobre cómo funciona AWS PrivateLink. Los consumidores crean puntos de conexión de VPC para conectarse a servicios y recursos de punto de conexión alojados por proveedores.



Proveedores

Comprenda los conceptos relacionados con un proveedor.

Proveedor de servicios

El propietario de un servicio es el proveedor del servicio. Los proveedores de servicios incluyen AWS, socios de AWS y otras Cuentas de AWS. Los proveedores de servicios pueden alojar sus servicios mediante recursos de AWS, como instancias de EC2, o mediante servidores en las instalaciones.

Proveedor de recursos

El propietario de un recurso, por ejemplo, una base de datos o una instancia de Amazon EC2, es el proveedor del recurso. Los proveedores de recursos incluyen servicios de AWS, socios de AWS y otras cuentas de AWS. Los proveedores de recursos pueden alojar sus recursos en VPC o en las instalaciones.

Conceptos

- Servicios de punto de conexión
- Nombres de servicios
- Estados del servicio
- Configuración de recursos
- Puerta de enlace de recursos

Servicios de punto de conexión

Un proveedor de servicio crea un servicio de punto de conexión para que su servicio esté disponible en una región. Un proveedor de servicio debe especificar un equilibrador de carga cuando crea un servicio de punto de conexión. El equilibrador de carga recibe solicitudes de los consumidores del servicio y las dirige al servicio.

De forma predeterminada, el servicio de punto de conexión no está disponible para los consumidores del servicio. Debe agregar permisos que permitan a entidades principales específicas de AWS conectarse al servicio de punto de conexión.

Nombres de servicios

Cada servicio de punto de conexión se identifica con un nombre de servicio. El consumidor del servicio debe especificar el nombre del servicio cuando crea un punto de conexión de VPC. Los consumidores de servicios pueden consultar los nombres de los servicios de Servicios de AWS. Los proveedores de servicios deben compartir los nombres de sus servicios con los consumidores de servicios.

Estados del servicio

A continuación, se muestran los posibles estados de un servicio de punto de conexión:

- Pendiente: el servicio de punto de conexión se está creando.
- Disponible: el servicio de punto de conexión está disponible.
- Con error: el servicio de punto de conexión no se pudo crear.
- Eliminándose: el proveedor del servicio eliminó el servicio de punto de conexión y la eliminación está en curso.
- Eliminado: el servicio de punto de conexión se eliminó.

Configuración de recursos

El proveedor de recursos crea una configuración de recursos para compartir un recurso. Una configuración de recursos es un objeto lógico que representa un único recurso, como puede ser una base de datos, 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 Relational Database Service (Amazon RDS).

Al compartir con otras cuentas, el proveedor de recursos debe compartir el recurso a través de un recurso compartido AWS Resource Access Manager (AWS RAM) para permitir que entidades

principales de AWS específicas de la otra cuenta se conecten al recurso a través de un punto de conexión de VPC de recursos.

Las configuraciones de recursos se pueden asociar a una red de servicios a la que se conectan las entidades principales a través de un punto de conexión de VPC de la red de servicios.

Puerta de enlace de recursos

Una puerta de enlace de recursos es un punto de entrada a una VPC desde donde se comparte un recurso. El proveedor crea una puerta de enlace de recursos para compartir los recursos de la VPC.

Consumidores de servicios o recursos

El usuario de un servicio o recurso es un consumidor. Los consumidores pueden acceder a los servicios y recursos de los puntos de conexión desde sus VPC o en las instalaciones.

Conceptos

- Puntos de conexión de VPC
- Interfaces de red de punto de conexión
- Políticas de punto de conexión
- Estados del punto de conexión

Puntos de conexión de VPC

Un consumidor crea un punto de conexión de VPC para conectar su VPC a un servicio o recurso de punto de conexión. El consumidor debe especificar el servicio, el recurso o la red de servicios de punto de conexión, cuando se crea un punto de conexión de VPC. Hay varios tipos de puntos de conexión de VPC. Debe crear el tipo de punto de conexión de VPC que resulte necesario.

- `Interface`: cree un punto de conexión de interfaz para enviar tráfico TCP o UDP a un servicio de punto de conexión. El tráfico destinado al servicio de punto de conexión se resuelve mediante DNS.
- `GatewayLoadBalancer`: se crea un punto de conexión del equilibrador de carga de la puerta de enlace para enviar tráfico a una flota de dispositivos virtuales mediante direcciones IP privadas. El tráfico se enruta desde su VPC al punto de conexión del equilibrador de carga de la puerta de enlace mediante tablas de enrutamiento. El equilibrador de carga de la puerta de enlace distribuye el tráfico a los dispositivos virtuales y puede escalar en función de la demanda.

- `Resource`: cree un punto de conexión de recurso para acceder a un recurso que se compartió con usted y que reside en otra VPC. Un punto de conexión de recursos le permite acceder de forma privada y segura a recursos como una base de datos, una instancia de Amazon EC2, un punto de conexión de aplicación, un destino de nombre de dominio o una dirección IP que puede estar en una subred privada de otra VPC o en un entorno en las instalaciones. Los puntos de conexión de recursos no requieren un equilibrador de carga y permiten el acceso directo al recurso.
- `Service network`: cree un punto de conexión de red de servicios para acceder a una red de servicios que haya creado o que se haya compartido con usted. Puede utilizar un único punto de conexión de la red de servicios para acceder de forma privada y segura a varios recursos y servicios asociados a una red de servicios.

Hay otro tipo de punto de conexión de VPC, `Gateway`, que crea un punto de conexión de puerta de enlace para enviar tráfico a Amazon S3 o a DynamoDB. Los puntos de conexión de puerta de enlace no utilizan AWS PrivateLink, a diferencia de los otros tipos de puntos de conexión de VPC. Para obtener más información, consulte the section called “Puntos de conexión de la puerta de enlace”.

Interfaces de red de punto de conexión

Una interfaz de red de punto de conexión es una interfaz de red administrada por el solicitante que sirve como punto de entrada para el tráfico destinado a un servicio, un recurso o una red de servicios de punto de conexión. Para cada subred que especifica cuando crea un punto de conexión de VPC, creamos una interfaz de red de punto de conexión en la subred.

Si un punto de conexión de VPC admite IPv4, sus interfaces de red de punto de conexión tienen direcciones IPv4. Si un punto de conexión de VPC admite IPv6, sus interfaces de red de punto de conexión tienen direcciones IPv6. No se puede acceder a la dirección IPv6 de una interfaz de red de punto de conexión desde Internet. Cuando describa una interfaz de red de punto de conexión con una dirección IPv6, observe que `denyAllIgwTraffic` esté habilitado.

Políticas de punto de conexión

Una política de punto de conexión de VPC es una política de recursos de IAM que se adjunta a un punto de conexión de VPC. Determina qué entidades principales pueden utilizar el punto de conexión de VPC para acceder al servicio de punto de conexión. La política de punto de conexión de VPC predeterminada permite que todas las entidades principales realicen todas las acciones en todos los recursos del punto de conexión de VPC.

Estados del punto de conexión

Cuando se crea un punto de conexión de VPC de interfaz, el servicio de punto de conexión recibe una solicitud de conexión. El proveedor del servicio puede aceptar o rechazar la solicitud. Si el proveedor del servicio acepta la solicitud, el consumidor del servicio puede utilizar el punto de conexión de VPC una vez que esté en estado Disponible.

A continuación, se muestran los posibles estados de un punto de conexión de VPC:

- Aceptación pendiente: la solicitud de conexión está pendiente. Este es el estado inicial si las solicitudes se aceptan de forma manual.
- Pendiente: el proveedor del servicio ha aceptado la solicitud de conexión. Este es el estado inicial si las solicitudes se aceptan de forma automática. El punto de conexión de VPC vuelve a este estado si el consumidor del servicio modifica el punto de conexión de VPC.
- Disponible: el punto de conexión de VPC está disponible para su uso.
- Rechazado: el proveedor del servicio rechazó la solicitud de conexión. El proveedor del servicio también puede rechazar una conexión después de que esté disponible para su uso.
- Caducado: la solicitud de conexión caducó.
- Con erro: el punto de conexión de VPC no está disponible.
- Eliminándose: el consumidor del servicio eliminó el punto de conexión de VPC y la eliminación está en curso.
- Eliminado: el punto de conexión de VPC se ha eliminado.

La API de AWS PrivateLink devuelve los estados posibles mediante camel case.

Conexiones de AWS PrivateLink

El tráfico de la VPC se envía a un servicio de punto de conexión o un recurso mediante una conexión entre el punto de conexión de VPC y el servicio o recurso de punto de conexión. El tráfico entre un punto de conexión de VPC y un servicio o recurso de punto de conexión permanece dentro de la red de AWS sin atravesar la Internet pública.

Un proveedor de servicios agrega permisos para que los consumidores del servicio puedan acceder al servicio de punto de conexión. Los consumidores del servicio inician la conexión y el proveedor de servicios acepta o rechaza la solicitud de conexión. El propietario de un recurso o de una red de servicios comparte una configuración de recursos o una red de servicios con los consumidores

mediante AWS Resource Access Manager para que estos puedan acceder a los recursos o a la red de servicios.

Con puntos de conexión de VPC de interfaz, los consumidores pueden utilizar políticas de punto de conexión para controlar qué entidades principales de IAM pueden utilizar un punto de conexión de VPC para tener acceso a un servicio de punto de conexión.

Zonas alojadas privadas

Una zona alojada es un contenedor de registros DNS que define cómo enrutar el tráfico de un dominio o un subdominio. Con una zona alojada pública, los registros especifican cómo enrutar el tráfico en Internet. Con una zona alojada privada, los registros especifican cómo enrutar el tráfico en las VPC.

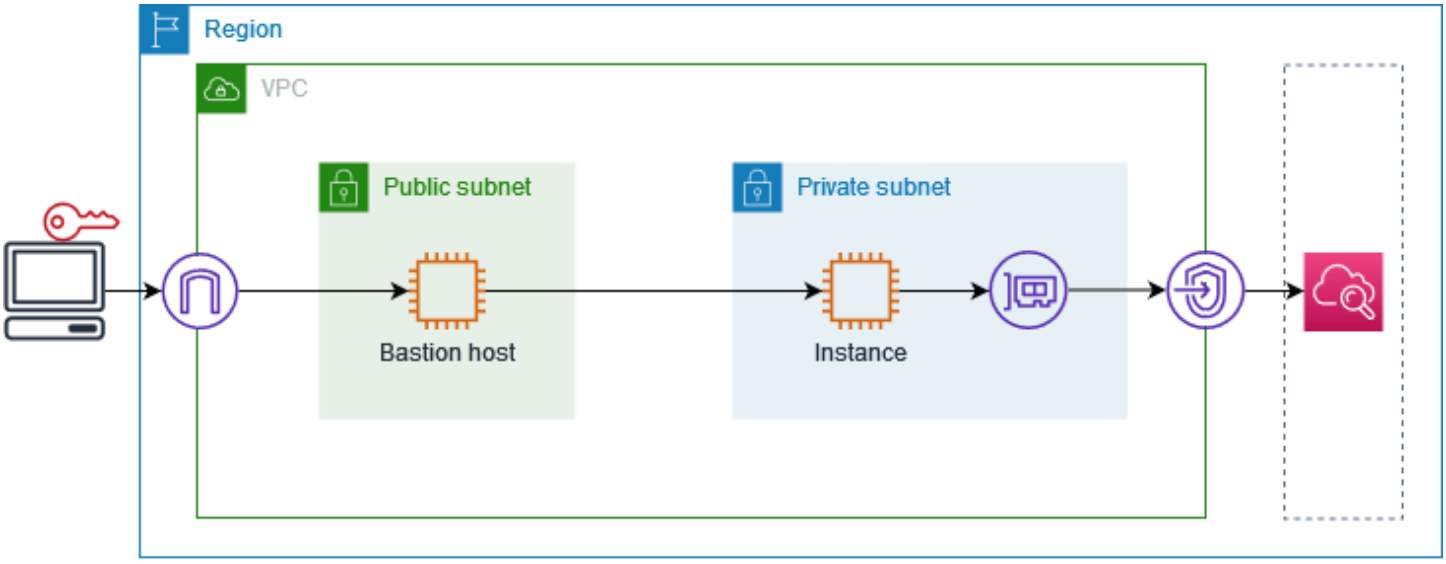
Puede configurar Amazon Route 53 para dirigir el tráfico del dominio a un punto de conexión de VPC. Para obtener más información, consulte Enrutamiento del tráfico a un punto de conexión de VPC mediante el nombre de dominio.

Puede utilizar Route 53 para configurar el DNS de horizonte dividido, donde puede utilizar el mismo nombre de dominio tanto para un sitio web público como para un servicio de punto de conexión con tecnología AWS PrivateLink. Las solicitudes DNS para el nombre de host público de la VPC del consumidor se resuelven en las direcciones IP privadas de las interfaces de red de punto de conexión, pero las solicitudes desde fuera de la VPC continúan resolviéndose en los puntos de conexión públicos. Para obtener más información, consulte Mecanismos de DNS para dirigir el tráfico y habilitar la conmutación por error para las implementaciones de AWS PrivateLink.

Empiece a utilizar AWS PrivateLink

Este tutorial demuestra cómo enviar una solicitud desde una instancia de EC2 en una subred privada a Amazon CloudWatch mediante AWS PrivateLink.

En el diagrama siguiente se proporciona información general sobre esta situación. Para conectarse desde el equipo a la instancia de la subred privada, primero se conectará a un host bastión de una subred pública. Tanto el host bastión como la instancia deben usar el mismo par de claves. Como el archivo `.pem` de la clave privada está en el equipo, no en el host bastión, utilizará el reenvío de claves SSH. A continuación, puede conectarse a la instancia desde el host bastión sin especificar el archivo `.pem` en el comando ssh. Tras configurar un punto de conexión de VPC para CloudWatch, el tráfico de la instancia destinada a CloudWatch se resuelve en la interfaz de red del punto de conexión y, a continuación, se envía a CloudWatch mediante el punto de conexión de VPC.



Para probar, puede utilizar una única zona de disponibilidad. En producción, se recomienda utilizar al menos dos zonas de disponibilidad para conseguir baja latencia y alta disponibilidad.

Tareas

- Paso 1: Creación de una VPC con subredes
- Paso 2: Lanzamiento de las instancias
- Paso 3: Prueba de acceso a CloudWatch
- Paso 4: Creación de un punto de conexión de VPC para acceder a CloudWatch
- Paso 5: Prueba del punto de conexión de VPC

Paso 1: Creación de una VPC con subredes

Utilice el siguiente procedimiento para crear una VPC con una subred pública y una subred privada.

Para crear la VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Seleccione Creación de VPC.
3. En Resources to create (Recursos para crear), elija VPC and more (VPC y más).
4. En Generación automática de etiquetas de nombre, ingrese un nombre para la VPC.
5. Para configurar las subredes, haga lo siguiente:
    a. En Number of Availability Zones (Número de zonas de disponibilidad), elija 1 o 2, según sus necesidades.
    b. En Number of public subnets (Número de subredes públicas), asegúrese de tener una subred pública por zona de disponibilidad.
    c. En Number of private subnets (Número de subredes privadas), asegúrese de tener una subred privada por zona de disponibilidad.
6. Seleccione Creación de VPC.

Paso 2: Lanzamiento de las instancias

Con la VPC que creó en el paso anterior, lance el host bastión en la subred pública y la instancia en la subred privada.

Requisitos previos

- Cree un par de claves con el formato .pem. Debe elegir este par de claves al lanzar tanto el host bastión como la instancia.
- Cree un grupo de seguridad para el host bastión que permita el tráfico SSH entrante desde el bloque CIDR para su equipo.
- Cree un grupo de seguridad para la instancia que permita el tráfico SSH entrante desde el grupo de seguridad para el host bastión.
- Cree un perfil de instancia de IAM y asocie la política CloudWatchReadOnlyAccess.

Para lanzar el host bastión

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Seleccione Iniciar instancia.
3. En Name (Nombre), ingrese un nombre para el host bastión.
4. Conserve la imagen y el tipo de instancia predeterminados.
5. En Key pair (Par de claves), seleccione su par de claves.
6. En Network settings (Configuración de red), haga lo siguiente:
    a. En VPC, elija su VPC.
    b. En Subnet (Subred), elija la subred pública.
    c. En Auto-assign public IP (Autoasignar IP pública), elija Enable (Habilitar).
    d. Para Firewall, elija Select existing security group (Seleccionar un grupo de seguridad existente) y, a continuación, elija el grupo de seguridad para el host bastión.
7. Seleccione Iniciar instancia.

Para lanzar la instancia

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Seleccione Iniciar instancia.
3. En Name (Nombre), ingrese un nombre para la instancia.
4. Conserve la imagen y el tipo de instancia predeterminados.
5. En Key pair (Par de claves), seleccione su par de claves.
6. En Network settings (Configuración de red), haga lo siguiente:
    a. En VPC, elija su VPC.
    b. En Subnet (Subred), elija la subred privada.
    c. En Auto-assign public IP (Autoasignar IP pública), elija Disable (Deshabilitar).
    d. Para Firewall, elija Select existing security group (Seleccionar un grupo de seguridad existente) y, a continuación, elija el grupo de seguridad para la instancia.
7. Amplíe Advanced details (Detalles avanzados). En IAM instance profile (Perfil de instancia de IAM), elija el perfil de instancia de IAM.
8. Seleccione Iniciar instancia.

Paso 3: Prueba de acceso a CloudWatch

Utilice el siguiente procedimiento para confirmar que la instancia no puede acceder a CloudWatch. Lo hará mediante un comando AWS CLI de solo lectura para CloudWatch.

Para probar el acceso a CloudWatch

1. Desde el equipo, agregue el par de claves al agente SSH mediante el siguiente comando, donde *key.pem* es el nombre del archivo .pem.

   ```
   ssh-add ./key.pem
   ```

   Si recibe un error que indica que los permisos de su par de claves están demasiado abiertos, ejecute el siguiente comando y, a continuación, vuelva a intentar el comando anterior.

   ```
   chmod 400 ./key.pem
   ```

2. Conéctese al bastión host desde el equipo. Debe especificar la opción `-A`, el nombre de usuario de la instancia (por ejemplo, `ec2-user`) y la dirección IP pública del host bastión.

   ```
   ssh -A ec2-user@bastion-public-ip-address
   ```

3. Conéctese a la instancia desde el host bastión. Debe especificar el nombre de usuario de la instancia (por ejemplo, `ec2-user`) y la dirección IP privada de la instancia.

   ```
   ssh ec2-user@instance-private-ip-address
   ```

4. Ejecute el comando list-metrics de CloudWatch en la instancia de la siguiente manera. Para la opción `--region`, especifique la región en la que creó la VPC.

   ```
   aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
   ```

5. Transcurridos unos minutos, se agota el tiempo de espera del comando. Esto demuestra que no puede acceder a CloudWatch desde la instancia con la configuración de VPC actual.

   ```
   Connect timeout on endpoint URL: https://monitoring.us-east-1.amazonaws.com/
   ```

6. Manténgase conectado a la instancia. Tras crear el punto de conexión de VPC, volverá a intentar este comando list-metrics.

Paso 4: Creación de un punto de conexión de VPC para acceder a CloudWatch

Utilice el siguiente procedimiento para crear un punto de conexión de VPC que se conecte a CloudWatch.

Requisito previo

Cree un grupo de seguridad para el punto de conexión de VPC que permita el tráfico a CloudWatch. Por ejemplo, agregue una regla que permita el tráfico HTTPS desde el bloque CIDR de VPC.

Para crear un punto de conexión de VPC para CloudWatch

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Elija Crear punto de conexión.
4. En Name tag (Etiqueta de nombre), ingrese un nombre para el punto de conexión.
5. En Categoría de servicios, elija Servicios de AWS.
6. En Service (Servicio), seleccione com.amazonaws.***region***.monitoring.
7. En VPC, seleccione la VPC.
8. En Subnets (Subredes), seleccione la zona de disponibilidad y, a continuación, seleccione la subred privada.
9. En Security group (Grupo de seguridad), seleccione el grupo de seguridad para el punto de conexión de VPC.
10. En Política, seleccione Acceso completo para permitir todas las operaciones de todas las entidades principales en todos los recursos del punto de conexión de VPC.
11. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
12. Elija Crear punto de conexión. El estado inicial es Pending (Pendiente). Antes de continuar con el paso siguiente, espere a que el estado sea Available (Disponible). Este proceso puede tardar unos minutos.

Paso 5: Prueba del punto de conexión de VPC

Compruebe que el punto de conexión de VPC esté enviando solicitudes desde su instancia a CloudWatch.

Para probar el punto de conexión de VPC

Ejecute el siguiente comando en la instancia. En la opción `--region`, especifique la región en la que creó el punto de conexión de VPC.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --region us-east-1
```

Si recibe una respuesta, aunque sea una respuesta con resultados vacíos, sabrá que está conectado a CloudWatch mediante AWS PrivateLink.

Si aparece el error `UnauthorizedOperation`, asegúrese de que la instancia tenga un rol de IAM que le permita acceder a CloudWatch.

Si se agota el tiempo de espera de la solicitud, compruebe lo siguiente:

- El grupo de seguridad del punto de conexión permite el tráfico a CloudWatch.
- La opción `--region` especifica la región en la que creó el punto de conexión de VPC.

Paso 6: limpiar

Si ya no necesita el host bastión y la instancia que creó para este tutorial, puede terminarlos.

Para terminar las instancias

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione ambas instancias de prueba y elija Instance state (Estado de la instancia) y Terminate instance (Terminar instancia).
4. Cuando se le indique que confirme, elija Finalizar.

Si ya no necesita el punto de conexión de VPC, puede eliminarlo.

Para eliminar el punto de conexión de VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de VPC.
4. Elija Acciones, Eliminar puntos de conexión de VPC.
5. Cuando se le pida confirmación, ingrese **`delete`** y elija Eliminar.

Acceda a través Servicios de AWS de AWS PrivateLink

Usted accede a un punto final y lo Servicio de AWS utiliza. Los puntos de conexión de servicio predeterminados son interfaces públicas, por lo que debe agregar una puerta de enlace de Internet a la VPC para que el tráfico pueda llegar desde la VPC al Servicio de AWS. Si esta configuración no se ajusta a los requisitos de seguridad de la red, puede utilizarla AWS PrivateLink para conectar la VPC Servicios de AWS como si estuviera en la VPC, sin necesidad de utilizar una puerta de enlace a Internet.

Puede acceder de forma privada a los Servicios de AWS que se integran AWS PrivateLink mediante puntos finales de VPC. Puede crear y administrar todas las capas de la pila de aplicaciones sin utilizar una puerta de enlace de Internet.

Precios

Se le facturará por cada hora de aprovisionamiento de punto de conexión de VPC de la interfaz en cada zona de disponibilidad. También se le factura por GB de datos procesados. Para obtener más información, consulte AWS PrivateLink Precios.

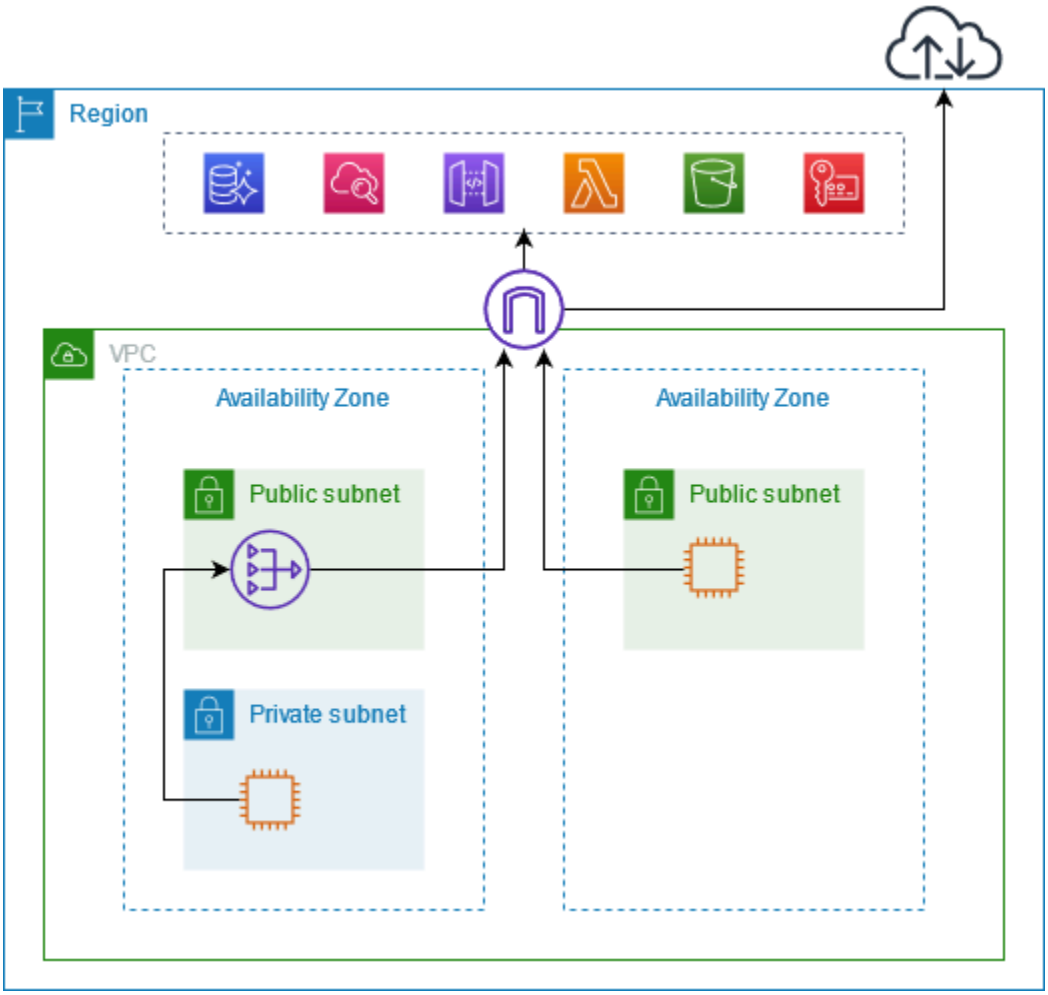
Contenido

Descripción general

Puede acceder a Servicios de AWS través de sus puntos finales de servicio público o conectarse a un usuario compatible. Servicios de AWS AWS PrivateLink Esta descripción general compara estos métodos.

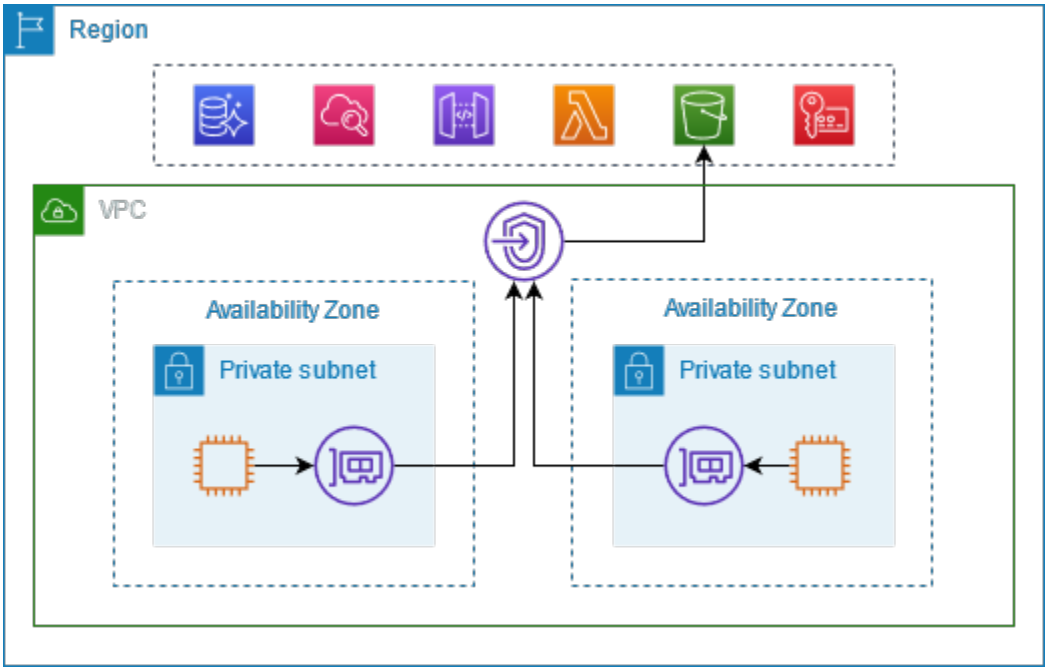
Acceso a través de puntos de conexión de servicio públicos

El siguiente diagrama muestra cómo las instancias acceden a Servicios de AWS través de los puntos finales del servicio público. El tráfico hacia y Servicio de AWS desde una instancia de una subred pública se enruta a la puerta de enlace de Internet de la VPC y, a continuación, a la. Servicio de AWS El tráfico a un Servicio de AWS desde una instancia de una subred privada se dirige a una puerta de enlace NAT, luego a la puerta de enlace de Internet para la VPC y, a continuación, al Servicio de AWS. Mientras este tráfico atraviesa la puerta de enlace de Internet, no sale de la red. AWS



Conéctese a través de AWS PrivateLink

El siguiente diagrama muestra cómo Servicios de AWS acceden las instancias AWS PrivateLink. En primer lugar, debe crear un punto final de la VPC de interfaz, que establece las conexiones entre las subredes de la VPC y una interfaz de red que utiliza. Servicio de AWS El tráfico destinado al Servicio de AWS se resuelve en las direcciones IP privadas de las interfaces de red de puntos finales mediante DNS y, a continuación, se envía a Servicio de AWS través de la conexión entre el punto final de la VPC y el. Servicio de AWS



Servicios de AWS acepta las solicitudes de conexión automáticamente. El servicio no puede iniciar solicitudes a los recursos a través del punto de conexión de VPC.

Nombre de host DNS

La mayoría Servicios de AWS ofrece puntos finales regionales públicos, que tienen la siguiente sintaxis.

```
protocol://service_code.region_code.amazonaws.com
```

Por ejemplo, el punto final público de Amazon CloudWatch en us-east-2 es el siguiente.

```
https://monitoring.us-east-2.amazonaws.com
```

Con AWS PrivateLink, se envía tráfico al servicio mediante puntos de enlace privados. Cuando crea un punto de enlace de VPC de interfaz, creamos nombres de DNS regionales y zonales que puede usar para comunicarse con él desde Servicio de AWS su VPC.

El nombre DNS regional para el punto de conexión de VPC de interfaz tiene la siguiente sintaxis:

```
endpoint_id.service_id.region.vpce.amazonaws.com
```

Los nombres de DNS de zona tienen la siguiente sintaxis:

```
endpoint_id-az_name.service_id.region.vpce.amazonaws.com
```

Al crear un punto final de VPC de interfaz para un Servicio de AWS, puede habilitar el DNS privado. Con el DNS privado, se pueden seguir realizando solicitudes a un servicio utilizando el nombre DNS de su punto de conexión público, al tiempo que se aprovecha la conectividad privada a través del punto de conexión de VPC de interfaz. Para obtener más información, consulte the section called "Resolución de los DNS".

El siguiente describe-vpc-endpointscomando muestra las entradas de DNS de un punto final de interfaz.

```
aws ec2 describe-vpc-endpoints --vpc-endpoint-id vpce-099deb00b40f00e22 --query
 VpcEndpoints[*].DnsEntries
```

El siguiente es un ejemplo de salida para un punto final de interfaz para Amazon CloudWatch con nombres DNS privados habilitados. La primera entrada es el punto de conexión regional privado. Las siguientes tres entradas son los puntos de conexión de zona privados. La entrada final proviene de la zona alojada privada y oculta, que resuelve las solicitudes al punto de conexión público para las direcciones IP privadas de las interfaces de red del punto de conexión.

```
[
    [
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2c.monitoring.us-
east-2.vpce.amazonaws.com",
```

```
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2a.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "vpce-099deb00b40f00e22-lj2wisx3-us-east-2b.monitoring.us-
east-2.vpce.amazonaws.com",
            "HostedZoneId": "ZC8PG0KIFKBRI"
        },
        {
            "DnsName": "monitoring.us-east-2.amazonaws.com",
            "HostedZoneId": "Z06320943MMOWYG6MAVL9"
        }
    ]
]
```

Resolución de los DNS

Los registros DNS que se crean para el punto de conexión de VPC de interfaz son públicos. Por lo tanto, estos nombres de DNS se pueden resolver de forma pública. Sin embargo, las solicitudes DNS desde fuera de la VPC siguen devolviendo las direcciones IP privadas de las interfaces de red de punto de conexión, por lo que estas direcciones IP no se pueden utilizar para acceder al servicio del punto de conexión a menos que tenga acceso a la VPC.

DNS privado

Si habilitas el DNS privado para el punto final de la VPC de la interfaz y tu VPC tiene habilitados tanto los nombres de host DNS como la resolución de DNS, crearemos una zona alojada privada oculta y AWS administrada para ti. La zona alojada contiene un registro configurado para el nombre DNS predeterminado para el servicio que lo resuelve en las direcciones IP privadas de las interfaces de red de punto de conexión en la VPC. Por lo tanto, si ya tienes aplicaciones que envían solicitudes a Servicio de AWS través de un punto de conexión regional público, esas solicitudes ahora pasan por las interfaces de red de los puntos finales, sin necesidad de que realices ningún cambio en esas aplicaciones.

Le recomendamos que habilite nombres DNS privados para su punto de conexión de VPC para los Servicios de AWS. Esto garantiza que las solicitudes que utilizan los puntos de enlace de servicio

público, como las solicitudes realizadas a través de un AWS SDK, se dirijan a su punto de enlace de VPC.

Amazon proporciona un servidor DNS para la VPC, denominado Route 53 Resolver. Route 53 Resolver resuelve automáticamente los nombres de dominio y registros de VPC locales de zonas alojadas privadas. No obstante, no se puede utilizar Route 53 Resolver desde fuera de la VPC. Si desea acceder al punto de conexión de VPC desde la red local, puede utilizar puntos de conexión de Route 53 Resolver y reglas de Resolver. Para obtener más información, consulte Integración AWS Transit Gateway con AWS PrivateLink y. Amazon Route 53 Resolver

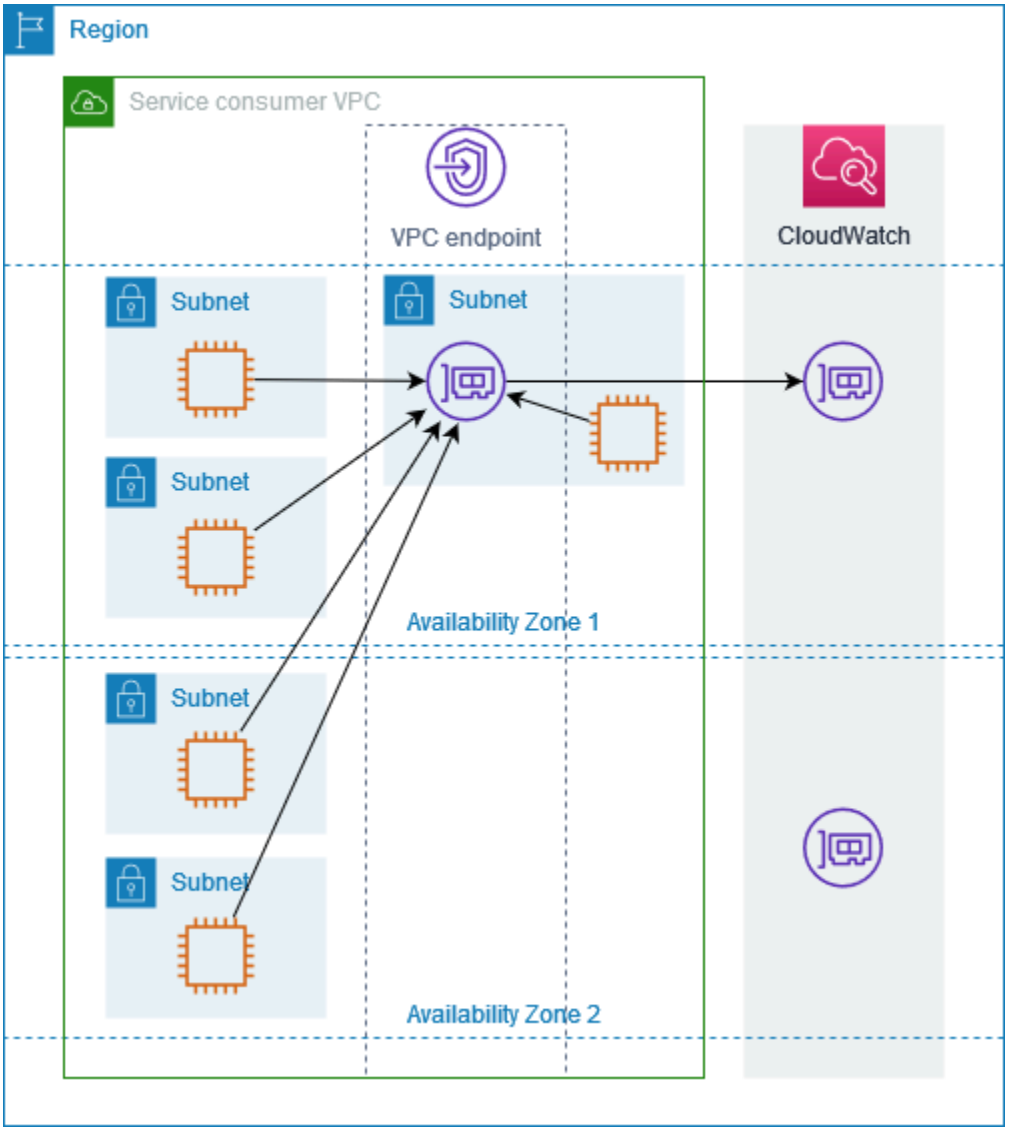
Subredes y zonas de disponibilidad

Puede configurar su punto de conexión de VPC con una subred por cada zona de disponibilidad. Creamos una interfaz de red de punto de conexión para el punto de conexión de VPC en la subred. Asignamos direcciones IP a cada interfaz de red de punto de conexión desde su subred, en función del tipo de dirección IP del punto de conexión de VPC. Las direcciones IP de una interfaz de red de punto de conexión no variarán durante la vida útil de su punto de conexión de VPC correspondiente.

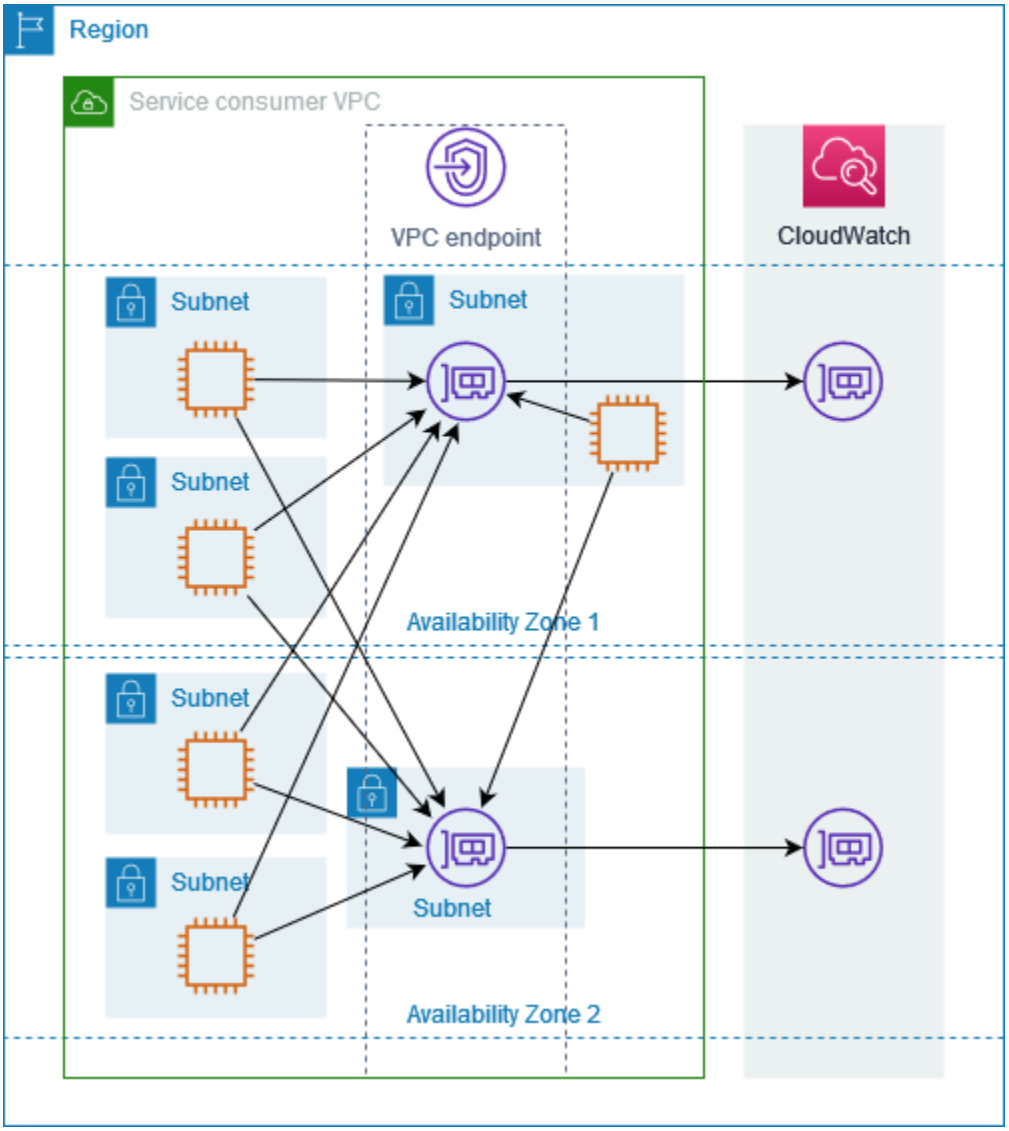
En un entorno de producción, para una alta disponibilidad y resiliencia, recomendamos lo siguiente:

- Configure al menos dos zonas de disponibilidad por punto final de VPC e implemente AWS los recursos que deben acceder a ellas Servicio de AWS en estas zonas de disponibilidad.
- Configurar nombres de DNS privados para el punto de conexión de VPC.
- Acceda a Servicio de AWS ellas mediante su nombre de DNS regional, también conocido como punto final público.

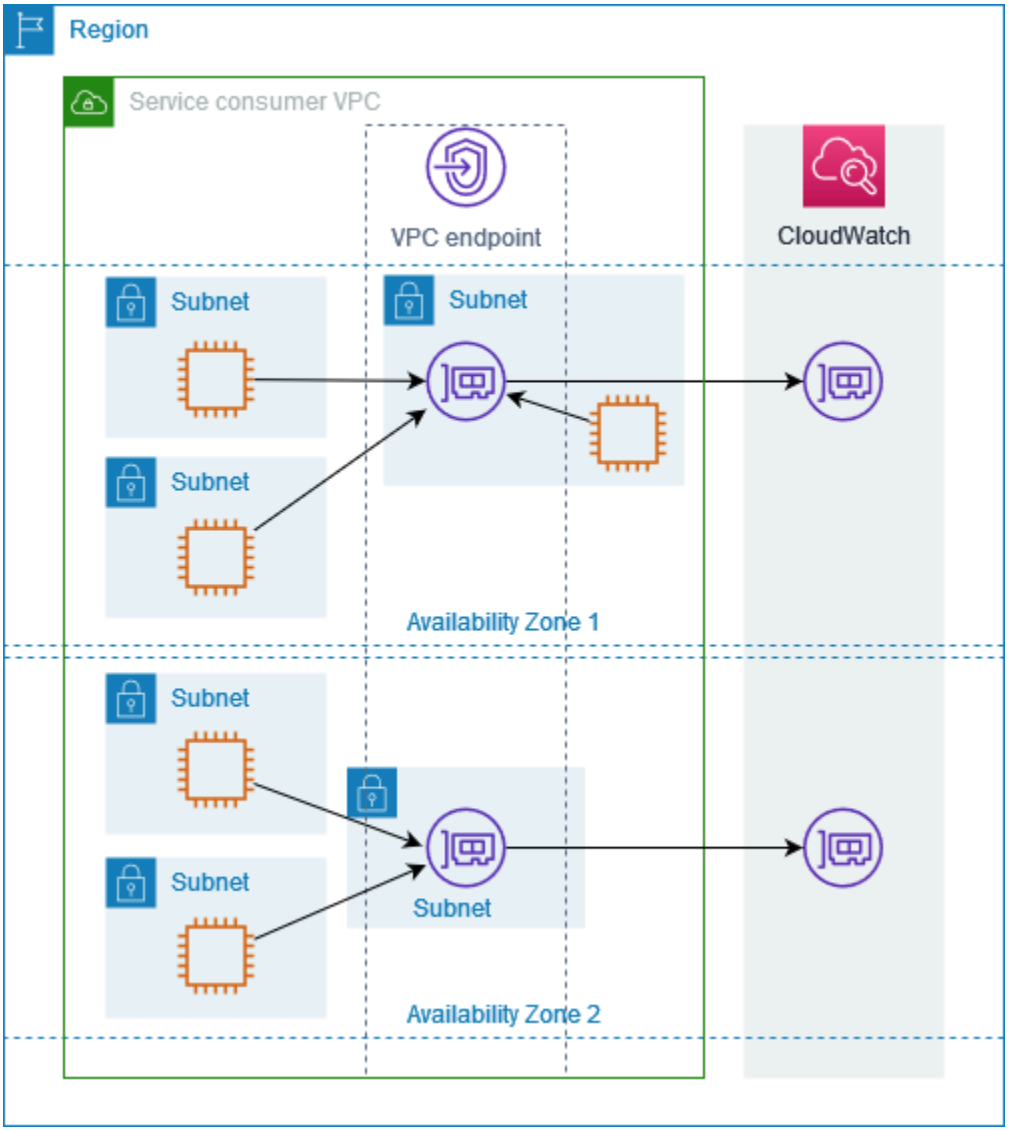
El siguiente diagrama muestra un punto de enlace de VPC para Amazon CloudWatch con una interfaz de red de puntos finales en una única zona de disponibilidad. Cuando cualquier recurso de cualquier subred de la VPC accede a CloudWatch Amazon mediante su punto de conexión público, resolvemos el tráfico a la dirección IP de la interfaz de red de punto final. Esto incluye el tráfico procedente de subredes de otras zonas de disponibilidad. Sin embargo, si la zona de disponibilidad 1 se ve afectada, los recursos de la zona de disponibilidad 2 pierden el acceso a Amazon CloudWatch.



El siguiente diagrama muestra un punto final de VPC para Amazon CloudWatch con interfaces de red de puntos finales en dos zonas de disponibilidad. Cuando cualquier recurso de cualquier subred de la VPC accede a CloudWatch Amazon mediante su punto de enlace público, seleccionamos una interfaz de red de puntos finales en buen estado y utilizamos el algoritmo de turnos rotativos para alternar entre ellos. A continuación, resolvemos el tráfico dirigido a la dirección IP de la interfaz de red de punto de conexión seleccionada.



Si es mejor para su caso de uso, puede enviar el tráfico de los recursos al Servicio de AWS utilizando la interfaz de red de punto de conexión de la misma zona de disponibilidad. Para ello, utilice el punto de conexión de zona privado o la dirección IP de la interfaz de red de punto de conexión.



Tipos de direcciones IP

Servicios de AWS pueden brindar soporte IPv6 a través de sus puntos de enlace privados, incluso si no lo hacen IPv6 a través de sus puntos de enlace públicos. Los puntos finales compatibles IPv6 pueden responder a las consultas de DNS con registros AAAA.

Requisitos para habilitar un punto IPv6 final de interfaz

- Servicio de AWS Debe hacer que sus puntos finales de servicio estén disponibles en. IPv6 Para obtener más información, consulte the section called “Ver IPv6 soporte”.
- El tipo de dirección IP de un punto de conexión de interfaz debe ser compatible con las subredes del punto de conexión de interfaz, como se describe a continuación:

- IPv4— Asigne IPv4 direcciones a las interfaces de red de sus puntos finales. Esta opción solo se admite si todas las subredes seleccionadas tienen rangos de IPv4 direcciones.
- IPv6— Asigne IPv6 direcciones a las interfaces de red de sus puntos finales. Esta opción solo se admite si todas las subredes seleccionadas son IPv6 solo subredes.
- Dualstack: IPv4 asigne ambas IPv6 direcciones a las interfaces de red de sus puntos finales. Esta opción solo se admite si todas las subredes seleccionadas tienen ambos IPv4 rangos de direcciones. IPv6

Si una interfaz de punto final de VPC admite IPv4, las interfaces de red de puntos finales tienen IPv4 direcciones. Si una interfaz de punto final de VPC admite IPv6, las interfaces de red de puntos finales tienen IPv6 direcciones. No se puede acceder a la IPv6 dirección de la interfaz de red de un punto final desde Internet. Si describe una interfaz de red de punto final con una IPv6 dirección, observe que `denyAllIgwTraffic` está habilitada.

Tipo de IP de registro de DNS

Según el tipo de dirección IP, al llamar a un punto final de la VPC, el AWS servicio puede devolver registros A, registros AAAA o registros A y AAAA. Puedes personalizar los tipos de registros que devuelve tu AWS servicio modificando el tipo de IP del registro DNS. En la siguiente tabla se muestran los tipos de IP de registro de DNS admitidos y los tipos de registro devueltos:

Tipo de IP de registro de DNS	Tipos de registros devueltos
IPv4	A
IPv6	AAAA
Pila doble	A y AAAA

De forma predeterminada, el tipo de registro de DNS es el mismo que el tipo de dirección IP. Se puede elegir un tipo de IP de registro de DNS diferente, pero se debe usar un tipo de dirección IP compatible para el servicio de punto de conexión. En la siguiente tabla se muestra el tipo de IP de registro de DNS compatible para cada tipo de dirección IP de los puntos de conexión de la interfaz:

Tipo de dirección IP	Tipos de IP de registros de DNS admitidos
IPv4	IPv4
IPv6	IPv6
Pila doble	Dualstack*, definido por el servicio IPv4 IPv6

* Representa el tipo de IP del registro de DNS predeterminado.

Un tipo de IP de registro de DNS definido por el servicio devuelve registros de DNS en función del punto de conexión del servicio al que se llame. Si se utiliza un tipo de IP de registro de DNS definido por el servicio, se debe asegurar que el servicio pueda gestionar llamadas variables desde los puntos de conexión del servicio. Para ver los registros DNS compatibles con el punto de enlace de la interfaz, consulte los nombres de DNS del punto de enlace de la VPC en Consola de administración de AWS, o use. DescribeVpcEndpoints

El comportamiento del tipo de IP del registro de DNS es diferente en los puntos de conexión de las puertas de enlace. Para obtener más información, consulte el tipo de IP del registro de DNS para los puntos de conexión de la puerta de enlace.

Servicios de AWS que se integran con AWS PrivateLink

Lo siguiente se Servicios de AWS integra con AWS PrivateLink. Puede crear un punto de conexión de VPC para conectarse a estos servicios de forma privada, como si se ejecutaran en su propia VPC.

Elija el enlace de la Servicio de AWScolumna para ver la documentación de los servicios que se integran con AWS PrivateLink. La columna Nombre del servicio contiene el nombre del servicio que especifica al crear el punto de conexión de VPC de la interfaz, o indica que ese servicio administra el punto de conexión.

Servicio de AWS	Nombre del servicio
AWS Account Management	com.amazonaws. *region*.cuenta
Amazon API Gateway	com.amazonaws. *region*.execute-api
	com.amazonaws. *region*.api gateway

Servicio de AWS	Nombre del servicio
AWS AppConfig	com.amazonaws. *region*.appconfig
	com.amazonaws. *region*.appconfig-fips
com.amazonaws. *region*.appconfigdata	
com.amazonaws. *region*.appconfigdata-fips	
AWS App Mesh	com.amazonaws. *region*.appmesh
	com.amazonaws. *region*. appmesh-envoy-management
AWS App Runner	com.amazonaws. *region*.apprunner
Servicios de AWS App Runner	com.amazonaws. *region*.apprunner.requests
Aplicación de escalado automático	com.amazonaws. *region*.escalado automático de aplicaciones
AWS Application Discovery Service	com.amazonaws. *region*.discovery
	com.amazonaws. *region*.arsenal-discovery
AWS Servicio de migración de aplicaciones	com.amazonaws. *region*.mgn
WorkSpaces Aplicaciones de Amazon	com.amazonaws. *region*.appstream.api
	com.amazonaws. *region*.appstream.streaming
AWS AppSync	com.amazonaws. *region*.appsync-api
Amazon Athena	com.amazonaws. *region*.athena
AWS Audit Manager	com.amazonaws. *region*.administrador de auditoría
Amazon Aurora	com.amazonaws. *region*.rds

Servicio de AWS	Nombre del servicio
	com.amazonaws. *region*.rds-fips
Amazon Aurora DSQL	com.amazonaws. *region*.dsql
AWS Auto Scaling	com.amazonaws. *region*.planes de escalado automático
AWS Intercambio de datos entre empresas	com.amazonaws. *region*.b2bi
AWS Backup	com.amazonaws. *region*.backup
	com.amazonaws. *region*.backup-gateway
AWS Batch	com.amazonaws. *region*.batch
Amazon Bedrock	com.amazonaws. *region*.bedrock
	com.amazonaws. *region*.bedrock-agent
	com.amazonaws. *region*. bedrock-agent-runtime
	com.amazonaws. *region*. bedrock-data-automation
	com.amazonaws. *region*. bedrock-data-automation-fips
	com.amazonaws. *region*. bedrock-data-automation-runtime
	com.amazonaws. *region*. bedrock-data-automation-runtime-consejos
	com.amazonaws. *region*.bedrock-runtime
Administración de facturación y costos de AWS	com.amazonaws. *region*.facturación
	com.amazonaws. *region*.freetier
	com.amazonaws. *region*.tax

Servicio de AWS	Nombre del servicio
AWS Billing Conductor	com.amazonaws. *region*.billingconductor
Amazon Braket	com.amazonaws. *region*.braket
AWS Certificate Manager	com.amazonaws. *region*.acm
	com.amazonaws. *region*.acm-fips
Salas limpias de AWS	com.amazonaws. *region*... salas limpias
	com.amazonaws. *region*.cleanrooms-tips
AWS Clean Rooms ML	com.amazonaws. *region*.cleanrooms-ml
API de control de nube de AWS	com.amazonaws. *region*.cloudcontrolapi
	com.amazonaws. *region*.cloudcontrolapi-fips
Amazon Cloud Directory	com.amazonaws. *region*Directorio.cloud
AWS CloudFormation	com.amazonaws. *region*.cloudformation
	com.amazonaws. *region*.cloudformation-fips
AWS CloudHSM	com.amazonaws. *region*.cloudhsmv2
AWS Cloud Map	com.amazonaws. *region*.servicediscovery
	com.amazonaws. *region*.servicediscovery-fips
	com.amazonaws. *region*.data-servicediscovery
	com.amazonaws. *region*. data-servicediscovery-fips
AWS CloudTrail	com.amazonaws. *region*.cloudtrail
AWS WAN en la nube	com.amazonaws. *region*.administrador de red
Amazon CloudWatch	com.amazonaws. *region*.señales de aplicación

Servicio de AWS	Nombre del servicio
	com.amazonaws. *region*. información sobre la aplicació n
	com.amazonaws. *region*.monitor de internet
	com.amazonaws. *region*.internetmonitor-tips
	com.amazonaws. *region*.monitoreo
	com.amazonaws. *region*.monitor de flujo de red
	com.amazonaws. *region*Informes de monitoreo de flujo de.network
	com.amazonaws. *region*.monitor de red
	com.amazonaws. *region*.observabilityadmin
	com.amazonaws. *region*.rum
	com.amazonaws. *region*.rum-dataplane
	com.amazonaws. *region*.sintéticos
	com.amazonaws. *region*.synthetics-fips
	com.amazonaws. *region*.oam
Amazon CloudWatch Logs	com.amazonaws. *region*.logs
AWS CodeArtifact	com.amazonaws. *region*.codeartifact.api
	com.amazonaws. *region*.codeartifact.repositorios
AWS CodeBuild	com.amazonaws. *region*.codebuild
	com.amazonaws. *region*.codebuild-tips
AWS CodeCommit	com.amazonaws. *region*.codecommit

Servicio de AWS	Nombre del servicio
AWS CodeConnections	com.amazonaws. *region*.codecommit-fips
	com.amazonaws. *region*.git-codecommit
	com.amazonaws. *region*. git-codecommit-fips
	com.amazonaws. *region*.codeconnections.api
	com.amazonaws. *region*.codestar-connections.api
AWS CodeDeploy	com.amazonaws. *region*.codedeploy
	com.amazonaws. *region*. codedeploy-commands-secure
	com.amazonaws. *region*.codedeploy-fips
Amazon CodeGuru Profiler	com.amazonaws. *region*.codeguru-profiler
CodeGuru Revisor de Amazon	com.amazonaws. *region*.codeguru-reviewer
AWS CodePipeline	com.amazonaws. *region*.codepipeline
Amazon Comprehend	com.amazonaws. *region*.comprender
Amazon Comprehend Medical	com.amazonaws. *region*. comprender medicina
AWS Compute Optimizer	com.amazonaws. *region*.compute-optimizador
AWS Config	com.amazonaws. *region*.config
	com.amazonaws. *region*.config-fips
Amazon Connect	com.amazonaws. *region*Integraciones de.app
	com.amazonaws. *region*.casos
	com.amazonaws. *region*.connect-campaigns
	com.amazonaws. *region*.perfil

Servicio de AWS	Nombre del servicio
	com.amazonaws. *region*.voiceid
	com.amazonaws. *region*.sabiduría
AWS Connector Service	com.amazonaws. *region*Conector.aws
AWS Control Catalog	com.amazonaws. *region*.catálogo de control
AWS Cost Explorer	com.amazonaws. *region*.ce
Centro de optimización de costes de AWS	com.amazonaws. *region*. cost-optimization-hub
AWS Control Tower	com.amazonaws. *region*... torre de control
	com.amazonaws. *region*.controltower-fips
AWS Data Exchange	com.amazonaws. *region*.intercambio de datos
Exportaciones de datos de AWS	aws.api. *region*. bcm-data-exports
	com.amazonaws. *region*. bcm-pricing-calculator
Amazon Data Firehose	com.amazonaws. *region*.kinesis-firehose
Gestionador de vida útil de datos de Amazon	com.amazonaws. *region*.dlm
	com.amazonaws. *region*.dlm-fips
AWS Database Migration Service	com.amazonaws. *region*.dms
	com.amazonaws. *region*.dms-fips
AWS DataSync	com.amazonaws. *region*.datasync
Amazon DataZone	com.amazonaws. *region*.datazone
	com.amazonaws. *region*.datazone-tips
AWS Deadline Cloud	com.amazonaws. *region*.deadline.management

Servicio de AWS	Nombre del servicio
	com.amazonaws. *region*.deadline.scheduling
Amazon Detective	com.amazonaws. *region*.detective
	com.amazonaws. *region*.consejos de detección
El DevOps gurú de Amazon	com.amazonaws. *region*.devops-guru
AWS Direct Connect	com.amazonaws. *region*.directconnect
	com.amazonaws. *region*.directconnect-fips
AWS Directory Service	com.amazonaws. *region*.ds
	com.amazonaws. *region*.ds-data
	com.amazonaws. *region*. ds-data-fips
Amazon DocumentDB	com.amazonaws. *region*.rds
Amazon DynamoDB	com.amazonaws. *region*.dynamodb
	com.amazonaws. *region*.dynamodb-fips
	com.amazonaws. *region*.dynamodb-streams
Amazon EBS directo APIs	com.amazonaws. *region*.ebs
	com.amazonaws. *region*.ebs-fips
Amazon EC2	com.amazonaws. *region*.ec2
	com.amazonaws. *region*.ec2-fips
Amazon EC2 Auto Scaling	com.amazonaws. *region*.escalado automático
	com.amazonaws. *region*.autoscaling-fips
EC2 Image Builder	com.amazonaws. *region*.creador de imágenes

Servicio de AWS	Nombre del servicio
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr.dkr
Amazon ECS	com.amazonaws. *region*.ecs
	com.amazonaws. *region*.ecs-agent
	com.amazonaws. *region*.ecs-telemetría
Amazon EKS	com.amazonaws. *region*.eks
	com.amazonaws. *region*.eks-auth
	com.amazonaws. *region*.eks-fips
	com.amazonaws. *region*.eks-proxy
AWS Elastic Beanstalk	com.amazonaws. *region*. tallo de frijol elástico
	com.amazonaws. *region*. tallo de habichuelas elásticas : salud
AWS Elastic Disaster Recovery	com.amazonaws. *region*.drs
Amazon Elastic File System	com.amazonaws. *region*.sistema de archivos elástico
	com.amazonaws. *region*.elasticfilesystem-fips
Elastic Load Balancing	com.amazonaws. *region*.balanceo de carga elástico
Amazon Elastic VMware Service	com.amazonaws. *region*.evs
	com.amazonaws. *region*.evs-fips
Amazon ElastiCache	com.amazonaws. *region*.dolor elástico
	com.amazonaws. *region*.elasticache-tips
AWS Elemental MediaConnect	com.amazonaws. *region*.mediaconnect

Servicio de AWS	Nombre del servicio
AWS Elemental MediaConvert	com.amazonaws. *region*.mediaconvert
	com.amazonaws. *region*.mediaconvert-fips
Amazon EMR	com.amazonaws. *region*.elasticmapreduce
	com.amazonaws. *region*.elasticmapreduce-fips
Amazon EMR en EKS	com.amazonaws. *region*.emr-containers
Amazon EMR sin servidor	com.amazonaws. *region*.emr-serverless
	com.amazonaws. *region*. emr-serverless-services.livy
	com.amazonaws. *region*.emr-serverless.dashboard
Amazon EMR WAL	com.amazonaws. *region*.merwal.prod
AWS Mensajería social para usuarios finales	com.amazonaws. *region*.mensajería social
	com.amazonaws. *region*. social-messaging-fips
AWS Entity Resolution	com.amazonaws. *region*.resolución de entidades
	com.amazonaws. *region*.entityresolution-fips
Amazon EventBridge	com.amazonaws. *region*.eventos
	com.amazonaws. *region*.events-tips
	com.amazonaws. *region*.pipas
	com.amazonaws. *region*.pipes-data
	com.amazonaws. *region*.pipes-fips
	com.amazonaws. *region*.esquemas
Amazon EventBridge Scheduler	com.amazonaws. *region*.scheduler

Servicio de AWS	Nombre del servicio
AWS Fault Injection Service	com.amazonaws. *region*.fis
	com.amazonaws. *region*.fis-fips
Amazon FinSpace	com.amazonaws. *region*.finspace
	com.amazonaws. *region*.finspace-api
AWS Firewall Manager	com.amazonaws. *region*.fms
	com.amazonaws. *region*.fms-fips
Amazon Forecast	com.amazonaws. *region*.pronóstico
	com.amazonaws. *region*.forecastquery
	com.amazonaws. *region*.forecast-fips
	com.amazonaws. *region*.forecastquery-fips
Amazon Fraud Detector	com.amazonaws. *region*.detector de fraudes
Amazon FSx	com.amazonaws. *region*.fsx
	com.amazonaws. *region*.fsx-fips
GameLift Servidores Amazon	com.amazonaws. *region*.gamelift
Amazon GameLift Streams	com.amazonaws. *region*Transmisiones de.gamelift
Redes globales de AWS para gateways de tránsito	com.amazonaws. *region*.administrador de red
AWS Glue	com.amazonaws. *region*.pegamento
	com.amazonaws. *region*.glue.dashboard
AWS Glue DataBrew	com.amazonaws. *region*.databrew
	com.amazonaws. *region*.databrew-fips

Servicio de AWS	Nombre del servicio
Amazon Managed Grafana	com.amazonaws. *region*.grafana
	com.amazonaws. *region*.grafana-workspace
AWS Ground Station	com.amazonaws. *region*. estación terrestre
	com.amazonaws. *region*.groundstation-fips
Amazon GuardDuty	com.amazonaws. *region*.guardduty
	com.amazonaws. *region*.guardduty-data
	com.amazonaws. *region*. guardduty-data-fips
	com.amazonaws. *region*.guardduty-fips
AWS HealthImaging	com.amazonaws. *region*. dicom-medical-imaging
	com.amazonaws. *region*.imagenología médica
	com.amazonaws. *region*. runtime-medical-imaging
AWS HealthLake	com.amazonaws. *region*.healthlake
AWS HealthOmics	com.amazonaws. *region*.analytics-omics
	com.amazonaws. *region*. analytics-omics-fips
	com.amazonaws. *region*. control-storage-omics
	com.amazonaws. *region*. control-storage-omics-fips
	com.amazonaws. *region*.storage-omics
	com.amazonaws. *region*.tags-omics
	com.amazonaws. *region*. tags-omics-fips
	com.amazonaws. *region*.workflows-omics

Servicio de AWS	Nombre del servicio
	com.amazonaws. *region*. workflows-omics-fips
AWS Identity and Access Management (YO SOY)	com.amazonaws.iam
Analizador de acceso de IAM	com.amazonaws. *region*.access-analyzer
	com.amazonaws. *region*. access-analyzer-fips
IAM Identity Center	com.amazonaws. *region*.tienda de identidad
IAM Roles Anywhere	com.amazonaws. *region*.roles en cualquier parte
	com.amazonaws. *region*.rolesanywhere-fips
Amazon Inspector	com.amazonaws. *region*.inspector 2
	com.amazonaws. *region*.inspector de 2 consejos
	com.amazonaws. *region*.inspector-scan
	com.amazonaws. *region*. inspector-scan-fips
Amazon Interactive Video Service	com.amazonaws. *region*.ivs.contribute
AWS IoT Core	com.amazonaws. *region*.iot.api
	com.amazonaws. *region*.iot-fips.api
	com.amazonaws. *region*.iot.data
	com.amazonaws. *region*.iot.credentials
AWS IoT Device Management tunelización segura	com.amazonaws. *region*.iot.tunneling.api
	com.amazonaws. *region*.iot-fips.tunneling.api
	com.amazonaws. *region*.iot.tunneling.data
	com.amazonaws. *region*.iot-fips.tunneling.data

Servicio de AWS	Nombre del servicio
AWS IoT Core Device Advisor	com.amazonaws. *region*.deviceadvisor.iot
Integraciones gestionadas para AWS IoT Device Management	com.amazonaws. *region*.iotmanagintegrations.api
	com.amazonaws. *region*.iotmanagintegrations-fips.api
AWS IoT Core para LoRaWAN	com.amazonaws. *region*.iotwireless.api
	com.amazonaws. *region*.lorawan.tazas
	com.amazonaws. *region*.lorawan.lns
AWS IoT FleetWise	com.amazonaws. *region*.iotfleetwise
AWS IoT Greengrass	com.amazonaws. *region*.greengrass
AWS IoT RoboRunner	com.amazonaws. *region*.iotroborunner
AWS IoT SiteWise	com.amazonaws. *region*.iotsitewise.api
	com.amazonaws. *region*.iotsitewise.data
AWS IoT TwinMaker	com.amazonaws. *region*.iottwinmaker.api
	com.amazonaws. *region*.iottwinmaker.data
Amazon Kendra	com.amazonaws. *region*.kendra
	aws.api. *region*.kendra-ranking
AWS Key Management Service	com.amazonaws. *region*.kms
	com.amazonaws. *region*.kms-fips
Amazon Keyspaces (para Apache Cassandra)	com.amazonaws. *region*.cassandra
	com.amazonaws. *region*.cassandra-fips
Amazon Kinesis Data Streams	com.amazonaws. *region*.kinesis-streams

Servicio de AWS	Nombre del servicio
	com.amazonaws. *region*. kinesis-streams-fips
AWS Lake Formation	com.amazonaws. *region*.formación lacustre
AWS Lambda	com.amazonaws. *region*.lambda
AWS Launch Wizard	com.amazonaws. *region*.launchwizard
Amazon Lex	com.amazonaws. *region*.models-v2-lex
	com.amazonaws. *region*.runtime-v2-lex
AWS License Manager	com.amazonaws. *region*.administrador de licencias
	com.amazonaws. *region*. license-manager-fips
	com.amazonaws. *region*. license-manager-linux-subscriptions
	com.amazonaws. *region*. license-manager-linux-subscriptions-consejos
	com.amazonaws. *region*. license-manager-user-subscriptions
	com.amazonaws. *region*. license-manager-user-subscriptions-consejos
Amazon Lightsail	com.amazonaws. *region*.lightsail
Amazon Location Service	com.amazonaws. *region*.geo.maps
	com.amazonaws. *region*.geo.places
	com.amazonaws. *region*.geo.routes
	com.amazonaws. *region*.geo.geofencing
	com.amazonaws. *region*.geo.tracking

Servicio de AWS	Nombre del servicio
	com.amazonaws. *region*.geo.metadata
Amazon Lookout for Equipment	com.amazonaws. *region*. equipo de vigilancia
Amazon Lookout for Metrics	com.amazonaws. *region*.lookoutmetrics
Amazon Lookout for Vision	com.amazonaws. *region*. lookoutvision
Amazon Macie	com.amazonaws. *region*.macie2
	com.amazonaws. *region*.macie2-fips
AWS Mainframe Modernization	com.amazonaws. *region*.apptest
	com.amazonaws. *region*.m2
Amazon Managed Blockchain	com.amazonaws. *region*.consulta de cadena de bloques gestionada
	com.amazonaws. *region*.managedblockchain.bitcoin.mainnet
	com.amazonaws. *region*.managedblockchain.bitcoin.testnet
AWS Marketplace Metering Service	com.amazonaws. *region*.metering-marketplace
Servicio administrado por Amazon para Prometheus	com.amazonaws. *region*.aps
	com.amazonaws. *region*.aps-espacios de trabajo
Amazon Managed Streaming for Apache Kafka (MSK)	com.amazonaws. *region*.kafka
	com.amazonaws. *region*.kafka-fips
Flujo de trabajo administrado de Amazon para Apache Airflow	com.amazonaws. *region*.airflow.api
	com.amazonaws. *region*.airflow.api-fips

Servicio de AWS	Nombre del servicio
	com.amazonaws. *region*.airflow.env
	com.amazonaws. *region*.airflow.env-fips
	com.amazonaws. *region*.airflow.ops
Amazon Route 53	com.amazonaws.route53
Consola de administración de AWS	com.amazonaws. *region*.consola
	com.amazonaws. *region*.iniciar sesión
Amazon MemoryDB	com.amazonaws. *region*.memory-db
	com.amazonaws. *region*.memorydb-fips
Orquestador de AWS Migration Hub	com.amazonaws. *region*.migrationhub-orchator
AWS Migration Hub Refactor Spaces	com.amazonaws. *region*.refactor-spaces
Recomendaciones de estrategias de Migration Hub	com.amazonaws. *region*.migrationhub: estrategia
Amazon MQ	com.amazonaws. *region*.mq
	com.amazonaws. *region*.mq-fips
Análisis por Amazon Neptune	com.amazonaws. *region*.neptune-graph
	com.amazonaws. *region*. neptune-graph-data
	com.amazonaws. *region*. neptune-graph-fips
AWS Network Firewall	com.amazonaws. *region*.network-firewall
	com.amazonaws. *region*. network-firewall-fips
OpenSearch Servicio Amazon	Estos puntos de conexión se administran mediante servicios

Servicio de AWS	Nombre del servicio
AWS Organizations	com.amazonaws. *region*.organizaciones
	com.amazonaws. *region*.consejos de organización
AWS Outposts	com.amazonaws. *region*... puestos de avanzada
AWS Panorama	com.amazonaws. *region*.panorama
AWS Criptografía de pagos	com.amazonaws. *region*.pago-criptografía.plano de control
	com.amazonaws. *region*.pago-criptografía.plano de datos
AWS PCS	com.amazonaws. *region*.piezas
	com.amazonaws. *region*.pcs-fips
Amazon Personalize	com.amazonaws. *region*.personalizar
	com.amazonaws. *region*.personalize-events
	com.amazonaws. *region*.personalize-runtime
Amazon Pinpoint	com.amazonaws. *region*.pinpoint
	com.amazonaws. *region*. pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws. *region*.polly
	com.amazonaws. *region*.polly-tips
Lista de precios de AWS	com.amazonaws. *region*.pricing.api
AWS Private Certificate Authority	com.amazonaws. *region*.acm-pca
	com.amazonaws. *region*. acm-pca-fips
	com.amazonaws. *region*. pca-connector-ad

Servicio de AWS	Nombre del servicio
	com.amazonaws. *region*. pca-connector-scep
AWS Proton	com.amazonaws. *region*.proton
Amazon Q Business	aws.api. *region*.qbusiness
Amazon Q Developer	com.amazonaws. *region*.codewhisperer
	com.amazonaws. *region*q.
	com.amazonaws. *region*.apps
Suscripciones de usuarios de Amazon Q	com.amazonaws. *region*.service.user-subscriptions
Quick Suite	com.amazonaws. *region*.quicksight-sitio web
Amazon RDS	com.amazonaws. *region*.rds
	com.amazonaws. *region*.rds-fips
API de datos de Amazon RDS	com.amazonaws. *region*.rds-data
Amazon RDS Performance Insights	com.amazonaws. *region*.pi
	com.amazonaws. *region*.pi-fips
AWS Re:Post Private	com.amazonaws. *region*.repostspace
Papelera de reciclaje	com.amazonaws. *region*.rbin
Amazon Redshift	com.amazonaws. *region*.redshift
	com.amazonaws. *region*.redshift-fips
	com.amazonaws. *region*.redshift: sin servidor
	com.amazonaws. *region*. redshift-serverless-fips
API de datos de Amazon Redshift	com.amazonaws. *region*.redshift-data

Servicio de AWS	Nombre del servicio
	com.amazonaws. *region*. redshift-data-fips
Amazon Rekognition	com.amazonaws. *region*.reconocimiento
	com.amazonaws. *region*.rekognition-tips
	com.amazonaws. *region*.streaming-recognition
	com.amazonaws. *region*. streaming-rekognition-fips
AWS Resource Access Manager	com.amazonaws. *region*.ram
	com.amazonaws. *region*.ram-fips
Explorador de recursos de AWS	com.amazonaws. *region*.resource-explorer-2
	com.amazonaws. *region*.resource-explorer-2-tips
Grupos de recursos de AWS	com.amazonaws. *region*.grupos de recursos
	com.amazonaws. *region*. resource-groups-fips
AWS Resource Groups Tagging API	com.amazonaws. *region*.etiquetado
Amazon S3	com.amazonaws. *region*.s3
	com.amazonaws. *region*Tablas.s3
Puntos de acceso multirregión de Amazon S3	com.amazonaws.s3-global.accesspoint
Amazon S3 en Outposts	com.amazonaws. *region*.s3-outposts
Amazon SageMaker AI	aws.sagemaker. *region*... experimentos
	aws.sagemaker. *region*.cuaderno
	aws.sagemaker. *region*.partner-app
	aws.sagemaker. *region*.studio

Servicio de AWS	Nombre del servicio
	com.amazonaws. *region*. sagemaker-data-science-assistant
	com.amazonaws. *region*.sagemaker.api
	com.amazonaws. *region*.sagemaker.api-fips
	com.amazonaws. *region*.sagemaker.featurestore-runtime
	com.amazonaws. *region*.sagemaker. featurestore-runtime-fips
	com.amazonaws. *region*.sagemaker.metrics
	com.amazonaws. *region*.sagemaker.runtime
	com.amazonaws. *region*.sagemaker.runtime-fips
Savings Plans	com.amazonaws.savingsplans
AWS Secrets Manager	com.amazonaws. *region*.administrador de secretos
AWS Security Hub CSPM	com.amazonaws. *region*.securityhub
	com.amazonaws. *region*.securityhub-fips
Amazon Security Lake	com.amazonaws. *region*.securitylake
	com.amazonaws. *region*.securitylake-fips
AWS Security Token Service	com.amazonaws. *region*.sts
	com.amazonaws. *region*.sts-fips
AWS Serverless Application Repository	com.amazonaws. *region*.serverlessrepo
Service Catalog	com.amazonaws. *region*.catálogo de servicios

Servicio de AWS	Nombre del servicio
	com.amazonaws. *region*.servicecatalog: registro de aplicaciones
Service Quotas	com.amazonaws. *region*.cuotas de servicio
Amazon SES	com.amazonaws. *region*.email-smtp
	com.amazonaws. *region*.mail-manager
	com.amazonaws. *region*. mail-manager-fips
	com.amazonaws. *region*. mail-manager-smtp.auth.fips
	com.amazonaws. *region*. mail-manager-smtp.open.fips
AWS SimSpace Weaver	com.amazonaws. *region*.simspaceweaver
AWS Snowball Edge Device Management	com.amazonaws. *region*. snow-device-management
Amazon SNS	com.amazonaws. *region*.sns
Amazon SQS	com.amazonaws. *region*.sqs
	com.amazonaws. *region*.sqs-fips
Amazon SWF	com.amazonaws. *region*.swf
	com.amazonaws. *region*.swf-fips
AWS Step Functions	com.amazonaws. *region*.estados
	com.amazonaws. *region*.sync-states
AWS Storage Gateway	com.amazonaws. *region*. gateway de almacenamiento
AWS Supply Chain	com.amazonaws. *region*.scn
AWS Systems Manager	com.amazonaws. *region*Mensajes.ec2

Servicio de AWS	Nombre del servicio
	com.amazonaws. *region*.ssm
	com.amazonaws. *region*.ssm-contacts
	com.amazonaws. *region*.ssm-incidents
	com.amazonaws. *region*. ssm-incidents-fips
	com.amazonaws. *region*.ssm-configuración rápida
	com.amazonaws. *region*Mensajes.ssm
AWS Systems Manager para SAP	com.amazonaws. *region*.ssm-sap
	com.amazonaws. *region*. ssm-sap-fips
AWS Creador de redes de telecomunicaciones	com.amazonaws. *region*.tnb
Amazon Textract	com.amazonaws. *region*.t extract
	com.amazonaws. *region*.textract-fips
Amazon Timestream	com.amazonaws. *region*.timestream.ingest- *cell*
	com.amazonaws. *region*.timestream.query- *cell*
Amazon Timestream for InfluxDB	com.amazonaws. *region*.timestream-influxdb
	com.amazonaws. *region*. timestream-influxdb-fips
Amazon Transcribe	com.amazonaws. *region*.transcribir
	com.amazonaws. *region*.transcriba la transmisión
	com.amazonaws. *region*.transcribestreaming-fips
Amazon Transcribe Medical	com.amazonaws. *region*.transcribir
	com.amazonaws. *region*.transcriba la transmisión

Servicio de AWS	Nombre del servicio
AWS Transfer for SFTP	com.amazonaws. *region*.transferir
	com.amazonaws. *region*.transfer.server
AWS Transform	com.amazonaws. *region*.transformar
Amazon Translate	com.amazonaws. *region*.traducir
AWS Trusted Advisor	com.amazonaws. *region*. asesor de confianza
AWS User Notifications	com.amazonaws. *region*.notificaciones
	com.amazonaws. *region*.notificaciones-contactos
Amazon Verified Permissions	com.amazonaws. *region*.permisos verificados
	com.amazonaws. *region*.permisos verificados - fips
Amazon VPC Lattice	com.amazonaws. *region*.vpc-lattice
AWS WAFV2	com.amazonaws. *region*.wafv2
	com.amazonaws. *region*.wafv2-fips
AWS Well-Architected Tool	com.amazonaws. *region*... bien diseñado
Amazon WorkMail	com.amazonaws. *region*.workmail
	com.amazonaws. *region*Flujo de mensajes de correo de.workmail
Amazon WorkSpaces	com.amazonaws. *region*.espacios de trabajo
Navegador Amazon WorkSpaces Secure	com.amazonaws. *region*.workspaces-web
	com.amazonaws. *region*. workspaces-web-fips
WorkSpaces streaming	com.amazonaws. *region*.highlander
Amazon WorkSpaces Thin Client	com.amazonaws. *region*.thinclient.api

Servicio de AWS	Nombre del servicio
AWS X-Ray	com.amazonaws. *region*.xray
Amazon Managed Service para Apache Flink	com.amazonaws. *region*.kinesisanalítica
	com.amazonaws. *region*.kinesisanalytics-fips

Ver los nombres de los Servicio de AWS disponibles

Puede usar el describe-vpc-endpoint-servicescomando para ver los nombres de los servicios que admiten los puntos finales de la VPC.

En el siguiente ejemplo, se muestran los puntos finales de la interfaz Servicios de AWS que admiten en la región especificada. La opción `--query` limita la salida a los nombres de servicio.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query ServiceNames
```

A continuación, se muestra un ejemplo del resultado. No se muestra el resultado completo.

```
[
    "api.aws.us-east-1.cassandra-streams",
    "aws.api.us-east-1.bcm-data-exports",
    "aws.api.us-east-1.emr-service-cell01",
    "aws.api.us-east-1.freetier",
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    . . .
     "com.amazonaws.us-east-1.xray"
]
```

Ver información sobre un servicio

Una vez que tenga el nombre del servicio, puede usar el describe-vpc-endpoint-servicescomando para ver información detallada sobre cada servicio de punto final.

El siguiente ejemplo muestra información sobre el punto final de la CloudWatch interfaz de Amazon en la región especificada.

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.monitoring" \
  --region us-east-1
```

A continuación, se muestra un ejemplo del resultado. `VpcEndpointPolicySupported` indica si las políticas de punto de conexión son compatibles. `SupportedIpAddressTypes` indica qué tipos de direcciones IP spn compatibles.

```
{
    "ServiceDetails": [
        {
            "ServiceName": "com.amazonaws.us-east-1.monitoring",
            "ServiceId": "vpce-svc-0fc975f3e7e5beba4",
            "ServiceType": [
                {
                    "ServiceType": "Interface"
                }
            ],
            "AvailabilityZones": [
                "us-east-1a",
                "us-east-1b",
                "us-east-1c",
                "us-east-1d",
                "us-east-1e",
                "us-east-1f"
            ],
            "Owner": "amazon",
            "BaseEndpointDnsNames": [
                "monitoring.us-east-1.vpce.amazonaws.com"
            ],
            "PrivateDnsName": "monitoring.us-east-1.amazonaws.com",
            "PrivateDnsNames": [
                {
                    "PrivateDnsName": "monitoring.us-east-1.amazonaws.com"
                },
                {
                    "PrivateDnsName": "monitoring.us-east-1.api.aws"
                },
                {
```

```
                    "PrivateDnsName": "monitoring-fips.us-east-1.amazonaws.com"
                },
                {
                    "PrivateDnsName": "monitoring-fips.us-east-1.api.aws"
                }           ],
            "VpcEndpointPolicySupported": true,
            "AcceptanceRequired": false,
            "ManagesVpcEndpoints": false,
            "Tags": [],
            "PrivateDnsNameVerificationState": "verified",
            "SupportedIpAddressTypes": [
                "ipv6",
                "ipv4"
            ]
        }
    ],
    "ServiceNames": [
        "com.amazonaws.us-east-1.monitoring"
    ]
}
```

Ver la compatibilidad con las políticas de puntos de conexión

Para comprobar si un servicio admite las políticas de puntos finales, describe-vpc-endpoint-servicesejecute el comando y compruebe el valor de`VpcEndpointPolicySupported`. Los valores posibles son `true` y `false`.

En el siguiente ejemplo, se comprueba si el servicio especificado admite políticas de punto de conexión en la región especificada. La opción `--query` limita el resultado al valor de `VpcEndpointPolicySupported`.

```
aws ec2 describe-vpc-endpoint-services \
  --service-name "com.amazonaws.us-east-1.s3" \
  --region us-east-1 \
  --query ServiceDetails[*].VpcEndpointPolicySupported \
  --output text
```

A continuación, se muestra un ejemplo del resultado.

```
True
```

En el siguiente ejemplo, se enumeran las Servicios de AWS que admiten las políticas de puntos finales en la región especificada. La opción `--query` limita la salida a los nombres de servicio. Para ejecutar este comando mediante la línea de comandos de Windows, elimine las comillas simples de la cadena de consulta y cambie el carácter de continuación de la línea de \ a ^.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`true`].ServiceName'
```

A continuación, se muestra un ejemplo del resultado. No se muestra el resultado completo.

```
[
    "api.aws.us-east-1.cassandra-streams",
    "aws.api.us-east-1.bcm-data-exports",
    "aws.api.us-east-1.emr-service-cell01",
    "aws.api.us-east-1.freetier",
    "aws.api.us-east-1.kendra-ranking",
    . . .
    "com.amazonaws.us-east-1.xray"
]
```

En el siguiente ejemplo, se enumeran las Servicios de AWS que no son compatibles con las políticas de puntos finales en la región especificada. La opción `--query` limita la salida a los nombres de servicio. Para ejecutar este comando mediante la línea de comandos de Windows, elimine las comillas simples de la cadena de consulta y cambie el carácter de continuación de la línea de \ a ^.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --query 'ServiceDetails[?VpcEndpointPolicySupported==`false`].ServiceName'
```

A continuación, se muestra un ejemplo del resultado. No se muestra el resultado completo.

```
[
    "com.amazonaws.us-east-1.appmesh-envoy-management",
    "com.amazonaws.us-east-1.apprunner.requests",
    "com.amazonaws.us-east-1.appstream.api",
    "com.amazonaws.us-east-1.appstream.streaming",
    "com.amazonaws.us-east-1.awsconnector",
    . . .
```

```
    "com.amazonaws.us-east-1.transfer.server"
]
```

Ver IPv6 soporte

Para ver el IPv6 soporte de AWS los servicios, consulte AWS los servicios que admiten IPv6. También puede usar el siguiente describe-vpc-endpoint-servicescomando para ver las áreas a las Servicios de AWS que puede acceder IPv6 en la región especificada. La opción `--query` limita la salida a los nombres de servicio.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=supported-ip-address-types,Values=ipv6 Name=owner,Values=amazon
 Name=service-type,Values=Interface \
  --region us-east-1 \
  --query ServiceNames
```

A continuación, se muestra un ejemplo del resultado. No se muestra el resultado completo.

```
[
    "api.aws.us-east-1.cassandra-streams",
    "aws.api.us-east-1.bcm-data-exports",
    "aws.api.us-east-1.freetier",
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    "aws.api.us-east-1.resource-explorer-2",
    "aws.api.us-east-1.resource-explorer-2-fips",
    "aws.sagemaker.us-east-1.experiments",
    "aws.sagemaker.us-east-1.partner-app",
    "com.amazonaws.iam",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    . . .
    "com.amazonaws.us-east-1.xray"
]
```

Activado para cruzar regiones Servicios de AWS

Lo siguiente se Servicios de AWS integra con una región cruzada. AWS PrivateLink Puede crear un punto final de interfaz para conectarse a estos servicios en otra AWS región, de forma privada, como si se ejecutaran en su propia VPC.

Elija el enlace de la Servicio de AWScolumna para ver la documentación del servicio. La columna Nombre del servicio contiene el nombre del servicio que se especifica al crear el punto final de la interfaz.

Servicio de AWS	Nombre del servicio
Amazon S3	com.amazonaws. *region*.s3
AWS Identity and Access Management (IAM)	com.amazonaws.iam
Amazon ECR	com.amazonaws. *region*.ecr.api
	com.amazonaws. *region*.ecr.dkr
AWS Key Management Service	com.amazonaws. *region*.kms
	com.amazonaws. *region*.kms-fips
Amazon ECS	com.amazonaws. *region*.ecs
AWS Lambda	com.amazonaws. *region*.lambda
Amazon Data Firehose	com.amazonaws. *region*.kinesis-firehose
Amazon Managed Service para Apache Flink	com.amazonaws. *region*.kinesisanalítica
	com.amazonaws. *region*.kinesisanalytics-fips
Amazon Route 53	com.amazonaws.route53

Ver los nombres de los Servicio de AWS disponibles

Puede usar el comando para ver los servicios habilitados para varias regiones describe-vpc-endpoint-services.

El siguiente ejemplo muestra a qué Servicios de AWS puede acceder un usuario de la `us-east-1` región a través de los puntos finales de la interfaz, a la región de servicio (`us-west-2`) especificada. La opción `--query` limita la salida a los nombres de servicio.

```
aws ec2 describe-vpc-endpoint-services \
  --filters Name=service-type,Values=Interface Name=owner,Values=amazon \
  --region us-east-1 \
  --service-region us-west-2 \
  --query ServiceNames
```

A continuación, se muestra un ejemplo del resultado. No se muestra el resultado completo.

```
[
    "com.amazonaws.us-west-2.ecr.api",
    "com.amazonaws.us-west-2.ecr.dkr",
    "com.amazonaws.us-west-2.ecs",
    "com.amazonaws.us-west-2.ecs-fips",
    ...
    "com.amazonaws.us-west-2.s3"
]
```

> **Note**
>
> Debe utilizar el DNS regional. El DNS zonal no es compatible cuando se accede Servicios de AWS desde otra región. Para obtener más información, consulte Ver y actualizar los atributos de DNS en la Guía del usuario de Amazon VPC.

Permisos y consideraciones

- De forma predeterminada, las entidades de IAM no tienen permiso para acceder a ninguna otra Servicio de AWS región. Para conceder los permisos necesarios para el acceso entre regiones, un administrador de IAM puede crear políticas de IAM que permitan la `vpce:AllowMultiRegion` acción únicamente con permisos.
- Asegúrese de que su política de control de servicios (SCP) no deniegue una acción que solo implique permisos. `vpce:AllowMultiRegion` Para utilizar AWS PrivateLink la función de conectividad entre regiones, tanto su política de identidad como su SCP deben permitir esta acción.
- Para controlar las regiones que una entidad de IAM puede especificar como región de servicio al crear un punto de conexión de VPC, se debe utilizar la clave de condición `ec2:VpceServiceRegion`.

- El consumidor del servicio debe optar por una región registrada antes de seleccionarla como la región de servicio para un punto de conexión. Siempre que sea posible, recomendamos que los consumidores de servicios accedan a un servicio mediante la conectividad intrarregional en lugar de la conectividad entre regiones. La conectividad intrarregional proporciona latencia y costos más bajos.
- Puede utilizar la nueva clave de condición `aws:SourceVpcArn` global de IAM para garantizar desde qué regiones Cuentas de AWS y recursos se puede acceder a VPCs sus recursos. Esta clave ayuda a implementar la residencia de los datos y el control de acceso por región.
- Para obtener una alta disponibilidad, cree un punto final de interfaz compatible con varias regiones en al menos dos zonas de disponibilidad. En este caso, los proveedores y los consumidores no están obligados a utilizar las mismas zonas de disponibilidad.
- Con el acceso entre regiones, AWS PrivateLink gestiona la conmutación por error entre las zonas de disponibilidad tanto en las regiones de servicio como en las de consumo. No administra la conmutación por error en todas las regiones.
- El acceso entre regiones no se admite en las siguientes zonas de disponibilidad: `use1-az3usw1-az2`, `apne1-az3apne2-az2`, `yapne2-az4`.
- Se puede utilizar AWS Fault Injection Service para simular eventos regionales y modelar escenarios de error para puntos finales de interfaz habilitados dentro y entre regiones. Para obtener más información, consulte la documentación.AWS FIS

Cree un punto final de interfaz con Servicio de AWS uno de otra región

Para crear un punto final de interfaz mediante la consola, consulte la sección Crear un punto final de VPC.

En la CLI, puede usar el create-vpc-endpointcomando para crear un punto final de VPC Servicio de AWS en una región diferente. En el siguiente ejemplo, se crea un punto de enlace de interfaz para Amazon S3 `us-west-2` desde una entrada de VPC. `us-east-1`

```
aws ec2 create-vpc-endpoint \
  --vpc-id vpc-id \
  --service-name com.amazonaws.us-west-2.s3 \
  --vpc-endpoint-type Interface \
  --subnet-ids subnet-id-1 subnet-id-2 \
  --region us-east-1 \
  --service-region us-west-2
```

Acceso y Servicio de AWS uso de un punto final de VPC de interfaz

Puede crear un punto final de VPC de interfaz para conectarse a los servicios impulsados por ellos AWS PrivateLink, incluidos muchos. Servicios de AWS Para obtener una descripción general, consulte the section called “Conceptos” y Acceso a Servicios de AWS.

Para cada subred que especifique en su VPC, creamos una interfaz de red de punto de conexión en la subred y le asignamos una dirección IP privada del intervalo de direcciones de subred. Una interfaz de red de punto de conexión es una interfaz de red administrada por el solicitante; puede verla en su Cuenta de AWS, pero no puede administrarla usted mismo.

Se le facturan los cargos por uso por hora y procesamiento de datos. Para obtener más información, consulte Precio de punto de enlace de la interfaz.

Contenido

Requisitos previos

- Implemente los recursos que accederán a ella Servicio de AWS en su VPC.
- Para utilizar el DNS privado, debe habilitar los nombres de host DNS y la resolución DNS para la VPC. Para obtener más información, consulte Ver y actualizar los atributos DNS en la Guía del usuario de VPC de Amazon.
- IPv6 Para habilitar un punto final de interfaz, Servicio de AWS debe admitir el acceso a través de IPv6. Para obtener más información, consulte the section called “Tipos de direcciones IP”.
- Cree un grupo de seguridad para la interfaz de red del punto de conexión que permita el tráfico esperado de los recursos de su VPC. Por ejemplo, para garantizar que AWS CLI puedan enviar solicitudes HTTPS al Servicio de AWS, el grupo de seguridad debe permitir el tráfico HTTPS entrante.
- Si sus recursos están en una subred con una ACL de red, compruebe que la ACL de red permita el tráfico entre los recursos de su VPC y las interfaces de red de los puntos de conexión.

- Hay cuotas en sus AWS PrivateLink recursos. Para obtener más información, consulte AWS PrivateLinkCuotas de .

Crear un punto de conexión de VPC

Utilice el siguiente procedimiento para crear un punto de conexión de VPC de tipo interfaz que se conecte a un Servicio de AWS.

Para crear un punto final de interfaz para un Servicio de AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Elija Crear punto de conexión.
4. En Tipo, elija Servicios de AWS .
5. (Opcional) Si va a crear un punto final Servicio de AWS en otra región, active la casilla Habilitar el punto final entre regiones y, a continuación, seleccione la región de servicio en el menú desplegable.
6. En Nombre del servicio, seleccione el servicio. Para obtener más información, consulte the section called “Servicios que se integran”.
7. En VPC, seleccione la VPC desde la que accederá al Servicio de AWS.
8. Si en el paso 5 seleccionó el nombre del servicio para Amazon S3 y desea configurar la compatibilidad con DNS privado, seleccione Configuración adicional, Habilitar nombre DNS. Cuando se realiza esta selección, también se selecciona automáticamente Habilitar DNS privado solo para punto de conexión entrante. Se puede configurar el DNS privado con un punto de conexión de Resolver entrante solo para puntos de conexión de interfaz para Amazon S3. Si no tiene un punto de conexión de puerta de enlace para Amazon S3 y selecciona Habilitar DNS privado solo para punto de conexión entrante, aparecerá un mensaje de error cuando intente ejecutar el último paso de este procedimiento.

   Si en el paso 5 seleccionó el nombre del servicio de cualquier servicio que no sea Amazon S3, Configuración adicional, Habilitar nombre DNS ya aparece seleccionado. Se recomienda mantener la configuración predeterminada. Esto garantiza que las solicitudes que utilizan los puntos de enlace de servicio público, como las solicitudes realizadas a través de un AWS SDK, se dirijan a su punto de enlace de VPC.
9. En Subredes, seleccione las subredes en las que se van a crear las interfaces de red de punto de conexión. Puede seleccionar una subred por zona de disponibilidad. No puede seleccionar

varias subredes de la misma zona de disponibilidad. Para obtener más información, consulte the section called “Subredes y zonas de disponibilidad”.

De forma predeterminada, seleccionamos las direcciones IP de los rangos de direcciones IP de la subred y las asignamos a las interfaces de red de los puntos de conexión. Para elegir las direcciones IP usted mismo, seleccione Designar direcciones IP. Tenga en cuenta que las cuatro primeras direcciones IP y la última dirección IP de un bloque CIDR de subred están reservadas para uso interno, por lo que no puede especificarlas para las interfaces de red de sus puntos de conexión.

10. En Tipo de dirección IP, elija entre las siguientes opciones:

    - IPv4— Asigne IPv4 direcciones a las interfaces de red de los puntos finales. Esta opción solo se admite si todas las subredes seleccionadas tienen rangos de IPv4 direcciones y el servicio acepta IPv4 solicitudes.
    - IPv6— Asigne IPv6 direcciones a las interfaces de red de los puntos finales. Esta opción solo se admite si todas las subredes seleccionadas son IPv6 solo subredes y el servicio acepta IPv6 solicitudes.
    - Dualstack: IPv4 asigne ambas IPv6 direcciones a las interfaces de red de los puntos finales. Esta opción solo se admite si todas las subredes seleccionadas tienen ambos rangos de IPv6 direcciones IPv4 y el servicio acepta ambos IPv4 tipos y solicitudes. IPv6

11. En Grupos de seguridad, seleccione los grupos de seguridad que deban asociarse a las interfaces de red del punto de conexión. Por defecto, asociamos el grupo de seguridad predeterminado para la VPC.
12. En Política, seleccione Acceso completo para permitir todas las operaciones de todas las entidades principales en todos los recursos del punto de conexión de interfaz. Para restringir el acceso, seleccione Personalizado e introduzca una política. Esta opción solo está disponible si el servicio admite las políticas de punto de conexión de VPC. Para obtener más información, consulte Políticas de punto de conexión.
13. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
14. Elija Crear punto de conexión.

Para crear un punto de conexión de interfaz mediante la línea de comandos

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Herramientas para Windows PowerShell)

Subredes compartidas

No puede crear, describir, modificar ni eliminar puntos de conexión de VPC en subredes que se compartan con usted. No obstante, puede usar los puntos de conexión de VPC en las subredes que se compartan con usted.

ICMP

Los puntos de conexión de la interfaz no responden a las solicitudes ping. En su lugar, puede utilizar los comandos nc o nmap.

Configuración de un punto de conexión de interfaz

Después de crear un punto de conexión de VPC, puede actualizar su configuración.

Tareas

- Agregado o eliminación de subredes
- Asociación de grupos de seguridad
- Edición de la política del punto de conexión de VPC
- Habilitación de nombres de DNS privados
- Administración de etiquetas

Agregado o eliminación de subredes

Puede elegir una subred por zona de disponibilidad para su punto de conexión de interfaz. Si agrega una subred, creamos una interfaz de red de punto de conexión en la subred y le asignamos una dirección IP privada del rango de direcciones IP de la subred. Si elimina una subred, eliminamos su interfaz de red de punto de conexión. Para obtener más información, consulte the section called “Subredes y zonas de disponibilidad”.

Para cambiar las subredes con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de interfaz.
4. Elija Actions (Acciones), Manage Subnets (Administrar subredes).

5. Seleccione o anule la selección de las zonas de disponibilidad según sea necesario. Para cada zona de disponibilidad, seleccione una subred. De forma predeterminada, seleccionamos las direcciones IP de los rangos de direcciones IP de la subred y las asignamos a las interfaces de red de los puntos de conexión. Para elegir las direcciones IP para una interfaz de red de punto final, seleccione Designar direcciones IP e introduzca una IPv4 dirección del rango de direcciones de la subred. Si el servicio de punto final lo admite IPv6, también puede introducir una IPv6 dirección del rango de direcciones de la subred.

   Si especifica una dirección IP para una subred que ya tiene una interfaz de red de puntos de conexión para este punto de conexión de VPC, sustituiremos la interfaz de red de puntos de conexión por una nueva. Este proceso desconecta temporalmente la subred y el punto de conexión de VPC.
6. Elija Modify subnets (Modificar subredes).

Para cambiar las subredes con la línea de comandos

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Herramientas para Windows PowerShell)

Asociación de grupos de seguridad

Puede cambiar los grupos de seguridad que están asociados con las interfaces de red para su punto de conexión de interfaz. Las reglas del grupo de seguridad controlan el tráfico que proviene de los recursos de la VPC y que se permite en la interfaz de red del punto de conexión.

Para cambiar los grupos de seguridad con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de interfaz.
4. Elija Actions, Manage security groups.
5. Seleccione o anule la selección de los grupos de seguridad según sea necesario.
6. Elija Modify security groups (Modificar grupos de seguridad).

Para cambiar los grupos de seguridad con la línea de comandos

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Herramientas para Windows PowerShell)

Edición de la política del punto de conexión de VPC

Si Servicio de AWS es compatible con las políticas de puntos finales, puede editar la política de puntos finales del punto final. Después de la actualización de una política de punto de conexión, los cambios pueden tardar unos minutos en aplicarse. Para obtener más información, consulte Políticas de punto de conexión.

Para cambiar la política del punto de conexión mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de interfaz.
4. Elija Actions (Acciones), Manage policy (Administrar política).
5. Elija Acceso completo para permitir el acceso completo al servicio, o bien elija Personalizar y adjunte una política personalizada.
6. Seleccione Save (Guardar).

Para cambiar la política de punto de conexión con la línea de comandos

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Herramientas para Windows PowerShell)

Habilitación de nombres de DNS privados

Le recomendamos que habilite nombres DNS privados para su punto de conexión de VPC para los Servicios de AWS. Esto garantiza que las solicitudes que utilizan los puntos de enlace de servicio público, como las solicitudes realizadas a través de un AWS SDK, se dirijan a su punto de enlace de VPC.

Para utilizar nombres de DNS privados, debe habilitar los nombres de host DNS y la resolución DNS para la VPC. Después de habilitar los nombres de DNS privados, es posible que las direcciones IP

privadas tarden unos minutos en estar disponibles. Los registros de DNS que se crean cuando se habilitan los nombres de DNS privados son privados. Por lo tanto, el nombre de DNS privado no se puede resolver de forma pública.

Para cambiar la opción de nombres de DNS privados con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de interfaz.
4. Elija Actions (Acciones), Modify Private DNS names (Modificar nombres de DNS privados).
5. Seleccione o desactive Enable for this endpoint (Habilitar para este punto de conexión) según sea necesario.
6. Si el servicio es Amazon S3, cuando se selecciona Habilitar para este punto de conexión en el paso anterior también se selecciona Habilitar DNS privado solo para punto de conexión entrante. Si prefiere la funcionalidad de DNS privado estándar, desmarque Habilitar DNS privado solo para punto de conexión entrante. Si no tiene un punto de conexión de puerta de enlace para Amazon S3 además de un punto de conexión de interfaz para Amazon S3 y selecciona Habilitar DNS privado solo para punto de conexión entrante, aparecerá un mensaje de error cuando guarde los cambios en el siguiente paso. Para obtener más información, consulte the section called “DNS privado”.
7. Elija Save changes (Guardar cambios).

Para cambiar la opción de nombres de DNS privados con la línea de comandos

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Herramientas para Windows) PowerShell

Administración de etiquetas

Puede etiquetar el punto de conexión de interfaz para identificarlo o clasificarlo en función de las necesidades de su organización.

Para administrar etiquetas con la consola

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

3. Seleccione el punto de conexión de interfaz.
4. Elija Actions (Acciones) y, a continuación, Manage tags (Administrar etiquetas).
5. Para cada etiqueta que desee agregar, elija Add new tag (Agregar etiqueta nueva) e ingrese la clave y el valor de la etiqueta.
6. Para eliminar una etiqueta, elija Remove (Eliminar) a la derecha de la clave y el valor de la etiqueta.
7. Seleccione Save (Guardar).

Para administrar etiquetas con la línea de comandos

- create-tags y delete-tags (AWS CLI)
- New-EC2Tagy Remove-EC2Tag(Herramientas para Windows PowerShell)

Reciba alertas para los eventos de punto de conexión de interfaz

Puede crear una notificación para recibir alertas para eventos específicos relacionados con el punto de conexión de interfaz. Por ejemplo, puede recibir un correo electrónico cuando se acepte o se rechace una solicitud de conexión.

Tareas

- Crear una notificación de SNS
- Agregar una política de acceso
- Agregar una política de claves

Crear una notificación de SNS

Siga este proceso para crear un tema de Amazon SNS para las notificaciones y suscribirse al tema.

Para crear una notificación para un punto de conexión de interfaz con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de interfaz.
4. En la pestaña Notificaciones, elija Crear notificación.

5. En el ARN de notificación, elija el nombre de recurso de Amazon (ARN) para el tema de SNS que se creó.
6. Para suscribirse a un evento, selecciónelo en Eventos.
   - Conectar: el consumidor del servicio creó el punto de conexión de interfaz. Esto envía una solicitud de conexión al proveedor del servicio.
   - Aceptar: el proveedor del servicio aceptó la solicitud de conexión.
   - Rechazar: el proveedor del servicio rechazó la solicitud de conexión.
   - Eliminar: el consumidor del servicio eliminó el punto de conexión de interfaz.
7. Elija Crear notificación.

Para crear una notificación para un punto de conexión de interfaz con la línea de comandos

- create-vpc-endpoint-connection-notificación ()AWS CLI
- New-EC2VpcEndpointConnectionNotification(Herramientas para Windows PowerShell)

Agregar una política de acceso

Añada una política de acceso al tema Amazon SNS que permita AWS PrivateLink publicar notificaciones en su nombre, como las siguientes. Para obtener más información, consulte ¿Cómo edito la política de acceso de mi tema de Amazon SNS? Utilice las claves de condición global `aws:SourceArn` y `aws:SourceAccount` para protegerse contra el problema de suplente confuso.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:us-east-1:111111111111:topic-name",
            "Condition": {
                "ArnLike": {
```

```
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint/endpoint-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
        }
    ]
}
```

Agregar una política de claves

Si utiliza temas de SNS cifrados, la política de recursos de la clave de KMS debe ser confiable para llamar AWS PrivateLink a las operaciones de la AWS KMS API. A continuación, se muestra una política de claves de ejemplo.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-1:111111111111:key/key-id",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint/endpoint-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
```

```
        }
    ]
}
```

Elimine un punto de conexión de interfaz

Cuando ya no necesite un punto de conexión de VPC, puede eliminarlo. Cuando se elimina un punto de conexión de interfaz también se eliminan sus interfaces de red de puntos de conexión.

Para eliminar un punto de conexión de interfaz con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de interfaz.
4. Elija Acciones, Eliminar puntos de conexión de VPC.
5. Cuando se le solicite confirmación, ingrese **delete**.
6. Elija Eliminar.

Para eliminar un punto de conexión de interfaz con la línea de comandos

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Herramientas para Windows PowerShell)

Puntos de conexión de la puerta de enlace

Los puntos de conexión de VPC de puerta de enlace proporcionan conectividad fiable a Amazon S3 y DynamoDB sin necesidad de una puerta de enlace de Internet o un dispositivo NAT para su VPC. Los puntos finales de puerta de enlace no utilizan AWS PrivateLink, a diferencia de otros tipos de puntos finales de VPC.

Amazon S3 y DynamoDB admiten tanto puntos de conexión de puerta de enlace como puntos de conexión de interfaz. Para comparar las opciones, consulte lo siguiente:

- Tipos de puntos de conexión de VPC para Amazon S3
- Tipos de puntos de conexión de VPC para Amazon DynamoDB

Precios

El uso de puntos de conexión de puerta de enlace no supone ningún cargo adicional.

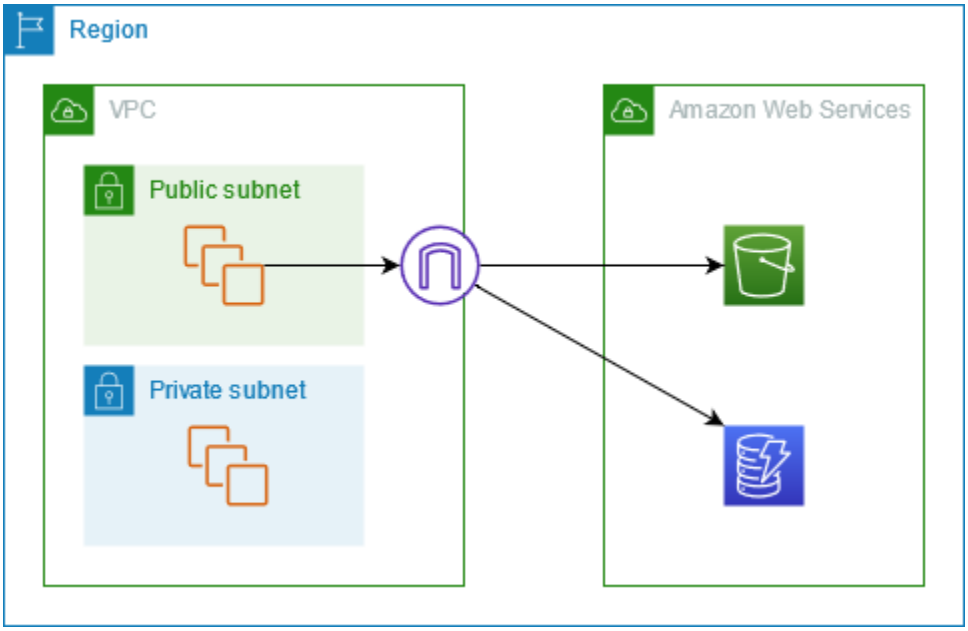
Contenido

Descripción general

Puede acceder a Amazon S3 y DynamoDB a través de sus puntos de conexión de servicio públicos o mediante puntos de conexión de la puerta de enlace. Esta descripción general compara estos métodos.

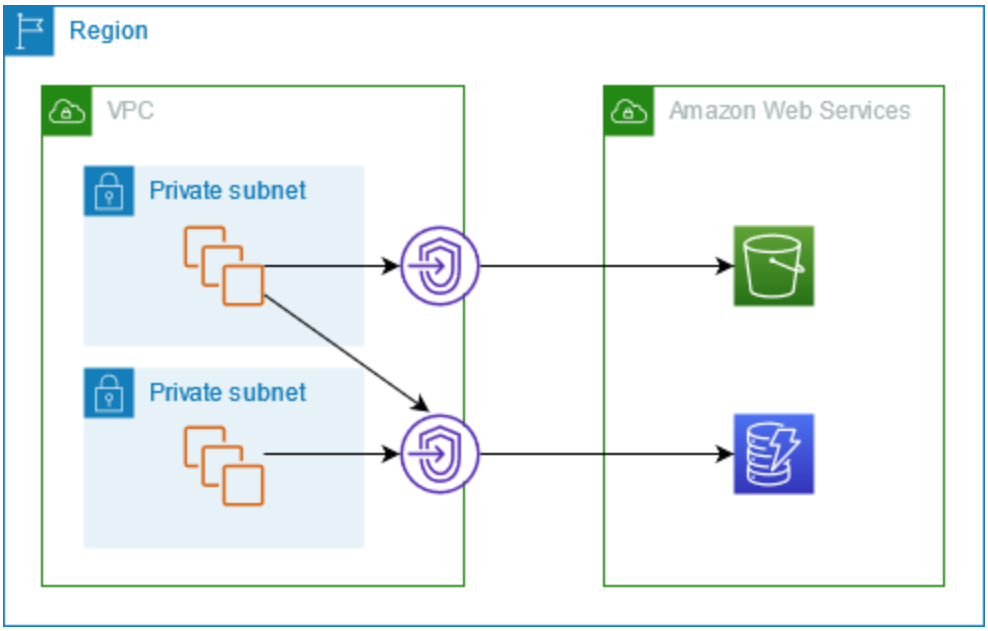
Acceso mediante una puerta de enlace de Internet

En el siguiente diagrama, se muestra cómo las instancias acceden a Amazon S3 y DynamoDB mediante sus puntos de conexión de servicio públicos. El tráfico a Amazon S3 o DynamoDB desde una instancia en una subred pública se dirige a la puerta de enlace de Internet de la VPC y, a continuación, al servicio. Las instancias en una subred privada no pueden enviar tráfico a Amazon S3 o DynamoDB, porque, por definición, las subredes privadas no tienen rutas a una puerta de enlace de Internet. Para permitir que las instancias de la subred privada envíen tráfico a Amazon S3 o DynamoDB, agregue un dispositivo NAT a la subred pública y dirija el tráfico de la subred privada al dispositivo NAT. Si bien el tráfico a Amazon S3 o DynamoDB atraviesa la puerta de enlace de Internet, no sale de la red. AWS



Acceso a través de un punto de conexión de la puerta de enlace

En el siguiente diagrama, se muestra cómo las instancias acceden a Amazon S3 y DynamoDB mediante un punto de conexión de la puerta de enlace. El tráfico desde su VPC hasta Amazon S3 o DynamoDB se dirige al punto de conexión de la puerta de enlace. Cada tabla de enrutamiento de subred debe tener una ruta que envíe el tráfico destinado al servicio al punto de conexión de la puerta de enlace mediante la lista de prefijos del servicio. Para obtener más información, consulte la lista de prefijos administrados de AWS en la Guía del usuario de Amazon VPC.



Enrutamiento

Cuando se crea un punto de conexión de la puerta de enlace, se seleccionan las tablas de enrutamiento de la VPC para las subredes que habilita. La siguiente ruta se agregará de forma automática a cada tabla de enrutamiento que seleccione. El destino es una lista de prefijos del servicio propiedad de AWS y el destino es el punto final de la puerta de enlace.

Destino	Destino
prefix_list_id	*gateway_endpoint_id*

Consideraciones

- Puede revisar las rutas del punto de conexión que agregamos a su tabla de enrutamiento, pero no puede modificarlas ni eliminarlas. Para agregar una ruta de punto de conexión a una tabla de enrutamiento, asóciela con el punto de conexión de la puerta de enlace. Eliminamos la ruta del punto de conexión cuando desasocia la tabla de enrutamiento del punto de conexión de la puerta de enlace o cuando elimina el punto de conexión de la puerta de enlace.
- Todas las instancias en las subredes asociadas con una tabla de enrutamiento asociada con un punto de conexión de la puerta de enlace utilizan de forma automática el punto de conexión de la puerta de enlace para acceder al servicio. Las instancias en las subredes que no están asociadas a estas tablas de enrutamiento utilizan el punto de conexión de servicio público, no el punto de conexión de la puerta de enlace.
- Una tabla de enrutamiento puede tener tanto una ruta de punto de conexión a Amazon S3 como una ruta de punto de conexión a DynamoDB. Puede tener rutas de punto de conexión al mismo servicio (Amazon S3 o DynamoDB) en varias tablas de enrutamiento. No puede tener varias rutas de punto de conexión al mismo servicio (Amazon S3 o DynamoDB) en una sola tabla de enrutamiento.
- Para determinar cómo dirigir tráfico, se usa la ruta más específica que coincida con el tráfico en cuestión (coincidencia del prefijo más largo). Para las tablas de enrutamiento con una ruta de punto de conexión, esto significa lo siguiente:
  - Si hay una ruta que envía todo el tráfico de Internet (0.0.0.0/0) a una puerta de enlace de Internet, la ruta del punto de conexión tiene prioridad sobre el tráfico destinado para el servicio (Amazon S3 o DynamoDB) en la región actual. El tráfico destinado a un destino diferente Servicio de AWS utiliza la puerta de enlace de Internet.

- El tráfico destinado al servicio (Amazon S3 o DynamoDB) en una región diferente va a la puerta de enlace de Internet porque las listas de prefijos son específicas de una región.
- Si hay una ruta que especifica el intervalo exacto de direcciones IP para el servicio (Amazon S3 o DynamoDB) en la misma región, esa ruta tiene prioridad sobre la ruta del punto de conexión.

Seguridad

Cuando sus instancias acceden a Amazon S3 o a DynamoDB a través de un punto de conexión de la puerta de enlace, acceden al servicio mediante su punto de conexión público. Los grupos de seguridad de estas instancias deben permitir el tráfico hacia y el servicio. A continuación, se muestra un ejemplo de una regla de salida. Hace referencia al ID de la lista de prefijos para el servicio.

Destino	Protocolo	Intervalo de puertos
prefix_list_id	TCP	443

La red ACLs de las subredes de estas instancias también debe permitir el tráfico hacia y desde el servicio. A continuación, se muestra un ejemplo de una regla de salida. No se puede hacer referencia a las listas de prefijos en las reglas de ACL de la red, pero se pueden obtener los rangos de direcciones IP del servicio desde su lista de prefijos.

Destino	Protocolo	Intervalo de puertos
service_cidr_block_1	TCP	443
service_cidr_block_2	TCP	443
service_cidr_block_3	TCP	443

Tipo de dirección IP

El tipo de dirección IP determina qué lista de prefijos está asociada a la tabla de enrutamiento.

Requisitos para habilitar un punto IPv6 final de puerta de enlace

- El tipo de dirección IP de un punto de conexión de puerta de enlace debe ser compatible con las subredes del punto de conexión de carga de puerta de enlace, como se describe a continuación:
  - IPv4— Agregue la lista de IPv4 prefijos del servicio a su tabla de rutas.
  - IPv6— Agregue la lista de IPv6 prefijos del servicio a su tabla de rutas. Esta opción solo se admite si todas las subredes seleccionadas son IPv6 solo subredes.
  - Dualstack: agregue la lista de IPv4 prefijos del servicio a la tabla de rutas y agregue la lista de prefijos del servicio a la tabla de IPv6 rutas. Esta opción solo se admite si todas las subredes seleccionadas tienen ambos rangos de direcciones. IPv4 IPv6

Tipo de IP de registro de DNS

De forma predeterminada, el punto final de una puerta de enlace devuelve los registros de DNS en función del punto final del servicio al que se llame. Si crea el punto de enlace mediante el punto de enlace del IPv4 servicio, por ejemplos`3.us-east-2.amazonaws.com`, Amazon S3 devuelve los registros A a sus clientes y todas las subredes de la tabla de enrutamiento los utilizan IPv4.

Por el contrario, si crea su punto de enlace de puerta de enlace mediante el punto de enlace del servicio de doble pilas`3.dualstack.us-east-2.amazonaws.com`, por ejemplo, Amazon S3 devuelve los registros A y AAAA a sus clientes, y las subredes de su tabla de rutas utilizan y. IPv4 IPv6

> **Note**
>
> En el caso de los buckets de directorio, o S3 Express One Zone, los puntos de enlace de la puerta de enlace para el plano de datos serían y, respectivamente. `s3express-use2-az1.us-east-2.amazonaws.com` `s3express-use2-az1.dualstack.us-east-2.amazonaws.com`

El tipo de IP del registro DNS afecta a la forma en que se enruta el tráfico a sus clientes. Si crea un punto de enlace mediante el punto de enlace del IPv4 servicio y, a continuación, llama al punto de enlace del servicio de doble pila, el tráfico que utiliza registros AAAA no se enrutará a través del punto de enlace de la puerta de enlace. El tráfico se interrumpirá o se enrutará a través de una ruta IPv6 compatible, si existe alguna. Si utilizas un tipo de IP de registro DNS definido por el servicio,

asegúrate de que tu servicio pueda gestionar llamadas variables desde varios puntos de conexión del servicio.

En lugar del tipo de IP de registro DNS predeterminado definido por el servicio, puedes personalizar el tipo de IP del registro DNS para elegir qué registros se devuelven para un punto final específico. En la siguiente tabla se muestran los tipos de IP de registro de DNS admitidos y los tipos de registro devueltos:

Tipo de IP de registro de DNS	Tipos de registros devueltos
IPv4	A
IPv6	AAAA
Pila doble	A y AAAA
definido por el servicio	Los registros dependen del punto final del servicio

Para elegir un tipo de IP de registro DNS, debe usar un tipo de dirección IP compatible para el servicio de punto final. En la siguiente tabla se muestra el tipo de IP de registro DNS compatible para cada tipo de dirección IP de los puntos de enlace de puerta de enlace:

Tipo de dirección IP	Tipos de IP de registros de DNS admitidos
IPv4	IPv4, definido por el servicio*
IPv6	IPv6, definido por el servicio*
Pila doble	IPv4, IPv6 Dualstack, definido por el servicio*

* Representa el tipo de IP del registro de DNS predeterminado.

> **Note**
>
> Para usar tipos de IP de registro DNS distintos de los definidos por el servicio para su punto de enlace de puerta de enlace, debe permitir `enableDnsSupport` y `enableDnsHostnames` atribuir atributos en la configuración de la VPC.

No puede cambiar el tipo de IP del registro DNS de un punto final de puerta de enlace de DynamoDB. DynamoDB solo admite el tipo de IP de registro DNS definido por el servicio.

El comportamiento del tipo de IP del registro de DNS es diferente en los puntos de conexión de interfaz. Para obtener más información, consulte el tipo de IP del registro de DNS para los puntos de conexión de interfaz.

Puntos de conexión de puerta de enlace para Amazon S3

Puede acceder a Amazon S3 desde la VPC mediante los puntos de conexión de VPC de la puerta de enlace. Después de crear el punto de conexión de la puerta de enlace, puede agregarlo como destino en la tabla de enrutamiento para el tráfico destinado desde la VPC a Amazon S3.

El uso de puntos de conexión de puerta de enlace no supone ningún cargo adicional.

Amazon S3 admite puntos de enlace de gateway y puntos de enlace de interfaz. Con un punto de conexión de puerta de enlace, se puede acceder a Amazon S3 desde la VPC sin necesidad de una puerta de enlace de Internet ni de un dispositivo NAT para la VPC, y sin costo adicional. Sin embargo, los puntos de enlace no permiten el acceso desde redes locales, desde redes interconectadas VPCs en otras AWS regiones ni a través de una puerta de enlace de tránsito. Para esos escenarios, se debe utilizar un punto de conexión de interfaz, que está disponible por un costo adicional. Para obtener más información, consulte Tipos de puntos de conexión para Amazon S3 en la Guía del usuario de Amazon S3.

Contenido

- Eliminación de un punto de conexión de la puerta de enlace

Consideraciones

- Un punto de conexión de una puerta de enlace solo está disponible en la región donde se creó. Asegúrese de crear el punto de conexión de la puerta de enlace en la misma región que sus buckets de S3.
- Si utiliza los servidores DNS de Amazon, debe habilitar tanto los nombres de host DNS como la resolución de los DNS para la VPC. O bien, si utiliza su propio servidor DNS, asegúrese de que las solicitudes a Amazon S3 se resuelvan de manera correcta en las direcciones IP mantenidas por AWS.
- Las reglas para los grupos de seguridad para las instancias que acceden a Amazon S3 a través del punto de conexión de la puerta de enlace deben permitir el tráfico a Amazon S3. Puede hacer referencia al ID de la lista de prefijos de Amazon S3 en las reglas de los grupos de seguridad.
- La ACL de la red para la subred para las instancias que acceden a Amazon S3 a través de un punto de conexión de la puerta de enlace debe permitir el tráfico hacia y desde Amazon S3. No se puede hacer referencia a las listas de prefijos en las reglas de ACL de la red, pero se pueden obtener los rangos de direcciones IP para Amazon S3 de la lista de prefijos para Amazon S3.
- Compruebe si está utilizando una Servicio de AWS que requiera acceso a un bucket de S3. Por ejemplo, un servicio puede requerir el acceso a depósitos que contienen archivos de registro o puede requerir que descargues controladores o agentes en tus EC2 instancias. Si es así, asegúrate de que tu política de puntos finales permita que el recurso Servicio de AWS o el recurso accedan a estos depósitos mediante la `s3:GetObject` acción.
- No puedes usar la condición `aws:SourceIp` en una política de identidad o una política de bucket para las solicitudes a Amazon S3 que atraviesan un punto de conexión de VPC. Como alternativa, utilice la clave de condición `aws:VpcSourceIp`. Como alternativa, puede usar tablas de enrutamiento para controlar qué EC2 instancias pueden acceder a Amazon S3 a través del punto de enlace de la VPC.
- La fuente IPv4 o IPv6 las direcciones de las instancias de las subredes afectadas, tal como las recibe Amazon S3, pasan de ser direcciones públicas a direcciones privadas en su VPC. Un punto de conexión cambia las rutas de red y desconecta las conexiones TCP abiertas. Las conexiones anteriores que utilizaban direcciones públicas no se reanudan. Se recomienda no tener ninguna tarea importante en ejecución al crear o modificar un punto de enlace o asegurarse de que el software se puede volver conectar automáticamente a Amazon S3 después de la interrupción de la conexión.

- Las conexiones de punto de conexión no se pueden ampliar más allá de la VPC. Los recursos del otro lado de una conexión VPN, una conexión de emparejamiento de VPC, una puerta de enlace de tránsito o Direct Connect una conexión de su VPC no pueden usar un punto de enlace de puerta de enlace para comunicarse con Amazon S3.
- Su cuenta tiene una cuota predeterminada de 20 puntos de conexión de puerta de enlace por región, este número puede ajustarse. Hay un límite de 255 puntos de conexión de la puerta de enlace por VPC.

DNS privado

Puede configurar el DNS privado para optimizar los costos cuando cree tanto un punto de conexión de puerta de enlace como un punto de conexión de interfaz para Amazon S3.

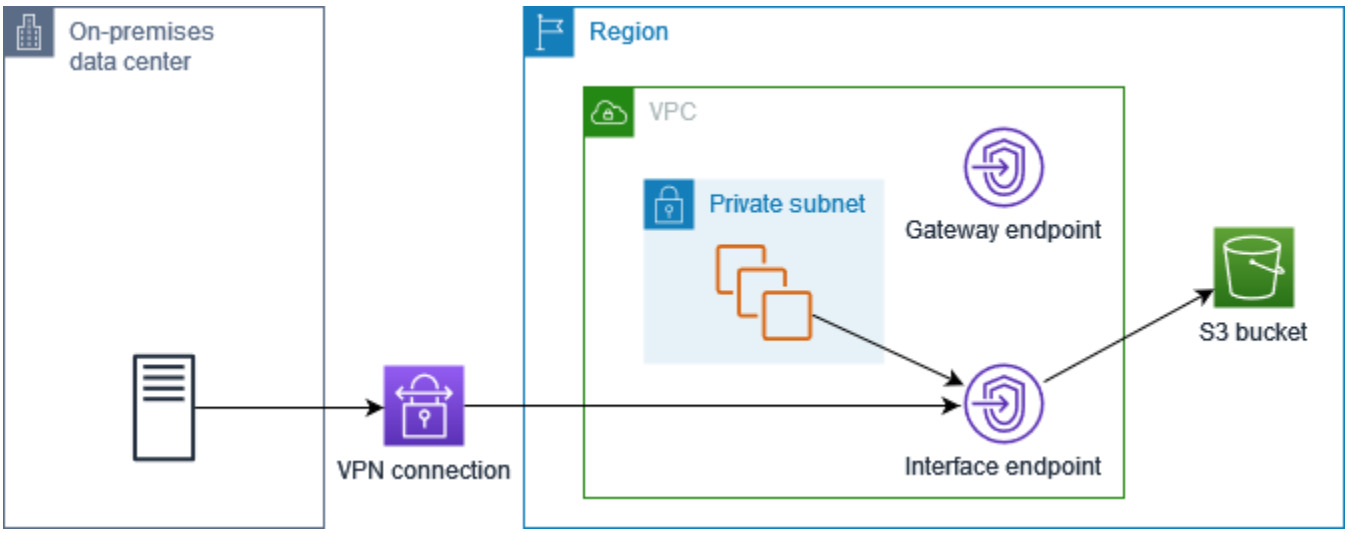
Route 53 Resolver

Amazon proporciona un servidor DNS, denominado Route 53 Resolver, para la VPC. Route 53 Resolver resuelve automáticamente los nombres de dominio y registros de VPC locales de zonas alojadas privadas. No obstante, no se puede utilizar Route 53 Resolver desde fuera de la VPC. Route 53 proporciona puntos de conexión y reglas de Resolver para que se pueda utilizar Route 53 Resolver desde fuera de la VPC. Un punto de conexión de Resolver entrante reenvía las consultas de DNS desde la red local a Route 53 Resolver. Un punto de conexión de Resolver saliente reenvía las consultas de DNS desde Route 53 Resolver a la red local.

Cuando se configura el punto de conexión de interfaz para Amazon S3 para que utilice el DNS privado solo para el punto de conexión de Resolver entrante, creamos un punto de conexión de Resolver entrante. El punto de conexión de Resolver entrante resuelve las consultas de DNS a Amazon S3 desde las instalaciones locales a las direcciones IP privadas del punto de conexión de interfaz. Además, agregamos registros ALIAS de Route 53 Resolver a la zona alojada pública para Amazon S3, de modo que las consultas de DNS de la VPC se resuelvan en las direcciones IP públicas de Amazon S3, que enruta el tráfico al punto de conexión de puerta de enlace.

DNS privado

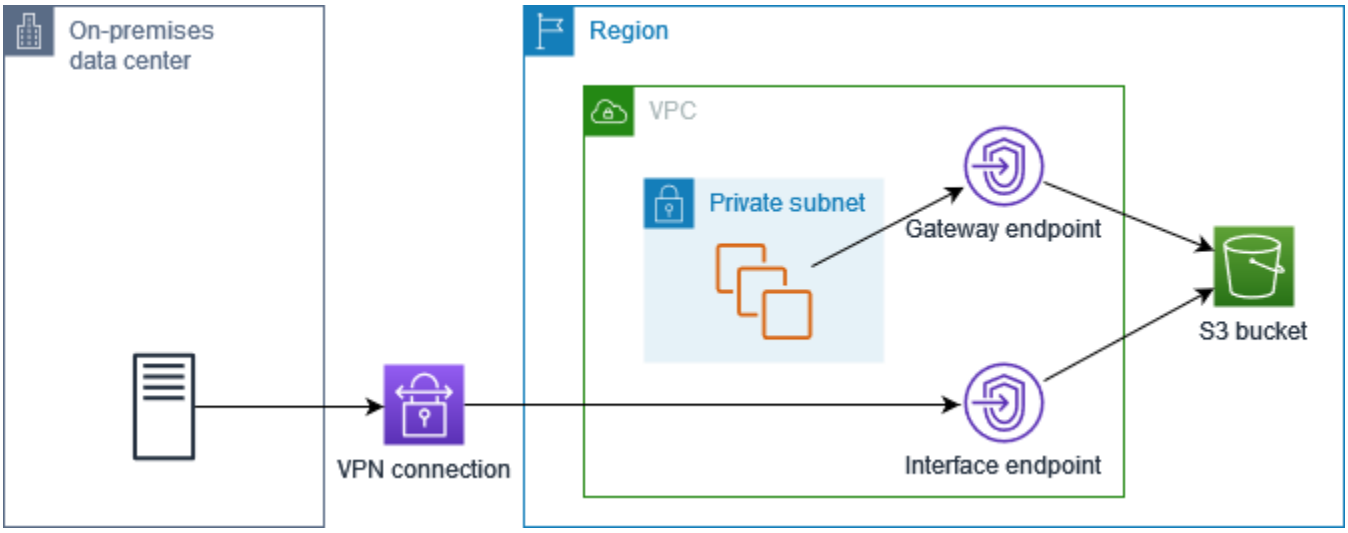
Si se configura el DNS privado para el punto de conexión de interfaz para Amazon S3 pero no se configura el DNS privado solo para el punto de conexión de Resolver entrante, las solicitudes procedentes de la red local y la VPC utilizan el punto de conexión de interfaz para acceder a Amazon S3. Por lo tanto, se debe pagar para utilizar el punto de conexión de interfaz para el tráfico procedente de la VPC, en lugar de utilizar el punto de conexión de puerta de enlace, que no tiene costo adicional.



DNS privado solo para el punto de conexión de Resolver entrante

Si se configura el DNS privado solo para el punto de conexión de Resolver entrante, las solicitudes procedentes de la red local utilizan el punto de conexión de interfaz para acceder a Amazon S3, mientras que las solicitudes procedentes de la VPC emplean el punto de conexión de puerta de enlace para ello. Por lo tanto, se optimizan los costos, ya que se paga por utilizar el punto de conexión de interfaz solo para el tráfico que no puede usar el punto de conexión de puerta de enlace.

Para configurarlo, el tipo de IP del registro DNS del punto de enlace debe coincidir con el punto de enlace de la interfaz o ser el mismo. `service-defined` AWS PrivateLink no admite ninguna otra combinación. Para obtener más información, consulte the section called “Tipo de IP de registro de DNS”.



Configurar DNS privado

Se puede configurar el DNS privado para un punto de conexión de interfaz para Amazon S3 cuando se crea o bien después de crearlo. Para obtener más información, consulte the section called “Crear un punto de conexión de VPC” (configuración durante la creación) o the section called “Habilitación de nombres de DNS privados” (configuración después de la creación).

Creación de un punto de conexión de un gateway

Utilice el siguiente procedimiento para crear un punto de conexión de la puerta de enlace que se conecte a Amazon S3.

Para crear un punto de enlace de gateway con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Elija Crear punto de conexión.
4. En Categoría de servicios, elija Servicios de AWS.
5. Para los servicios, añada el filtro Type = Gateway.

   Si sus datos de Amazon S3 se almacenan en depósitos de uso general, seleccione com.amazonaws. *region*.s3.

   Si sus datos de Amazon S3 están almacenados en buckets de directorio, seleccione com.amazonaws. *region*.s3express.
6. En VPC, seleccione la VPC en la que desea crear el punto de conexión.
7. En Tipo de dirección IP, elija entre las siguientes opciones:

   - IPv4— Asigne IPv4 direcciones a las interfaces de red de los puntos finales. Esta opción solo se admite si todas las subredes seleccionadas tienen rangos de IPv4 direcciones y el servicio acepta IPv4 solicitudes.
   - IPv6— Asigne IPv6 direcciones a las interfaces de red de los puntos finales. Esta opción solo se admite si todas las subredes seleccionadas son IPv6 solo subredes y el servicio acepta IPv6 solicitudes.
   - Dualstack: IPv4 asigne ambas IPv6 direcciones a las interfaces de red de los puntos finales. Esta opción solo se admite si todas las subredes seleccionadas tienen ambos rangos de IPv6 direcciones IPv4 y el servicio acepta ambos IPv4 tipos y solicitudes. IPv6

8. En Route tables (Tablas de enrutamiento), seleccione las tablas de enrutamiento que debe utilizar el punto de conexión. De forma automática, se agregará una ruta para dirigir el tráfico destinado al servicio a la interfaz de red del punto de conexión.
9. En Policy (Política), seleccione Full access (Acceso completo) para permitir todas las operaciones de todas las entidades principales en todos los recursos del punto de conexión de VPC. De lo contrario, seleccione Custom (Personalizar) para adjuntar una política de punto de conexión de VPC que controle los permisos que tienen las entidades principales para realizar acciones en los recursos a través del punto de conexión de VPC.
10. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
11. Elija Crear punto de conexión.

Para crear un punto de conexión de la puerta de enlace mediante la línea de comandos

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Herramientas para Windows PowerShell)

Control del acceso mediante políticas de bucket

Puede usar políticas de bucket para controlar el acceso a los buckets desde puntos de conexión específicos VPCs, rangos de direcciones IP y. Cuentas de AWS En estos ejemplos se presupone que también hay instrucciones de política que permiten el acceso requerido para sus casos de uso.

Example Ejemplo: restringir el acceso a un punto de conexión específico

Puede crear una política de bucket para restringir el acceso a un punto de conexión específico mediante la clave de condición aws:sourceVpce. La siguiente política deniega el acceso al bucket especificado utilizando las acciones especificadas a menos que se utilice el punto de conexión de puerta de enlace especificado. Tenga en cuenta que esta política bloquea el acceso al bucket especificado mediante las acciones especificadas a través de Consola de administración de AWS.

JSON

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

```
      "Sid": "Allow-access-to-specific-VPCE",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
                   "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}
```

Example Ejemplo: restringir el acceso a una VPC específica

Puede crear una política de bucket que restrinja el acceso a determinados grupos VPCs mediante la clave de condición aws:SourceVPC. Esto es útil si tiene múltiples puntos de conexión configurados en la misma VPC. La siguiente política deniega el acceso al bucket especificado mediante las acciones especificadas si la solicitud no provienen de la VPC especificada. Tenga en cuenta que esta política bloquea el acceso al bucket especificado mediante las acciones especificadas a través de Consola de administración de AWS.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::example_bucket",
                   "arn:aws:s3:::example_bucket/*"],
      "Condition": {
        "StringNotEquals": {
          "aws:sourceVpc": "vpc-111bbb22"
        }
      }
```

```
    }
  ]
}
```

Example Ejemplo: restringir del acceso a un rango de direcciones IP específico

Puede crear una política que restrinja el acceso a intervalos de direcciones IP específicos mediante la clave de condición aws:. VpcSourceIp La siguiente política deniega el acceso al bucket especificado mediante las acciones especificadas si la solicitud no provienen de la dirección IP especificada. Tenga en cuenta que esta política bloquea el acceso al bucket especificado mediante las acciones especificadas a través de Consola de administración de AWS.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-VPC-CIDR",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject", "s3:GetObject", "s3:DeleteObject"],
      "Resource": ["arn:aws:s3:::bucket_name",
                   "arn:aws:s3:::bucket_name/*"],
      "Condition": {
        "NotIpAddress": {
          "aws:VpcSourceIp": "172.31.0.0/16"
        }
      }
    }
  ]
}
```

Example Ejemplo: restrinja el acceso a los buckets de un área específica Cuenta de AWS

Puede crear una política para restringir el acceso a los buckets de S3 en una Cuenta de AWS específica con la clave de condición `s3:ResourceAccount`. La siguiente política deniega el acceso a los bucket de S3 mediante las acciones especificadas a menos que sean propiedad de la Cuenta de AWS especificada.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-bucket-in-specific-account",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:GetObject", "s3:PutObject", "s3:DeleteObject"],
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "s3:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

Asociación de tablas de enrutamiento

Puede cambiar las tablas de enrutamiento asociadas a su punto de conexión de la puerta de enlace. Cuando asocia una tabla de enrutamiento, se agrega de forma automática una ruta que dirige el tráfico destinado al servicio a la interfaz de red del punto de conexión. Cuando desasocia una tabla de enrutamiento, se elimina de forma automática la ruta del punto de conexión de la tabla de enrutamiento.

Para asociar tablas de enrutamiento mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de la puerta de enlace.
4. Elija Actions, Manage route tables.
5. Seleccione o anule la selección de las tablas de enrutamiento según sea necesario.
6. Elija Modify route tables (Modificar tablas de enrutamiento).

Para asociar tablas de enrutamiento mediante la línea de comandos

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Herramientas para Windows PowerShell)

Edición de la política del punto de conexión de VPC

Puede editar la política de punto de conexión para un punto de conexión de una puerta de enlace, que controla el acceso a Amazon S3 desde la VPC a través del punto de conexión. Después de la actualización de una política de punto de conexión, los cambios pueden tardar unos minutos en aplicarse. La política predeterminada permite el acceso completo. Para obtener más información, consulte Políticas de punto de conexión.

Para cambiar la política del punto de conexión mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de la puerta de enlace.
4. Elija Actions (Acciones), Manage policy (Administrar política).
5. Elija Acceso completo para permitir el acceso completo al servicio, o bien elija Personalizar y adjunte una política personalizada.
6. Seleccione Save (Guardar).

A continuación, se muestran ejemplos de políticas de punto de enlace para acceder a Amazon S3.

Example Ejemplo: restringir el acceso a un bucket específico

Puede crear una política que restrinja el acceso únicamente a unos buckets específicos de S3. Esto resulta útil si tiene otras Servicios de AWS en su VPC que utilizan buckets S3.

JSON

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

```
      "Sid": "Allow-access-to-specific-bucket",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
         "s3:ListBucket",
         "s3:GetObject",
         "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::bucket_name",
        "arn:aws:s3:::bucket_name/*"
      ]
    }
  ]
}
```

Example Ejemplo: restringir el acceso a un rol de IAM específico

Puede crear una política que restrinja el acceso a un rol de IAM específico. Debe utilizar `aws:PrincipalArn` para conceder acceso a una entidad principal.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-IAM-role",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
        }
      }
    }
  ]
}
```

Example Ejemplo: restringir el acceso a los usuarios en una cuenta específica

Puede crear una política que restrinja el acceso a una cuenta específica.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "Allow-callers-from-specific-account",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:PrincipalAccount": "111122223333"
        }
      }
    }
  ]
}
```

Eliminación de un punto de conexión de la puerta de enlace

Cuando ya no necesite un punto de conexión de la puerta de enlace, puede eliminarlo. Cuando elimina un punto de conexión de la puerta de enlace, se elimina la ruta del punto conexión desde las tablas de enrutamiento de la subred.

No se puede eliminar un punto de conexión de puerta de enlace si el DNS privado está habilitado.

Para eliminar un punto de conexión de la puerta de enlace con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de la puerta de enlace.
4. Elija Actions (Acciones), Delete VPC endpoints (Eliminar puntos de conexión de VPC).
5. Cuando se le solicite confirmación, ingrese **delete**.

6. Elija Delete (Eliminar).

Para eliminar un punto de conexión de la puerta de enlace mediante la línea de comandos

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Herramientas para Windows) PowerShell

Puntos de conexión de la puerta de enlace para Amazon DynamoDB

Puede acceder a Amazon DynamoDB desde la VPC mediante los puntos de conexión de VPC de la puerta de enlace. Después de crear el punto de conexión de la puerta de enlace, puede agregarlo como destino en la tabla de enrutamiento para el tráfico destinado desde la VPC a DynamoDB.

El uso de puntos de conexión de puerta de enlace no supone ningún cargo adicional.

DynamoDB admite tanto puntos de conexión de puerta de enlace como puntos de conexión de interfaz. Con un punto de conexión de puerta de enlace, se puede acceder a DynamoDB desde su VPC sin necesidad de una puerta de enlace de Internet ni de un dispositivo NAT para la VPC, y sin costo adicional. Sin embargo, los puntos de enlace no permiten el acceso desde redes locales, desde redes interconectadas VPCs en otras AWS regiones o a través de una puerta de enlace de tránsito. Para esos escenarios, se debe utilizar un punto de conexión de interfaz, que está disponible por un costo adicional. Para obtener más información, consulte Tipos de puntos de conexión de VPC para DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Contenido

- Consideraciones
- Creación de un punto de conexión de un gateway
- Control del acceso mediante políticas de IAM
- Asociación de tablas de enrutamiento
- Edición de la política del punto de conexión de VPC
- Eliminación de un punto de conexión de la puerta de enlace

Consideraciones

- Un punto de conexión de una puerta de enlace solo está disponible en la región donde se creó. Asegúrese de crear el punto de conexión de la puerta de enlace en la misma región que las tablas de DynamoDB.
- Si utiliza los servidores DNS de Amazon, debe habilitar tanto los nombres de host DNS como la resolución de los DNS para la VPC. Si utiliza su propio servidor DNS, asegúrese de que las solicitudes a DynamoDB se resuelvan de forma correcta en las direcciones IP mantenidas por AWS.
- Las reglas para los grupos de seguridad para las instancias que acceden a DynamoDB a través del punto de conexión de la puerta de enlace deben permitir el tráfico hacia y desde DynamoDB. Puede hacerse referencia al ID de la lista de prefijos de DynamoDB en las reglas de los grupos de seguridad.
- La ACL de la red para la subred para las instancias que acceden a DynamoDB a través de un punto de conexión de la puerta de enlace debe permitir el tráfico hacia y desde DynamoDB. No se puede hacer referencia a las listas de prefijos en las reglas de ACL de la red, pero se puede obtener el rango de direcciones IP de DynamoDB en la lista de prefijos de DynamoDB.
- Si utiliza AWS CloudTrail para registrar las operaciones de DynamoDB, los archivos de registro contienen las direcciones IP privadas de las instancias de EC2 la VPC del consumidor de servicios y el ID del punto de enlace de cualquier solicitud realizada a través del punto de enlace.
- Los puntos de enlace de puerta de enlace solo admiten tráfico. IPv4
- IPv4 Las direcciones de origen de las instancias de las subredes afectadas cambian de IPv4 direcciones públicas a IPv4 direcciones privadas de la VPC. Un punto de enlace cambia las rutas de red y desconecta las conexiones TCP abiertas. Las conexiones anteriores que utilizaban IPv4 direcciones públicas no se reanudan. Se recomienda no tener ninguna tarea importante en ejecución al crear o modificar un punto de conexión de una puerta de enlace. También puede realizar una prueba para asegurarse de que el software se puede volver a conectar de forma automática a DynamoDB si se interrumpe la conexión.
- Las conexiones de punto de conexión no se pueden ampliar más allá de la VPC. Los recursos del otro lado de una conexión VPN, una conexión de emparejamiento de VPC, una puerta de enlace de tránsito o Direct Connect una conexión de su VPC no pueden usar un punto de enlace de puerta de enlace para comunicarse con DynamoDB.
- Su cuenta tiene una cuota predeterminada de 20 puntos de conexión de puerta de enlace por región, este número puede ajustarse. Hay un límite de 255 puntos de conexión de la puerta de enlace por VPC.

Creación de un punto de conexión de un gateway

Utilice el siguiente procedimiento para crear un punto de conexión de una puerta de enlace que se conecte a DynamoDB.

Para crear un punto de enlace de gateway con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Elija Crear punto de conexión.
4. En Categoría de servicios, elija Servicios de AWS.
5. En el caso de los servicios, añada el filtro Type = Gateway y seleccione com.amazonaws.*region*.dynamodb.
6. En VPC, seleccione la VPC en la que desea crear el punto de conexión.
7. En Route tables (Tablas de enrutamiento), seleccione las tablas de enrutamiento que debe utilizar el punto de conexión. De forma automática, se agregará una ruta para dirigir el tráfico destinado al servicio a la interfaz de red del punto de conexión.
8. En Policy (Política), seleccione Full access (Acceso completo) para permitir todas las operaciones de todas las entidades principales en todos los recursos del punto de conexión de VPC. De lo contrario, seleccione Custom (Personalizar) para adjuntar una política de punto de conexión de VPC que controle los permisos que tienen las entidades principales para realizar acciones en los recursos a través del punto de conexión de VPC.
9. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
10. Elija Crear punto de conexión.

Para crear un punto de conexión de la puerta de enlace mediante la línea de comandos

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Herramientas para Windows) PowerShell

Control del acceso mediante políticas de IAM

Puede crear políticas de IAM para controlar qué entidades principales de IAM pueden acceder a las tablas de DynamoDB mediante un punto de conexión de VPC específico.

Example Ejemplo: restringir el acceso a un punto de conexión específico

Puede crear una política para restringir el acceso a un punto de conexión de VPC específico mediante la clave de condición aws:sourceVpce. La siguiente política deniega el acceso a las tablas de DynamoDB de la cuenta, a menos que se utilice el punto de conexión de VPC especificado. En este ejemplo se supone que también hay una declaración de política que permite el acceso necesario para los casos de uso.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-endpoint",
         "Effect": "Deny",
         "Principal": "*",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:us-east-1:111111111111:table/*",
         "Condition": {
            "StringNotEquals" : {
               "aws:sourceVpce": "vpce-11aa22bb"
            }
         }
      }
   ]
}
```

Example Ejemplo: permitir el acceso desde un rol de IAM específico

Puede crear una política que permita obtener acceso mediante un rol de IAM específico. La siguiente política concede acceso al rol de IAM especificado.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-IAM-role",
```

```
         "Effect": "Allow",
         "Principal": "*",
         "Action": "*",
         "Resource": "*",
         "Condition": {
            "ArnEquals": {
               "aws:PrincipalArn": "arn:aws:iam::111122223333:role/role_name"
            }
         }
      }
   ]
}
```

Example Ejemplo: permite acceder desde una cuenta específica

También puede crear una política que solo permita el acceso desde una cuenta específica. La siguiente política concede acceso a los usuarios de la cuenta especificada.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Sid": "Allow-access-from-account",
         "Effect": "Allow",
         "Principal": "*",
         "Action": "*",
         "Resource": "*",
         "Condition": {
            "StringEquals": {
               "aws:PrincipalAccount": "111122223333"
            }
         }
      }
   ]
}
```

Asociación de tablas de enrutamiento

Puede cambiar las tablas de enrutamiento asociadas a su punto de conexión de la puerta de enlace. Cuando asocia una tabla de enrutamiento, se agrega de forma automática una ruta que dirige el tráfico destinado al servicio a la interfaz de red del punto de conexión. Cuando desasocia una tabla de enrutamiento, se elimina de forma automática la ruta del punto de conexión de la tabla de enrutamiento.

Para asociar tablas de enrutamiento mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de la puerta de enlace.
4. Elija Actions, Manage route tables.
5. Seleccione o anule la selección de las tablas de enrutamiento según sea necesario.
6. Elija Modify route tables (Modificar tablas de enrutamiento).

Para asociar tablas de enrutamiento mediante la línea de comandos

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Herramientas para Windows PowerShell)

Edición de la política del punto de conexión de VPC

Puede editar la política de un punto de conexión para un punto de conexión de una puerta de enlace, que controle el acceso a DynamoDB desde la VPC a través del punto de conexión. Después de la actualización de una política de punto de conexión, los cambios pueden tardar unos minutos en aplicarse. La política predeterminada permite el acceso completo. Para obtener más información, consulte Políticas de punto de conexión.

Para cambiar la política del punto de conexión mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de la puerta de enlace.
4. Elija Actions (Acciones), Manage policy (Administrar política).

5. Elija Acceso completo para permitir el acceso completo al servicio, o bien elija Personalizar y adjunte una política personalizada.
6. Elija Save (Guardar).

Para modificar un punto de conexión de la puerta de enlace con la línea de comandos

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Herramientas para Windows PowerShell)

A continuación, se muestran políticas de punto de enlace de ejemplo para acceder a DynamoDB.

Example Ejemplo: permitir acceso de solo lectura

Puede crear una política que restrinja el acceso a solo lectura. La siguiente política concede permiso para enumerar y describir las tablas de DynamoDB.

```
{
  "Statement": [
    {
      "Sid": "ReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "dynamodb:DescribeTable",
        "dynamodb:ListTables"
      ],
      "Resource": "*"
    }
  ]
}
```

Example Ejemplo: Restringir el acceso a una tabla específica

Puede crear una política que restrinja el acceso a una tabla específica de DynamoDB. La siguiente política permite acceder a la tabla de DynamoDB especificada.

```
{
  "Statement": [
    {
      "Sid": "Allow-access-to-specific-table",
```

```
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "dynamodb:Batch*",
        "dynamodb:Delete*",
        "dynamodb:DescribeTable",
        "dynamodb:GetItem",
        "dynamodb:PutItem",
        "dynamodb:Update*"
      ],
      "Resource": "arn:aws:dynamodb:region:123456789012:table/table_name"
    }
  ]
}
```

Eliminación de un punto de conexión de la puerta de enlace

Cuando ya no necesite un punto de conexión de la puerta de enlace, puede eliminarlo. Cuando elimina un punto de conexión de la puerta de enlace, se elimina la ruta del punto conexión desde las tablas de enrutamiento de la subred.

Para eliminar un punto de conexión de la puerta de enlace con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de la puerta de enlace.
4. Elija Actions (Acciones), Delete VPC endpoints (Eliminar puntos de conexión de VPC).
5. Cuando se le solicite confirmación, ingrese **`delete`**.
6. Elija Delete (Eliminar).

Para eliminar un punto de conexión de la puerta de enlace mediante la línea de comandos

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Herramientas para Windows PowerShell)

Acceda a productos SaaS mediante AWS PrivateLink

Mediante AWS PrivateLink, puede acceder a los productos de SaaS de forma privada, como si se ejecutaran en su propia VPC.

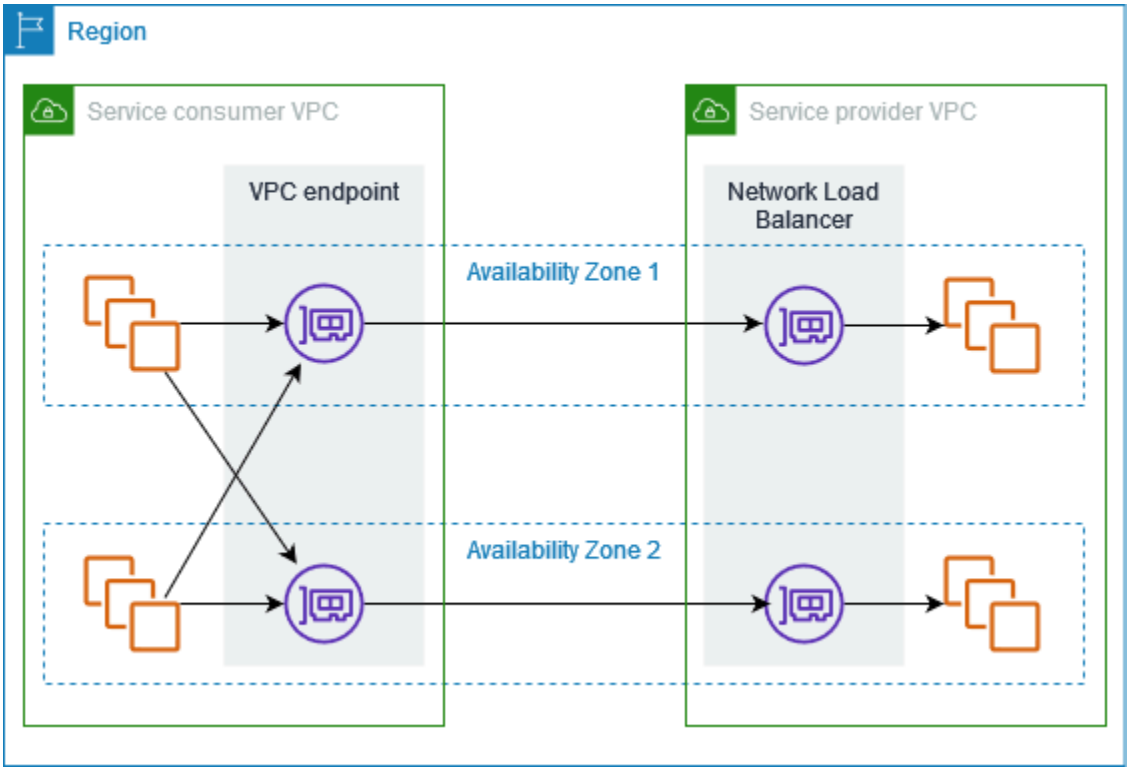
Contenido

Descripción general

Puede descubrir, comprar y aprovisionar productos SaaS con la tecnología de AWS PrivateLink través de AWS Marketplace. Para obtener más información, consulte Acceder a las aplicaciones SaaS de forma segura y privada mediante AWS PrivateLink.

También puede encontrar productos de SaaS con la tecnología de AWS PrivateLink desde socios de AWS. Para obtener más información, consulte Socios de AWS PrivateLink.

El siguiente diagrama muestra cómo se utilizan los puntos de conexión de VPC para conectarse a los productos de SaaS. El proveedor del servicio crea un servicio de punto de conexión y concede a sus clientes acceso al servicio de punto de conexión. Como consumidor del servicio, crea un punto de conexión de VPC de interfaz, que establece conexiones entre una o más subredes de la VPC y el servicio de punto de conexión.



Creación de un punto de conexión de interfaz

Utilice el siguiente procedimiento para crear un punto de conexión de VPC de interfaz que se conecte con el producto de SaaS.

Requisito

Suscríbase al servicio.

Para crear un punto de conexión de interfaz para un servicio de socio

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Elija Crear punto de conexión.
4. Si adquirió el servicio de AWS Marketplace, realice lo siguiente:
    a. En Tipo, elija Servicios de AWS Marketplace.
    b. Seleccione el servicio.
5. Si se suscribió a un servicio con la designación de AWS Service Ready, realice lo siguiente:

a. En Tipo, elija Servicios para socios de PrivateLink Ready.

b. Ingrese el nombre del servicio y elija Verificar servicio.

6. En VPC, seleccione la VPC desde la que accederá al producto.
7. En Subredes, seleccione las subredes en las que se van a crear las interfaces de red de punto de conexión.
8. En Grupos de seguridad, seleccione los grupos de seguridad que deban asociarse a las interfaces de red del punto de conexión. Las reglas del grupo de seguridad deben permitir el tráfico entre los recursos en la VPC y las interfaces de red de punto de conexión.
9. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
10. Elija Crear punto de conexión.

Para configurar un punto de conexión de interfaz

Para obtener más información sobre cómo configurar el punto de conexión de interfaz, consulte the section called “Configuración de un punto de conexión de interfaz”.

Acceso a dispositivos virtuales a través de AWS PrivateLink

Puede utilizar un punto de enlace del balanceador de carga de gateway para distribuir tráfico a una flota de dispositivos virtuales de red. Los dispositivos se pueden utilizar para inspecciones de seguridad, cumplimiento, controles de políticas y otros servicios de red. El equilibrador de carga de puerta de enlace se especifica cuando se crea un servicio de punto de conexión de VPC. Otras entidades principales de AWS acceden al servicio de punto de conexión mediante la creación de un punto de conexión del equilibrador de carga de puerta de enlace.

Precios

Se le facturará por cada hora de aprovisionamiento del punto de conexión del equilibrador de carga de la puerta de enlace en cada zona de disponibilidad. También se le factura por GB de datos procesados. Para más información, consulte Precios de AWS PrivateLink.

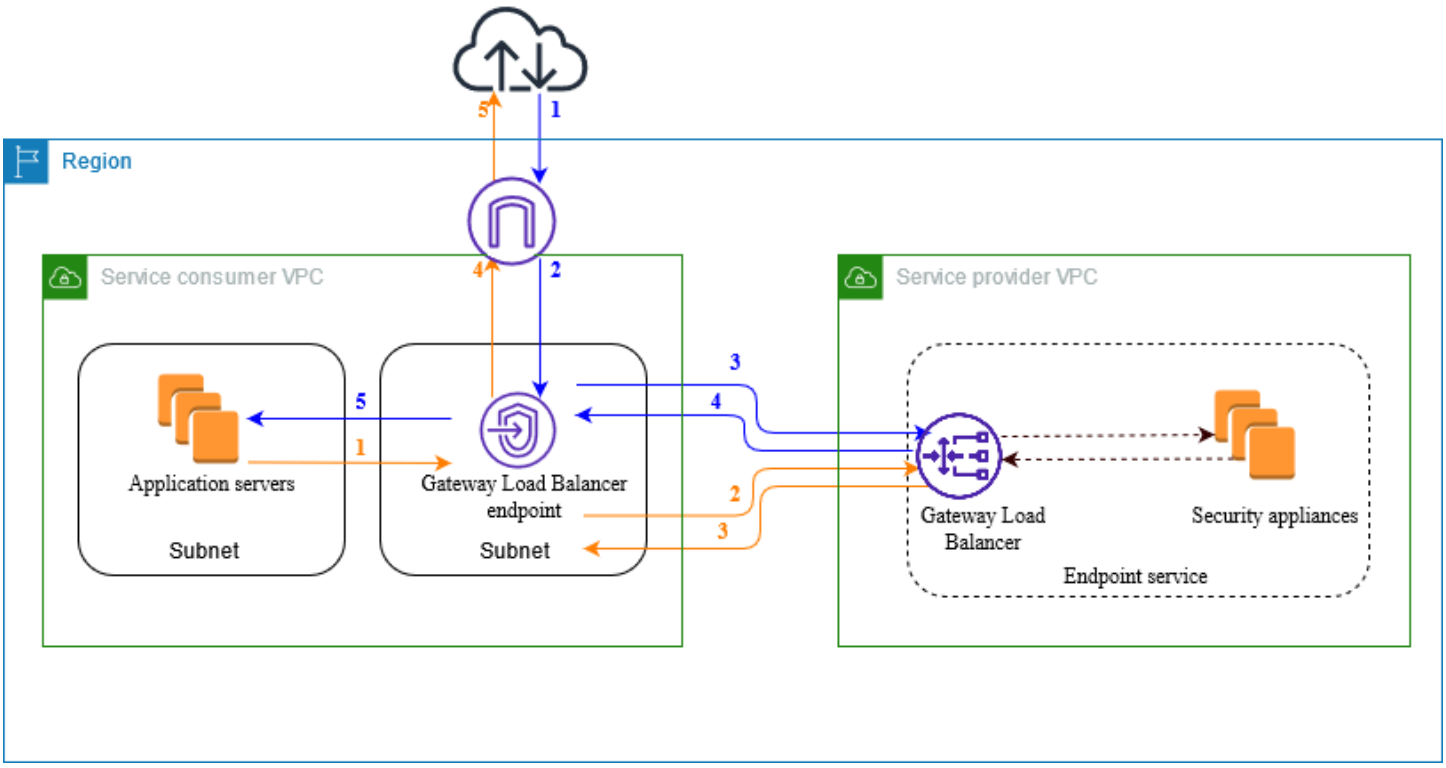
Contenido

Para obtener más información, consulte Balanceadores de carga de puerta de enlace.

Descripción general

En el siguiente diagrama, se muestra cómo los servidores de aplicaciones acceden a los dispositivos de seguridad a través de AWS PrivateLink. Los servidores de aplicaciones se ejecutan en una subred de la VPC del consumidor del servicio. Crea un punto de conexión del equilibrador de carga de puerta de enlace en otra subred de la misma VPC. Todo el tráfico que ingresa a la VPC del consumidor del servicio a través de la puerta de enlace de Internet se dirige primero al punto de conexión del equilibrador de carga de puerta de enlace para su inspección y, luego, se dirige a la subred de destino. Del mismo modo, todo el tráfico que sale de los servidores de aplicaciones se

dirige al punto de conexión del equilibrador de carga de puerta de enlace para su inspección antes de que se dirija nuevamente a través de la puerta de enlace de Internet.



Tráfico de Internet a los servidores de aplicaciones (flechas azules):

1. El tráfico ingresa a la VPC del consumidor del servicio a través de la puerta de enlace de Internet.
2. El tráfico se envía al punto de conexión del equilibrador de carga de la puerta de enlace, en función de la configuración de la tabla de enrutamiento.
3. El tráfico se envía al equilibrador de carga de la puerta de enlace para su inspección a través del dispositivo de seguridad.
4. El tráfico se envía nuevamente al punto de conexión del equilibrador de carga de la puerta de enlace después de la inspección.
5. El tráfico se envía a los servidores de aplicaciones, en función de la configuración de la tabla de enrutamiento.

Tráfico de los servidores de aplicaciones a Internet (flechas naranjas):

1. El tráfico se envía al punto de conexión del equilibrador de carga de la puerta de enlace, en función de la configuración de la tabla de enrutamiento.

2. El tráfico se envía al equilibrador de carga de la puerta de enlace para su inspección a través del dispositivo de seguridad.
3. El tráfico se envía nuevamente al punto de conexión del equilibrador de carga de la puerta de enlace después de la inspección.
4. El tráfico se envía a la puerta de enlace de Internet en función de la configuración de la tabla de enrutamiento.
5. El tráfico se dirige nuevamente a Internet.

Tipos de direcciones IP

Los proveedores de servicios pueden poner sus puntos de conexión de servicio a disposición de los consumidores del servicio mediante IPv4, IPv6 o tanto IPv4 como IPv6, incluso si los dispositivos de seguridad solo admiten IPv4. Si habilita la compatibilidad con dualstack, los consumidores actuales pueden seguir utilizando IPv4 para acceder al servicio y los consumidores nuevos pueden elegir utilizar IPv6 para acceder al servicio.

Si un punto de conexión de equilibrador de carga de puerta de enlace admite IPv4, las interfaces de red del punto de conexión tienen direcciones IPv4. Si un punto de conexión de equilibrador de carga de puerta de enlace admite IPv6, las interfaces de red del punto de conexión tienen direcciones IPv6. No se puede acceder a la dirección IPv6 de una interfaz de red de punto de conexión desde Internet. Si describe una interfaz de red de punto de conexión con una dirección IPv6, observe que `denyAllIgwTraffic` esté habilitado.

Requisitos para habilitar IPv6 para un servicio de punto de conexión

- La VPC y las subredes del servicio de punto de conexión deben tener bloques de CIDR IPv6 asociados.
- El equilibrador de carga de puerta de enlace del servicio de punto de conexión debe utilizar el tipo de dirección IP de doble pila. No es necesario que los dispositivos de seguridad admitan tráfico IPv6.

Requisitos para habilitar IPv6 para un punto de conexión de equilibrador de carga de puerta de enlace

- El servicio de punto de conexión debe tener un tipo de dirección IP compatible con IPv6.

- El tipo de dirección IP de un punto de conexión de equilibrador de carga de puerta de enlace debe ser compatible con la subred del punto de conexión de equilibrador de carga de puerta de enlace, como se describe a continuación:
  - IPv4: se asignan direcciones IPv4 a las interfaces de red del punto de conexión. Esta opción solo se admite si todas las subredes seleccionadas tienen rangos de direcciones IPv4.
  - IPv6: se asignan direcciones IPv6 a las interfaces de red del punto de conexión. Esta opción solo se admite si todas las subredes seleccionadas son subredes IPv6.
  - Dualstack: se asignan direcciones IPv4 e IPv6 a las interfaces de red del punto de conexión. Esta opción solo se admite si todas las subredes seleccionadas tienen rangos de direcciones IPv4 e IPv6.
- Las tablas de enrutamiento de las subredes de la VPC del consumidor del servicio deben enrutar el tráfico IPv6 y las ACL de red de estas subredes deben permitir el tráfico IPv6.

Enrutamiento

Para dirigir el tráfico al servicio de punto de conexión, especifique el punto de conexión del equilibrador de carga de la puerta de enlace como destino en las tablas de enrutamiento, con el ID. En el diagrama anterior, agregue rutas a las tablas de enrutamiento de la siguiente manera. Cuando se utiliza un punto de conexión del equilibrador de carga de la puerta de enlace como destino, no se puede especificar una lista de prefijos como destino. Tenga en cuenta que, en estas tablas, las rutas IPv6 se incluyen en una configuración de doble pila.

Tabla de enrutamiento para la puerta de enlace de Internet

Esta tabla de enrutamiento debe tener una ruta que envíe el tráfico destinado a los servidores de aplicaciones al punto de conexión del equilibrador de carga de la puerta de enlace.

Destino	Objetivo
CIDR IPv4 de VPC	Local
CIDR IPv6 de VPC	Local
CIDR de la subred IPv4 de la aplicación	*vpc-endpoint-id*

Destino	Objetivo
CIDR de la subred IPv6 de la aplicación	*vpc-endpoint-id*

Tabla de enrutamiento para la subred con los servidores de aplicaciones

Esta tabla de enrutamiento debe tener una ruta que envíe todo el tráfico desde los servidores de aplicaciones al punto de conexión del equilibrador de carga de la puerta de enlace.

Destino	Objetivo
CIDR IPv4 de VPC	Local
CIDR IPv6 de VPC	Local
0.0.0.0/0	*vpc-endpoint-id*
::/0	*vpc-endpoint-id*

Tabla de enrutamiento para la subred con el punto de conexión del equilibrador de carga de la puerta de enlace

Esta tabla de enrutamiento debe enviar el tráfico que se devuelve de la inspección a su destino final. En el caso del tráfico que proviene de Internet, la ruta local envía el tráfico a los servidores de aplicaciones. Para el tráfico que proviene de los servidores de aplicaciones, agregue una ruta que dirija todo el tráfico a la puerta de enlace de Internet.

Destino	Objetivo
CIDR IPv4 de VPC	Local
CIDR IPv6 de VPC	Local
0.0.0.0/0	*internet-puerta de enlace -id*
::/0	*internet-puerta de enlace -id*

Creación de un sistema de inspección como servicio de punto de conexión del equilibrador de carga de la puerta de enlace

Puede crear su propio servicio con tecnología AWS PrivateLink, conocido como servicio de punto de conexión. Usted es el proveedor del servicio y las entidades principales de AWS que crean conexiones con su servicio son los consumidores del servicio.

Los servicios de punto de conexión requieren un equilibrador de carga de red o un equilibrador de carga de puerta de enlace. En este caso, usted creará un servicio de punto de conexión con un equilibrador de carga de puerta de enlace. Para obtener más información sobre cómo crear un servicio de punto de conexión con un equilibrador de carga de red, consulte Creación de un servicio de punto de conexión.

Contenido

Consideraciones

- Un servicio de punto de conexión está disponible en la región donde se creó.
- Cuando los consumidores de servicios recuperan información sobre un servicio de punto de conexión, solo pueden ver las zonas de disponibilidad que tienen en común con el proveedor de servicios. Cuando el proveedor del servicio y el consumidor del servicio están en cuentas distintas, se puede asignar un nombre de zona de disponibilidad, como `us-east-1a`, a una zona de disponibilidad física diferente en cada Cuenta de AWS. Puede utilizar los ID de las zonas de disponibilidad para identificar de forma consistente las zonas de disponibilidad de su servicio. Para obtener más información, consulte ID de AZ en la Guía del usuario de Amazon EC2.
- Hay cuotas en los recursos de AWS PrivateLink. Para obtener más información, consulte AWS PrivateLinkCuotas de .

Requisitos previos

- Cree una VPC del proveedor del servicio con al menos dos subredes en la zona de disponibilidad en la que el servicio debería estar disponible. Una subred es para las instancias del dispositivo de seguridad y la otra es para el equilibrador de carga de la puerta de enlace.
- Cree un equilibrador de carga de puerta de enlace en la VPC del proveedor del servicio. Si planea habilitar la compatibilidad con IPv6 en su servicio de punto de conexión, debe habilitar la compatibilidad con doble pila en su equilibrador de carga de puerta de enlace. Para obtener más información, consulte Introducción a los balanceadores de carga de gateway.
- Inicie los dispositivos de seguridad en la VPC del proveedor del servicio y regístrelos en un grupo de destino del equilibrador de carga.

Creación del servicio de punto de conexión

Utilice el siguiente procedimiento para crear un servicio de punto de conexión con un equilibrador de carga de puerta de enlace.

Para crear un servicio de punto de conexión con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Elija Create endpoint service (Crear servicio de punto de conexión).
4. En Load balancer type (Tipo de equilibrador de carga), elija Puerta de enlace.
5. Para Available load balancers (Equilibradores de carga disponibles), seleccione el equilibrador de carga de la puerta de enlace.
6. En Require acceptance for endpoint (Solicitar aceptación para punto de conexión), seleccione Acceptance required (Aceptación solicitada) para establecer que las solicitudes de conexión al servicio de punto de conexión se deben aceptar de forma manual. De lo contrario, se aceptan de forma automática.
7. En Supported IP address types (Tipos de direcciones IP compatibles), haga una de las siguientes acciones:
   - Seleccione IPv4: se habilita el servicio de punto de conexión para aceptar solicitudes de IPv4.
   - Seleccione IPv6: se habilita el servicio de punto de conexión para aceptar solicitudes de IPv6.

- Seleccione IPv4 y IPv6: se habilita el servicio de punto de conexión para aceptar solicitudes de IPv4 y IPv6.

8. (Opcional) Para agregar una etiqueta, elija Add new tag (Agregar etiqueta nueva) e ingrese la clave y el valor de la etiqueta.
9. Seleccione Crear.

Para crear un servicio de punto de conexión con la línea de comandos

- create-vpc-endpoint-service-configuration (AWS CLI)
- New-EC2VpcEndpointServiceConfiguration (Herramientas para Windows PowerShell)

Ponga a disposición su servicio de punto de conexión

Los proveedores de servicios deben hacer lo siguiente para que sus servicios estén disponibles para los consumidores de servicios.

- Agregue permisos que permitan a cada consumidor de servicios conectarse a su servicio de punto de conexión. Para obtener más información, consulte the section called “Administración de permisos”.
- Proporcione al consumidor del servicio el nombre de su servicio y las zonas de disponibilidad compatibles para que pueda crear un punto de conexión de interfaz y conectarse al servicio. Para obtener más información, consulte el siguiente procedimiento.
- Acepte la solicitud de conexión del punto de conexión del consumidor del servicio. Para obtener más información consulte () the section called “Aceptación o rechazo de solicitudes de conexión”.

Las entidades principales de AWS pueden conectarse a su servicio de punto de conexión de forma privada mediante la creación de un punto de conexión del equilibrador de carga de puerta de enlace. Para obtener más información, consulte Creación de un punto de conexión del equilibrador de carga de gateway.

Acceso a un sistema de inspección con un punto de conexión del equilibrador de carga de puerta de enlace

Puede crear un punto de conexión del equilibrador de carga de puerta de enlace para conectarse a servicios de punto de conexión con tecnología AWS PrivateLink.

Para cada subred que especifique en su VPC, creamos una interfaz de red de punto de conexión en la subred y le asignamos una dirección IP privada del intervalo de direcciones de subred. Una interfaz de red de punto de conexión es una interfaz de red administrada por el solicitante; puede verla en su Cuenta de AWS, pero no puede administrarla usted mismo.

Se le facturan los cargos por uso por hora y procesamiento de datos. Para obtener más información, consulte Precio de punto de enlace del equilibrador de carga de Gateway.

Contenido

Consideraciones

- Solo puede elegir una zona de disponibilidad en la VPC del consumidor del servicio. Luego no puede cambiar esta subred. Para utilizar un punto de conexión del equilibrador de carga de puerta de enlace en una subred diferente, debe crear un punto de conexión del equilibrador de carga de puerta de enlace nuevo.
- Puede crear un único punto de conexión del equilibrador de carga de puerta de enlace por zona de disponibilidad por servicio, pero debe seleccionar la zona de disponibilidad que admita el equilibrador de carga de puerta de enlace. Cuando el proveedor del servicio y el consumidor del servicio están en cuentas distintas, se puede asignar un nombre de zona de disponibilidad, como `us-east-1a`, a una zona de disponibilidad física diferente en cada Cuenta de AWS. Puede utilizar los ID de las zonas de disponibilidad para identificar de forma consistente las zonas de disponibilidad de su servicio. Para obtener más información, consulte ID de AZ en la Guía del usuario de Amazon EC2.
- Antes de que pueda utilizar el servicio de punto de conexión, el proveedor del servicio debe aceptar las solicitudes de conexión. El servicio no puede iniciar solicitudes a los recursos en la VPC a través del punto de conexión de VPC. El punto de conexión solo proporciona respuestas al tráfico que se inició a partir de los recursos de la VPC.

- Cada punto de conexión del equilibrador de carga de la puerta de enlace admite un ancho de banda de hasta 10 Gbps por cada zona de disponibilidad y escala verticalmente y de forma automática hasta 100 Gbps.
- Si un servicio de punto de conexión está asociado con varios equilibradores de carga de puerta de enlace, un punto de conexión del equilibrador de carga de puerta de enlace establece una conexión solo con un equilibrador de carga por zona de disponibilidad.
- Para mantener el tráfico dentro de la misma zona de disponibilidad, se recomienda crear un punto de conexión del equilibrador de carga de puerta de enlace en cada zona de disponibilidad a la que se enviará tráfico.
- La preservación de IP del cliente del Network Load Balancer no se admite cuando el tráfico se enruta a través de un punto de conexión del equilibrador de carga de una puerta de enlace, incluso si el destino se encuentra en la misma VPC que el Network Load Balancer.
- Si los servidores de aplicaciones y el punto de conexión del equilibrador de carga de la puerta de enlace se encuentran en la misma subred, las reglas de la NACL se evalúan para el tráfico desde los servidores de aplicaciones al punto de conexión del equilibrador de carga de la puerta de enlace.
- Si utiliza un equilibrador de carga de puerta de enlace con una puerta de enlace de Internet de solo salida, se descarta el tráfico IPv6. En su lugar, utilice una puerta de enlace de Internet y reglas de firewall de entrada.
- Hay cuotas en los recursos de AWS PrivateLink. Para obtener más información, consulte AWS PrivateLinkCuotas de .

Requisitos previos

- Cree una VPC del consumidor del servicio con al menos dos subredes en la zona de disponibilidad desde la que accederá al servicio. Una subred es para los servidores de aplicaciones y la otra es para el punto de conexión del equilibrador de carga de puerta de enlace.
- Para verificar qué zonas de disponibilidad son compatibles con el servicio de punto de conexión, describa el servicio de punto de conexión con la consola o el comando describe-vpc-endpoint-services.
- Si sus recursos están en una subred con una ACL de red, compruebe que la ACL de red permita el tráfico entre las interfaces de red de punto de conexión y los recursos en la VPC.

Creación del punto de enlace

Utilice el siguiente procedimiento para crear un punto de conexión del equilibrador de carga de puerta de enlace que se conecte al servicio de punto de conexión para el sistema de inspección.

Para crear un punto de conexión del equilibrador de carga de puerta de enlace con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Elija Crear punto de conexión.
4. En Tipo, elija Servicios de punto de conexión que utilizan NLB y GWLB.
5. En Service name (Nombre del servicio), ingrese el nombre del servicio y luego elija Verify service (Comprobar servicio).
6. Para VPC, seleccione la VPC desde la que accederá al servicio de punto de conexión.
7. En Subredes, seleccione una subred en la que se va a crear la interfaz de red de punto de conexión.
8. En Tipo de dirección IP, elija entre las siguientes opciones:
   - IPv4: se asignan direcciones IPv4 a la interfaz de red del punto de conexión. Esta opción solo se admite si la subred seleccionada tiene rangos de direcciones IPv4.
   - IPv6: se asignan direcciones IPv6 a la interfaz de red del punto de conexión. Esta opción solo se admite si la subred seleccionada es únicamente una subred IPv6.
   - Doble pila: se asignan direcciones IPv4 e IPv6 a la interfaz de red del punto de conexión. Esta opción solo se admite si la subred seleccionada tiene rangos de direcciones IPv4 e IPv6.
9. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
10. Elija Crear punto de conexión. El estado inicial es `pending acceptance`.

Para crear un punto de conexión del equilibrador de carga de puerta de enlace con la línea de comandos

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint (Herramientas para Windows PowerShell)

Configuración del enrutamiento

Utilice el siguiente procedimiento para configurar las tablas de enrutamiento para la VPC del consumidor del servicio. Esto permite que los dispositivos de seguridad realicen una inspección de seguridad del tráfico entrante con destino a los servidores de aplicaciones. Para obtener más información, consulte the section called “Enrutamiento”.

Para configurar el enrutamiento con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Route Tables.
3. Seleccione la tabla de enrutamiento para la puerta de enlace de Internet y realice lo siguiente:
   a. Elija Actions (Acciones), Edit routes (Editar rutas).
   b. Si admite IPv4, elija Agregar ruta. En Destination (Destino), ingrese el bloque de CIDR IPv4 de la subred para los servidores de aplicaciones. En Target (Objetivo), seleccione el punto de conexión de VPC.
   c. Si admite IPv6, elija Agregar ruta. En Destination (Destino), ingrese el bloque de CIDR IPv6 de la subred para los servidores de aplicaciones. En Target (Objetivo), seleccione el punto de conexión de VPC.
   d. Elija Guardar cambios.
4. Seleccione la tabla de enrutamiento para la subred con los servidores de aplicaciones y haga lo siguiente:
   a. Elija Actions (Acciones), Edit routes (Editar rutas).
   b. Si admite IPv4, elija Agregar ruta. En Destino, escriba **`0.0.0.0/0`**. En Target (Objetivo), seleccione el punto de conexión de VPC.
   c. Si admite IPv6, elija Agregar ruta. En Destino, escriba **`::/0`**. En Target (Objetivo), seleccione el punto de conexión de VPC.
   d. Elija Guardar cambios.
5. Seleccione la tabla de enrutamiento para la subred con el punto de conexión del equilibrador de carga de puerta de enlace y realice lo siguiente:
   a. Elija Actions (Acciones), Edit routes (Editar rutas).
   b. Si admite IPv4, elija Agregar ruta. En Destino, escriba **`0.0.0.0/0`**. En Target (Objetivo), seleccione la puerta de enlace de Internet.

c. Si admite IPv6, elija Agregar ruta. En Destino, escriba **::/0**. En Target (Objetivo), seleccione la puerta de enlace de Internet.

d. Elija Guardar cambios.

Para configurar el enrutamiento con la línea de comandos

- create-route (AWS CLI)
- New-EC2Route (Herramientas para Windows PowerShell)

Administración de etiquetas

Puede etiquetar el punto de conexión del equilibrador de carga de puerta de enlace para identificarlo o clasificarlo en función de las necesidades de su organización.

Para administrar etiquetas con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de interfaz.
4. Elija Actions (Acciones) y, a continuación, Manage tags (Administrar etiquetas).
5. Para cada etiqueta que desee agregar, elija Add new tag (Agregar etiqueta nueva) e ingrese la clave y el valor de la etiqueta.
6. Para eliminar una etiqueta, elija Remove (Eliminar) a la derecha de la clave y el valor de la etiqueta.
7. Seleccione Save (Guardar).

Para administrar etiquetas con la línea de comandos

- create-tags y delete-tags (AWS CLI)
- New-EC2Tag y Remove-EC2Tag (Herramientas para Windows PowerShell)

Eliminación de un punto de conexión del equilibrador de carga de puerta de enlace

Cuando ya no necesite un punto de conexión, puede eliminarlo. Cuando se elimina un punto de conexión del equilibrador de carga de puerta de enlace, también se eliminan las interfaces de red del punto de conexión. No puede eliminar un punto de conexión del equilibrador de carga de puerta de enlace si hay rutas en las tablas de enrutamiento que apunten al punto de conexión.

Para eliminar un punto de conexión del equilibrador de carga de puerta de enlace

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoints y seleccione el punto de conexión.
3. Elija Actions, Delete Endpoint.
4. En la pantalla de confirmación, elija Yes, Delete.

Para eliminar un punto de conexión del equilibrador de carga de puerta de enlace

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint (AWS Tools for Windows PowerShell)

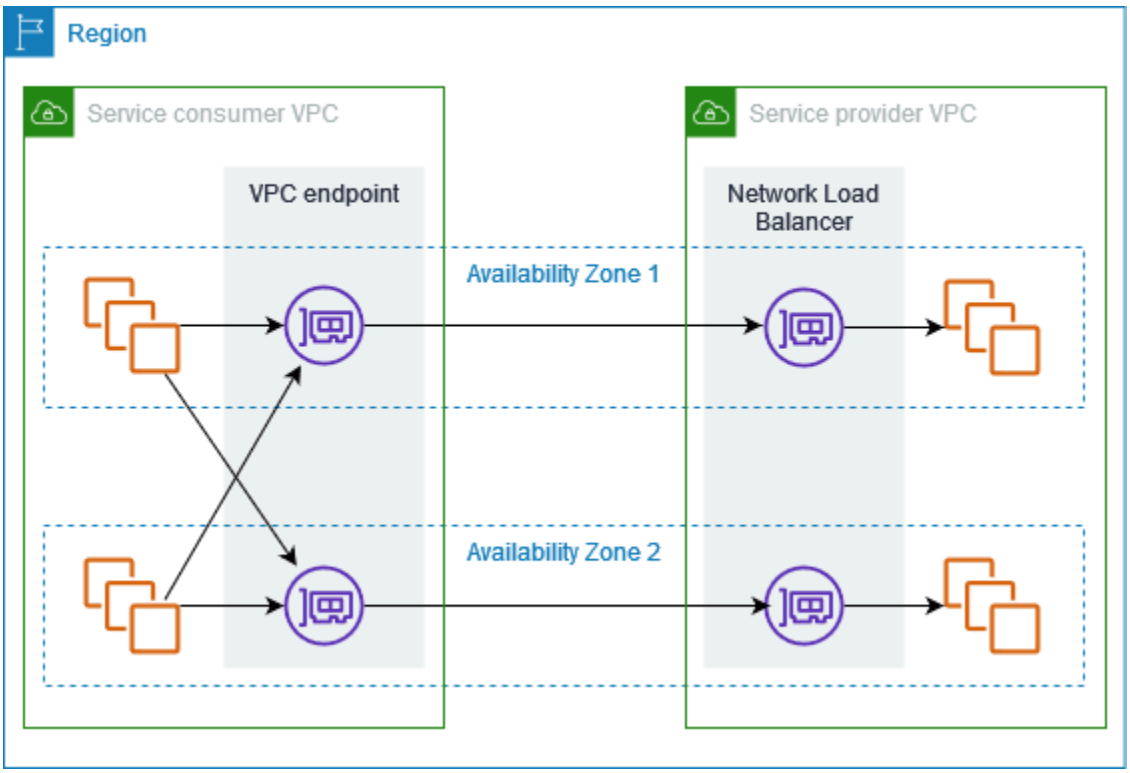
Comparta sus servicios a través de AWS PrivateLink

Puede alojar su propio servicio AWS PrivateLink avanzado, conocido como servicio de punto final, y compartirlo con otros AWS clientes.

Contenido

Descripción general

El siguiente diagrama muestra cómo compartes el servicio que está hospedado AWS con otros AWS clientes y cómo esos clientes se conectan a tu servicio. Como el proveedor del servicio, usted crea un equilibrador de carga de red en su VPC como el servicio frontend. Luego, selecciona este equilibrador de carga cuando crea la configuración del servicio de punto de conexión de VPC. Concede permisos a entidades principales específicas de AWS para que puedan conectarse al servicio. Como consumidor del servicio, el consumidor crea un punto de conexión de VPC de interfaz, que establece conexiones entre las subredes que selecciona de la VPC y el servicio de punto de conexión. El equilibrador de carga recibe solicitudes del consumidor del servicio y las dirige a los destinos que alojan el servicio.



Para conseguir baja latencia y alta disponibilidad, se recomienda que el servicio esté disponible en al menos dos zonas de disponibilidad.

Nombre de host DNS

Cuando un proveedor de servicios crea un servicio de punto final de VPC, AWS genera un nombre de host DNS específico del punto final para el servicio. Estos nombres tienen la siguiente sintaxis:

```
endpoint_service_id.region.vpce.amazonaws.com
```

A continuación, se muestra un ejemplo de nombre de host de DNS para un servicio de punto de conexión de VPC en la región us-east-2:

```
vpce-svc-071afff70666e61e0.us-east-2.vpce.amazonaws.com
```

Cuando un consumidor de servicios crea un punto de conexión de VPC de interfaz, creamos nombres de DNS regionales y de zona que el consumidor del servicio puede utilizar para comunicarse con el servicio de punto de conexión. Los nombres regionales tienen la siguiente sintaxis:

```
endpoint_id.endpoint_service_id.service_region.vpce.amazonaws.com
```

Los nombres de zona tienen la siguiente sintaxis:

```
endpoint_id-endpoint_zone.endpoint_service_id.service_region.vpce.amazonaws.com
```

DNS privado

El proveedor de un servicio también puede asociar un nombre de DNS privado a su servicio de punto de conexión, de modo que los consumidores del servicio puedan seguir accediendo al servicio con el nombre de DNS existente. Si un proveedor de servicios asocia un nombre DNS privado a su servicio de punto de conexión, los consumidores del servicio pueden habilitar nombres DNS privados para sus puntos de conexión de interfaz. Si un proveedor de servicios no habilita el DNS privado, es posible que los consumidores del servicio tengan que actualizar sus aplicaciones para utilizar el nombre DNS público del servicio de punto de conexión de VPC. Para obtener más información, consulte Administración de nombres de DNS.

Subredes y zonas de disponibilidad

Su servicio de punto de conexión está disponible en las zonas de disponibilidad que se habilitan para el equilibrador de carga de red. Para obtener una alta disponibilidad y resiliencia, te recomendamos que habilites el balanceador de carga en al menos dos zonas de disponibilidad, implementes instancias en cada zona habilitada y registres estas EC2 instancias en el grupo objetivo del balanceador de carga.

Puede habilitar el equilibrio de carga entre zonas como alternativa al alojamiento del servicio de punto de conexión en varias zonas de disponibilidad. Sin embargo, los consumidores perderán el acceso al servicio de puntos de conexión desde ambas zonas si la zona que aloja el servicio de puntos de conexión falla. Tenga en cuenta también que cuando habilita el equilibrio de carga entre zonas para un Network Load Balancer EC2 , se aplican cargos por transferencia de datos.

El consumidor puede crear puntos de conexión de VPC de interfaz en las zonas de disponibilidad en las que esté disponible su servicio de punto de conexión. Creamos una interfaz de red de punto de conexión en cada subred que el consumidor configura para el punto de conexión de VPC. Asignamos direcciones IP a cada interfaz de red de punto de conexión desde su subred, en función del tipo de dirección IP del punto de conexión de VPC. Cuando una solicitud utiliza el punto de conexión regional del servicio de punto de conexión de VPC, seleccionamos una interfaz de red

de punto de conexión en buen estado, y se emplea el algoritmo round robin para alternar entre las interfaces de red en diferentes zonas de disponibilidad. A continuación, resolvemos el tráfico dirigido a la dirección IP de la interfaz de red de punto de conexión seleccionada.

El consumidor puede usar los puntos de conexión zonales para el punto de conexión de VPC si es mejor para su caso de uso mantener el tráfico en la misma zona de disponibilidad.

Acceso entre regiones

Un proveedor de servicios puede alojar un servicio en una región y ponerlo a disposición en un conjunto de regiones compatibles. Un consumidor de servicios selecciona una región de servicio durante la creación de un punto de conexión.

Permisos

- De forma predeterminada, las entidades de IAM no tienen permiso para hacer que un servicio de punto de conexión esté disponible en varias regiones ni acceder a un servicio de punto de conexión en todas las regiones. Para conceder los permisos necesarios para el acceso entre regiones, un administrador de IAM puede crear políticas de IAM que permitan la acción solo con permisos `vpce:AllowMultiRegion`.
- Para controlar las regiones que una entidad de IAM puede especificar como regiones compatibles al crear un servicio de punto de conexión, se debe utilizar la clave de condición `ec2:VpceSupportedRegion`.
- Para controlar las regiones que una entidad de IAM puede especificar como región de servicio al crear un punto de conexión de VPC, se debe utilizar la clave de condición `ec2:VpceServiceRegion`.

Consideraciones

- Un proveedor de servicios debe optar por una región registrada antes de agregarla como región compatible para un servicio de punto de conexión.
- Se debe poder acceder al servicio de puntos de conexión desde la región del host. No se puede eliminar la región del host del conjunto de regiones compatibles. Para garantizar la redundancia, puede implementar su servicio de puntos de conexión en varias regiones y habilitar el acceso entre regiones para cada servicio de punto de conexión.
- El consumidor del servicio debe optar por una región registrada antes de seleccionarla como la región de servicio para un punto de conexión. Siempre que sea posible, recomendamos que los

consumidores de servicios accedan a un servicio mediante la conectividad intrarregional en lugar de la conectividad entre regiones. La conectividad intrarregional proporciona latencia y costos más bajos.

- Si un proveedor de servicios elimina una región del conjunto de regiones compatibles, los consumidores de servicios no podrán seleccionar esa región como región de servicio durante la creación de nuevos puntos de conexión. Tenga en cuenta que esto no afecta el acceso al servicio de puntos de conexión desde los puntos de conexión existentes que utilizan esta región como región de servicio.
- Para obtener alta disponibilidad, los proveedores deben utilizar al menos dos zonas de disponibilidad. El acceso entre regiones no requiere que los proveedores y los consumidores utilicen las mismas zonas de disponibilidad.
- El acceso entre regiones no se admite en las siguientes zonas de disponibilidad: `use1-az3`, `usw1-az2`, `apne1-az3`, `apne2-az2` y `apne2-az4`.
- Con el acceso entre regiones, AWS PrivateLink gestiona la conmutación por error entre las zonas de disponibilidad. No administra la conmutación por error en todas las regiones.
- Los equilibradores de carga de red con un valor personalizado configurado para el tiempo de espera de inactividad del TCP no son compatibles con el acceso entre regiones.
- La fragmentación UDP no admite el acceso entre regiones.
- El acceso entre regiones solo se admite para los servicios a través de los cuales se comparte. AWS PrivateLink

Tipos de direcciones IP

Los proveedores de servicios pueden poner sus terminales de servicio a disposición de los consumidores de servicios a través IPv4 de ellos o de ambas formas IPv4 IPv6, incluso si sus servidores de backend solo son compatibles. IPv6 IPv4 Si habilita el soporte de doble pila, los consumidores actuales pueden seguir utilizándolo para acceder IPv4 a su servicio y los nuevos consumidores pueden optar por utilizarlo IPv6 para acceder a su servicio.

Si una interfaz de punto final de VPC admite IPv4, las interfaces de red de puntos finales tienen IPv4 direcciones. Si una interfaz de punto final de VPC admite IPv6, las interfaces de red de puntos finales tienen IPv6 direcciones. No se puede acceder a la IPv6 dirección de la interfaz de red de un punto final desde Internet. Si describe una interfaz de red de punto final con una IPv6 dirección, observe que `denyAllIgwTraffic` está habilitada.

Requisitos IPv6 para habilitar un servicio de punto final

- La VPC y las subredes del servicio de punto final deben tener bloques CIDR asociados IPv6 .
- Todos los equilibradores de carga de red del servicio de punto de conexión deben utilizar el tipo de dirección IP dualstack. No es necesario que los destinos admitan tráfico. IPv6 Si el servicio procesa las direcciones IP de origen del encabezado de la versión 2 del protocolo proxy, debe procesar IPv6 las direcciones.

Requisitos IPv6 para habilitar un punto final de interfaz

- El servicio de punto final debe admitir IPv6 las solicitudes.
- El tipo de dirección IP de un punto de conexión de interfaz debe ser compatible con las subredes del punto de conexión de interfaz, como se describe a continuación:
  - IPv4— Asigne IPv4 direcciones a las interfaces de red de sus puntos finales. Esta opción solo se admite si todas las subredes seleccionadas tienen rangos de IPv4 direcciones.
  - IPv6— Asigne IPv6 direcciones a las interfaces de red de sus puntos finales. Esta opción solo se admite si todas las subredes seleccionadas son IPv6 solo subredes.
  - Dualstack: IPv4 asigne ambas IPv6 direcciones a las interfaces de red de sus puntos finales. Esta opción solo se admite si todas las subredes seleccionadas tienen ambos IPv4 rangos de direcciones. IPv6

Tipo de dirección IP de registro DNS para un punto de conexión de interfaz

El tipo de dirección IP de registro DNS que admite un punto de conexión de interfaz determina los registros DNS que se crean. El tipo de dirección IP de registro DNS de un punto de conexión de interfaz debe ser compatible con el tipo de dirección IP del punto de conexión de interfaz, como se describe a continuación:

- IPv4— Cree registros A para los nombres DNS privados, regionales y zonales. El tipo de dirección IP debe ser IPv4Dualstack.
- IPv6— Cree registros AAAA para los nombres DNS privados, regionales y zonales. El tipo de dirección IP debe ser Dualstack IPv6.
- Dualstack: se crean registros A y AAAA para los nombres de DNS privados, regionales y de zonas. El tipo de dirección IP debe ser Dualstack.

Cree un servicio impulsado por AWS PrivateLink

Puede crear su propio servicio impulsado por AWS PrivateLink, conocido como servicio de punto final. Usted es el proveedor del servicio y las entidades principales de AWS que crean conexiones con su servicio son los consumidores del servicio.

Los servicios de punto de conexión requieren un equilibrador de carga de red o un equilibrador de carga de puerta de enlace. El equilibrador de carga recibe solicitudes de los consumidores del servicio y las dirige al servicio. En este caso, usted creará un servicio de punto de conexión con un equilibrador de carga de red. Para obtener más información sobre cómo crear un servicio de punto de conexión con un equilibrador de carga de puerta de enlace, consulte Acceso a dispositivos virtuales.

Contenido

Consideraciones

- Un servicio de punto de conexión está disponible en la región donde se creó. Los consumidores pueden acceder a su servicio desde otras regiones si se habilita el acceso entre regiones o si utilizan la interconexión de VPC o una puerta de enlace de tránsito.
- Cuando los consumidores de servicios recuperan información sobre un servicio de punto de conexión, solo pueden ver las zonas de disponibilidad que tienen en común con el proveedor de servicios. Cuando el proveedor del servicio y el consumidor del servicio están en cuentas distintas, se puede asignar un nombre de zona de disponibilidad, como `us-east-1a`, a una zona de disponibilidad física diferente en cada Cuenta de AWS. Puede usar AZ IDs para identificar de forma coherente las zonas de disponibilidad de su servicio. Para obtener más información, consulta AZ IDs en la Guía del EC2 usuario de Amazon.
- Cuando los consumidores de servicios envían tráfico a un servicio a través de un punto de conexión de interfaz, las direcciones IP de origen proporcionadas a la aplicación son las direcciones IP privadas de los nodos del equilibrador de carga y no las direcciones IP de los

consumidores de servicios. Si habilitas el protocolo proxy en el balanceador de cargas, puedes obtener las direcciones de los consumidores del servicio y de los puntos finales IDs de la interfaz desde el encabezado del protocolo proxy. Para obtener más información, consulte Proxy Protocol en la Guía del usuario de balanceadores de carga de red.

- Un equilibrador de carga de red puede asociarse a un único servicio de punto de conexión, pero un servicio de punto de conexión puede asociarse a varios balanceadores de carga de red.
- Si un servicio de punto de conexión está asociado a varios equilibradores de carga de red, cada interfaz de red de punto de conexión está asociada a un equilibrador de carga. Cuando se inicia la primera conexión desde una interfaz de red de punto de conexión, seleccionamos de manera aleatoria uno de los equilibradores de carga de red en la misma zona de disponibilidad de la interfaz de red de punto de conexión. Todas las solicitudes de conexión posteriores de esta interfaz de red de punto de conexión utilizan el equilibrador de carga seleccionado. Le recomendamos que utilice la misma configuración de oyente y grupo de destino para todos los equilibradores de carga de un servicio de punto de conexión, de modo que los consumidores puedan utilizar el servicio de punto de conexión correctamente independientemente del equilibrador de carga que se elija.
- Hay cuotas en sus recursos. AWS PrivateLink Para obtener más información, consulte AWS PrivateLinkCuotas de .

Requisitos previos

- Cree una VPC para su servicio de punto de conexión con al menos una subred en cada zona de disponibilidad en la que el servicio debería estar disponible.
- Para que los consumidores de servicios puedan crear puntos de enlace de VPC de IPv6 interfaz para su servicio de punto final, la VPC y las subredes deben tener bloques CIDR asociados. IPv6
- Cree un equilibrador de carga de red en su VPC. Seleccione una subred por zona de disponibilidad en la que el servicio debería estar disponible para los consumidores del servicio. Para conseguir baja latencia y tolerancia a errores, se recomienda que el servicio esté disponible en al menos dos zonas de disponibilidad de la región.
- Si su Equilibrador de carga de red tiene un grupo de seguridad, debe permitir el tráfico entrante desde las direcciones IP de los clientes. Como alternativa, puede desactivar la evaluación de las reglas de los grupos de seguridad entrantes para el tráfico que los atraviesa. AWS PrivateLink Para obtener más información, consulte Grupos de seguridad en la Guía del usuario de Equilibradores de carga de red.

- Para permitir que su servicio de punto final acepte IPv6 solicitudes, sus balanceadores de carga de red deben usar el tipo de dirección IP de doble pila. No es necesario que los destinos admitan tráfico. IPv6 Para obtener más información, consulte Tipo de dirección IP en la Guía del usuario de equilibradores de carga de red.

  Si procesa las direcciones IP de origen desde el encabezado de la versión 2 del protocolo proxy, compruebe que puede procesar IPv6 las direcciones.
- Lance instancias en cada zona de disponibilidad en la que el servicio debería estar disponible y regístrelas en un grupo de destino del equilibrador de carga. Si no lanza instancias en todas las zonas de disponibilidad habilitadas, puede habilitar el equilibrio de carga entre zonas para admitir consumidores de servicios que utilicen nombres de host de DNS de zona para acceder al servicio. Cuando habilita el equilibrio de carga entre zonas, se aplican cargos por transferencia de datos regionales. Para obtener más información, consulte Equilibrio de carga entre zonas en la Guía del usuario de Equilibradores de carga de red.

Creación de un servicio de punto de conexión

Utilice el siguiente procedimiento para crear un servicio de punto de conexión con un equilibrador de carga de red.

Para crear un servicio de punto de conexión con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Elija Create endpoint service (Crear servicio de punto de conexión).
4. En Load balancer type (Tipo de equilibrador de carga), elija Network (Red).
5. En Equilibradores de carga de red, seleccione los equilibradores de carga de red que desea asociar con el servicio de punto de conexión. Para ver las zonas de disponibilidad que están habilitadas para el equilibrador de carga que se ha seleccionado, consulte Detalles de los equilibradores de carga seleccionados, incluidas las zonas de disponibilidad. Su servicio de punto de conexión estará disponible en estas zonas de disponibilidad.
6. (Opcional) Para que su servicio de punto de conexión esté disponible en regiones distintas de la región en la que está alojado, seleccione las regiones en Regiones de servicio. Para obtener más información, consulte the section called “Acceso entre regiones”.
7. En Require acceptance for endpoint (Solicitar aceptación para punto de conexión), seleccione Acceptance required (Aceptación solicitada) para establecer que las solicitudes de conexión

al servicio de punto de conexión se deben aceptar de forma manual. De lo contrario, estas solicitudes se aceptan de forma automática.

8. En Enable private DNS name (Habilitar nombre de DNS privado), seleccione Associate a private DNS name with the service (Asociar un nombre de DNS privado al servicio) para asociar un nombre de DNS privado que los consumidores del servicio puedan utilizar para acceder al servicio y luego, ingrese el nombre de DNS privado. De lo contrario, los consumidores de servicios pueden usar el nombre DNS específico del punto final proporcionado por. AWS Antes de que los consumidores del servicio puedan utilizar el nombre de DNS privado, el proveedor del servicio debe comprobar que es propietario del dominio. Para obtener más información, consulte Administración de nombres de DNS.
9. En Supported IP address types (Tipos de direcciones IP compatibles), haga una de las siguientes acciones:
   - Seleccione IPv4: habilite el servicio de punto final para que acepte solicitudes. IPv4
   - Seleccione IPv6: habilite el servicio de punto final para que acepte IPv6 solicitudes.
   - Seleccione IPv4y IPv6: habilite el servicio de punto final para que acepte tanto IPv6 las solicitudes como IPv4 las demás.
10. (Opcional) Para agregar una etiqueta, elija Add new tag (Agregar etiqueta nueva) e ingrese la clave y el valor de la etiqueta.
11. Seleccione Crear.

Para crear un servicio de punto de conexión con la línea de comandos

- create-vpc-endpoint-service-configuración ()AWS CLI
- New-EC2VpcEndpointServiceConfiguration(Herramientas para Windows PowerShell)

Ponga a disposición su servicio de punto de conexión para los consumidores de servicios

AWS los principales pueden conectarse a su servicio de punto final de forma privada mediante la creación de un punto final de VPC de interfaz. Los proveedores de servicios deben hacer lo siguiente para que sus servicios estén disponibles para los consumidores de servicios.

- Agregue permisos que permitan a cada consumidor de servicios conectarse a su servicio de punto de conexión. Para obtener más información, consulte the section called “Administración de permisos”.
- Proporcione al consumidor del servicio el nombre de su servicio y las zonas de disponibilidad compatibles para que pueda crear un punto de conexión de interfaz y conectarse al servicio. Para obtener más información, consulte the section called “Conexión a un servicio de punto de conexión como consumidor del servicio”.
- Acepte la solicitud de conexión del punto de conexión del consumidor del servicio. Para obtener más información, consulte the section called “Aceptación o rechazo de solicitudes de conexión”.

Conexión a un servicio de punto de conexión como consumidor del servicio

Un consumidor de servicios utiliza el siguiente procedimiento para crear un punto de conexión de interfaz para conectarse al servicio de punto de conexión.

Para crear un punto de conexión de interfaz con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Elija Crear punto de conexión.
4. En Tipo, elija los servicios de punto final que utilizan NLBs y. GWLBs
5. En Nombre del servicio, ingrese el nombre del servicio (por ejemplo, `com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`), y elija Verificar servicio.
6. (Opcional) Para conectarse a un servicio de punto de conexión que esté disponible en una región distinta de la región de punto de conexión, seleccione Región de servicio, a continuación elija Activar punto de conexión entre regiones y, a continuación, seleccione la región. Para obtener más información, consulte the section called “Acceso entre regiones”.
7. Para VPC, seleccione la VPC desde la que accederá al servicio de punto de conexión.
8. En Subredes, seleccione las subredes en las que se van a crear las interfaces de red de punto de conexión.
9. En Tipo de dirección IP, elija entre las siguientes opciones:

- IPv4— Asigne IPv4 direcciones a las interfaces de red de los puntos finales. Esta opción solo se admite si todas las subredes seleccionadas tienen rangos de IPv4 direcciones y el servicio de punto final acepta IPv4 solicitudes.
- IPv6— Asigne IPv6 direcciones a las interfaces de red de puntos finales. Esta opción solo se admite si todas las subredes seleccionadas son IPv6 solo subredes y el servicio de punto final acepta IPv6 solicitudes.
- Dualstack: IPv4 asigne ambas IPv6 direcciones a las interfaces de red de puntos finales. Esta opción solo se admite si todas las subredes seleccionadas tienen ambos rangos de IPv6 direcciones IPv4 y el servicio de punto final acepta ambos IPv4 tipos y solicitudes. IPv6

10. En DNS record IP type (Tipo de IP del registro DNS), elija entre las siguientes opciones:

    - IPv4— Cree registros A para los nombres DNS privados, regionales y zonales. El tipo de dirección IP debe ser IPv4Dualstack.
    - IPv6— Cree registros AAAA para los nombres DNS privados, regionales y zonales. El tipo de dirección IP debe ser Dualstack IPv6.
    - Dualstack: se crean registros A y AAAA para los nombres de DNS privados, regionales y de zonas. El tipo de dirección IP debe ser Dualstack.
    - Service defined (Servicio definido): se crean registros A para los nombres de DNS privados, regionales y de zonas, y registros AAAA para los nombres de DNS regionales y de zonas. El tipo de dirección IP debe ser Dualstack.
11. En Grupo de seguridad, seleccione los grupos de seguridad que deban asociarse a las interfaces de red de punto de conexión.
12. Elija Crear punto de conexión.

Para crear un punto de conexión de interfaz mediante la línea de comandos

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Herramientas para Windows) PowerShell

Configuración de un servicio de punto de conexión

Después de crear un servicio de punto de conexión, puede actualizar su configuración.

Tareas

Administración de permisos

La combinación de los ajustes de permisos y aceptación le ayuda a controlar qué consumidores de servicios (AWS principales) pueden acceder a su servicio de punto final. Por ejemplo, puede conceder permisos a entidades principales específicas de confianza y aceptar de forma automática todas las solicitudes de conexión, o puede conceder permisos a un grupo más amplio de entidades principales y aceptar de forma manual únicamente las solicitudes de conexión específicas en las que confíe.

De forma predeterminada, el servicio de punto de conexión no está disponible para los consumidores del servicio. Debe agregar permisos que permitan a entidades AWS principales específicas crear un punto final de VPC de interfaz para conectarse a su servicio de punto final. Para añadir permisos a una entidad AWS principal, necesita su nombre de recurso de Amazon (ARN). La siguiente lista incluye ejemplos ARNs de entidades AWS principales compatibles.

ARNs para directores AWS

Cuenta de AWS (incluye todos los principales de la cuenta)

arn:aws:iam: :root *account_id*

Rol

arn:aws:iam: :role/ *account_id role_name*

Usuario

arn:aws:iam: ::user/ *account_id user_name*

Todos los directores en total Cuentas de AWS

*

Consideraciones

- Si concede permiso a todos los usuarios para que accedan al servicio de punto de conexión y configura el servicio de punto de conexión para que acepte todas las solicitudes, el equilibrador de carga será público incluso si no tiene una dirección IP pública.
- Si elimina los permisos, esto no afectará a las conexiones existentes entre el punto de conexión y el servicio que se aceptaron anteriormente.

Para administrar los permisos de su servicio de punto de conexión utilizando la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Seleccione el servicio de punto de conexión y elija la pestaña Allow principals (Permitir entidades principales).
4. Para agregar permisos, elija Allow principals (Permitir entidades principales). En Principals to add (Entidades principales a agregar), ingrese el ARN de la entidad principal. Para agregar más entidades principales, elija Add principal (Agregar entidad principal). Cuando haya terminado de agregar las entidades principales, elija Allow principals (Permitir entidades principales).
5. Para eliminar permisos, seleccione la entidad principal y elija Actions(Acciones), Delete (Eliminar). Cuando le pidan confirmación, escriba **`delete`** y elija Eliminar.

Para agregar permisos para el servicio de punto de conexión con la línea de comandos

- modify-vpc-endpoint-service-permisos ()AWS CLI
- Edit-EC2EndpointServicePermission(Herramientas para Windows PowerShell)

Aceptación o rechazo de solicitudes de conexión

La combinación de los ajustes de permisos y aceptación le ayuda a controlar qué consumidores de servicios (AWS principales) pueden acceder a su servicio de punto final. Por ejemplo, puede conceder permisos a entidades principales específicas de confianza y aceptar de forma automática todas las solicitudes de conexión, o puede conceder permisos a un grupo más amplio de entidades principales y aceptar de forma manual únicamente las solicitudes de conexión específicas en las que confíe.

Puede configurar su servicio de punto de conexión para que acepte solicitudes de conexión de forma automática. De lo contrario, debe aceptarlas o rechazarlas de forma manual. Si no acepta una solicitud de conexión, el consumidor del servicio no podrá acceder al servicio de punto de conexión.

Si concede permiso a todos los usuarios para que accedan al servicio de punto de conexión y configura el servicio de punto de conexión para que acepte todas las solicitudes, el equilibrador de carga será público incluso si no tiene una dirección IP pública.

Puede recibir una notificación cuando se acepte o se rechace una solicitud de conexión. Para obtener más información, consulte the section called “Reciba alertas de los eventos del servicio de punto de conexión”.

Para modificar la opción de aceptación con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Seleccione el servicio de punto de conexión.
4. Elija Actions, Modify endpoint acceptance setting.
5. Seleccione o desactive Acceptance required (Aceptación necesaria).
6. Elija Guardar cambios.

Para modificar la configuración de aceptación con la línea de comandos

- modify-vpc-endpoint-service-configuración ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Herramientas para Windows PowerShell)

Para aceptar o rechazar una solicitud de conexión con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Seleccione el servicio de punto de conexión.
4. En la pestaña Endpoint connections (Conexiones del punto de conexión), seleccione la conexión del punto de conexión.
5. Para aceptar la solicitud de conexión, elija Actions (Acciones), Accept endpoint connection request (Aceptar solicitud de conexión del punto de conexión). Cuando se le solicite confirmación, ingrese **`accept`** y luego, elija Accept (Aceptar).

6. Para rechazar la solicitud de conexión, elija Actions (Acciones), Reject endpoint connection request (Rechazar solicitud de conexión del punto de enlace). Cuando se le solicite confirmación, ingrese **`reject`** y luego, elija Reject (Rechazar).

Para aceptar o rechazar una solicitud de conexión con la línea de comandos

- accept-vpc-endpoint-connectionso reject-vpc-endpoint-connections(AWS CLI)
- Approve-EC2EndpointConnectiono Deny-EC2EndpointConnection(Herramientas para Windows PowerShell)

Administrar equilibradores de carga

Puede administrar los equilibradores de carga que están asociados a su servicio de punto de conexión. No es posible desasociar un equilibrador de carga cuando hay puntos de conexión conectados al servicio de punto de conexión.

Si habilita otra zona de disponibilidad para sus equilibradores de carga, la zona de disponibilidad aparecerá en la pestaña Equilibradores de carga de la página Servicios de punto de conexión. Sin embargo, no estará habilitada para el servicio de punto de conexión ni aparecerá en la pestaña Detalles de su servicio de punto de conexión en la Consola de administración de AWS. Debe habilitar el servicio de punto de conexión para la nueva zona de disponibilidad.

Es posible que la zona de disponibilidad del equilibrador de carga tarde unos minutos en estar lista para su servicio de punto de conexión. Si utiliza una automatización, le recomendamos que agregue una espera al proceso de automatización antes de habilitar el servicio de punto de conexión para la nueva zona de disponibilidad.

Para administrar los equilibradores de carga de un servicio de punto de conexión con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Seleccione el servicio de punto de conexión.
4. Elija Actions (Acciones), Associate or disassociate load balancers (Asociar o desasociar equilibradores de carga).
5. Cambie la configuración del servicio de punto de conexión según sea necesario. Por ejemplo:
   - Seleccione la casilla de verificación de un equilibrador de carga para asociarlo con el servicio de punto de conexión.

- Desactive la casilla de verificación de un equilibrador de carga para desvincularlo del servicio de punto de conexión. Debe mantener seleccionado al menos un equilibrador de carga.

6. Elija Guardar cambios.

   El servicio de punto de conexión se habilitará para cualquier zona de disponibilidad nueva que se haya agregado a su equilibrador de cargas. La nueva zona de disponibilidad aparece en la pestaña Equilibradores de carga y en la pestaña Detalles del servicio de puntos de conexión.

Después de habilitar una zona de disponibilidad para el servicio de punto de conexión, los consumidores del servicio pueden agregar una subred de esa zona de disponibilidad a los puntos de conexión de VPC de la interfaz.

Para administrar los equilibradores de carga de un servicio de punto de conexión con la línea de comandos

- modify-vpc-endpoint-service-configuración ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Herramientas para Windows PowerShell)

Para habilitar el servicio de punto de conexión en una zona de disponibilidad que se habilitó recientemente para el equilibrador de cargas, solo tiene que llamar al comando con el ID del servicio de punto de conexión.

Asociación de un nombre de DNS privado

Puede asociar un nombre de DNS privado a su servicio de punto de conexión. Después de asociar un nombre de DNS privado, debe actualizar la entrada del dominio en su servidor DNS. Antes de que los consumidores del servicio puedan utilizar el nombre de DNS privado, el proveedor del servicio debe comprobar que es propietario del dominio. Para obtener más información, consulte Administración de nombres de DNS.

Para modificar un nombre de DNS privado de un servicio de punto de enlace mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Seleccione el servicio de punto de conexión.
4. Elija Actions (Acciones), Modify private DNS name (Modificar nombre de DNS privado).

5. Seleccione Associate a private DNS name with the service (Asociar un nombre de DNS privado al servicio) e ingrese el nombre de DNS privado.

   - Los nombres de dominio deben estar en minúsculas.
   - Puede utilizar comodines en los nombres de dominio (por ejemplo, **`*.myexampleservice.com`**).

6. Elija Guardar cambios.
7. El nombre de DNS privado está listo para que lo utilicen los consumidores del servicio cuando el estado de verificación es verified (verificado). Si el estado de verificación cambia, se rechazan las solicitudes de conexión nuevas, pero las conexiones existentes no se ven afectadas.

Para modificar el nombre de DNS privado de un servicio de punto de conexión con la línea de comandos

- modify-vpc-endpoint-service-configuración ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Herramientas para Windows PowerShell)

Para iniciar el proceso de verificación de dominio con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Seleccione el servicio de punto de conexión.
4. Elija Actions (Acciones), Verify domain ownership for private DNS name (Verificar la propiedad del dominio para el nombre de DNS privado).
5. Cuando se le solicite confirmar, ingrese **`verify`** y, a continuación, elija Verify (Comprobar).

Para iniciar el proceso de verificación de dominio con la línea de comandos

- start-vpc-endpoint-service-private-dns-verification (AWS CLI)
- Start-EC2VpcEndpointServicePrivateDnsVerification(Herramientas para Windows PowerShell)

Modificar las regiones admitidas

Puede modificar el conjunto de regiones compatibles para su servicio de punto de conexión. Se debe activar una región registrada antes de agregarla. No se puede eliminar la región que aloja su servicio de punto de conexión.

Tras eliminar una región, los consumidores del servicio no pueden crear nuevos puntos de conexión que la especifiquen como región de servicio. La eliminación de una región no afecta a los puntos de conexión existentes que la especifican como región de servicio. Al eliminar una región, se recomienda que rechace las conexiones de punto de conexión existentes en esa región.

Para modificar las regiones compatibles con su servicio de punto de conexión

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Seleccione el servicio de punto de conexión.
4. Elija Acciones y, a continuación Modificar las regiones compatibles.
5. Seleccione y cancele la selección de las regiones según sea necesario.
6. Seleccione Save changes (Guardar cambios).

Modificación de los tipos de direcciones IP compatibles

Puede cambiar los tipos de direcciones IP que son compatibles con su servicio de punto de conexión.

Consideración

Para permitir que su servicio de punto final acepte IPv6 solicitudes, sus balanceadores de carga de red deben usar el tipo de dirección IP de doble pila. No es necesario que los destinos admitan tráfico. IPv6 Para obtener más información, consulte Tipo de dirección IP en la Guía del usuario de equilibradores de carga de red.

Para modificar los tipos de direcciones IP compatibles con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Seleccione el servicio de punto de conexión de VPC.

4. Elija Actions (Acciones), Modify supported IP address types (Modificar los tipos de direcciones IP admitidos).
5. En Supported IP address types (Tipos de direcciones IP compatibles), haga una de las siguientes acciones:
   - Seleccione IPv4: habilite el servicio de punto final para que acepte IPv4 solicitudes.
   - Seleccione IPv6: habilite el servicio de punto final para que acepte IPv6 solicitudes.
   - Seleccione IPv4y IPv6: habilite el servicio de punto final para que acepte tanto IPv6 las solicitudes como IPv4 las demás.
6. Seleccione Save changes (Guardar cambios).

Para modificar los tipos de direcciones IP compatibles con la línea de comandos

- modify-vpc-endpoint-service-configuración ()AWS CLI
- Edit-EC2VpcEndpointServiceConfiguration(Herramientas para Windows PowerShell)

Administración de etiquetas

Puede etiquetar sus recursos para ayudarle a identificarlos o clasificarlos según las necesidades de su organización.

Para administrar las etiquetas de su servicio de punto de conexión utilizando la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Seleccione el servicio de punto de conexión de VPC.
4. Elija Actions (Acciones) y, a continuación, Manage tags (Administrar etiquetas).
5. Para cada etiqueta que desee agregar, elija Add new tag (Agregar etiqueta nueva) e ingrese la clave y el valor de la etiqueta.
6. Para eliminar una etiqueta, elija Remove (Eliminar) a la derecha de la clave y el valor de la etiqueta.
7. Seleccione Save (Guardar).

Para administrar las etiquetas de las conexiones de sus puntos de conexión mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Seleccione el servicio de punto de conexión de VPC y luego elija la pestaña Endpoint connections (Conexiones de punto de conexión).
4. Seleccione la conexión del punto de conexión, y luego elija Actions (Acciones), Manage tags (Administrar etiquetas).
5. Para cada etiqueta que desee agregar, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
6. Para eliminar una etiqueta, elija Remove (Eliminar) a la derecha de la clave y el valor de la etiqueta.
7. Seleccione Save (Guardar).

Para agregar permisos para el servicio de punto de conexión con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Seleccione el servicio de punto de conexión de VPC y, a continuación, elija la pestaña Allow principals (Permitir entidades principales).
4. Seleccione la entidad principal que desea etiquetar y, a continuación, elija Actions (Acciones), Manage tags (Administrar etiquetas).
5. Para cada etiqueta que desee agregar, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
6. Para eliminar una etiqueta, elija Remove (Eliminar) a la derecha de la clave y el valor de la etiqueta.
7. Seleccione Save (Guardar).

Para agregar y eliminar etiquetas con la línea de comandos

- create-tags y delete-tags (AWS CLI)
- New-EC2Tagy Remove-EC2Tag(Herramientas para Windows PowerShell)

Administración de nombres de DNS para servicios de punto de conexión de VPC

Los proveedores de servicios pueden configurar nombres de DNS privados para sus servicios de punto de conexión. Supongamos que un proveedor de servicios hace que su servicio esté disponible a través de un punto de conexión público y como un servicio de punto de conexión. Si el proveedor de servicios utiliza el nombre de DNS del punto de conexión público como nombre de DNS privado del servicio de punto de conexión, los consumidores del servicio pueden acceder al punto de conexión público o al servicio de punto de conexión mediante la misma aplicación del cliente, sin modificaciones. Si una solicitud proviene de la VPC del consumidor del servicio, los servidores DNS privados resuelven el nombre de DNS en las direcciones IP de las interfaces de red de los puntos de conexión. De lo contrario, los servidores DNS públicos resuelven el nombre de DNS en el punto de conexión público.

Antes de configurar un nombre de DNS privado para su servicio de punto de conexión, debe demostrar que es el propietario del dominio mediante una verificación de propiedad de dominio.

Consideraciones

- Un servicio de punto de conexión solo puede tener un nombre de DNS privado.
- Cuando el consumidor crea un punto de conexión de interfaz para conectarse al servicio, se crea una zona alojada privada que se asocia a la VPC del consumidor del servicio. Creamos un registro CNAME en la zona alojada privada que asigna el nombre de DNS privado del servicio de punto de conexión al nombre de DNS regional del punto de conexión de VPC. Cuando un consumidor del servicio envía una solicitud al nombre de DNS público del servicio, los servidores DNS privados resuelven el nombre de DNS en las direcciones IP de las interfaces de red de los puntos de conexión.
- Para verificar un dominio, debe tener un nombre de host público o un proveedor de DNS público.
- Puede verificar el dominio de un subdominio. Por ejemplo, puede verificar example.com, en lugar de a.example.com. Cada etiqueta DNS puede tener hasta 63 caracteres y el nombre de dominio completo no debe superar una longitud total de 255 caracteres.

  Si agrega un subdominio adicional, debe verificar el subdominio o el dominio. Por ejemplo, supongamos que tenía a.example.com, y verifica example.com. Ahora agrega b.example.com como nombre de DNS privado. Debe verificar example.com o b.example.com antes de que los consumidores del servicio puedan utilizar el nombre.

- Los nombres de DNS privados no son compatibles con los puntos de conexión del equilibrador de carga de puerta de enlace.

Verificación de la propiedad de dominio

Su dominio está asociado a un conjunto de registros de servicio de nombres de dominio (DNS) que se administra a través del proveedor de DNS. Un registro TXT es un tipo de registro de DNS que proporciona información adicional acerca de su dominio. Consta de un nombre y un valor. Como parte del proceso de verificación, debe agregar un registro TXT al servidor DNS para el dominio público.

La verificación de propiedad de dominio se completa cuando se detecta la existencia del registro TXT en la configuración de DNS del dominio.

Después de agregar un registro, puede comprobar el estado del proceso de verificación de dominio con la consola de Amazon VPC. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión). Seleccione el servicio de punto de conexión y compruebe el valor de Domain verification status (Estado de verificación del dominio) en la pestaña Details (Detalles). Si la verificación del dominio está pendiente, espere unos minutos y actualice la pantalla. Si es necesario, puede iniciar el proceso de verificación de forma manual. Elija Actions (Acciones), Verify domain ownership for private DNS name (Verificar la propiedad de dominio para el nombre de DNS privado).

El nombre de DNS privado está listo para que lo utilicen los consumidores del servicio cuando el estado de verificación es verified (verificado). Si el estado de verificación cambia, se rechazan las solicitudes de conexión nuevas, pero las conexiones existentes no se ven afectadas.

Si el estado de verificación es failed (error), consulte the section called “Solución de problemas de la verificación de dominio”.

Obtención del nombre y el valor

Le proporcionamos el nombre y el valor que utiliza en el registro TXT. Por ejemplo, la información está disponible en la Consola de administración de AWS. Seleccione el servicio de punto de conexión y consulte Domain verification name (Nombre de verificación de dominio) y Domain verification value (Valor de verificación de dominio) en la pestaña Details (Detalles) del servicio de punto de conexión. También puede usar el siguiente AWS CLI comando describe-vpc-endpoint-service-configuration para recuperar información sobre la configuración del nombre DNS privado del servicio de punto final especificado.

```
aws ec2 describe-vpc-endpoint-service-configurations \
    --service-ids vpce-svc-071afff70666e61e0 \
    --query ServiceConfigurations[*].PrivateDnsNameConfiguration
```

A continuación, se muestra un ejemplo del resultado. Cuando cree el registro TXT, utilizará `Value` y `Name`.

```
[
    {
        "State": "pendingVerification",
        "Type": "TXT",
        "Value": "vpce:l6p0ERxlTt45jevFwOCp",
        "Name": "_6e86v84tqgqubxbwii1m"
    }
]
```

Por ejemplo, supongamos que el nombre de dominio es example.com y que `Value` y `Name` son como muestra el ejemplo de resultado anterior. La siguiente tabla es un ejemplo de la configuración del registro TXT.

Name	Tipo	Valor
_6e86v84tqgqubxbwi i1m.example.com	TXT	vpce:l6p0 tt45jevfw ERxl OCp

Le sugerimos que utilice `Name` como subdominio del registro, ya que es posible que el nombre de dominio base ya esté en uso. Sin embargo, si su proveedor de DNS no permite que los nombres de los registros DNS contengan guiones bajos, puede omitir “_6e86v84tqgqubxbwii1m” y simplemente utilizar “example.com” en el registro TXT.

Después de verificar “_6e86v84tqgqubxbwii1m.example.com”, los consumidores del servicio pueden utilizar “example.com” o un subdominio (por ejemplo, “service.example.com” o “my.service.example.com”).

Agregue un registro TXT al servidor DNS de su dominio

El procedimiento para añadir registros TXT al servidor DNS de su dominio depende de quien proporcione su servicio DNS. Es posible que el proveedor de DNS sea Amazon Route 53 u otro registrador de nombres de dominio.

Amazon Route 53

Cree un registro para la zona alojada pública mediante una política de enrutamiento sencilla. Use los siguientes valores:

- En Record name (Nombre del registro), ingrese el dominio o el subdominio.
- En Record type (Tipo de registro), elija TXT.
- En Value/Route traffic to (Valor/ruta de destino del tráfico), ingrese el valor de verificación de dominio.
- En TTL (seconds) (TTL [segundos]), ingrese **`1800`**.

Para obtener más información, consulte Creación de registros con la consola en la Guía para desarrolladores de Amazon Route 53.

Procedimiento general

Diríjase al sitio web del proveedor de DNS e inicie sesión en su cuenta. Busque la página para actualizar los registros DNS para su dominio. Agregue un registro TXT con el nombre y el valor que le proporcionamos. Las actualizaciones del registro DNS pueden tardar hasta 48 horas en surtir efecto; sin embargo, muchas veces suelen hacerlo mucho antes.

Para obtener instrucciones más específicas, consulte la documentación de su proveedor de DNS. La próxima tabla proporciona enlaces a la documentación de varios proveedores de DNS habituales. Esta lista no tiene como fin ser exhaustiva ni ser una recomendación de los productos o los servicios que ofrecen estas empresas.

Proveedor de DNS/alojamiento	Enlace a la documentación
GoDaddy	Agregar un registro TXT
Dreamhost	Agregar registros DNS personalizados

Proveedor de DNS/alojamiento	Enlace a la documentación
Cloudflare	Administrar registros DNS
HostGator	Administre los registros DNS con /eNOM HostGator
Namecheap	¿Cómo agrego TXT/SPF/DKIM/DMARC registros para mi dominio?
Names.co.uk	Cambiar la configuración de DNS del dominio
Wix	Agregar o actualizar los registros TXT en la cuenta de Wix

Verificación de la publicación del registro TXT

Puede verificar que el registro TXT de verificación de propiedad de dominio de nombre de DNS privado se publica correctamente en el servidor DNS mediante los siguientes pasos. Ejecutará el comando nslookup, que está disponible para Windows y Linux.

Consultarás los servidores DNS que sirven a tu dominio porque esos servidores contienen la mayor cantidad de up-to-date información de tu dominio. La información de su dominio tarda en propagarse a otros servidores DNS.

Para verificar que su registro TXT se publica en su servidor DNS

1. Busque los servidores de nombres para su dominio con el siguiente comando.

   ```
   nslookup -type=NS example.com
   ```

   La salida enumera los servidores de nombres que sirven a su dominio. Consultará a uno de estos servidores en el siguiente paso.
2. Comprueba que el registro TXT se ha publicado correctamente con el siguiente comando, donde *name_server* aparece uno de los servidores de nombres que encontraste en el paso anterior.

   ```
   nslookup -type=TXT  _6e86v84tqgqubxbwii1m.example.com name_server
   ```
3. En la salida del paso anterior, verifique que la cadena que sigue a `text =` coincida con el valor TXT.

En nuestro ejemplo, si el registro se publica correctamente, la salida incluye lo siguiente.

```
_6e86v84tqgqubxbwii1m.example.com text = "vpce:l6p0ERxlTt45jevFwOCp"
```

Solución de problemas de la verificación de dominio

Si el proceso de verificación de dominio falla, la siguiente información puede ayudarlo a solucionar los problemas.

- Verifique si su proveedor de DNS permite guiones bajos en los nombres de los registros TXT. Si su proveedor de DNS no permite guiones bajos, puede omitir el nombre de verificación de dominio (por ejemplo, “_6e86v84tqgqubxbwii1m”) del registro TXT.
- Verifique si su proveedor de DNS agregó el nombre de dominio al final del registro TXT. Algunos proveedores de DNS anexan automáticamente el nombre de su dominio al nombre de atributo del registro TXT. Para evitar la duplicación del nombre de dominio, agregue un punto al final del nombre de dominio cuando cree el registro TXT. Esto indica al proveedor de DNS que no es necesario agregar el nombre de dominio al registro TXT.
- Verifique si su proveedor de DNS modificó el valor del registro DNS para utilizar solo letras minúsculas. Verificamos el dominio solo cuando hay un registro de verificación con un valor de atributo que coincide exactamente con el valor que proporcionamos. Si el proveedor de DNS cambió los valores del registro TXT para utilizar solo letras minúsculas, póngase en contacto con el proveedor para obtener ayuda.
- Es posible que deba verificar su dominio más de una vez, ya que admite varias regiones o varias Cuentas de AWS. Si su proveedor de DNS no permite tener más de un registro TXT con el mismo nombre de atributo, verifique si su proveedor de DNS permite asignar varios valores de atributo al mismo registro TXT. Por ejemplo, si Amazon Route 53 administra su DNS, puede utilizar el siguiente procedimiento.
  1. En la consola de Route 53, elija el registro TXT que creó cuando verificó el dominio en la primera región.
  2. En Value (Valor), diríjase al final del valor de atributo existente y pulse Intro.
  3. Agregue el valor de atributo para la región adicional y, a continuación, guarde el conjunto de registros.

Si su proveedor de DNS no permite asignar varios valores al mismo registro TXT, puede verificar el dominio una vez con el valor en el nombre de atributo del registro TXT y otra vez sin el valor en el nombre de atributo. Sin embargo, solo puede verificar el mismo dominio dos veces.

Reciba alertas de los eventos del servicio de punto de conexión

Puede crear una notificación para recibir alertas de eventos específicos relacionados con el servicio de punto de conexión. Por ejemplo, puede recibir un correo electrónico cuando se acepte o se rechace una solicitud de conexión.

Tareas

- Crear una notificación de SNS
- Agregar una política de acceso
- Agregar una política de claves

Crear una notificación de SNS

Siga este proceso para crear un tema de Amazon SNS para las notificaciones y suscribirse al tema.

Para crear una notificación para un servicio de punto de conexión con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Seleccione el servicio de punto de conexión.
4. En la pestaña Notifications (Notificaciones), elija Create notification (Crear notificación).
5. En Notificación de ARN, elija el ARN del tema de SNS que creó.
6. Para suscribirse a un evento, selecciónelo en Eventos.
   - Conectar: el consumidor del servicio creó el punto de conexión de interfaz. Esto envía una solicitud de conexión al proveedor del servicio.
   - Aceptar: el proveedor del servicio aceptó la solicitud de conexión.
   - Rechazar: el proveedor del servicio rechazó la solicitud de conexión.
   - Eliminar: el consumidor del servicio eliminó el punto de conexión de interfaz.
7. Elija Create Notification (Crear notificación).

Para crear una notificación para un servicio de punto de conexión con la línea de comandos

- create-vpc-endpoint-connection-notificación ()AWS CLI
- New-EC2VpcEndpointConnectionNotification(Herramientas para Windows PowerShell)

Agregar una política de acceso

Agregue una política de acceso al tema de SNS que AWS PrivateLink permita publicar notificaciones en su nombre, como las siguientes. Para obtener más información, consulte ¿Cómo edito la política de acceso de mi tema de Amazon SNS? Utilice las claves de condición global `aws:SourceArn` y `aws:SourceAccount` para protegerse contra el problema de suplente confuso.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
            },
            "Action": "SNS:Publish",
            "Resource": "arn:aws:sns:us-east-1:111111111111:topic-name",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint-service/service-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
        }
    ]
}
```

Agregar una política de claves

Si utilizas temas de SNS cifrados, la política de recursos de la clave de KMS debe ser confiable para llamar AWS PrivateLink a las operaciones de la AWS KMS API. A continuación, se muestra una política de claves de ejemplo.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "vpce.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey*",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-east-1:111111111111:key/key-id",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:ec2:us-east-1:111111111111:vpc-
endpoint-service/service-id"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                }
            }
        }
    ]
}
```

Eliminación de un servicio de punto de conexión

Cuando ya no necesite un servicio de punto de conexión, puede eliminarlo. No se podrá eliminar un servicio de punto de conexión si hay algún punto de conexión en estado `available` o `pending-acceptance` conectado al servicio de punto de conexión.

La eliminación de un servicio de punto de conexión no elimina el equilibrador de carga asociado y no afecta a los servidores de aplicaciones registrados en los grupos de destino del equilibrador de carga.

Para eliminar un servicio de punto de conexión con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Seleccione el servicio de punto de conexión.
4. Elija Actions (Acciones), Delete endpoint services (Eliminar servicios de punto de enlace).
5. Cuando le pidan confirmación, escriba **`delete`** y elija Eliminar.

Para eliminar un servicio de punto de conexión con la línea de comandos

- delete-vpc-endpoint-service-configuraciones ()AWS CLI
- Remove-EC2EndpointServiceConfiguration(Herramientas para Windows PowerShell)

Acceda a los recursos de VPC a través de AWS PrivateLink

Puede acceder de forma privada a un recurso de VPC en otra VPC mediante un punto de conexión de VPC de recursos (punto de conexión de recursos). Un punto de enlace de recursos le permite acceder de forma privada y segura a los recursos de la VPC, como una base de datos, una EC2 instancia de Amazon, un punto de enlace de una aplicación, un destino de nombre de dominio o una dirección IP que puede estar en una subred privada de otra VPC o en un entorno local. Sin puntos de enlace de recursos, debe agregar una puerta de enlace de Internet a su VPC o acceder al recurso mediante AWS PrivateLink un punto de enlace de interfaz y un Network Load Balancer. Los puntos de conexión de recursos no requieren un equilibrador de carga y permiten el acceso directo al recurso de VPC. Un recurso de VPC se representa mediante una configuración de recursos. Una configuración de recursos está asociada a una puerta de enlace de recursos.

Precios

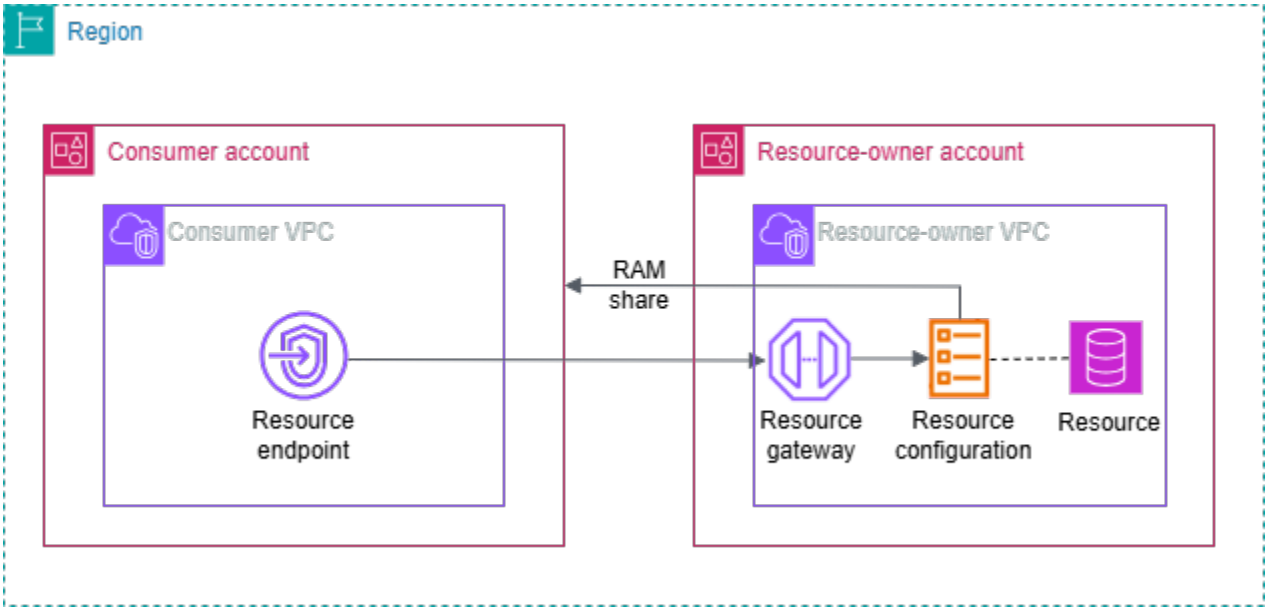
Cuando accede a los recursos mediante puntos de conexión de recursos, se le facturará por cada hora de aprovisionamiento de punto de conexión de VPC de recursos. También se le factura por GB de datos procesados cuando se accede a los recursos. Para obtener más información, consulte Precios de AWS PrivateLink. Cuando se habilita el acceso a sus recursos mediante configuraciones de recursos y puertas de enlace de recursos, se le facturará por GB de datos procesados por sus puertas de enlace de recursos. Para obtener más información, consulte Precios de Amazon VPC Lattice.

Contenido

Descripción general

Puede acceder a los recursos de su cuenta o a los que le hayan compartido desde otra cuenta. Para acceder a un recurso, debe crear un punto de conexión de VPC de interfaz, que establece conexiones entre las subredes en la VPC y el recurso mediante interfaces de red. El tráfico destinado para el recurso se resuelve en las direcciones IP privadas de las interfaces de red del punto de conexión del recurso mediante DNS. A continuación, el tráfico se envía al recurso mediante la conexión entre el punto de conexión de VPC y el recurso a través de la puerta de enlace de recursos.

La siguiente imagen muestra un punto final de recurso en una cuenta de consumidor que accede a un recurso que es propiedad de otra cuenta y a través del cual se comparte: AWS RAM



Consideraciones

- Se admite el tráfico TCP. No admite tráfico UDP.
- Las conexiones de red deben iniciarse desde la VPC que contiene el punto de conexión del recurso y no desde la VPC que tiene el recurso. La VPC del recurso no puede iniciar conexiones de red en la VPC del punto de conexión.
- Los únicos recursos basados en ARN compatibles son los recursos de Amazon RDS.
- Deben superponerse al menos una zona de disponibilidad del punto de conexión de VPC y la puerta de enlace de recursos

Nombre de host DNS

Con AWS PrivateLink, se envía tráfico a los recursos mediante puntos de enlace privados. Cuando se crea un punto de conexión de VPC de recursos, se crean nombres de DNS regionales (denominados nombre de DNS predeterminado) que se pueden utilizar para comunicarse con el recurso y el servicio desde la VPC y en las instalaciones. Te recomendamos que utilices DNS en lugar de un punto final IPs para conectarte a tus recursos. El nombre de DNS predeterminado para el punto de conexión de VPC de recurso tiene la siguiente sintaxis:

```
endpoint_id.rcfgId.randomHash.vpc-lattice-rsc.region.on.aws
```

Al crear un punto final de VPC de recursos para determinadas configuraciones de recursos que se utilizan ARNs, puede habilitar el DNS privado. Con el DNS privado, puedes seguir realizando solicitudes al recurso con el nombre de DNS proporcionado para el recurso por el AWS servicio y, al mismo tiempo, aprovechar la conectividad privada a través del punto final de la VPC del recurso. Para obtener más información, consulte the section called “Resolución de los DNS”.

El siguiente describe-vpc-endpoint-associationscomando muestra las entradas de DNS de un punto final de recurso.

```
aws ec2 describe-vpc-endpoint-associations --vpc-endpoint-id vpce-123456789abcdefgh --
query 'VpcEndpointAssociations[*].*'
```

A continuación, se muestra un resultado de ejemplo para un punto de conexión de recursos para la base de datos de Amazon RDS con nombres de DNS privados habilitados. El primer nombre de DNS es el nombre de DNS predeterminado. El segundo nombre de DNS proviene de la zona alojada privada y oculta, que resuelve las solicitudes al punto de conexión público para las direcciones IP privadas de las interfaces de red del punto de conexión.

```
[
    [
        "vpce-rsc-asc-abcd1234abcd",
        "vpce-123456789abcdefgh",
        "Accessible",
        {
            "DnsName": "vpce-1234567890abcdefg-
snra-1234567890abcdefg.rcfg-abcdefgh123456789.4232ccc.vpc-lattice-rsc.us-
east-1.on.aws",
            "HostedZoneId": "ABCDEFGH123456789000"
```

```
        },
        {
            "DnsName": "database-5-test.cluster-ro-example.us-
east-1.rds.amazonaws.com",
            "HostedZoneId": "A1B2CD3E4F5G6H8I91234"
        },
        "arn:aws:vpc-lattice:us-east-1:111122223333:resourceconfiguration/
rcfg-1234567890abcdefg",
        "arn:aws:vpc-lattice:us-east-1:111122223333:resourceconfiguration/
rcfg-1234567890xyz"
    ]
]
```

Resolución de los DNS

Los registros DNS que se crean para el punto de conexión de VPC de recursos son públicos. Por lo tanto, estos nombres de DNS se pueden resolver de forma pública. Sin embargo, las solicitudes de DNS desde fuera de la VPC siguen devolviendo las direcciones IP privadas de las interfaces de red del punto de conexión del recurso. Se pueden usar estos nombres de DNS para acceder al recurso en las instalaciones, siempre que se tenga acceso a la VPC en la que se encuentra el punto de conexión de recursos, a través de VPN o Direct Connect.

DNS privado

Si habilita el DNS privado para el punto final de la VPC de recursos para determinadas configuraciones de recursos que utiliza ARNs, y su VPC tiene habilitados tanto los nombres de host DNS como la resolución de DNS, creamos zonas AWS alojadas privadas ocultas y administradas para las configuraciones de recursos con un nombre de DNS personalizado. La zona alojada contiene un registro configurado para el nombre de DNS predeterminado para el recurso que lo resuelve en las direcciones IP privadas de las interfaces de red de punto de conexión en la VPC.

Amazon proporciona un servidor DNS para la VPC, denominado Route 53 Resolver. Route 53 Resolver resuelve automáticamente los nombres de dominio y registros de VPC locales de zonas alojadas privadas. No obstante, no se puede utilizar Route 53 Resolver desde fuera de la VPC. Si desea acceder al punto de conexión de VPC desde la red en las instalaciones, puede utilizar el nombre de DNS personalizado o los puntos de conexión de Route 53 Resolver y reglas de Resolver. Para obtener más información, consulta Integrar con y. AWS Transit GatewayAWS PrivateLinkAmazon Route 53 Resolver

Subredes y zonas de disponibilidad

Puede configurar su punto de conexión de VPC con una subred por cada zona de disponibilidad. Creamos una interfaz de red de punto de conexión para el punto de conexión de VPC en la subred. Asignamos direcciones IP a cada interfaz de red de punto de conexión desde su subred, en función del tipo de dirección IP del punto de conexión de VPC. En un entorno de producción, para una alta disponibilidad y resiliencia, recomendamos configurar al menos dos zonas de disponibilidad para cada punto de conexión de VPC.

Tipos de direcciones IP

Los puntos finales de recursos pueden admitir IPv4 IPv6, o direcciones de doble pila. Los puntos finales compatibles IPv6 pueden responder a las consultas de DNS con registros AAA. El tipo de dirección IP de un punto de conexión de recursos debe ser compatible con las subredes del punto de conexión de interfaz, como se describe a continuación:

- IPv4— Asigne IPv4 direcciones a las interfaces de red de sus puntos finales. Esta opción solo se admite si todas las subredes seleccionadas tienen rangos de IPv4 direcciones.
- IPv6— Asigne IPv6 direcciones a las interfaces de red de sus puntos finales. Esta opción solo se admite si todas las subredes seleccionadas son IPv6 solo subredes.
- Dualstack: IPv4 asigne ambas IPv6 direcciones a las interfaces de red de sus puntos finales. Esta opción solo se admite si todas las subredes seleccionadas tienen ambos IPv4 rangos de direcciones. IPv6

Si un punto final de VPC de recursos es compatible IPv4, las interfaces de red del punto final tienen IPv4 direcciones. Si un punto final de VPC de recursos es compatible IPv6, las interfaces de red del punto final tienen IPv6 direcciones. No se puede acceder a la IPv6 dirección de la interfaz de red de un punto final desde Internet. Si describe una interfaz de red de punto final con una IPv6 dirección, observe que `denyAllIgwTraffic` está habilitada.

Acceder a un recurso a través de un punto de conexión de VPC de recursos

Puede acceder a un recurso de VPC, como un nombre de dominio, una dirección IP o una base de datos de Amazon RDS, mediante un punto de conexión de recursos. Un punto de conexión de

recursos proporciona acceso privado a un recurso. Al crear el punto de conexión de recursos, se especifica una configuración de recursos de tipo único, de grupo o de ARN. Los puntos de conexión de recursos se pueden asociar solo a una configuración de recursos. La configuración de recursos puede representar un único recurso o a un grupo de recursos.

Requisitos previos

Para crear un punto de conexión de recursos, debe cumplir los siguientes requisitos previos.

- Debe tener una configuración de recursos que haya creado u que haya creado y compartido con usted otra cuenta a través de AWS RAM.
- Si otra cuenta le comparte una configuración de recursos, debe revisar y aceptar el recurso compartido que contiene la configuración de recursos. Para obtener más información, consulte Accepting and rejecting invitations en la Guía del usuario de AWS RAM .

Creación de un punto de conexión de VPC

Utilice el siguiente procedimiento para crear un punto de conexión de recursos de VPC. Tras crear un punto de conexión de recursos, solo puede modificar sus grupos de seguridad o etiquetas.

Creación de un punto de conexión de recursos de VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Elija Crear punto de conexión.
4. Se puede especificar un nombre para facilitar la búsqueda y la administración del punto de conexión.
5. En Tipo de recurso, elija Recursos.
6. Para las configuraciones de recursos, seleccione la configuración de recursos.
7. En Configuración de redes, seleccione la VPC desde la que accederá a los recursos.
8. Si desea configurar la compatibilidad con DNS privado para las configuraciones de recursos, seleccione Configuración adicional y Habilite el nombre DNS. Para usar esta característica, asegúrese de que los atributos Habilitar nombres de host de DNS y Habilitar soporte para DNS estén habilitados para su VPC. Para obtener más información, consulte the section called “Nombres de dominio personalizados para los consumidores de recursos”.

9. En Subredes, seleccione una subred para crear las interfaces de red de punto de conexión.

   En un entorno de producción, para una alta disponibilidad y resiliencia, recomendamos configurar al menos dos zonas de disponibilidad para cada punto de conexión de VPC.

10. En Grupos de seguridad, seleccione un grupo de seguridad.

    Si no se especifica un grupo de seguridad, se asociará el grupo de seguridad predeterminado para la VPC.

11. Elija Crear punto de conexión.

Para crear un punto de conexión de recursos mediante la línea de comandos

- create-vpc-endpoint (AWS CLI)
- New-EC2VpcEndpoint(Herramientas para Windows PowerShell)

Administración de puntos de conexión de recursos

Tras crear un punto de conexión de recursos, puede modificar sus grupos de seguridad o etiquetas.

Tareas

- Eliminación de un punto de conexión
- Actualizar un punto de conexión

Eliminación de un punto de conexión

Cuando ya no necesite un punto de conexión de VPC, puede eliminarlo.

Para eliminar un punto de conexión con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Selección del punto de conexión.
4. Elija Acciones, Eliminar puntos de conexión de VPC.
5. Cuando se le solicite confirmación, ingrese **`delete`**.
6. Elija Eliminar.

Para eliminar un punto de conexión con la línea de comandos

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Herramientas para Windows PowerShell)

Actualizar un punto de conexión

Puede actualizar un punto de conexión de VPC.

Para actualizar un punto de conexión mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión.
4. Elija Acciones y la opción adecuada.
5. Siga los pasos de la consola para enviar la actualización.

Para actualizar un punto de conexión mediante la línea de comandos

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Herramientas para Windows PowerShell)

Configuración de recursos para recursos de VPC

Una configuración de recursos representa un recurso o un grupo de recursos a los que desea que estén accesibles a 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 el tráfico.

Contenido

- Nombres de dominio personalizados para los propietarios de la red de servicios
- Definición del recurso
- Protocolo
- Intervalos de puertos
- Acceso a recursos de
- Asociación con el tipo de red de servicio
- Tipos de redes de servicio
- Compartir configuraciones de recursos mediante AWS RAM
- Monitorización
- Creación de una configuración de recursos en VPC Lattice
- Administración de asociaciones para una configuración de recursos de VPC Lattice

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: una dirección IP o un nombre de dominio. Se puede compartir de forma independiente.
- Configuración de recursos de grupo: un conjunto de configuraciones de recursos secundarios. Se puede compartir de forma independiente.
- Configuración de recursos de grupo: un miembro de una configuración de recursos de grupos. Representa una dirección IP o un nombre de dominio. No se puede compartir de forma independiente y solo se puede compartir como parte de un grupo. Se puede añadir y eliminar de un grupo sin problemas. Cuando se agrega, quienes pueden acceder al grupo tienen acceso automático a este.
- Configuración de recursos del ARN: representa un tipo de recurso compatible aprovisionado por un servicio. AWS Por ejemplo, una base de datos Amazon RDS. AWS administra las configuraciones de recursos secundarios de manera automática.

Puerta de enlace 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 con 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 la puerta de enlace de recursos de esa VPC.

Nombres de dominio personalizados para los proveedores de recursos

Los proveedores de recursos pueden adjuntar un nombre de dominio personalizado a una configuración de recursos, por ejemplo`example.com`, qué recursos pueden usar los consumidores para acceder a la configuración de recursos. El nombre de dominio personalizado puede ser propiedad del proveedor de recursos y estar verificado por él, o puede ser un AWS dominio o un tercero. Los proveedores de recursos pueden usar las configuraciones de recursos para compartir clústeres de caché y clústeres de Kafka, aplicaciones basadas en TLS u otros AWS recursos.

Las siguientes consideraciones se aplican a los proveedores de configuraciones de recursos:

- Una configuración de recursos solo puede tener un dominio personalizado.
- El nombre de dominio personalizado de una configuración de recursos no se puede cambiar.
- El nombre de dominio personalizado está visible para todos los consumidores de configuraciones de recursos.
- Puedes verificar tu nombre de dominio personalizado mediante el proceso de verificación del nombre de dominio de VPC Lattice. Para obtener más información Para obtener más información, consulte. https://docs.aws.amazon.com/vpc-lattice/latest/ug/create-and-verify.html
- Para las configuraciones de recursos de tipo grupo e hijo, primero debe especificar un dominio de grupo en la configuración de recursos del grupo. Después, las configuraciones de recursos secundarios pueden tener dominios personalizados que sean subdominios del dominio del grupo. Si el grupo no tiene un dominio de grupo, puedes usar cualquier nombre de dominio personalizado para el elemento secundario, pero VPC Lattice no aprovisionará ninguna zona alojada para los nombres de dominio secundarios en la VPC del consumidor de recursos.

Nombres de dominio personalizados para los consumidores de recursos

Cuando los consumidores de recursos habilitan la conectividad a una configuración de recursos que tiene un nombre de dominio personalizado, pueden permitir que VPC Lattice administre una zona alojada privada de Route 53 en su VPC. Los consumidores de recursos tienen opciones detalladas para los dominios en los que desean permitir que VPC Lattice administre las zonas alojadas privadas.

Los consumidores de recursos pueden establecer el `private-dns-enabled` parámetro al habilitar la conectividad con las configuraciones de recursos a través de un punto final de recursos, un punto final de red de servicio o una asociación de VPC de red de servicio. Junto con el `private-dns-enabled` parámetro, los consumidores pueden usar las opciones de DNS para especificar los dominios en los que quieren que VPC Lattice administre las zonas alojadas privadas. Los consumidores pueden elegir entre las siguientes preferencias de DNS privado:

`ALL_DOMAINS`

VPC Lattice proporciona zonas alojadas privadas para todos los nombres de dominio personalizados.

`VERIFIED_DOMAINS_ONLY`

VPC Lattice aprovisiona una zona alojada privada solo si el proveedor ha verificado el nombre de dominio personalizado.

`VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS`

VPC Lattice aprovisiona zonas alojadas privadas para todos los nombres de dominio personalizados verificados y otros nombres de dominio que especifique el consumidor de recursos. El consumidor de recursos especifica los nombres de dominio en el `private DNS specified domains` parámetro.

`SPECIFIED_DOMAINS_ONLY`

VPC Lattice proporciona una zona alojada privada para los nombres de dominio especificados por el consumidor de recursos. El consumidor de recursos especifica los nombres de dominio en el `private DNS specified domains` parámetro.

Al habilitar el DNS privado, VPC Lattice crea una zona alojada privada en la VPC para el nombre de dominio personalizado asociado a la configuración de recursos. De forma predeterminada, la preferencia de DNS privado está establecida en. `VERIFIED_DOMAINS_ONLY` Esto significa que las zonas alojadas privadas se crean solo si el proveedor de recursos ha verificado el nombre de dominio personalizado. Si estableces tu preferencia de DNS privado en `ALL_DOMAINS` o`SPECIFIED_DOMAINS_ONLY`, a continuación, VPC Lattice crea zonas alojadas privadas independientemente del estado de verificación del nombre de dominio personalizado. Cuando se crea una zona alojada privada para un dominio determinado, todo el tráfico a ese dominio desde la VPC se enruta a través de VPC Lattice. Le recomendamos que utilice las `SPECIFIED_DOMAINS_ONLY` preferencias

`ALL_DOMAINSVERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS`, o solo cuando desee que el tráfico a estos nombres de dominio personalizados pase por VPC Lattice.

Recomendamos que los consumidores de recursos establezcan sus preferencias de DNS privado en. `VERIFIED_DOMAINS_ONLY` Esto permite a los consumidores reforzar su perímetro de seguridad al permitir que VPC Lattice solo aprovisione zonas alojadas privadas para dominios verificados en la cuenta del consumidor de recursos.

Para seleccionar dominios en los dominios especificados por el DNS privado, los consumidores de recursos pueden introducir un nombre de dominio completo, por ejemplo, `my.example.com` o utilizar un comodín como. `*.example.com`

Las siguientes consideraciones se aplican a los consumidores de configuraciones de recursos:

- El parámetro de DNS privado habilitado no se puede cambiar.
- El DNS privado debe estar habilitado en una asociación de recursos de red de servicio para que un alojamiento privado se cree en una VPC. Para una configuración de recursos, el estado habilitado para el DNS privado de la asociación de recursos de la red de servicio anula el estado habilitado para el DNS privado del punto final de la red de servicio o de la asociación de VPC de la red de servicio.

Nombres de dominio personalizados para los propietarios de la red de servicios

La propiedad habilitada para el DNS privado de la asociación de recursos de la red de servicio anula la propiedad habilitada para el DNS privado del punto final de la red de servicio y la asociación de VPC de la red de servicio.

Si el propietario de una red de servicios crea una asociación de recursos de red de servicios y no habilita el DNS privado, VPC Lattice no aprovisionará zonas alojadas privadas para esa configuración de recursos en ninguna zona a la VPCs que esté conectada la red de servicio, aunque el DNS privado esté habilitado en el punto final de la red de servicio o en las asociaciones de VPC de la red de servicio.

Para las configuraciones de recursos de tipo ARN, el indicador de DNS privado es verdadero e inmutable.

Definición del recurso

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

- 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 se puede crear una configuración de recursos para un clúster de acceso público.
- Por destino de nombre de dominio: 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. En la actualidad solo se admite el protocolo de TCP.

Intervalos de puertos

Al crear una configuración de recursos, se pueden 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 configuraciones de recursos directamente desde su VPC mediante un punto de conexión de VPC o a través de una red de servicio. 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 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 de conexión de recursos, consulte Acceder a los recursos de VPC en la guía del usuario de AWS PrivateLink.

- Acceso a una configuración de recursos a través de una red de servicios

  Se 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 red de servicios, consulte Administrar las asociaciones para una red de servicios de VPC Lattice.

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

Cuando el DNS privado está habilitado para la VPC, no se puede crear un punto de conexión de recursos y un punto de conexión de red de servicios 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, se puede especificar que la configuración de recursos no se pueda agregar a las redes de servicios que se puedan compartir entre cuentas. Si se especifica esto, la cuenta B no podrá agregar su configuración de recursos a las redes de servicios que se comparten o se pueden compartir con otra cuenta en el futuro.

Tipos de redes de servicio

Cuando compartes una configuración de recursos con otra cuenta, por ejemplo, la Cuenta B AWS RAM, la Cuenta B puede acceder al recurso de una de estas tres maneras:

- Uso de un punto de conexión de VPC de tipo recurso (punto de conexión de VPC de recurso).

- Uso de un punto de conexión de VPC de tipo red de servicios (punto de conexión de VPC de red de servicio).
- Uso de una asociación de VPC de red de servicio.

  Cuando utilizas 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 de conexión de VPC de la red de servicio y la asociación de VPC de la red de servicio, la configuración de recursos tendría que colocarse en 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, se puede impedir que su configuración de recursos se agregue a las redes de servicio que se pueden compartir entre cuentas. Si no se permite, la cuenta B no podrá agregar su 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. También se puede compartir la configuración con otra cuenta mediante 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, con 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 Recursos compartidos con usted en la Guía del usuario de AWS RAM .

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

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

Creación de una configuración de recursos en VPC Lattice

Cree una configuración de recursos.

Consola de administración de AWS

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 una configuración de recursos.
4. Introduzca un nombre que sea único en su AWS cuenta. No se puede cambiar este nombre después de crear la configuración de los 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 puerta de enlace de recursos que haya creado anteriormente o cree una ahora.
7. (Opcional) Para introducir un nombre de dominio personalizado, realiza una de las siguientes acciones:
   - Si tiene una configuración de recursos de tipo único, puede introducir un nombre de dominio personalizado. Los consumidores de recursos pueden usar este nombre de dominio para acceder a sus configuraciones de recursos.
   - Si tiene una configuración de recursos de tipo grupo y secundaria, primero debe especificar un dominio de grupo en la configuración de recursos de grupo. A continuación, las configuraciones de recursos secundarios pueden tener dominios personalizados que sean subdominios del dominio del grupo.
8. (Opcional) Introduzca el ID de verificación.

   Proporciona un identificador de verificación si quieres que se verifique tu nombre de dominio. Esto permite a los consumidores de recursos saber que eres el propietario del nombre de dominio.
9. Elija el identificador del recurso que desea que represente esta configuración de recursos.
10. Elija los intervalos de puertos a través de los cuales desea compartir el recurso.
11. En Configuración de asociación, especifique si esta configuración de recursos se puede asociar a redes de servicios que se puedan compartir.

12. En la configuración de recursos compartidos, elija los recursos compartidos que identifiquen a las entidades principales que pueden acceder a este recurso.
13. (Opcional) Para el monitoreo, habilite 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.
14. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
15. Seleccione Crear una configuración de recursos.

AWS CLI

El siguiente create-resource-configurationcomando crea una configuración de recursos única y la asocia al nombre de dominio personalizado`example.com`.

```
aws vpc-lattice create-resource-configuration \
    --name my-resource-config \
    --type SINGLE \
    --resource-gateway-identifier rgw-0bba03f3d56060135 \
    --resource-configuration-definition 'ipResource={ipAddress=10.0.14.85}' \
    --custom-domain-name example.com \
    --verification-id dv-aaaa0000000111111
```

El siguiente create-resource-configurationcomando crea una configuración de recursos de grupo y la asocia al nombre de dominio personalizado`example.com`.

```
aws vpc-lattice-custom-dns create-resource-configuration \
  --name my-custom-dns-resource-config-group \
  --type GROUP \
  --resource-gateway-identifier rgw-0bba03f3d56060135 \
  --domain-verification-identifier dv-aaaa0000000111111
```

El siguiente create-resource-configurationcomando crea una configuración de recursos secundarios y la asocia al nombre de dominio personalizado`child.example.com`.

```
aws vpc-lattice-custom-dns create-resource-configuration \
  --name my-custom-dns-resource-config-child \
  --type CHILD \
  --resource-configuration-definition 'dnsResource={domainName=my-alb-123456789.us-
west-2.elb.amazonaws.com,ipAddressType=IPV4}' \
```

```
--resource-configuration-group-identifier rcfg-07129f3acded87626 \
--custom-domain-name child.example.com
```

Administración de asociaciones para una configuración de recursos de VPC Lattice

Las cuentas de consumidor con las que se comparte una configuración de recursos y los clientes de su cuenta pueden acceder a la configuración de recursos de manera directa con un punto de conexión de VPC de recursos o a través de un punto de conexión de red de servicio. Como resultado, la configuración de recursos tendrá asociaciones de puntos de conexión y asociaciones de redes de servicios.

Gestione las asociaciones de recursos de la red de servicios

Cree o elimine una asociación de red de servicios.

> **Note**
>
> Si recibe un mensaje de acceso denegado al crear la asociación entre la red de servicio y la configuración de 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 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 Lattice PrivateLink y Lattice, selecciona Configuraciones de recursos.
3. Elija el nombre de la configuración del recurso 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. (Opcional) Para habilitar los nombres DNS privados para esta asociación de recursos de red de servicios, elija habilitar el nombre DNS privado. Para obtener más información, consulte the section called “Nombres de dominio personalizados para los propietarios de la red de servicios”.
9. Elija Save changes (Guardar cambios).
10. Para eliminar una asociación, seleccione la casilla de verificación de la asociación y, luego, 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 de recursos

Las cuentas de consumidores con acceso a su configuración de recursos o los clientes de su cuenta pueden acceder a la configuración de recursos mediante un punto final de VPC de recursos. Si la configuración de sus recursos tiene un nombre de dominio personalizado, puede usar Enable Private DNS para permitir que VPC Lattice aprovisione zonas alojadas privadas para su punto final de recursos o punto final de red de servicios. De este modo, los clientes pueden curvar directamente el nombre de dominio para acceder a la configuración de recursos. Para obtener más información, consulte the section called “Nombres de dominio personalizados para los consumidores de recursos”.

Consola de administración de AWS

1. Para crear una nueva asociación de terminales, vaya a PrivateLink Lattice en el panel de navegación izquierdo y elija Endpoints.
2. Elija Crear puntos de conexión.
3. Seleccione la configuración de recursos que desee conectar a la VPC.
4. Seleccione la VPC, las subredes y los grupos de seguridad.
5. (Opcional) Para activar el DNS privado y configurar las opciones de DNS, selecciona Habilitar el nombre DNS.
6. (Opcional) Para etiquetar su punto de conexión de VPC, elija Agregar etiqueta nueva e ingrese una clave y un valor de etiqueta.

7. Elija Crear punto de conexión.

AWS CLI

El siguiente create-vpc-endpointcomando crea un punto final de VPC que usa un DNS privado. Las preferencias de DNS privado están configuradas en `VERIFIED_AND_SELECTED` y los dominios seleccionados son `example.com` y`example.org`. VPC Lattice solo aprovisiona zonas alojadas privadas para cualquier dominio verificado o. `example.com` `example.org`

```
aws ec2 create-vpc-endpoint \
  --vpc-endpoint-type Resource \
  --vpc-id vpc-111122223333aabbc \
  --subnet-ids subnet-0011aabbcc2233445 \
  --resource-configuration-arn arn:aws:vpc-lattice:us-
west-2:111122223333:resourceconfiguration/rcfg-07129f3acded87625 \
  --private-dns-enabled \
  --private-dns-preferences VERIFIED_DOMAINS_AND_SPECIFIED_DOMAINS \
  --private-domains-set example.com, example.org
```

Para crear una asociación de puntos de conexión de VPC mediante 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.

Puertas de enlace de recursos en VPC Lattice

Una puerta de enlace de recursos es un punto de entrada de tráfico a la VPC donde reside un recurso. Se extiende en varias zonas de disponibilidad

Una VPC debe tener una puerta de enlace de recursos si se tiene la intención de hacer que los recursos de la VPC sean accesibles desde otras VPC o cuentas. Cada recurso que se comparte está asociado a una puerta de enlace de recursos. Cuando los clientes de otras VPC o cuentas acceden a un recurso de su VPC, el recurso ve el tráfico que proviene de manera local de la puerta de enlace de recursos de esa VPC. La IP de origen del tráfico es la dirección IP de la puerta de enlace de recursos. Se pueden asignar varias direcciones IP a una puerta de enlace de recursos para permitir

más conexiones de red con el recurso. Se pueden asociar varios recursos de una VPC con la misma puerta de enlace de recursos.

Una puerta de enlace de recursos no proporciona capacidades de equilibrio de carga.

Contenido

Consideraciones

Las siguientes consideraciones se aplican a las puertas de enlace de recursos:

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

Reglas de salida recomendadas para el tráfico que fluye desde una puerta de enlace de recursos hasta 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 oyente y los rangos de puertos aceptados por el recurso.

Destino	Protocolo	Intervalo de puertos	Comentario
Rango de CIDR para el recurso	TCP	3306	Permite el tráfico desde la puerta de enlace de recursos a las bases de datos.

Tipos de direcciones IP

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

- IPv4: se asignan direcciones IPv4 a las interfaces de red de la puerta de enlace. Esta opción solo se admite si todas las subredes seleccionadas tienen rangos de direcciones IPv4, y el recurso también tiene una dirección IPv4.
- IPv6: se asignan direcciones IPv6 a las interfaces de red de la puerta de enlace. Esta opción solo se admite si todas las subredes seleccionadas son subredes IPv6, y el recurso también tiene una dirección IPv6.
- Doble pila: se asignan direcciones IPv4 e IPv6 a las interfaces de red de la puerta de enlace. Esta opción solo se admite si todas las subredes seleccionadas tienen rangos de direcciones IPv4 e IPv6, y el recurso tiene una dirección IPv4 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 de conexión de VPC a través del cual se accede al recurso.

Direcciones IPv4 por ENI

Si la puerta de enlace de recursos tiene un tipo de dirección IP IPv4 o de doble pila, se puede configurar la cantidad de direcciones IPv4 asignadas a cada ENI de la puerta de enlace de recursos. Al crear una puerta de enlace de recursos, puede elegir entre 1 y 62 direcciones IPv4. Una vez que se haya establecido el número de direcciones IPv4, el valor no se puede cambiar.

Las direcciones IPv4 se utilizan para la traducción de direcciones de red y determinan el número máximo de conexiones IPv4 simultáneas a un recurso. De forma predeterminada, a todas las puertas

de enlace de recursos se les asignan 16 direcciones IPv4 por ENI. Esta es una cantidad adecuada de direcciones IP para establecer conexiones con sus recursos de backend.

Si la puerta de enlace de recursos usa el tipo de dirección IPv6, entonces recibe automáticamente un CIDR de /80 por ENI. Este valor no se puede cambiar.

Creación de una puerta de enlace de recursos en VPC Lattice

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

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 PrivateLink y Lattice, seleccione Puerta de enlace de recursos.
3. Seleccione Crear una puerta de enlace de recursos.
4. Introduzca un nombre que sea exclusivo dentro de su cuenta de AWS.
5. Elija el tipo de dirección IP para la puerta de enlace de recursos
6. En Tipo de dirección IP, elija el tipo de dirección IP para la puerta de enlace de recursos
   - Si se seleccionó IPv4 o Doble pila como el tipo de dirección IP, se puede introducir el número de direcciones IPv4 por ENI para su puerta de enlace de recursos.

     El valor predeterminado es de 16 direcciones IPv4 por ENI. Esta es una cantidad adecuada de direcciones IP para establecer conexiones con sus recursos de backend.
7. Elija la VPC en la que se encuentra el recurso.
8. Elija hasta cinco grupos de seguridad para controlar el tráfico entrante desde la VPC hacia la red de servicio.
9. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
10. Seleccione Crear una puerta de enlace de recursos.

Para crear una puerta de enlace de recursos con la AWS CLI

Utilice el comando create-resource-gateway.

Eliminación de una puerta de enlace de recursos en VPC Lattice

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

Para eliminar una puerta de enlace de recursos con 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, seleccione Puerta de enlace de recursos.
3. Seleccione la casilla de verificación de la puerta de enlace 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 la AWS CLI

Utilice el comando delete-resource-gateway.

Acceder a las redes de servicios a través de AWS PrivateLink

Puede conectarse de forma privada a una red de servicio desde su VPC mediante un punto de conexión de VPC de la red de servicio (punto de conexión de la red de servicio). Un punto de conexión de la red de servicios permite acceder de forma privada y segura a los recursos y servicios asociados a la red de servicios. De esta forma, se puede acceder de forma privada a varios recursos y servicios a través de un único punto de conexión de VPC.

Una red de servicios es una recopilación lógica de configuraciones de recursos y servicios de VPC Lattice. Con un punto de conexión de red de servicio, se puede conectar una red de servicio a su VPC y acceder a esos recursos y servicios de forma privada desde su VPC o en las instalaciones. El punto de conexión de red de servicios permite la conexión a una red de servicios. Para conectarse a varias redes de servicio desde su VPC, se pueden crear varios puntos de conexión de red de servicio, donde cada uno apunte a una red de servicio diferente.

Las redes de servicio están integradas con AWS Resource Access Manager (AWS RAM). Puede compartir su red de servicios con otra cuenta a través de AWS RAM. Cuando compartes una red de servicio con otra AWS cuenta, esa cuenta puede crear un punto final de la red de servicio para conectarse a la red de servicio. Puede compartir una red de servicios mediante un recurso compartido en AWS RAM.

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

Precios

La facturación de las configuraciones de recursos asociadas a su red de servicios se le facturarán por hora. También se le factura por GB de datos procesados cuando se accede a los recursos a través del punto de conexión de VPC de red de servicios. No se le facturará por hora el propio punto de conexión de VPC de la red de servicio. Para obtener más información, consulte Precios de Amazon VPC Lattice.

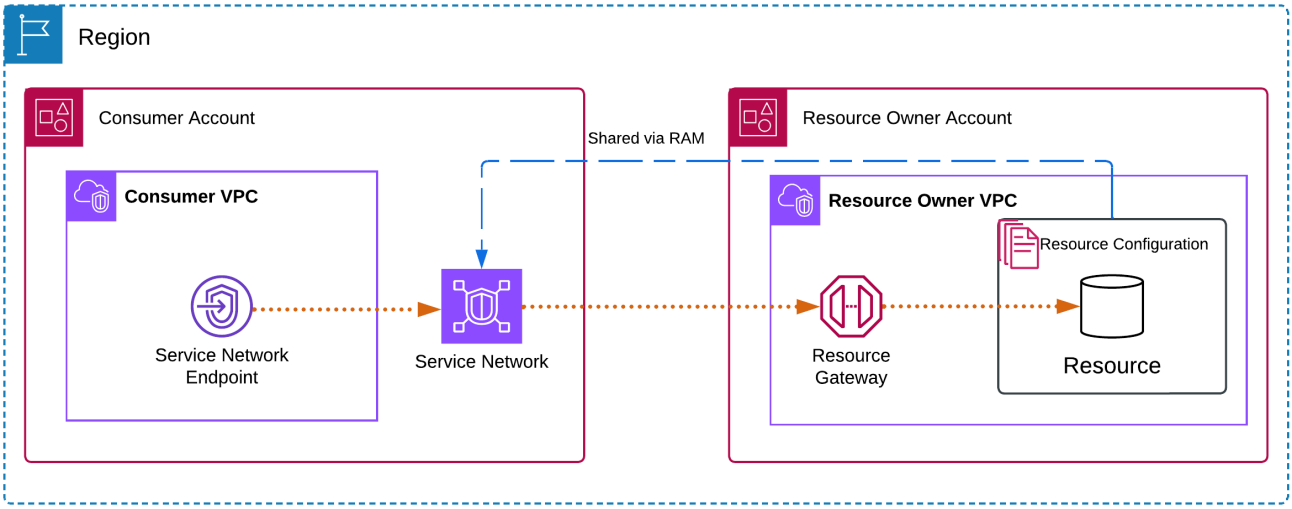
Contenido

- Nombre de host DNS
- Resolución de los DNS
- DNS privado
- Subredes y zonas de disponibilidad
- Tipos de direcciones IP
- Acceda a una red de servicios a través de un punto de conexión en la red de servicios
- Administrar los puntos de conexión de la red de servicios

Descripción general

Puede crear su propia red de servicios o le pueden compartir una red de servicios con usted desde otra cuenta. De cualquier forma, puede crear un punto de conexión de red de servicios para conectarse con él desde su VPC. Para obtener más información sobre cómo crear una red de servicios y asociarle configuraciones de recursos, consulte la Guía del usuario de Amazon VPC Lattice.

En el siguiente diagrama, se muestra cómo un punto de conexión de la red de servicios de su VPC accede a una red de servicios.



Las conexiones de red solo se pueden iniciar desde la VPC que tiene el punto de conexión de la red de servicio hacia los recursos y servicios de la red de servicio. La VPC con los recursos y los servicios no puede iniciar conexiones de red en la VPC del punto de conexión.

Nombre de host DNS

Con AWS PrivateLink, envía el tráfico a las redes de servicio mediante puntos finales privados. Cuando se crea un punto de conexión de VPC de red de servicios, se crean nombres de DNS regionales (denominados nombre de DNS predeterminado) para cada recurso y servicio que se pueden utilizar para comunicarse con el recurso y el servicio desde la VPC y en las instalaciones. Pueden cambiar las direcciones IP asociadas a un punto de conexión. Le recomendamos que utilice DNS en lugar de un punto final IPs para conectarse a sus redes de servicio.

El nombre de DNS predeterminado de un recurso de la red de servicios tiene la siguiente sintaxis:

```
endpointId-snraId.rcfgId.randomHash.vpc-lattice-rsc.region.on.aws
```

El nombre de DNS predeterminado de un servicio Lattice de la red de servicios tiene la siguiente sintaxis:

```
endpointId-snsaId.randomHash.vpc-lattice-svcs.region.on.aws
```

Si utilizas el Consola de administración de AWS, puedes encontrar el nombre DNS en la pestaña Asociaciones. Si estás usando el AWS CLI, usa el describe-vpc-endpoint-associationscomando.

Solo se puede habilitar el DNS privado cuando la red de servicios tiene una configuración de recursos de tipo ARN para un servicio de base de datos de Amazon RDS. Con el DNS privado, puede seguir realizando solicitudes al recurso mediante el nombre de DNS proporcionado para el recurso por el AWS servicio y, al mismo tiempo, aprovechar la conectividad privada a través del punto final de VPC de la red de servicio. Para obtener más información, consulte the section called “Resolución de los DNS”.

Resolución de los DNS

Al crear un punto de conexión de la red de servicios, creamos nombres de DNS para cada configuración de recursos y servicios de Lattice que esté asociado a la red de servicios. Estos registros de DNS son públicos. Por lo tanto, estos nombres de DNS se pueden resolver de forma pública. Sin embargo, las solicitudes de DNS desde fuera de la VPC siguen devolviendo las direcciones IP privadas de las interfaces de red del punto de conexión de la red de servicios. Se pueden usar estos nombres de DNS para acceder al recurso y los servicios en las instalaciones, siempre que se tenga acceso a la VPC en la que se encuentra el punto de conexión de la red del servicio, a través de VPN o Direct Connect.

DNS privado

Si habilita el DNS privado para el punto final de la VPC de la red de servicios y su VPC tiene habilitados tanto los nombres de host DNS como la resolución de DNS, creamos zonas AWS alojadas privadas ocultas y administradas para las configuraciones de recursos que tienen nombres de DNS personalizados. La zona alojada contiene un registro configurado para el nombre de DNS predeterminado para el recurso que lo resuelve en las direcciones IP privadas de las interfaces de red del punto de conexión de la red de servicios en la VPC.

Amazon proporciona un servidor DNS para la VPC, denominado Route 53 Resolver. Route 53 Resolver resuelve automáticamente los nombres de dominio y registros de VPC locales de zonas alojadas privadas. No obstante, no se puede utilizar Route 53 Resolver desde fuera de la VPC. Si desea acceder al punto de conexión de VPC desde la red en las instalaciones, puede utilizar los nombres de DNS predeterminados o utilizar los puntos de conexión de Route 53 Resolver y las reglas de Resolver. Para obtener más información, consulte Integración con y. AWS Transit GatewayAWS PrivateLinkAmazon Route 53 Resolver

Subredes y zonas de disponibilidad

Puede configurar su punto de conexión de VPC con una subred por cada zona de disponibilidad. Creamos una interfaz de red elástica para el punto de conexión de VPC en la subred. Asignamos direcciones IP a cada interfaz de red elástica desde su subred en múltiplos de /28, si el tipo de dirección IP del punto final de la VPC es. IPv4 La cantidad de direcciones IP asignadas en cada subred depende de la cantidad de configuraciones de recursos y agregamos bloques adicionales IPs en /28 según sea necesario. En un entorno de producción, para obtener una alta disponibilidad y resiliencia, recomendamos configurar al menos dos zonas de disponibilidad para cada punto final de VPC y tener IPs disponibles contiguas.

Tipos de direcciones IP

Los puntos finales de la red de servicios pueden admitir direcciones de doble pila o apilarlas. IPv4 IPv6 Los puntos finales compatibles IPv6 pueden responder a las consultas de DNS con registros AAAA. El tipo de dirección IP de un punto de conexión de red de servicios debe ser compatible con las subredes del punto de conexión de recursos, como se describe a continuación:

- IPv4— Asigne IPv4 direcciones a las interfaces de red de sus puntos finales. Esta opción solo se admite si todas las subredes seleccionadas tienen rangos de IPv4 direcciones.

- IPv6— Asigne IPv6 direcciones a las interfaces de red de sus puntos finales. Esta opción solo se admite si todas las subredes seleccionadas son IPv6 solo subredes.
- Dualstack: IPv4 asigne ambas IPv6 direcciones a las interfaces de red de sus puntos finales. Esta opción solo se admite si todas las subredes seleccionadas tienen ambos IPv4 rangos de direcciones. IPv6

Si un punto final de VPC de una red de servicio es compatible IPv4, las interfaces de red del punto final tienen direcciones. IPv4 Si un punto final de VPC de una red de servicio es compatible IPv6, las interfaces de red del punto final tienen direcciones. IPv6 No se IPv6 puede acceder a la dirección de una interfaz de red de puntos finales desde Internet. Si describe una interfaz de red de punto final con una IPv6 dirección, observe que `denyAllIgwTraffic` está habilitada.

Acceda a una red de servicios a través de un punto de conexión en la red de servicios

Puede acceder a una red de servicio mediante un punto de conexión de la red de servicio. Un punto de conexión de la red de servicios proporciona acceso privado a las configuraciones de recursos y los servicios de la red de servicios.

Requisitos previos

Para crear un punto de conexión de interfaz, debe cumplir los siguientes requisitos previos:

- Debe tener una red de servicios que haya sido creada por usted o que le hayan compartido desde otra cuenta a través de AWS RAM.
- Si le comparten una red de servicio desde otra cuenta, debe revisar y aceptar el recurso compartido que contiene la red de servicio. Para obtener más información, consulte Accepting and rejecting invitations en la Guía del usuario de AWS RAM .
- Un punto final de una red de servicios requiere inicialmente un bloque contiguo de IPv4 direcciones de /28 disponible en una zona de disponibilidad. Si agrega una configuración de recursos a la red de servicios asociada a su punto de conexión, necesitará un bloque /28 adicional disponible en la misma subred, ya que cada recurso consume una IP única por zona de disponibilidad.

  Si planea agregar más de 16 configuraciones de recursos a una red de servicio, se consumirán bloques /28 adicionales en el punto de conexión de la red de servicio para dar cabida a los nuevos recursos. Le recomendamos que, si necesita evitar el uso del CIDR de VPC IPs, utilice una

asociación de VPC de una red de servicio. Para obtener más información, consulte Administrar las asociaciones de punto de conexión de VPC en la Guía del usuario de Amazon VPC Lattice.

Creación de un punto de conexión de red de servicios

Cree un punto de conexión de la red de servicios para acceder a la red de servicio que se compartió con usted. Tras crear un punto de conexión de red de servicios, solo puede modificar sus grupos de seguridad o etiquetas.

Para crear un punto de conexión de red de servicios

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en PrivateLink y Lattice, elija Endpoints.
3. Elija Crear punto de conexión.
4. Se puede especificar un nombre para facilitar la búsqueda y la administración del punto de conexión.
5. En Tipo, elija Redes de servicios.
6. Para las Redes de servicios, seleccione la red de servicios.
7. En Configuración de redes, seleccione la VPC desde la que accederá a la red de servicios.
8. Si desea configurar la compatibilidad con el DNS privado, seleccione Configuración adicional y, a continuación, Habilitar el nombre de DNS privado. Para usar esta característica, asegúrese de que los atributos Habilitar nombres de host de DNS y Habilitar soporte para DNS estén habilitados para su VPC.
9. En Subredes, seleccione una subred para crear las interfaces de red de punto de conexión.

   En un entorno de producción, para una alta disponibilidad y resiliencia, recomendamos configurar al menos dos zonas de disponibilidad para cada punto de conexión de VPC.
10. En Grupos de seguridad, seleccione un grupo de seguridad.

    Si no se especifica un grupo de seguridad, se asociará el grupo de seguridad predeterminado para la VPC.
11. Elija Crear punto de conexión.

Para crear un punto de conexión de red de servicios con la línea de comandos

- create-vpc-endpoint (AWS CLI)

- New-EC2VpcEndpoint(Herramientas para Windows PowerShell)

Administrar los puntos de conexión de la red de servicios

Tras crear un punto de conexión de red de servicios, puede actualizar sus grupos de seguridad o etiquetas.

Tareas

- Eliminación de un punto de conexión
- Actualización de un punto de conexión de red de servicios

Eliminación de un punto de conexión

Cuando ya no necesite un punto de conexión de VPC, puede eliminarlo.

Para eliminar un punto de conexión con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de la red de servicios.
4. Elija Acciones, Eliminar puntos de conexión de VPC.
5. Cuando se le solicite confirmación, ingrese **`delete`**.
6. Elija Eliminar.

Para eliminar un punto de conexión con la línea de comandos

- delete-vpc-endpoints (AWS CLI)
- Remove-EC2VpcEndpoint(Herramientas para Windows PowerShell)

Actualización de un punto de conexión de red de servicios

Puede actualizar un punto de conexión de VPC.

Para actualizar un punto de conexión mediante la consola

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

2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión.
4. Elija Acciones y la opción adecuada.
5. Siga los pasos de la consola para enviar la actualización.

Para actualizar un punto de conexión mediante la línea de comandos

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Herramientas para Windows PowerShell)

Administración de identidad y acceso para AWS PrivateLink

AWS Identity and Access Management (IAM) es un sistema Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a los AWS recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar los recursos. AWS PrivateLink La IAM es una Servicio de AWS opción que puede utilizar sin coste adicional.

Contenido

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo en el que se realice. AWS PrivateLink

Usuario del servicio: si utiliza el AWS PrivateLink servicio para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que vaya utilizando más AWS PrivateLink funciones para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador.

Administrador de servicios: si estás a cargo de AWS PrivateLink los recursos de tu empresa, probablemente tengas acceso total a ellos AWS PrivateLink. Su trabajo consiste en determinar a qué AWS PrivateLink funciones y recursos deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a AWS PrivateLink.

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en su Cuenta de AWS en la Guía del usuario de AWS Sign-In .

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear un Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz que tiene acceso completo a todos Servicios de AWS los recursos. Recomendamos encarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, recomendamos AWS IAM Identity Center. Para obtener más información, consulte ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad con permisos específicos para una sola persona o aplicación. Recomendamos utilizar credenciales temporales en lugar de usuarios de IAM con credenciales a largo plazo. Para obtener más información, consulte Exigir a los usuarios humanos que utilicen la

federación con un proveedor de identidad para acceder AWS mediante credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica una colección de usuarios de IAM y facilita la administración de los permisos para grandes conjuntos de usuarios. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad con permisos específicos que proporciona credenciales temporales. Puede asumir un rol cambiando de un rol de usuario a uno de IAM (consola) o llamando a una AWS CLI operación de AWS API. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Las funciones de IAM son útiles para el acceso de usuarios federados, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon. EC2 Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración de acceso mediante políticas

AWS Para controlar el acceso, puede crear políticas y adjuntarlas a identidades o recursos. AWS Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las añade a los roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método utilizado para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar

las identidades, sobre 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.

Las políticas basadas en identidad pueden ser políticas insertadas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener más información sobre cómo elegir entre políticas administradas o políticas insertadas, consulte Selección entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de políticas JSON que se asocian a un recurso. Algunos ejemplos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Debe especificar una entidad principal en una política en función de recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en la identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCPs): establece los permisos máximos disponibles para los recursos de tus cuentas. Para obtener más información, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

¿Cómo AWS PrivateLink funciona con IAM

Antes de utilizar IAM para gestionar el acceso AWS PrivateLink, infórmese sobre las funciones de IAM disponibles para su uso. AWS PrivateLink

Característica de IAM	AWS PrivateLink soporte
Políticas basadas en identidades	Sí
Políticas basadas en recursos	Sí
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACLs	No
ABAC (etiquetas en políticas)	Sí
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	No
Roles vinculados al servicio	No

Para obtener una visión general de cómo Servicios de AWS funcionan la mayoría de las funciones de IAM AWS PrivateLink y otras funciones, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en la identidad para AWS PrivateLink

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. 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.

Ejemplos de políticas basadas en la identidad para AWS PrivateLink

Para ver ejemplos de políticas AWS PrivateLink basadas en la identidad, consulte. Ejemplos de políticas basadas en la identidad para AWS PrivateLink

Políticas basadas en recursos incluidas AWS PrivateLink

Compatibilidad con las políticas basadas en recursos: sí

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. 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. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

AWS PrivateLink el servicio admite un tipo de política basada en recursos, conocida como política de punto final. Una política de punto de conexión controla qué entidades principales de AWS pueden utilizar el punto de conexión para acceder al servicio de punto de conexión. Para obtener más información, consulte the section called “Políticas de punto de conexión”.

Acciones políticas para AWS PrivateLink

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Acciones en el espacio de nombres ec2

Algunas acciones AWS PrivateLink forman parte de la EC2 API de Amazon. Estas acciones políticas utilizan el prefijo `ec2`. Para obtener más información, consulta AWS PrivateLink las acciones en la referencia de la EC2 API de Amazon.

Acciones en el espacio de nombres vpce

AWS PrivateLink también proporciona la acción de `AllowMultiRegion` solo permisos. Esta acción de política usa el prefijo `vpce`.

Recursos de políticas para AWS PrivateLink

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Para las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Claves de condición de la política para AWS PrivateLink

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 puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. 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. 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.

Las siguientes claves de condición son específicas de: AWS PrivateLink

- `ec2:VpceMultiRegion`
- `ec2:VpceServiceName`
- `ec2:VpceServiceOwner`
- `ec2:VpceServicePrivateDnsName`
- `ec2:VpceServiceRegion`
- `ec2:VpceSupportedRegion`

Para obtener más información, consulta Claves de estado de Amazon EC2.

ACLs in AWS PrivateLink

Soportes 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.

ABAC con AWS PrivateLink

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 denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso.

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.

Utilizar credenciales temporales con AWS PrivateLink

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza la federación o se cambia de rol. 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 y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Permisos principales entre servicios para AWS PrivateLink

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos de la persona principal que llama Servicio de AWS, junto con la solicitud, Servicio de AWS para realizar solicitudes a los servicios descendentes. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Funciones de servicio para AWS PrivateLink

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.

Funciones vinculadas al servicio para AWS PrivateLink

Compatibilidad con roles vinculados al servicio: no

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.

Ejemplos de políticas basadas en la identidad para AWS PrivateLink

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de AWS PrivateLink . Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

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 AWS PrivateLink, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon EC2 en la Referencia de autorización de servicio.

Ejemplos

- Control del uso de puntos de enlace de la VPC
- Control de la creación de puntos de enlace de la VPC en función del propietario del servicio
- Controlar los nombres de DNS privados que pueden especificarse para los servicios de punto de enlace de la VPC
- Controlar los nombres de servicio que pueden especificarse para los servicios de punto de enlace de la VPC

Control del uso de puntos de enlace de la VPC

De forma predeterminada, los usuarios no tienen permiso para trabajar con puntos de conexión. Puede crear una política basada en identidad que conceda permisos a los usuarios para crear, modificar, describir y eliminar puntos de conexión. A continuación se muestra un ejemplo.

JSON

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Effect": "Allow",
            "Action":"ec2:*VpcEndpoint*",
            "Resource":"*"
        }
    ]
}
```

Para obtener información acerca del control de acceso a servicios utilizando puntos de enlace de la VPC, consulte the section called “Políticas de punto de conexión”.

Control de la creación de puntos de enlace de la VPC en función del propietario del servicio

Puede usar la clave de condición `ec2:VpceServiceOwner` para controlar qué punto de enlace de la VPC se puede crear en función de quién sea el propietario del servicio (`amazon`, `aws-marketplace` o el ID de cuenta). En el siguiente ejemplo se concede permiso para crear extremos de VPC con el propietario del servicio especificado. Para utilizar este ejemplo, cambie la región, el ID de cuenta y el propietario del servicio.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc/*",
                "arn:aws:ec2:us-east-1:111111111111:security-group/*",
                "arn:aws:ec2:us-east-1:111111111111:subnet/*",
                "arn:aws:ec2:us-east-1:111111111111:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceOwner": [
                        "amazon"
                    ]
                }
            }
        }
    ]
}
```

Controlar los nombres de DNS privados que pueden especificarse para los servicios de punto de enlace de la VPC

Puede utilizar la clave de condición `ec2:VpceServicePrivateDnsName` para controlar qué servicio de punto de enlace de la VPC se puede modificar o crear en función del nombre de DNS privado asociado a dicho servicio. En el siguiente ejemplo se concede permiso para crear un servicio de punto de enlace de la VPC con el nombre DNS privado especificado. Para utilizar este ejemplo, cambie la región, el ID de cuenta y el nombre de DNS privado.

JSON

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

```
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServiceConfiguration",
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint-service/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServicePrivateDnsName": [
                        "example.com"
                    ]
                }
            }
        }
    ]
}
```

Controlar los nombres de servicio que pueden especificarse para los servicios de punto de enlace de la VPC

Puede utilizar la clave de condición `ec2:VpceServiceName` para controlar qué punto de enlace de la VPC se puede crear en función del nombre del servicio de punto de enlace de la VPC. En el siguiente ejemplo se concede permiso para crear un punto de enlace de la VPC con el nombre del servicio especificado. Para utilizar este ejemplo, cambie la región, el ID de cuenta y el nombre del servicio.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc/*",
                "arn:aws:ec2:us-east-1:111111111111:security-group/*",
                "arn:aws:ec2:us-east-1:111111111111:subnet/*",
```

```
                "arn:aws:ec2:us-east-1:111111111111:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:us-east-1:111111111111:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.111111111111.s3"
                    ]
                }
            }
        }
    ]
}
```

Uso de políticas de punto de conexión para controlar el acceso a puntos de conexión de VPC

Una política de punto final es una política basada en recursos que se adjunta a un punto final de VPC para controlar qué entidades AWS principales pueden usar el punto final para acceder a un. Servicio de AWS

Una política de punto de conexión no anula ni reemplaza las políticas basadas en identidad o basadas en recursos. Por ejemplo, si utiliza un punto de enlace de interfaz para conectarse a Amazon S3, también puede utilizar las políticas de bucket de Amazon S3 para controlar el acceso a los buckets desde puntos de enlace específicos o específicos. VPCs

Contenido

Consideraciones

- Una política de punto de conexión es un documento de política JSON que utiliza el lenguaje de políticas de IAM. Debe contener un elemento Principal. El tamaño de una política de punto de conexión no puede superar los 20 480 caracteres, incluidos espacios en blanco.
- Al crear una interfaz o punto de enlace para un punto de enlace Servicio de AWS, puede adjuntar una política de punto final único al punto final. Puede actualizar la política de punto de conexión en cualquier momento. Si no asocia una política de punto de conexión, se adjunta la política de punto de conexión predeterminada.
- No todos Servicios de AWS admiten políticas de puntos finales. Si an Servicio de AWS no es compatible con las políticas de puntos finales, permitimos el acceso total al servicio a cualquier punto final. Para obtener más información, consulte the section called “Ver la compatibilidad con las políticas de puntos de conexión”.
- Cuando se crea un punto de conexión de VPC para un servicio de punto de conexión distinto de un Servicio de AWS, se permite acceso completo al punto de conexión.
- No se pueden usar caracteres comodín (* o ?) u operadores de condición numéricos con claves de contexto globales que hacen referencia a los identificadores generados por el sistema (por ejemplo, `aws:PrincipalAccount` o `aws:SourceVpc`).
- Al usar un operador de condición de cadena, debe usar al menos seis caracteres consecutivos antes o después de cada carácter comodín.
- Al especificar un ARN en un elemento de recurso o condición, la parte de cuenta del ARN puede incluir un identificador de cuenta o un carácter comodín, pero no ambos.
- Después de la actualización de una política de punto de conexión, los cambios pueden tardar unos minutos en aplicarse.

Política de punto de conexión predeterminada

La política de punto de conexión predeterminada concede acceso completo al punto de conexión.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*"
```

```
        }
    ]
}
```

Políticas para puntos de conexión de interfaz

Para ver, por ejemplo, las políticas de puntos finales para Servicios de AWS, consultethe section called “Servicios que se integran”. La primera columna de la tabla contiene enlaces a la AWS PrivateLink documentación de cada una de ellas Servicio de AWS. Si una empresa Servicio de AWS es compatible con las políticas de puntos finales, su documentación incluye ejemplos de políticas de puntos finales.

Entidades principales para puntos de conexión de puerta de enlace

En el caso de los puntos de conexión de la puerta de enlace, el elemento `Principal` debe estar establecido en `*`. Para especificar una entidad principal, utilice la clave de condición de `aws:PrincipalArn`.

```
"Condition": {
    "StringEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:user/endpointuser"
    }
}
```

Si especifica la entidad principal en uno el siguiente formato, se concede acceso solo a Usuario raíz de la cuenta de AWS y no a todos los usuarios y roles de la cuenta.

```
"AWS": "account_id"
```

Para ver ejemplos de políticas de punto de conexión para puntos de conexión de puerta de enlace, consulte lo siguiente:

- Puntos de conexión para Amazon S3
- Puntos de conexión para DynamoDB

Actualización de una política de punto de conexión de VPC

Utilice el siguiente procedimiento para actualizar una política de punto de conexión para un Servicio de AWS. Después de la actualización de una política de punto de conexión, los cambios pueden tardar unos minutos en aplicarse.

Para actualizar una política de punto de conexión mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión.
3. Seleccione el punto de conexión de VPC.
4. Elija Acciones, Administrar política.
5. Elija Acceso completo para permitir el acceso completo al servicio, o bien elija Personalizar y adjunte una política personalizada.
6. Seleccione Save.

Para actualizar una política de punto de conexión mediante la línea de comandos

- modify-vpc-endpoint (AWS CLI)
- Edit-EC2VpcEndpoint(Herramientas para Windows PowerShell)

AWS políticas gestionadas para AWS PrivateLink

Una política AWS administrada 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 PrivateLink actualizaciones de las políticas gestionadas AWS

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas AWS PrivateLink desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del AWS PrivateLink documento.

Cambio	Descripción	Fecha
AWS PrivateLink comenzó a rastrear los cambios	AWS PrivateLink comenzó a realizar un seguimiento de los cambios de sus políticas AWS gestionadas.	1 de marzo de 2021

Métricas de CloudWatch para AWS PrivateLink

AWS PrivateLink publica puntos de datos en Amazon CloudWatch para los puntos de conexión de interfaz, los puntos de conexión del equilibrador de carga de puerta de enlace y los servicios de puntos de conexión. CloudWatch permite recuperar las estadísticas sobre estos puntos de datos como un conjunto ordenado de datos de serie temporal denominado métricas. Una métrica es una variable que hay que monitorizar y los puntos de datos son los valores de esa variable a lo largo del tiempo. Cada punto de datos tiene una marca temporal asociada y una unidad de medida opcional.

Puede utilizar estas métricas para comprobar si el sistema funciona de acuerdo con lo esperado. Por ejemplo, puede crear una alarma de CloudWatch para monitorizar una métrica determinada e iniciar una acción (por ejemplo, enviar una notificación a una dirección de correo electrónico) si la métrica no está comprendida dentro del intervalo que considera aceptable.

Se publican métricas para todos los puntos de conexión de interfaz, los puntos de conexión del equilibrador de carga de puerta de enlace y los servicios de puntos de conexión. No se publican para los puntos de conexión de la puerta de enlace ni para los consumidores de servicios de puntos de extensión que utilizan el acceso entre regiones. De forma predeterminada, AWS PrivateLink envía métricas a CloudWatch en intervalos de un minuto, sin costo adicional.

Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch.

Contenido

Dimensiones y métricas de puntos de conexión

El espacio de nombres de `AWS/PrivateLinkEndpoints` incluye las siguientes métricas para los puntos de conexión de interfaz y los puntos de conexión del equilibrador de carga de puerta de enlace.

Métrica	Descripción
`ActiveConnections`	El número de conexiones simultáneas activas. Incluye las conexiones en los estados SYN_SENT y ESTABLISHED. Criterios de notificación: el punto de conexión recibió tráfico durante el periodo de un minuto. Estadísticas: las estadísticas más útiles son `Average`, `Maximum` y `Minimum`. Dimensiones • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`
`BytesProcessed`	El número de bytes intercambiados entre los puntos de conexión y los servicios de puntos de conexión, agregados en ambas direcciones. Es el número de bytes facturados al propietario del punto de conexión. La factura muestra este valor en GB. Criterios de notificación: el punto de conexión recibió tráfico durante el periodo de un minuto. Estadísticas: las estadísticas más útiles son `Average`, `Sum`, `Maximum` y `Minimum`. Dimensiones • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`
`NewConnections`	Número de conexiones nuevas establecidas a través del punto de conexión. Criterios de notificación: el punto de conexión recibió tráfico durante el periodo de un minuto.

Métrica	Descripción
	Estadísticas: las estadísticas más útiles son `Average`, `Sum`, `Maximum` y `Minimum`. Dimensiones • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`
`PacketsDropped`	Número de paquetes abandonados por el punto de conexión. Es posible que esta métrica no capture todas las perdidas de paquetes. El aumento de los valores podría indicar que el punto de conexión o el servicio de punto de conexión no está en buen estado. Criterios de notificación: el punto de conexión recibió tráfico durante el periodo de un minuto. Estadísticas: las estadísticas más útiles son `Average`, `Sum` y `Maximum`. Dimensiones • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Métrica	Descripción
`RstPacketsReceived`	Número de paquetes RST recibidos por el punto de conexión.. El aumento de los valores podría indicar que el servicio de punto de conexión no está en buen estado. Criterios de notificación: el punto de conexión recibió tráfico durante el periodo de un minuto. Estadísticas: las estadísticas más útiles son `Average`, `Sum` y `Maximum`. Dimensiones • `Endpoint Type`, `Service Name`, `VPC Endpoint Id`, `VPC Id` • `Endpoint Type`, `Service Name`, `Subnet Id`, `VPC Endpoint Id`, `VPC Id`

Para filtrar estas métricas, utilice las siguientes dimensiones.

Dimensión	Descripción
`Endpoint Type`	Filtra los datos de métricas por tipo de punto de conexión (`Interface` | `GatewayLoadBalancer`).
`Service Name`	Filtra los datos de métricas por nombre de servicio.
`Subnet Id`	Filtra los datos de métricas por subred.
`VPC Endpoint Id`	Filtra los datos de métricas por tipo de punto de conexión de VPC.
`VPC Id`	Filtra los datos de métricas por VPC.

Métricas y dimensiones del servicio de puntos de conexión

El espacio de nombres de `AWS/PrivateLinkServices` incluye las siguientes métricas para los servicios de puntos de conexión.

Métrica	Descripción
`ActiveConnections`	El número máximo de conexiones activas de clientes a objetivos a través de los puntos de conexión. El aumento de los valores podría indicar la necesidad de agregar objetivos al equilibrador de carga. Criterios de notificación: un punto de conexión conectado al servicio de punto de conexión envió tráfico durante el periodo de un minuto. Estadísticas: las estadísticas más útiles son `Average` y `Maximum`. Dimensiones • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`
`BytesProcessed`	El número de bytes intercambiados entre los servicios de puntos de conexión y los puntos de conexión, en ambas direcciones. Criterios de notificación: un punto de conexión conectado al servicio de punto de conexión envió tráfico durante el periodo de un minuto. Estadísticas: las estadísticas más útiles son `Average`, `Sum` y `Maximum`. Dimensiones • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`
`EndpointsCount`	El número de puntos de conexión conectados al servicio de puntos de conexión.

Métrica	Descripción
	Criterios de notificación: hay un valor distinto de cero durante el periodo de cinco minutos. Estadísticas: las estadísticas más útiles son `Average` y `Maximum`. Dimensiones • `Service Id`
`NewConnections`	El número de nuevas conexiones establecidas desde los clientes a los objetivos a través de los puntos de conexión. El aumento de los valores podría indicar la necesidad de agregar objetivos al equilibrador de carga. Criterios de notificación: un punto de conexión conectado al servicio de punto de conexión envió tráfico durante el periodo de un minuto. Estadísticas: las estadísticas más útiles son `Average`, `Sum` y `Maximum`. Dimensiones • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`

Métrica	Descripción
`RstPacketsSent`	El número de paquetes RST enviados a los puntos de conexión por el servicio de puntos de conexión. El aumento de los valores podría indicar que hay objetivos en mal estado. Criterios de notificación: un punto de conexión conectado al servicio de punto de conexión envió tráfico durante el periodo de un minuto. Estadísticas: las estadísticas más útiles son `Average`, `Sum` y `Maximum`. Dimensiones • `Service Id` • `Az`, `Service Id` • `Load Balancer Arn`, `Service Id` • `Az`, `Load Balancer Arn`, `Service Id` • `Service Id`, `VPC Endpoint Id`

Para filtrar estas métricas, utilice las siguientes dimensiones.

Dimensión	Descripción
`Az`	Filtra los datos de métricas por zona de disponibilidad.
`Load Balancer Arn`	Filtra los datos de métricas por equilibrador de carga.
`Service Id`	Filtra los datos de métricas por servicio de punto de conexión.
`VPC Endpoint Id`	Filtra los datos de métricas por tipo de punto de conexión de VPC.

Ver las métricas de CloudWatch

Puede ver estas métricas de CloudWatch mediante la consola de Amazon VPC, la consola de CloudWatch o la AWS CLI de la siguiente manera.

Para consultar las métricas desde la consola de Amazon VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puntos de conexión. Seleccione el punto de conexión y, a continuación, elija la pestaña Monitoring (Supervisión).
3. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión). Seleccione el servicio del punto de conexión y, a continuación, elija la pestaña Monitoring (Supervisión).

Para consultar métricas mediante la consola de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Métricas.
3. Seleccione el espacio de nombres de AWS/PrivateLinkEndpoints.
4. Seleccione el espacio de nombres de AWS/PrivateLinkServices.

Cómo ver métricas a través de la AWS CLI

Utilice el siguiente comando list-metrics a fin de enumerar las métricas disponibles para los puntos de conexión de la interfaz y los puntos de conexión del equilibrador de carga de la puerta de enlace:

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkEndpoints
```

Utilice el siguiente comando list-metrics para enumerar las métricas disponibles para los servicios de puntos de conexión:

```
aws cloudwatch list-metrics --namespace AWS/PrivateLinkServices
```

Utilizar las reglas integradas de Contributor Insights

AWS PrivateLink proporciona reglas integradas de Contributor Insights para los servicios de puntos de conexión a fin de ayudarlo a encontrar cuáles son los principales contribuyentes de cada métrica admitida. Para obtener más información, consulte Contributor Insights en la Guía del usuario de Amazon CloudWatch.

AWS PrivateLink proporciona las siguientes reglas:

- `VpcEndpointService-ActiveConnectionsByEndpointId-v1`: clasifica los puntos de conexión según el número de conexiones activas.
- `VpcEndpointService-BytesByEndpointId-v1`: clasifica los puntos de conexión según el número de bytes procesados.
- `VpcEndpointService-NewConnectionsByEndpointId-v1`: clasifica los puntos de conexión según el número de conexiones nuevas.
- `VpcEndpointService-RstPacketsByEndpointId-v1`: clasifica los puntos de conexión según el número de paquetes RST enviados a los puntos de conexión.

Antes de poder utilizar una regla incorporada, debe habilitarla. Después de habilitar una regla, ésta empieza a recoger los datos de los contribuyentes. Para obtener información sobre los cargos de Contributor Insights, consulte los precios de Amazon CloudWatch.

Debe tener los siguientes permisos para usar Contributor Insights:

- `cloudwatch:DeleteInsightRules`: Para eliminar las reglas de Contributor Insights.
- `cloudwatch:DisableInsightRules`: Para deshabilitar las reglas de Contributor Insights.
- `cloudwatch:GetInsightRuleReport`: Para obtener los datos.
- `cloudwatch:ListManagedInsightRules`: Para enumerar las reglas de Contributor Insights.
- `cloudwatch:PutManagedInsightRules`: Para habilitar las reglas de Contributor Insights.

Tareas

- Habilite las reglas de Contributor Insights
- Deshabilitar reglas de Contributor Insights
- Eliminar reglas de Contributor Insights

Habilite las reglas de Contributor Insights

Utilice los siguientes procedimientos para habilitar las reglas integradas para AWS PrivateLink utilizando cualquiera de las Consola de administración de AWS o la AWS CLI.

Para habilitar las reglas de Contributor Insights para AWS PrivateLink usando la consola

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

2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Seleccione el servicio de punto de conexión.
4. En la pestaña del Contributor Insights, elija Disable (Habilitar).
5. (Opcional) De forma predeterminada, se habilitan todas las reglas. Para habilitar solo reglas específicas, seleccione las reglas que no deberían habilitarse y, a continuación, elija Actions (Acciones), Disable rule (Deshabilitar regla). Cuando se le indique que confirme, elija Disable (Desactivar).

Para habilitar las reglas de Contributor Insights para AWS PrivateLink utilizando la AWS CLI

1. Utilice el comando list-managed-insight-rules de la siguiente manera para enumerar las reglas disponibles. Para la opción `--resource-arn`, especifique el ARN de su servicio de punto de conexión.

```
aws cloudwatch list-managed-insight-rules --resource-arn
 arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-svc-0123456789EXAMPLE
```

2. En la salida del comando `list-managed-insight-rules`, copia el nombre de la plantilla del `TemplateName`. A continuación se muestra un ejemplo de este campo.

```
"TemplateName": "VpcEndpointService-NewConnectionsByEndpointId-v1"
```

3. Utilice el comando put-managed-insight-rules de la siguiente manera para habilitar la regla. Debe especificar el nombre de la plantilla y el ARN de su servicio de punto de conexión.

```
aws cloudwatch put-managed-insight-rules --managed-rules
 TemplateName=VpcEndpointService-NewConnectionsByEndpointId-
v1,ResourceARN=arn:aws:ec2:region:account-id:vpc-endpoint-service/vpc-
svc-0123456789EXAMPLE
```

Deshabilitar reglas de Contributor Insights

Puede deshabilitar las reglas integradas para AWS PrivateLink en cualquier momento. Tras deshabilitar una regla, deja de recopilar los datos de los colaboradores, pero los datos de los colaboradores existentes se conservan hasta que tengan 15 días de antigüedad. Una vez que haya desactivado una regla, puede activarla de nuevo para reanudar la recopilación de datos de los colaboradores.

Para deshabilitar las reglas de Contributor Insights para AWS PrivateLink utilizando la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Endpoint Services (Servicios de punto de conexión).
3. Seleccione el servicio de punto de enlace.
4. En la pestaña del Contributor Insights, elija Disable all (Deshabilitar todo) para deshabilitar todas las reglas. Como alternativa, despliegue el panel de Rules (Reglas), seleccione las reglas que desea deshabilitar y, a continuación, elija Actions (Acciones), Disable rule (Deshabilitar regla)
5. Cuando se le indique que confirme, elija Disable (Desactivar).

Para deshabilitar las reglas de Contributor Insights para AWS PrivateLink utilizando la AWS CLI

Utilice el comando disable-insight-rules para deshabilitar una regla.

Eliminar reglas de Contributor Insights

Utilice los siguientes procedimientos para eliminar reglas integradas de AWS PrivateLinkutilizando cualquiera de las Consola de administración de AWS o la AWS CLI. Después de eliminar una regla, ésta deja de recoger los datos de los contribuyentes y nosotros eliminamos los datos de los contribuyentes existentes.

Para eliminar reglas de Contributor Insights para AWS PrivateLink utilizando la consola

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Insights y, luego, Contributor Insights.
3. Despliegue el panel de Rules (Reglas) y seleccione las reglas.
4. En Actions (Acciones), y Delete (Eliminar).
5. Cuando se le pida confirmación, seleccione Eliminar.

Para eliminar reglas de Contributor Insights para AWS PrivateLink utilizando la AWS CLI

Utilice el comando delete-insight-rules para eliminar una regla.

AWS PrivateLinkCuotas de

La cuenta de AWS tiene cuotas predeterminadas para cada servicio de AWS (estas cuotas anteriormente se denominaban “límites”). A menos que se indique lo contrario, cada cuota es específica de la región de . Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar. Si solicita un aumento de cuota que se aplica a cada uno de los recursos, aumente la cuota para todos los recursos de la región.

Para solicitar un aumento de cuota, consulte Solicitud de un aumento de cuota en la Guía de usuario de Service Quotas.

Limitación controlada de solicitudes

Las acciones de la API para AWS PrivateLink son parte de la API de Amazon EC2. Amazon EC2 limita sus solicitudes de API al nivel de Cuenta de AWS. Para obtener más información, consulte Solicitar limitaciones en la Guía para desarrolladores de Amazon EC2. Además, las solicitudes de API también se limitan a nivel de la organización para mejorar el rendimiento de AWS PrivateLink. Si utiliza AWS Organizations y recibe un código de error `RequestLimitExceeded` mientras aún está dentro de los límites de la API a nivel de cuenta, consulte Cómo identificar cuentas de AWS que crean un gran número de llamadas a la API. Si necesita ayuda, contacte a su equipo de cuentas o aba un caso de soporte técnico mediante el servicio de VPC y la categoría puntos de conexión de VPC. Asegúrese de adjuntar una imagen del código de error `RequestLimitExceeded`.

Cuotas de puntos de conexión de VPC

Su cuenta de AWS tiene las siguientes cuotas relacionadas con los puntos de conexión de VPC.

Nombre	Valor predeterminado	Ajustable	Comentarios
Interfaz y puntos de enlace del balanceador de carga de gateway por VPC	50	Sí	Esta es una cuota combinada para los puntos de conexión de interfaz y los puntos de conexión del equilibrador de carga de la puerta de enlace
Puntos de enlace de la VPC de tipo gateway por región	20	Sí	Puede crear hasta 255 puntos de conexión de puerta de enlace por VPC

Nombre	Valor predeterminado	Ajustable	Comentarios
Puntos de conexión de VPC de recursos por VPC	200	Sí	
Puntos de conexión de VPC de red de servicios por VPC	50	Sí	
Caracteres por política de punto de conexión de VPC	20 480	No	El tamaño máximo de una política de punto de conexión de VPC incluye espacios en blanco

Las siguientes consideraciones se aplican al tráfico que pasa a través de un punto de conexión de VPC:

- De manera predeterminada, cada punto de conexión de VPC admite un ancho de banda de hasta 10 Gbps por cada zona de disponibilidad, y escala hasta 100 Gbps. El ancho de banda máximo para un punto de conexión de VPC cuando se distribuye la carga entre todas las zonas de disponibilidad es el número de zonas de disponibilidad multiplicado por 100 Gbps. Si su aplicación necesita un rendimiento mayor, póngase en contacto con el soporte técnico de AWS.
- La unidad de transmisión máxima (MTU) de una conexión de red es el tamaño, en bytes, del mayor paquete permitido que se puede transferir a través de un punto de conexión de VPC. Cuanto mayor sea la MTU, mayor cantidad de datos se podrán transferir en un solo paquete. Un punto de enlace de la VPC admite una MTU de 8500 bytes. Se eliminan los paquetes con un tamaño superior a 8500 bytes que llegan al punto de enlace de la VPC.
- No se admite la Detección de la MTU de la ruta (PMTUD). Los puntos de conexión de VPC no generan el siguiente mensaje ICMP: `Destination Unreachable: Fragmentation needed and Don't Fragment was Set` (tipo 3, código 4).
- Los puntos de conexión de VPC aplican el bloqueo de tamaño máximo de segmento (MSS) a todos los paquetes. Para obtener más información, consulte RFC879.

Historial de documentos de AWS PrivateLink

En la tabla siguiente se describen las versiones de las AWS PrivateLink.

Cambio	Descripción	Fecha
Acceder a recursos y redes de servicios	AWS PrivateLink admite el acceso a los recursos y las redes de servicios a través de los límites de las cuentas y las VPC.	1 de diciembre de 2024
Acceso entre regiones	Un proveedor de servicios puede alojar un servicio en una región y ponerlo a disposición en un conjunto de regiones de AWS. Un consumidor de servicios selecciona una región de servicio al crear un punto de conexión.	26 de noviembre de 2024
Direcciones IP designadas	Puede especificar las direcciones IP de las interfaces de red de los puntos de conexión al crear o modificar el punto de conexión de VPC.	17 de agosto de 2023
Compatibilidad con IPv	Puede configurar los servicios de punto de conexión de equilibrador de carga de puerta de enlace y los puntos de conexión del equilibrador de carga de puerta de enlace para que admitan direcciones IPv4 e IPv6 o solo direcciones IPv6.	12 de diciembre de 2022

Contributor Insights	Puede utilizar las reglas integradas de Contributor Insights para identificar los puntos de conexión específicos que son los principales contribuyentes a las métricas de CloudWatch para AWS PrivateLink.	18 de agosto de 2022
Compatibilidad con IPv	Los proveedores de servicios pueden permitir que sus servicios de punto de conexión acepten solicitudes de IPv6, incluso si sus servicios de backend solo admiten IPv4. Si un servicio de punto de conexión acepta solicitudes de IPv6, los consumidores del servicio pueden habilitar la compatibilidad con IPv6 para sus puntos de conexión de interfaz y así, acceder al servicio de punto de conexión a través de IPv6.	11 de mayo de 2022
Métricas de CloudWatch	AWS PrivateLink publica las métricas de CloudWatch para los puntos de conexión de la interfaz, los puntos de conexión del equilibrador de carga de la puerta de enlace y los servicios de puntos de conexión.	27 de enero de 2022

Puntos de conexión del equilibrador de carga de la puerta de enlace	Puede crear un punto de enlace del balanceador de carga de gateway en la VPC para enrutar el tráfico a un servicio de punto de enlace de la VPC que haya configurado mediante un balanceador de carga de gateway.	10 de noviembre de 2020
Políticas de punto de enlace de VPC	Puede adjuntar una política de IAM a un punto de conexión de VPC de la interfaz para un servicio de AWS a fin de controlar el acceso al servicio.	23 de marzo de 2020
Claves de condición para puntos de enlace de la VPC y servicios de los puntos de enlace	Puede utilizar claves de condición de EC2 para controlar el acceso al punto de conexión de VPC y a los servicios del punto de conexión.	6 de marzo de 2020
Etiquetar los puntos de conexión de VPC y los servicios de punto de conexión en creación	Puede agregar etiquetas al crear un punto de conexión de VPC o servicios de puntos de conexión.	5 de febrero de 2020
Nombres de DNS privados	Puede obtener acceso a los servicios basados en AWS PrivateLink desde la VPC mediante nombres DNS privados.	6 de enero de 2020

Servicios de punto de conexión de VPC	Puede crear sus propios servicios de punto de conexión y habilitar otras Cuentas de AWS y usuarios para que se conecten con su servicio a través de un punto de conexión de VPC de interfaz. Puede ofrecer los servicios de puntos de conexión para suscribirse en el AWS Marketplace.	28 de noviembre de 2017
Puntos de conexión de VPC de interfaz para Servicios de AWS	Puede crear un punto de conexión de interfaz para conectarse a los Servicios de AWS que se integran con AWS PrivateLink sin utilizar una puerta de enlace de Internet o un dispositivo NAT.	8 de noviembre de 2017
Puntos de enlace de la VPC para DynamoDB	Puede crear un punto de conexión de VPC de puerta de enlace para acceder a Amazon DynamoDB desde la VPC sin utilizar una puerta de enlace de Internet o un dispositivo NAT.	16 de agosto de 2017
Puntos de enlace de la VPC para Amazon S3	Puede crear un punto de conexión de VPC de puerta de enlace para acceder a Amazon S3 desde la VPC sin utilizar una puerta de enlace de Internet o un dispositivo NAT.	11 de mayo de 2015

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.