AWS PrivateLink

Amazon Virtual Private Cloud

Amazon Virtual Private Cloud: AWS PrivateLink

Table of Contents

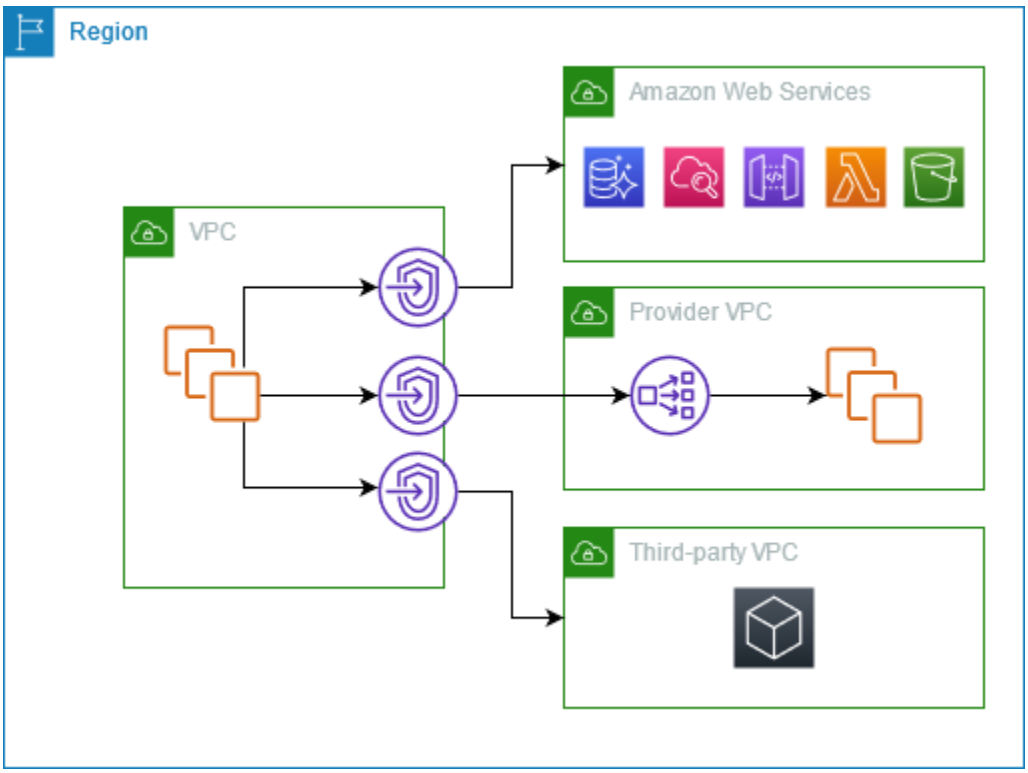
¿Qué es AWS PrivateLink?

AWS PrivateLink es una tecnología escalable y de alta disponibilidad que puede utilizar para conectar de forma privada su VPC a los servicios como si estuvieran en su VPC. No necesita usar una puerta de enlace a Internet, un dispositivo NAT, una dirección IP pública, una AWS Direct Connect conexión o una AWS Site-to-Site VPN conexión para permitir la comunicación con el servicio desde sus 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 enlace de VPC para conectar los recursos de su VPC a los servicios con los que se integra. AWS PrivateLink Puede crear su propio servicio de punto final de VPC y ponerlo a disposición de otros AWS clientes. Para obtener más información, consulte the section called “Conceptos”.

En el siguiente diagrama, la VPC de la izquierda tiene varias instancias EC2 en una subred privada y tres puntos de conexión de VPC de interfaz. El punto final de VPC más alto se conecta a un. Servicio de AWS El punto final de la VPC central se conecta a un servicio hospedado por otro Cuenta de AWS (un servicio de punto final de la VPC). El punto final de VPC inferior se conecta a un servicio AWS Marketplace asociado.



Más información

- the section called “Conceptos”
- Acceder 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:

- AWS Management Console— Proporciona una interfaz web que puede utilizar para acceder a sus AWS PrivateLink recursos. Abra la consola de Amazon VPC y elija Endpoints o Endpoint services.
- AWS Command Line Interface (AWS CLI): proporciona comandos para un amplio conjunto de Servicios de AWS, entre los que se incluyen. AWS PrivateLink Para obtener más información sobre los comandos de AWS PrivateLink, consulte ec2 en la Referencia de AWS CLI comandos.

- AWS 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 siguientes AWS PrivateLink recursos:
  - AWS::EC2::VPCEndpoint
  - Notificación de AWS: :EC2: :VPC EndpointConnection
  - AWS::EC2::VPCEndpointService
  - Permisos de AWS: :EC2: :VPC EndpointService
  - AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS SDK: proporcionan API específicas para cada idioma. Los SDK de 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 sobre las que basarse. 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 PrivateLink conceptos

Puede utilizar Amazon VPC para definir una nube privada virtual (VPC), que es una red virtual aislada lógicamente. Puede lanzar AWS recursos en su VPC. Puede permitir que los recursos de su VPC se conecten a recursos fuera de la 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. También puede utilizar esta opción AWS PrivateLink para permitir que los recursos de su VPC se conecten a los servicios de otras VPC mediante direcciones IP privadas, como si esos servicios estuvieran alojados directamente en su VPC.

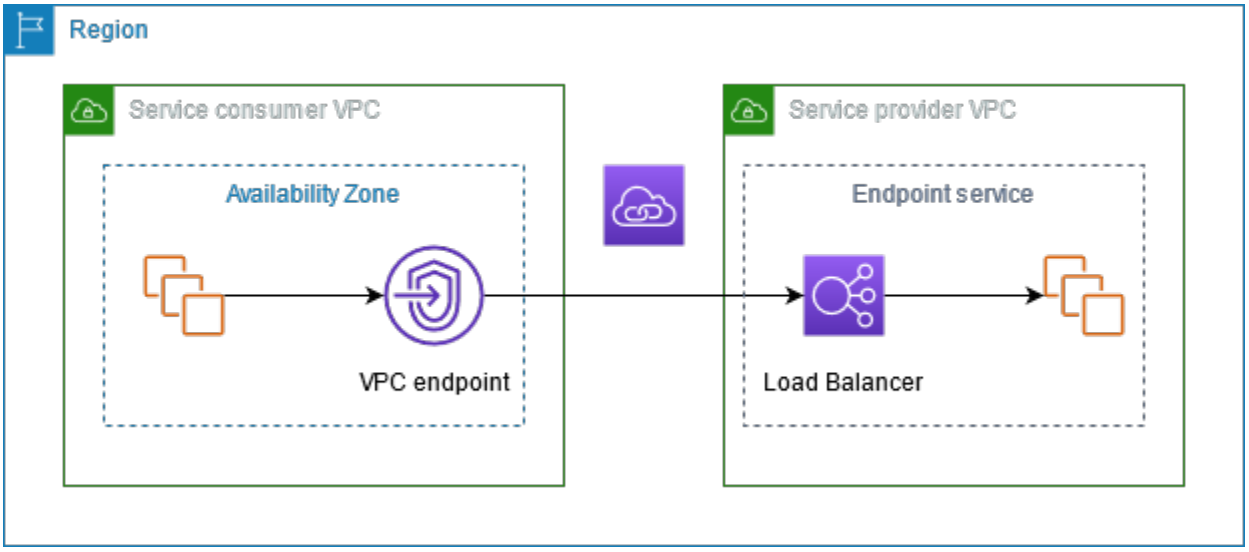
Los siguientes conceptos son importantes y deben comprenderse cuando se comienza a utilizar AWS PrivateLink.

Contenido

- Diagrama de arquitectura
- Proveedores de servicios
- Consumidores de servicios
- AWS PrivateLink conexiones
- Zonas alojadas privadas

Diagrama de arquitectura

El siguiente diagrama proporciona una descripción general de alto nivel de su funcionamiento. AWS PrivateLink Los consumidores de servicios crean puntos de conexión de VPC de interfaz para conectarse a servicios de punto de conexión alojados por proveedores de servicios.



Proveedores de servicios

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

Conceptos

- Servicios de punto de conexión
- Nombres de servicios
- Estados del servicio

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 añadir permisos que permitan a entidades AWS principales específicas conectarse a su servicio de punto final.

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 AWS servicios. 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:

- `Pending`: el servicio de punto de conexión se está creando.
- `Available`: el servicio de punto de conexión está disponible.
- `Failed`: el servicio de punto de conexión no se pudo crear.
- `Deleting`: el proveedor del servicio eliminó el servicio de punto de conexión y la eliminación está en curso.
- `Deleted`: el servicio de punto de conexión se eliminó.

Consumidores de servicios

El usuario de un servicio es un consumidor del servicio. Los consumidores de servicios pueden acceder a los servicios de punto final desde AWS recursos, como instancias EC2, o desde servidores locales.

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

El consumidor del servicio crea un punto de conexión de VPC para conectar su VPC a un servicio de punto de conexión. Cuando el consumidor del servicio crea un punto de conexión de VPC, debe especificar el nombre del servicio de punto de conexión. Hay varios tipos de puntos de conexión de VPC. Debe crear el tipo de punto de conexión de VPC que requiere el servicio de punto de conexión.

- `Interface`: cree un punto de conexión de interfaz para enviar tráfico TCP 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.

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 enlace de puerta de enlace no utilizan AWS PrivateLink, a diferencia de los otros tipos de puntos de enlace 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 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.

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.

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, 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 `Available`.

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

- `PendingAcceptance`: la solicitud de conexión está pendiente. Este es el estado inicial si las solicitudes se aceptan de forma manual.
- `Pending`: 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.
- `Available`: el punto de conexión de VPC está disponible para su uso.
- `Rejected`: 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.
- `Expired`: la solicitud de conexión caducó.
- `Failed`: el punto de conexión de VPC no está disponible.
- `Deleting`: el consumidor del servicio eliminó el punto de conexión de VPC y la eliminación está en curso.
- `Deleted`: el punto de conexión de VPC se ha eliminado.

AWS PrivateLink conexiones

El tráfico de la VPC se envía a un servicio de punto de conexión mediante una conexión entre el punto de conexión de VPC y el servicio de punto de conexión. El tráfico entre un punto final de VPC y un servicio de punto final permanece dentro de la AWS red, 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.

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

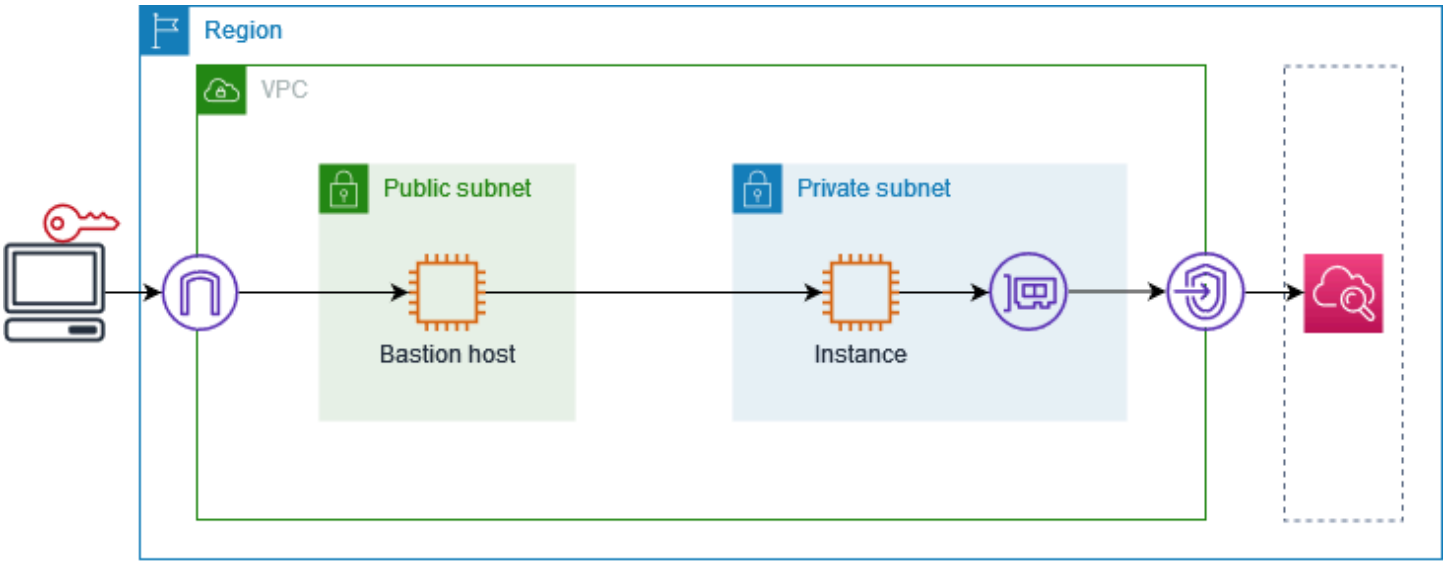
Puede configurar Amazon Route 53 para dirigir el tráfico del dominio a un punto de conexión de VPC. Para obtener más información, consulte Enrutamiento del tráfico a un punto de conexión de VPC mediante el nombre de dominio.

Puede usar Route 53 para configurar un DNS de horizonte dividido, en el que se usa el mismo nombre de dominio tanto para un sitio web público como para un servicio de punto final 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.

Comience con AWS PrivateLink

En este tutorial se muestra cómo enviar una solicitud desde una instancia EC2 de 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. Después de configurar un punto de enlace de VPC para CloudWatch, el tráfico de la instancia a la que CloudWatch está destinado se resuelve en la interfaz de red de puntos finales y, a continuación, se envía a CloudWatch través del punto de enlace 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: Probar CloudWatch el acceso
- Paso 4: Crear un punto final de VPC al que acceder 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 Crear 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 Crear 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 adjunte la política de acceso. CloudWatch ReadOnly

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: Probar CloudWatch el acceso

Usa el siguiente procedimiento para confirmar que la instancia no puede acceder CloudWatch. Para ello, utilizará un AWS CLI comando de solo lectura para. CloudWatch

Para probar el acceso 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. Ejecuta el comando CloudWatch list-metrics 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 puedes acceder 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: Crear un punto final de VPC al que acceder CloudWatch

Utilice el siguiente procedimiento para crear un punto final de VPC al que se conecte. CloudWatch

Requisito previo

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

Para crear un punto final 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. Seleccione 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

Comprueba que el punto final de la VPC envía solicitudes desde tu 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 recibes una respuesta, incluso una respuesta con resultados vacíos, estás conectado a ella CloudWatch . AWS PrivateLink

Si recibes un `UnauthorizedOperation` error, asegúrate de que la instancia tenga una función de IAM que permita el acceso a CloudWatch.

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

- El grupo de seguridad del punto final permite que el tráfico entre. 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 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 Terminar.

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.

Acceso a Servicios de AWS través 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 que se aprovisione el punto final de la 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.

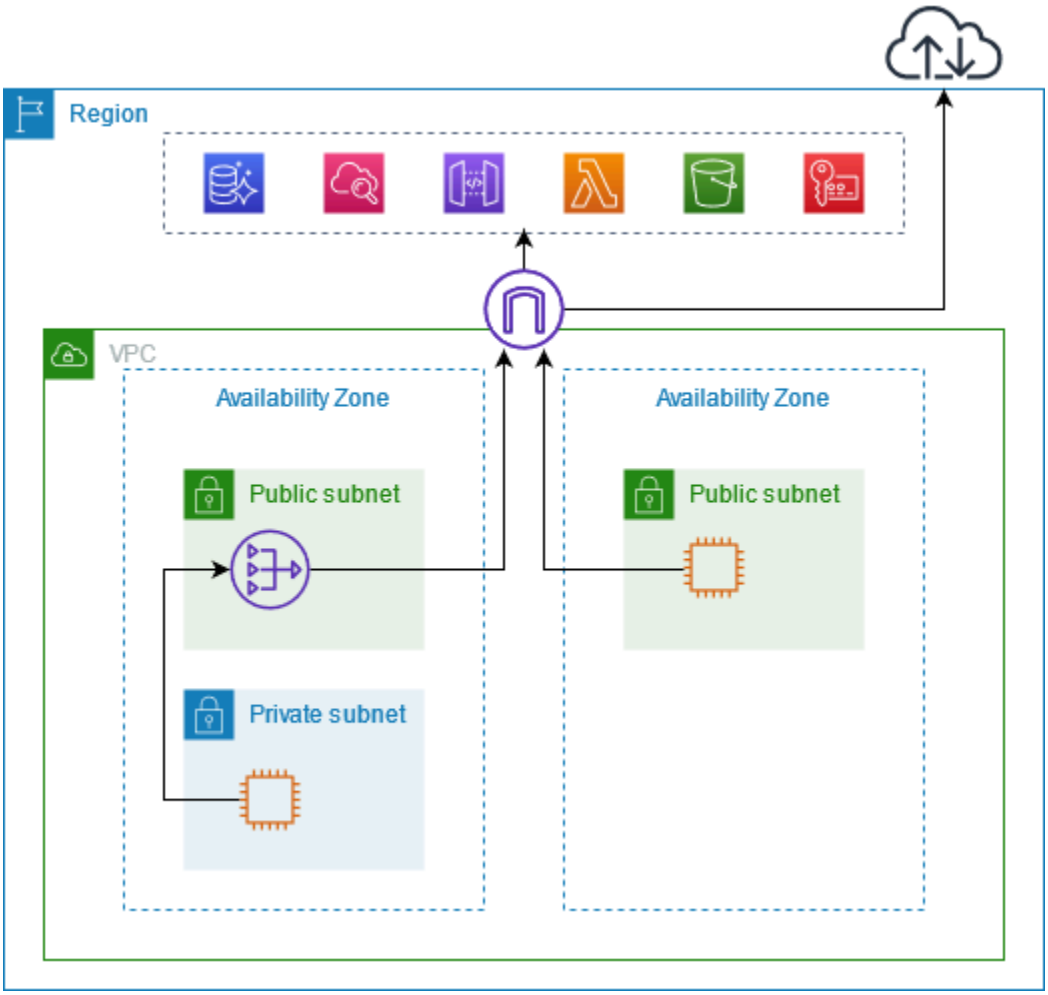
Contenido

Información 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.

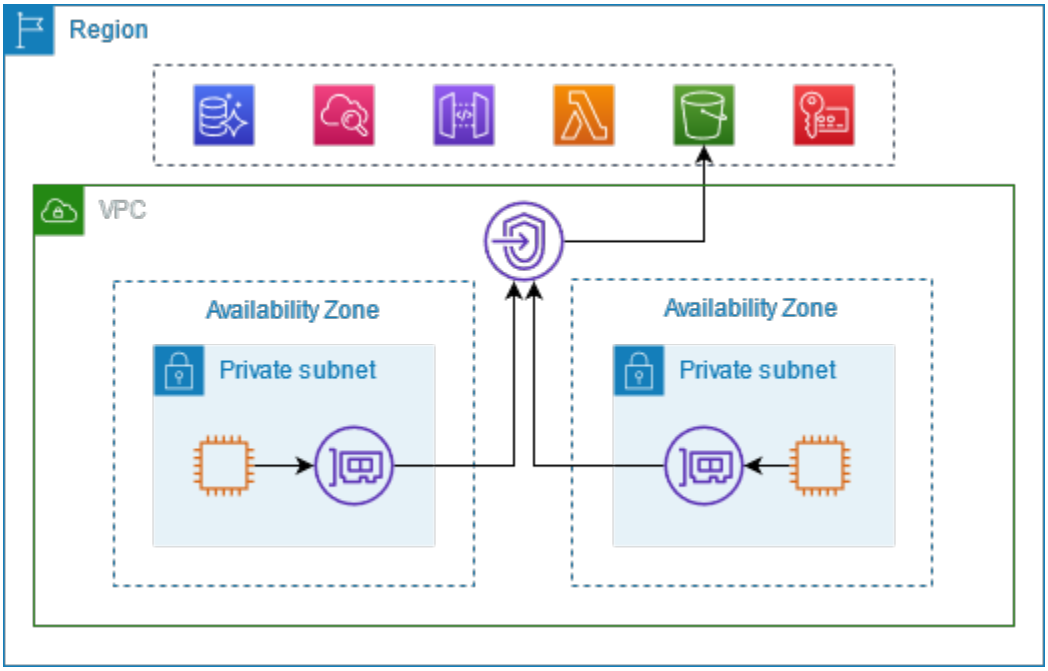
Acceso a través de puntos de conexión de servicio públicos

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

En el siguiente diagrama se 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 comando describe-vpc-endpoints muestra las entradas DNS para un punto de conexión 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 los nombres DNS privados para los puntos de conexión de la VPC. 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

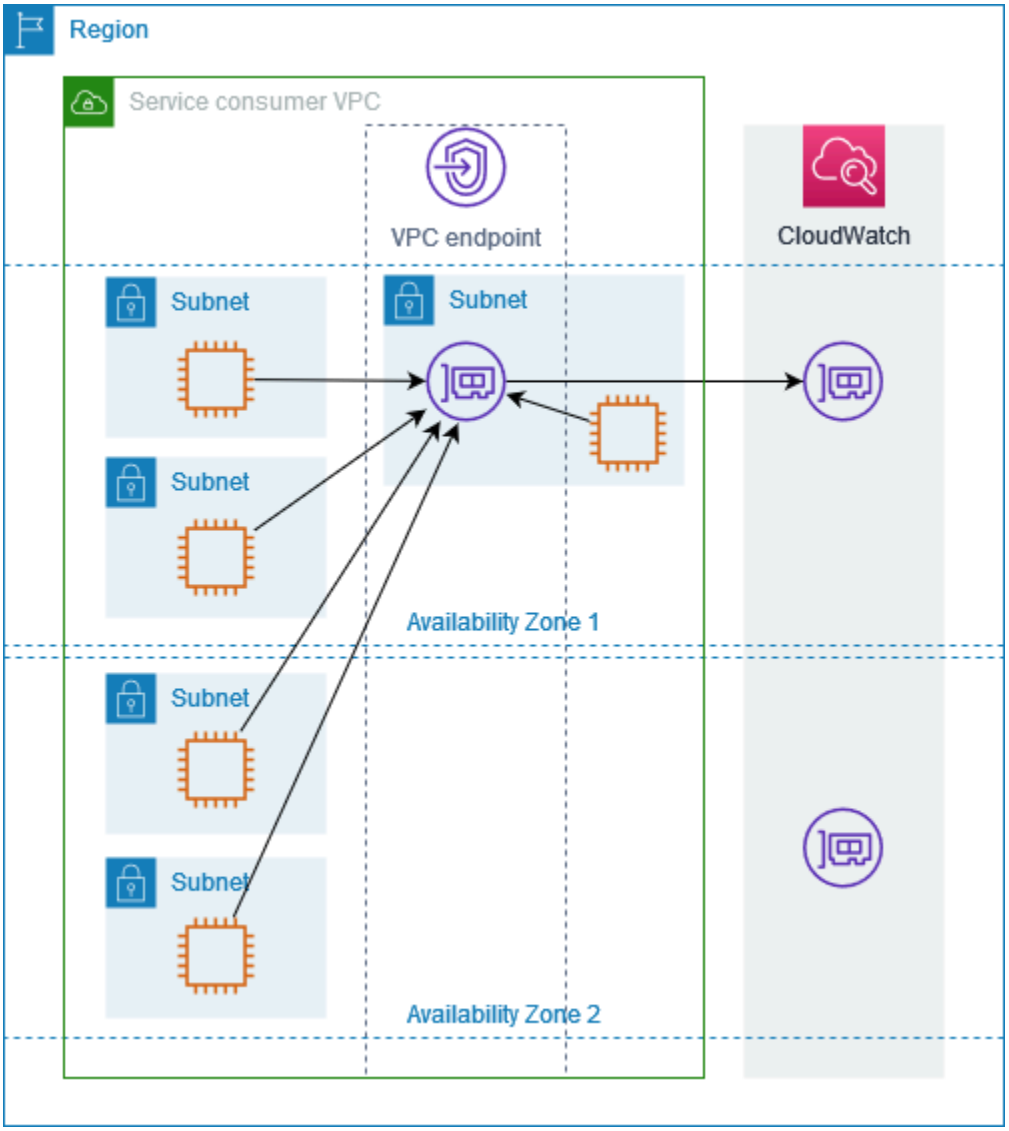
Subredes y zonas de disponibilidad

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.

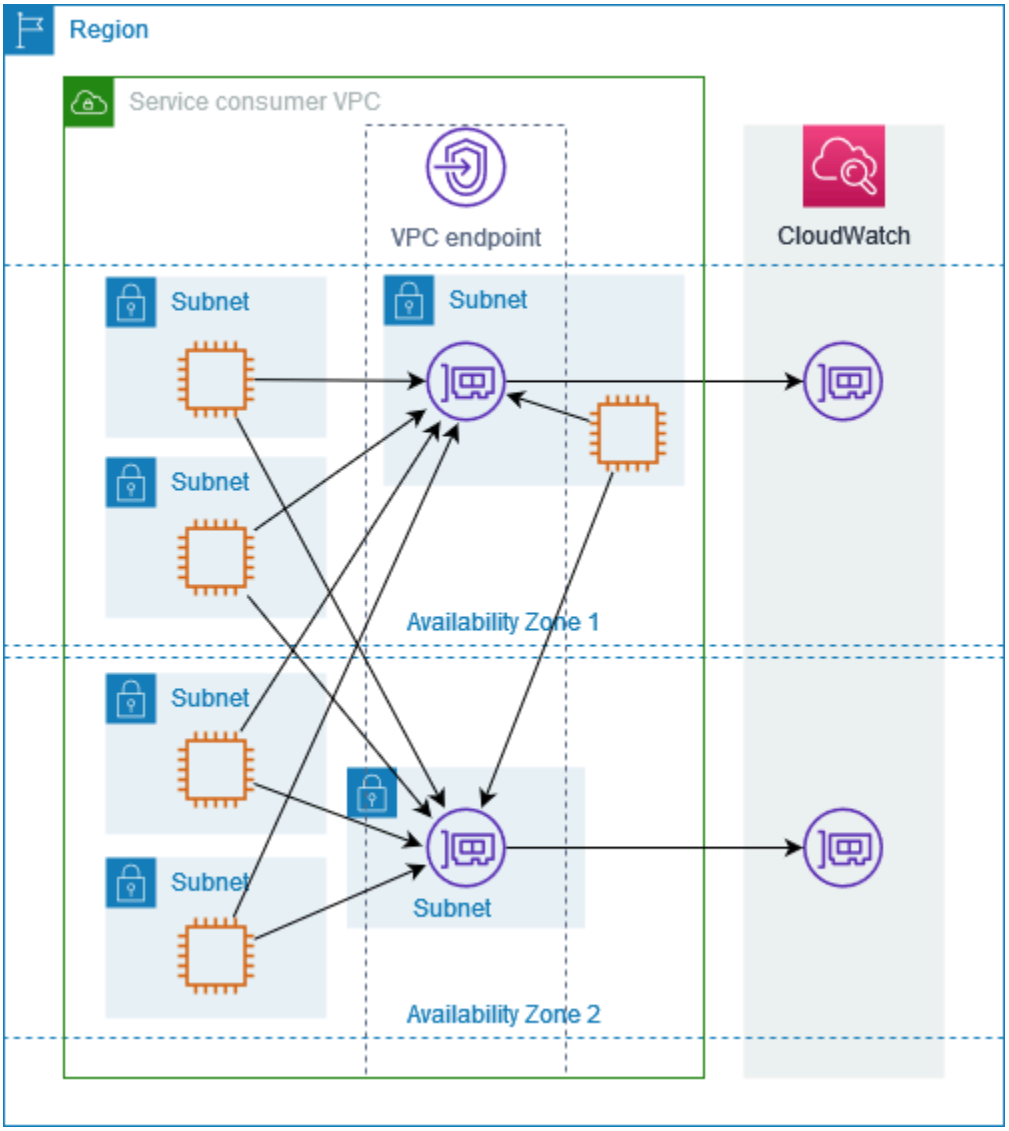
En un entorno de producción, para una alta disponibilidad y resiliencia, recomendamos lo siguiente:

- 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.

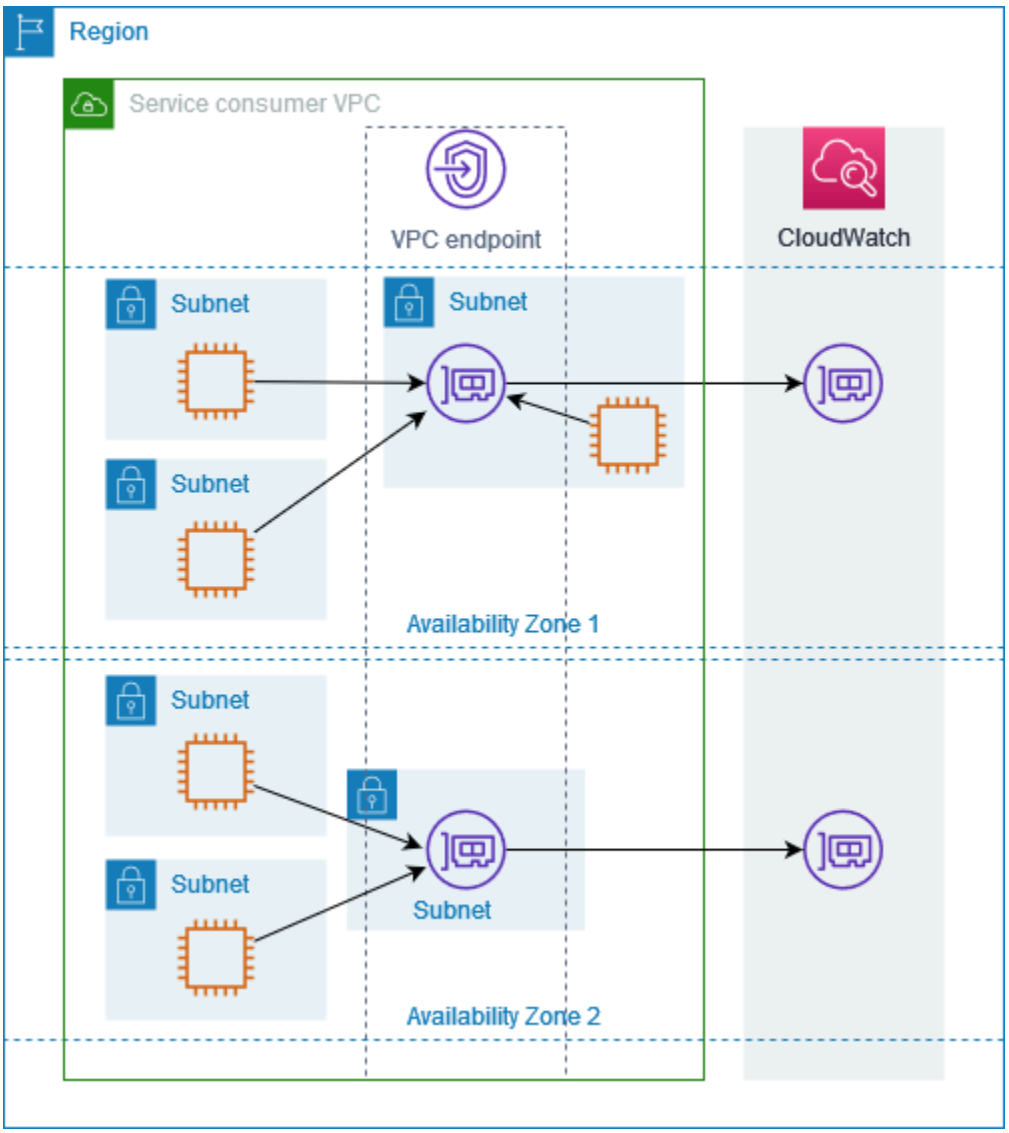
En el siguiente diagrama, se muestra un punto de enlace de VPC para Amazon CloudWatch con una interfaz de red de puntos finales en una única zona de disponibilidad. Cuando cualquier recurso de cualquier subred de la VPC accede a CloudWatch Amazon mediante su punto de conexión público, resolvemos el tráfico 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.



En el siguiente diagrama, se muestra un punto de enlace 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 admitir IPv6 a través de sus puntos de conexión privados, incluso si no admiten IPv6 a través de sus puntos de conexión públicos. Los puntos de conexión que admiten IPv6 pueden responder a consultas de DNS con registros AAAA.

Requisitos para habilitar IPv6 para un punto de conexión de interfaz

- Servicio de AWS Deben hacer que sus puntos finales de servicio estén disponibles a través de IPv6. Para obtener más información, consulte the section called “Ver compatibilidad con IPv6”.
- 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: 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.

Si un punto de conexión de VPC de interfaz admite IPv4, las interfaces de red del punto de conexión tienen direcciones IPv4. Si un punto de conexión de VPC de interfaz 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.

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 especificas al crear el punto final de la VPC de la interfaz o indica que el servicio administra el punto final.

Servicio de AWS	Nombre del servicio
Analizador de acceso	com.amazonaws.*region*.access-analyzer
AWS Account Management	com.amazonaws.*region*.account
Amazon API Gateway	com.amazonaws.*region*.execute-api
AWS AppConfig	com.amazonaws.*region*.appconfig
	com.amazonaws.*region*.appconfigdata
AWS App Mesh	com.amazonaws.*region*.appmesh

Servicio de AWS	Nombre del servicio
	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*.application-autoscaling
AWS Servicio de migración de aplicaciones	com.amazonaws.*region*.mgn
Amazon AppStream 2.0	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*.auditmanager
Amazon Aurora	com.amazonaws.*region*.rds
AWS Auto Scaling	com.amazonaws.*region*.autoscaling-plans
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

Servicio de AWS	Nombre del servicio
	com.amazonaws.*region*.bedrock-runtime
AWS Billing Conductor	com.amazonaws.*region*.billingconductor
Amazon Braket	com.amazonaws.*region*.braket
Salas limpias de AWS	com.amazonaws.*region*.cleanrooms
AWS Salas limpias ML	com.amazonaws. *región .cleanrooms-ml*
AWS Cloud Control API	com.amazonaws.*region*.cloudcontrolapi
	com.amazonaws.*region*.cloudcontrolapi-fips
Amazon Cloud Directory	com.amazonaws.*region*.clouddirectory
AWS CloudFormation	com.amazonaws.*region*.cloudformation
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
Amazon CloudWatch	com.amazonaws.*region*.evidently
	com.amazonaws.*region*.evidently-dataplane
	com.amazonaws.*region*.monitoring
	com.amazonaws.*region*.rum
	com.amazonaws.*region*.rum-dataplane

Servicio de AWS	Nombre del servicio
	com.amazonaws.*region*.synthetics
Amazon CloudWatch Logs	com.amazonaws.*region*.logs
Monitor CloudWatch de red Amazon	com.amazonaws. *region .networkmonitor*
AWS CodeArtifact	com.amazonaws.*region*.codeartifact.api
	com.amazonaws.*region*.codeartifact.repositories
AWS CodeBuild	com.amazonaws.*region*.codebuild
	com.amazonaws.*region*.codebuild-fips
AWS CodeCommit	com.amazonaws.*region*.codecommit
	com.amazonaws.*region*.codecommit-fips
	com.amazonaws.*region*.git-codecommit
	com.amazonaws.*region*.git-codecommit-fips
AWS CodeConnections	com.amazonaws. *región .codeconnections.api*
	com.amazonaws.*region*.codestar-connections.api
AWS CodeDeploy	com.amazonaws.*region*.codedeploy
	com.amazonaws.*region*.codedeploy-commands-secure
Amazon CodeGuru Profiler	com.amazonaws.*region*.codeguru-profiler
CodeGuru Revisor de Amazon	com.amazonaws.*region*.codeguru-reviewer
AWS CodePipeline	com.amazonaws.*region*.codepipeline
Amazon CodeWhisperer	com.amazonaws.*region*.codewhisperer
Amazon Comprehend	com.amazonaws.*region*.comprehend

Servicio de AWS	Nombre del servicio
Amazon Comprehend Medical	com.amazonaws.*region*.comprehendmedical
AWS Config	com.amazonaws.*region*.config
Amazon Connect	com.amazonaws.*region*.app-integrations
	com.amazonaws.*region*.cases
	com.amazonaws.*region*.connect-campaigns
	com.amazonaws.*region*.profile
	com.amazonaws.*region*.voiceid
	com.amazonaws.*region*.wisdom
AWS Connector Service	com.amazonaws.*region*.awsconnector
AWS Control Catalog	com.amazonaws. *region. catálogo de control*
AWS Data Exchange	com.amazonaws.*region*.dataexchange
Amazon Data Firehose	com.amazonaws.*region*.kinesis-firehose
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
AWS Deadline Cloud	com.amazonaws. *region .deadline.management*
	com.amazonaws. *region .deadline.scheduling*
El DevOps gurú de Amazon	com.amazonaws.*region*.devops-guru
AWS Directory Service	com.amazonaws.*region*.ds

Servicio de AWS	Nombre del servicio
Amazon DynamoDB	com.amazonaws. *región: .dynamodb*
API directas de Amazon EBS	com.amazonaws.*region*.ebs
Amazon EC2	com.amazonaws.*region*.ec2
Amazon EC2 Auto Scaling	com.amazonaws.*region*.autoscaling
EC2 Image Builder	com.amazonaws.*region*.imagebuilder
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-telemetry
Amazon EKS	com.amazonaws.*region*.eks
	com.amazonaws.*region*.eks
AWS Elastic Beanstalk	com.amazonaws.*region*.elasticbeanstalk
	com.amazonaws.*region*.elasticbeanstalk-health
AWS Elastic Disaster Recovery	com.amazonaws.*region*.drs
Amazon Elastic File System	com.amazonaws.*region*.elasticfilesystem
	com.amazonaws.*region*.elasticfilesystem-fips
Amazon Elastic Inference	com.amazonaws.*region*.elastic-inference.runtime
Elastic Load Balancing	com.amazonaws.*region*.elasticloadbalancing
Amazon ElastiCache	com.amazonaws.*region*.elasticache

Servicio de AWS	Nombre del servicio
	com.amazonaws.*region*.elasticache-fips
AWS Elemental MediaConnect	com.amazonaws.*region*.mediaconnect
Amazon EMR	com.amazonaws.*region*.elasticmapreduce
Amazon EMR en EKS	com.amazonaws.*region*.emr-containers
Amazon EMR sin servidor	com.amazonaws.*region*.emr-serverless
Amazon EMR WAL	com.amazonaws. *región .emrwal.prod*
AWS Entity Resolution	com.amazonaws.*region*.entityresolution
Amazon EventBridge	com.amazonaws.*region*.events
	com.amazonaws. *región .pipes-data*
AWS Fault Injection Service	com.amazonaws.*region*.fis
Amazon FinSpace	com.amazonaws.*region*.finspace
	com.amazonaws.*region*.finspace-api
Amazon Forecast	com.amazonaws.*region*.forecast
	com.amazonaws.*region*.forecastquery
	com.amazonaws.*region*.forecast-fips
	com.amazonaws.*region*.forecastquery-fips
Amazon Fraud Detector	com.amazonaws.*region*.frauddetector
Amazon FSx	com.amazonaws.*region*.fsx
	com.amazonaws.*region*.fsx-fips
AWS Glue	com.amazonaws.*region*.glue

Servicio de AWS	Nombre del servicio
AWS Glue DataBrew	com.amazonaws.*region*.databrew
Amazon Managed Grafana	com.amazonaws.*region*.grafana
	com.amazonaws.*region*.grafana-workspace
AWS Ground Station	com.amazonaws.*region*.groundstation
Amazon GuardDuty	com.amazonaws.*region*.guardduty-data
	com.amazonaws.*region*.guardduty-data-fips
AWS HealthImaging	com.amazonaws. *región .dicom-medical-imaging*
	com.amazonaws.*region*.medical-imaging
	com.amazonaws.*region*.runtime-medical-imaging
AWS HealthLake	com.amazonaws.*region*.healthlake
AWS HealthOmics	com.amazonaws.*region*.analytics-omics
	com.amazonaws.*region*.control-storage-omics
	com.amazonaws.*region*.storage-omics
	com.amazonaws.*region*.tags-omics
	com.amazonaws.*region*.workflows-omics
IAM Identity Center	com.amazonaws.*región*.identitystore
Funciones de IAM en cualquier lugar	com.amazonaws.*región*.rolesanywhere
Amazon Inspector	com.amazonaws.*region*.inspector2
AWS IoT Core	com.amazonaws.*region*.iot.data
	com.amazonaws.*region*.iot.credentials

Servicio de AWS	Nombre del servicio
	com.amazonaws.*región*.iot.fleethub.api
AWS IoT Core Device Advisor	com.amazonaws.*region*.deviceadvisor.iot
AWS IoT Core para LoRaWAN	com.amazonaws.*region*.iotwireless.api
	com.amazonaws.*region*.lorawan.cups
	com.amazonaws.*region*.lorawan.lns
AWS IoT FleetWise	com.amazonaws.*región*.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
AWS Lake Formation	com.amazonaws.*region*.lakeformation

Servicio de AWS	Nombre del servicio
AWS Lambda	com.amazonaws.*region*.lambda
Amazon Lex	com.amazonaws.*region*.models-v2-lex
	com.amazonaws.*region*.runtime-v2-lex
AWS License Manager	com.amazonaws.*region*.license-manager
	com.amazonaws.*region*.license-manager-fips
	com.amazonaws.*region*.license-manager-user-subscriptions
Amazon Lookout for Equipment	com.amazonaws.*region*.lookoutequipment
Amazon Lookout for Metrics	com.amazonaws.*region*.lookoutmetrics
Amazon Lookout for Vision	com.amazonaws.*region*.lookoutvision
Amazon Macie	com.amazonaws.*region*.macie2
AWS Mainframe Modernization	com.amazonaws.*region*.m2
Amazon Managed Blockchain	com.amazonaws.*region*.managedblockchain-query
	com.amazonaws.*region*.managedblockchain.bitcoin.mainnet
	com.amazonaws.*region*.managedblockchain.bitcoin.testnet
Servicio administrado por Amazon para Prometheus	com.amazonaws.*region*.aps
	com.amazonaws.*region*.aps-workspaces
Flujo de trabajo administrado de Amazon para Apache Airflow	com.amazonaws.*region*.airflow.api
	com.amazonaws.*region*.airflow.env

Servicio de AWS	Nombre del servicio
	com.amazonaws.*region*.airflow.ops
AWS Management Console	com.amazonaws.*region*.console
	com.amazonaws.*region*.signin
Amazon MemoryDB para Redis	com.amazonaws.*region*.memory-db
	com.amazonaws.*region*.memorydb-fips
Orquestador de AWS Migration Hub	com.amazonaws.*region*.migrationhub-orchestrator
AWS Migration Hub Refactor Spaces	com.amazonaws.*region*.refactor-spaces
Recomendaciones de estrategias de Migration Hub	com.amazonaws.*region*.migrationhub-strategy
Análisis de Amazon Neptune	com.amazonaws.*region*.neptune-graph
Amazon Nimble Studio	com.amazonaws.*region*.nimble
OpenSearch Servicio Amazon	Estos puntos de conexión se administran mediante servicios
AWS Organizations	com.amazonaws. *región. organizaciones*
	com.amazonaws. *region .organizations-fips*
AWS Outposts	com.amazonaws. *región. puestos de avanzada*
AWS Panorama	com.amazonaws.*region*.panorama
AWS Criptografía de pagos	com.amazonaws.*región*.payment-cryptography.controlplane
	com.amazonaws.*región*.payment-cryptography.dataplane
Amazon Personalize	com.amazonaws.*región*.personalize

Servicio de AWS	Nombre del servicio
	com.amazonaws.*región*.personalize-events
	com.amazonaws.*región*.personalize-runtime
AWS Supply Chain	com.amazonaws. *región: .scn*
Amazon Pinpoint	com.amazonaws.*region*.pinpoint
	com.amazonaws.*region*.pinpoint-sms-voice-v2
Amazon Polly	com.amazonaws.*region*.polly
AWS 5G privado	com.amazonaws.*region*.private-networks
AWS Private Certificate Authority	com.amazonaws.*region*.acm-pca
	com.amazonaws.*region*.pca-connector-ad
AWS Proton	com.amazonaws.*region*.proton
Amazon Q Business	aws.api. *región. qbusiness*
Amazon QLDB	com.amazonaws.*region*.qldb.session
Amazon QuickSight	com.amazonaws. *region .quicksight-website*
Amazon RDS	com.amazonaws.*region*.rds
API de datos de Amazon RDS	com.amazonaws.*region*.rds-data
AWS Re:Post Private	com.amazonaws. *region .repostspace*
Amazon Redshift	com.amazonaws.*region*.redshift
	com.amazonaws.*region*.redshift-fips
API de datos de Amazon Redshift	com.amazonaws.*region*.redshift-data
	com.amazonaws. *región .redshift-data-fips*

Servicio de AWS	Nombre del servicio
Amazon Rekognition	com.amazonaws.*region*.rekognition
	com.amazonaws.*region*.rekognition-fips
	com.amazonaws.*region*.streaming-rekognition
	com.amazonaws.*region*.streaming-rekognition-fips
AWS RoboMaker	com.amazonaws.*region*.robomaker
Amazon S3	com.amazonaws.*region*.s3
Puntos de acceso multirregión de Amazon S3	com.amazonaws.s3-global.accesspoint
Amazon S3 en Outposts	com.amazonaws.*region*.s3-outposts
Amazon SageMaker	aws.sagemaker.*region*.notebook
	aws.sagemaker.*region*.studio
	com.amazonaws.*region*.sagemaker.api
	com.amazonaws.*region*.sagemaker.featurestore-runtime
	com.amazonaws.*region*.sagemaker.metrics
	com.amazonaws.*region*.sagemaker.runtime
	com.amazonaws.*region*.sagemaker.runtime-fips
AWS Secrets Manager	com.amazonaws.*region*.secretsmanager
AWS Security Hub	com.amazonaws.*region*.securityhub
AWS Security Token Service	com.amazonaws.*region*.sts
Service Catalog	com.amazonaws.*region*.servicecatalog

Servicio de AWS	Nombre del servicio
	com.amazonaws.*region*.servicecatalog-appregistry
Amazon SES	com.amazonaws.*region*.email-smtp
AWS SimSpace Weaver	com.amazonaws.*region*.simspaceweaver
AWS Snow Device Management	com.amazonaws.*region*.snow-device-management
Amazon SNS	com.amazonaws.*region*.sns
Amazon SQS	com.amazonaws.*region*.sqs
Amazon SWF	com.amazonaws.*region*.swf
	com.amazonaws.*region*.swf-fips
AWS Step Functions	com.amazonaws.*region*.states
	com.amazonaws.*region*.sync-states
AWS Storage Gateway	com.amazonaws.*region*.storagegateway
AWS Systems Manager	com.amazonaws.*region*.ec2messages
	com.amazonaws.*region*.ssm
	com.amazonaws.*region*.ssm-contacts
	com.amazonaws.*region*.ssm-incidents
	com.amazonaws.*region*.ssmmessages
AWS Creador de redes de telecomunicaciones	com.amazonaws.*region*.tnb
Amazon Textract	com.amazonaws.*region*.textract
	com.amazonaws.*region*.textract-fips
Amazon Timestream	com.amazonaws.*region*.timestream.ingest-*cell*

Servicio de AWS	Nombre del servicio
	com.amazonaws.*region*.timestream.query-*cell*
Amazon Timestream para InfluxDB	com.amazonaws. *región* .*timestream-influxdb*
Amazon Transcribe	com.amazonaws.*region*.transcribe
	com.amazonaws.*region*.transcribestreaming
Amazon Transcribe Medical	com.amazonaws.*region*.transcribe
	com.amazonaws.*region*.transcribestreaming
AWS Transfer for SFTP	com.amazonaws.*region*.transfer
	com.amazonaws.*region*.transfer.server
Amazon Translate	com.amazonaws.*region*.translate
AWS Trusted Advisor	com.amazonaws.*region*.trustedadvisor
Amazon Verified Permissions	com.amazonaws.*region*.verifiedpermissions
Amazon VPC Lattice	com.amazonaws.*region*.vpc-lattice
Amazon WorkSpaces	com.amazonaws.*region*.workspaces
Amazon WorkSpaces Thin Client	com.amazonaws. *región* .*thinclient.api*
AWS X-Ray	com.amazonaws.*region*.xray

Ver los nombres de los Servicio de AWS disponibles

Puede utilizar el comando describe-vpc-endpoint-services para ver los nombres de servicio que admiten puntos de enlace de la VPC.

El siguiente ejemplo muestra los puntos finales de la interfaz Servicios de AWS compatibles 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 de la salida:

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.s3-global.accesspoint",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    ...
]
```

Ver información sobre un servicio

Después de tener el nombre del servicio, puede usar el comando describe-vpc-endpoint-services para ver información detallada sobre cada servicio de punto de conexión.

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

Ver la compatibilidad con las políticas de puntos de conexión

Para comprobar si un servicio es compatible con las políticas de punto de conexión, accione el comando describe-vpc-endpoint-services 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 los 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.

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.sagemaker.us-east-1.notebook",
    "aws.sagemaker.us-east-1.studio",
    "com.amazonaws.s3-global.accesspoint",
    "com.amazonaws.us-east-1.access-analyzer",
    "com.amazonaws.us-east-1.account",
    ...
]
```

En el siguiente ejemplo, se enumeran las Servicios de AWS que no admiten 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.

```
[
    "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.cleanrooms",
    "com.amazonaws.us-east-1.cleanrooms-ml",
    "com.amazonaws.us-east-1.cloudtrail",
    "com.amazonaws.us-east-1.codeguru-profiler",
    "com.amazonaws.us-east-1.codeguru-reviewer",
    "com.amazonaws.us-east-1.codepipeline",
    "com.amazonaws.us-east-1.codewhisperer",
    "com.amazonaws.us-east-1.datasync",
    "com.amazonaws.us-east-1.datazone",
    "com.amazonaws.us-east-1.deadline.management",
    "com.amazonaws.us-east-1.deadline.scheduling",
    "com.amazonaws.us-east-1.deviceadvisor.iot",
    "com.amazonaws.us-east-1.eks",
    "com.amazonaws.us-east-1.elastic-inference.runtime",
    "com.amazonaws.us-east-1.email-smtp",
    "com.amazonaws.us-east-1.grafana-workspace",
    "com.amazonaws.us-east-1.iot.credentials",
    "com.amazonaws.us-east-1.iot.data",
    "com.amazonaws.us-east-1.iotwireless.api",
    "com.amazonaws.us-east-1.lorawan.cups",
    "com.amazonaws.us-east-1.lorawan.lns",
    "com.amazonaws.us-east-1.macie2",
    "com.amazonaws.us-east-1.neptune-graph",
    "com.amazonaws.us-east-1.nimble",
    "com.amazonaws.us-east-1.organizations",
    "com.amazonaws.us-east-1.outposts",
    "com.amazonaws.us-east-1.pipes-data",
    "com.amazonaws.us-east-1.redshift-data",
    "com.amazonaws.us-east-1.redshift-data-fips",
    "com.amazonaws.us-east-1.refactor-spaces",
    "com.amazonaws.us-east-1.sagemaker.runtime-fips",
    "com.amazonaws.us-east-1.storagegateway",
    "com.amazonaws.us-east-1.transfer",
```

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

Ver compatibilidad con IPv6

Puede usar el siguiente comando describe-vpc-endpoint-services para ver las regiones a las Servicios de AWS que puede acceder a través de 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 de la salida:

```
[
    "aws.api.us-east-1.kendra-ranking",
    "aws.api.us-east-1.qbusiness",
    "com.amazonaws.us-east-1.athena",
    "com.amazonaws.us-east-1.data-servicediscovery",
    "com.amazonaws.us-east-1.data-servicediscovery-fips",
    "com.amazonaws.us-east-1.eks-auth",
    "com.amazonaws.us-east-1.glue",
    "com.amazonaws.us-east-1.lakeformation",
    "com.amazonaws.us-east-1.quicksight-website",
    "com.amazonaws.us-east-1.s3-outposts",
    "com.amazonaws.us-east-1.servicediscovery",
    "com.amazonaws.us-east-1.servicediscovery-fips",
    "com.amazonaws.us-east-1.timestream-influxdb"
]
```

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 Acceder 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.
- Para habilitar IPv6 en 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 de puntos finales que permita el tráfico esperado de los recursos de la VPC. Por ejemplo, para asegurarse de que AWS CLI puede enviar solicitudes HTTPS a la Servicio de AWS, el grupo de seguridad debe permitir el tráfico HTTPS entrante.
- Si los recursos se encuentran en una subred con una ACL de red, compruebe que la ACL de red permita el tráfico entre los recursos de la VPC y las interfaces de red del punto final.
- Hay cuotas en sus recursos. AWS PrivateLink Para obtener más información, consulte AWS PrivateLink cuotas.

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 Categoría de servicios, elija Servicios de AWS.
5. En Nombre del servicio, seleccione el servicio. Para obtener más información, consulte the section called “Servicios que se integran”.
6. En VPC, seleccione la VPC desde la que accederá al Servicio de AWS.
7. 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.
8. En Subredes, seleccione una subred por zona de disponibilidad desde la que tendrá acceso al Servicio de AWS. No puede seleccionar varias subredes de la misma zona de disponibilidad. Para obtener más información, consulte the section called “Subredes y zonas de disponibilidad”.

   Crearemos una interfaz de red de punto de conexión en cada subred seleccionada. 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 puntos de conexión, seleccione Designar direcciones IP e introduzca una dirección IPv4 del rango de direcciones de la subred. Si el servicio del punto de conexión admite IPv6, también puede introducir una dirección IPv6 del rango de direcciones de la subred. Ten 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 puedes especificarlas para las interfaces de red de los terminales.

9. En IP address type (Tipo de dirección IP), elija entre las siguientes opciones:

   - 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 y el servicio acepta solicitudes 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 solo subredes IPv6 y el servicio acepta solicitudes 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 y el servicio acepta solicitudes IPv4 e IPV6.

10. En Security groups (Grupos de seguridad), seleccione los grupos de seguridad para asociarlas a las interfaces de red del punto de conexión para el punto de conexión de VPC. Por defecto, asociamos el grupo de seguridad predeterminado para la VPC.
11. 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. De lo contrario, seleccione 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. 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.
12. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
13. Seleccione 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.

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 puntos de conexión, seleccione Designar direcciones IP e introduzca una dirección IPv4 del rango de direcciones de la subred. Si el servicio del punto de conexión admite IPv6, también puede introducir una dirección IPv6 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 los nombres DNS privados para los puntos de conexión de la VPC. 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. Seleccione 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 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 ha creado 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-notification (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.

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

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.

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

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 puntos de enlace de puerta de enlace y puntos de enlace de interfaz. Para ver una comparación de las opciones, consulte lo siguiente:

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

Precios

El uso de puntos de enlace de gateway no supone ningún cargo adicional.

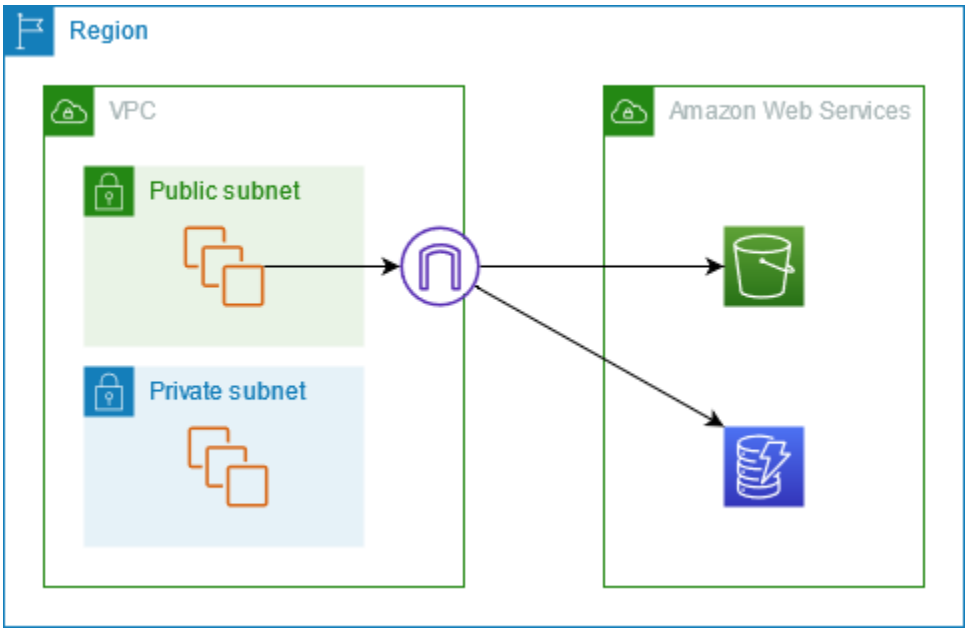
Contenido

Información 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.

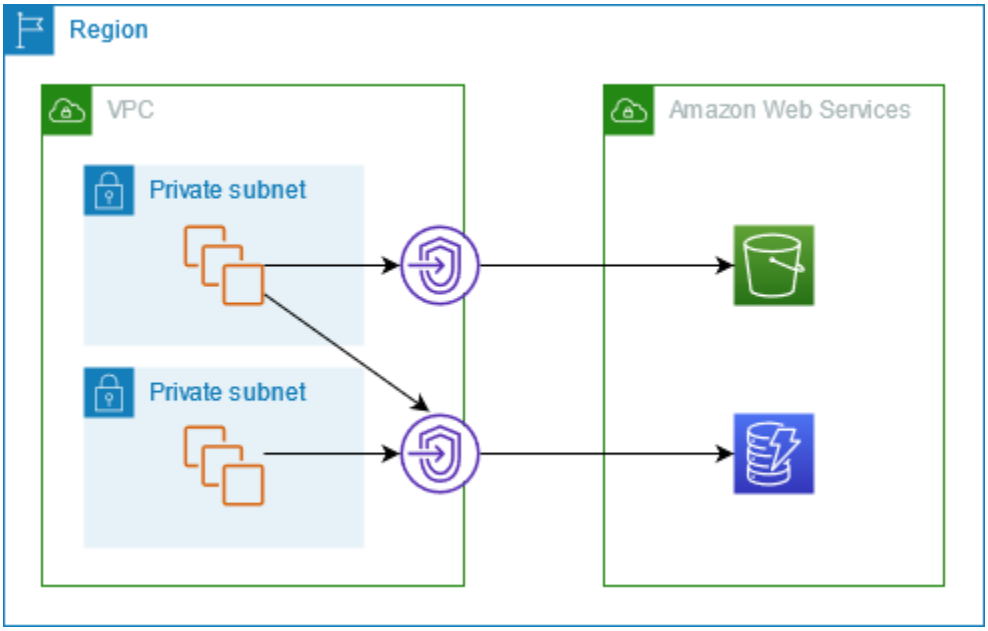
Acceso mediante una puerta de enlace de Internet

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	Objetivo
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

Las ACL de la red de las subredes de estas instancias también deben 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

Puntos de enlace de gateway 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 enlace de gateway 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 de puerta de enlace no permiten el acceso desde redes locales, desde VPC interconectadas 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 para Amazon S3 en la Guía del usuario de Amazon S3.

Contenido

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 acceso a buckets que contienen archivos de registro o puede requerir que descargue controladores o agentes a sus instancias de EC2. Si es así, asegúrese de que su 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`. O bien, puede usar tablas de enrutamiento para controlar qué instancias de EC2 pueden acceder a Amazon S3 a través del punto de conexión de VPC.
- Los puntos de conexión de la puerta de enlace solo son compatibles con el tráfico IPv4.
- Las direcciones IPv4 de origen de las instancias de las subredes afectadas según lo recibido por Amazon S3 cambian de direcciones IPv4 públicas a direcciones IPv4 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 IPv4 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 AWS 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.

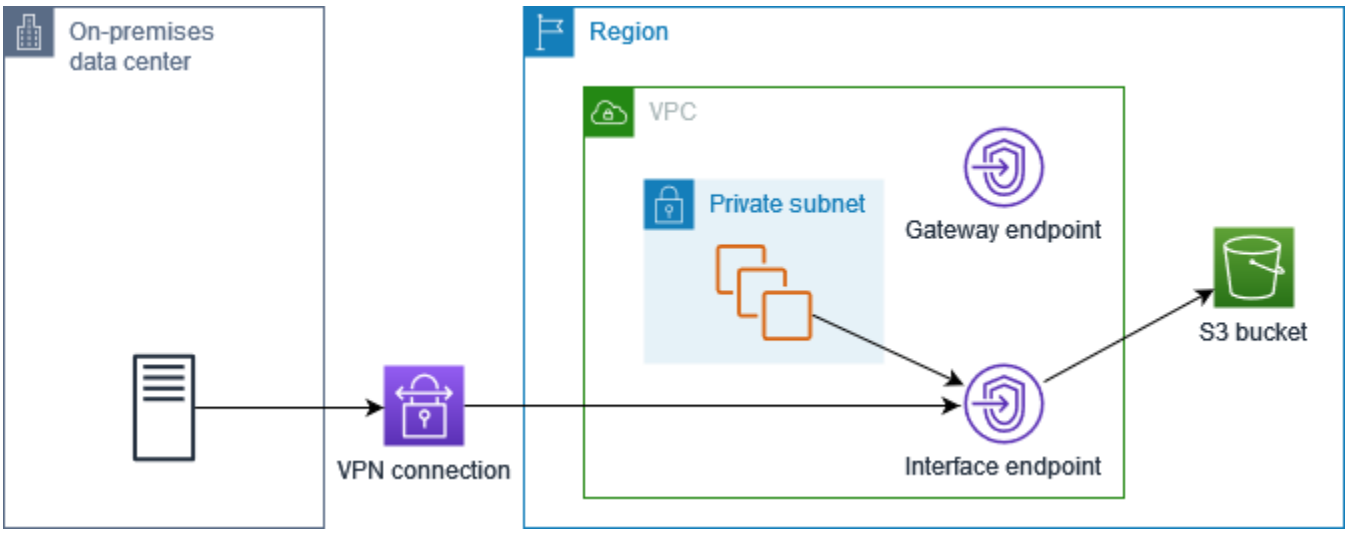
Route 53 Resolver

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.

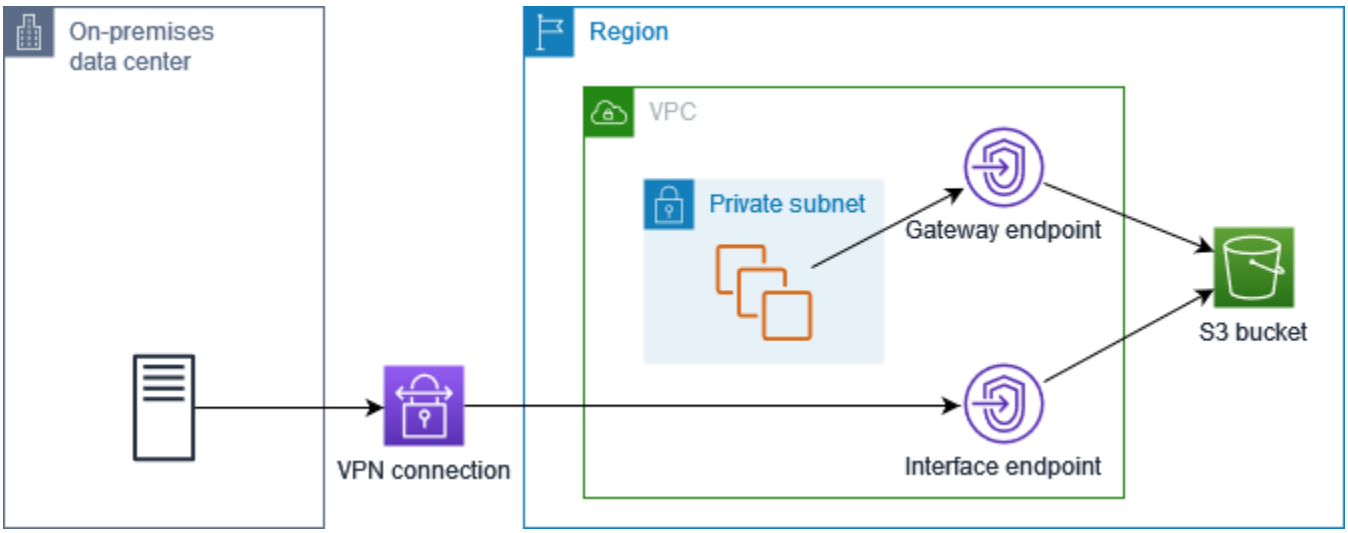
DNS privado

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.



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. En Servicios, añada el filtro Type = Gateway y seleccione com.amazonaws. ***región s.s3.***
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. Seleccione 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, VPC, rangos de direcciones IP específicos 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 AWS Management Console.

```
{
  "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 para restringir el acceso a VPC específicas 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 AWS Management Console.

```
{
  "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

Puedes crear una política que restrinja el acceso a intervalos de direcciones IP específicos mediante la clave de condición aws: VpcSource Ip. 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 AWS Management Console.

```
{
  "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.

```
{
  "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. 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.

```
{
  "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.

```
{
  "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.

```
{
```

```
  "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 enlace de gateway no supone ningún cargo adicional.

DynamoDB admite puntos finales de puerta de enlace y puntos finales de interfaz. Con un punto de enlace de puerta de enlace, puede acceder a DynamoDB desde su VPC, sin necesidad de una puerta de enlace a Internet o un dispositivo NAT para su VPC y sin coste adicional. Sin embargo, los puntos de enlace de enlace no permiten el acceso desde redes locales, desde VPC interconectadas 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 enlace de VPC para DynamoDB en la Guía para desarrolladores de Amazon DynamoDB.

Contenido

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 EC2 de 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 conexión de la puerta de enlace solo son compatibles con el tráfico IPv4.
- Las direcciones IPv4 de origen de las instancias de las subredes afectadas cambiarán de direcciones IPv4 públicas a direcciones IPv4 privadas desde la VPC. Un punto de enlace cambia las rutas de red y desconecta las conexiones TCP abiertas. Las conexiones anteriores que utilizaban direcciones IPv4 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 AWS 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. Seleccione 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.

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

```
   "Statement": [
      {
         "Sid": "Allow-access-from-specific-endpoint",
         "Effect": "Deny",
         "Action": "dynamodb:*",
         "Resource": "arn:aws:dynamodb:region:account-id: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.

```
{
   "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.

```
{
   "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. 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 los productos SaaS a través de AWS PrivateLink

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

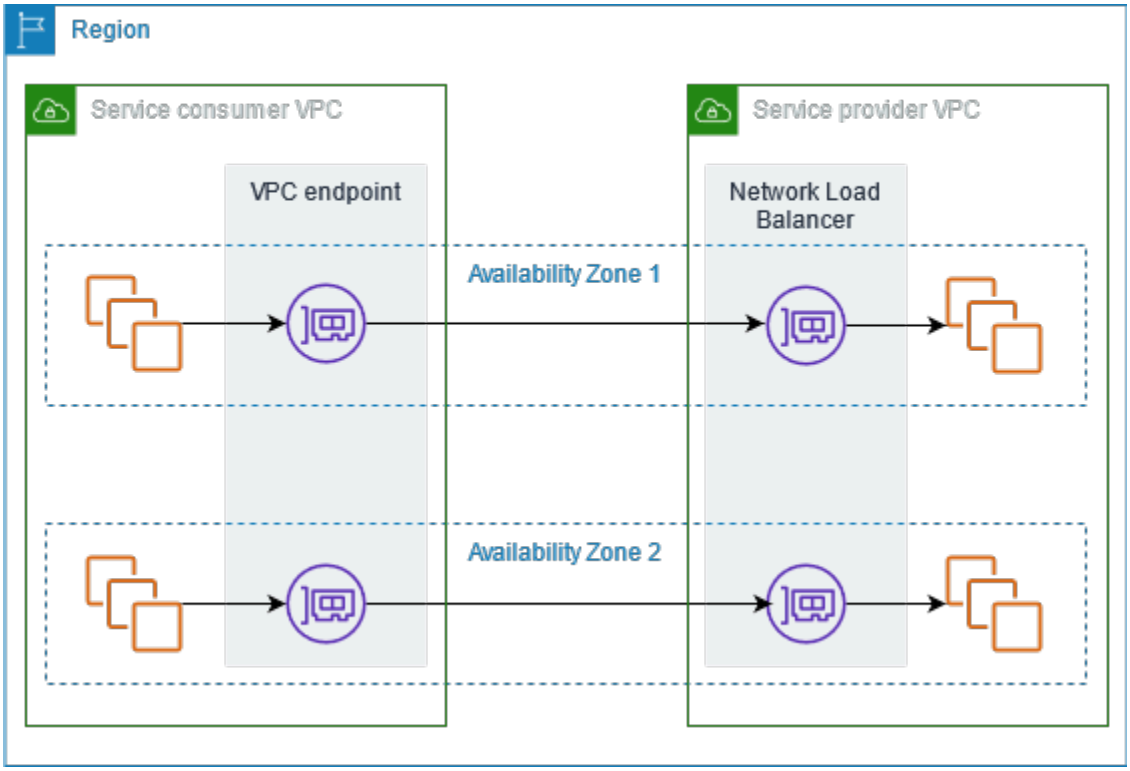
Contenido

Información general

Puede descubrir, comprar y aprovisionar productos SaaS con la tecnología de Through. AWS PrivateLink AWS Marketplace Para obtener más información, consulte AWS Marketplace: - PrivateLink.

También puede encontrar productos SaaS AWS PrivateLink impulsados AWS por socios. 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 ha adquirido el servicio en AWS Marketplace, haga lo siguiente:
    a. En Service category (Categoría de servicios), elija AWS Marketplace Services (Servicios de AWC).
    b. Ingrese el nombre del servicio.

5. Si se ha suscrito a un servicio con la designación de listo para el AWS servicio, haga lo siguiente:

   a. En la categoría de servicio, elija los servicios asociados de PrivateLink Ready.

   b. Ingrese el nombre del servicio y elija Verify service (Verificar servicio).

6. En VPC, seleccione la VPC desde la que accederá al producto.
7. En Subnets (Subredes), seleccione una subred por zona de disponibilidad desde la que accederá al producto.
8. En Grupo de seguridad, seleccione los grupos de seguridad que deban asociarse a las interfaces de red de 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. Seleccione 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”.

Acceda a los 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 que se aprovisione su punto final de Gateway Load Balancer en cada zona de disponibilidad. También se le factura por GB de datos procesados. Para obtener más información, consulte AWS PrivateLink Precios.

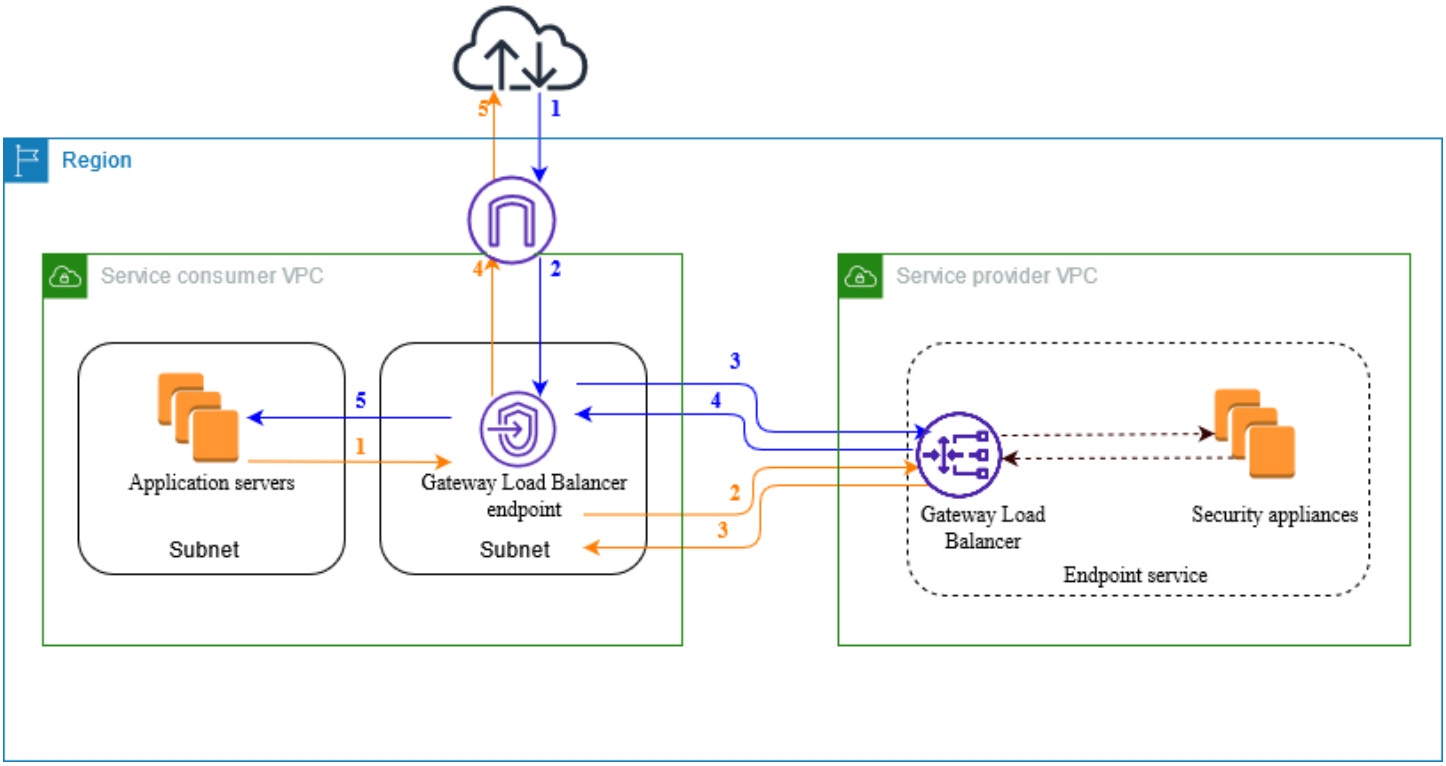
Contenido

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

Información general

El siguiente diagrama muestra cómo los servidores de aplicaciones acceden a los dispositivos de seguridad a través AWS PrivateLink de ellos. 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. Tenga en cuenta que 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*
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 impulsado por AWS PrivateLink, conocido como servicio de punto final. Usted es el proveedor del servicio y AWS los principales responsables de crear 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 los ID de AZ en la Guía del usuario de Amazon EC2.
- Hay cuotas en sus AWS PrivateLink recursos. Para obtener más información, consulte AWS PrivateLink cuotas.

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”.

AWS los principales pueden conectarse a su servicio de puntos finales de forma privada mediante la creación de un punto final de Gateway Load Balancer. Para obtener más información, consulte Creación de un punto de enlace 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 final es una interfaz de red administrada por el solicitante; puede verla en la suya 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 los 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.
- Hay cuotas en sus AWS PrivateLink recursos. Para obtener más información, consulte AWS PrivateLink cuotas.

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 Service category (Categoría del servicio), elija Other endpoint services (Otros servicios de punto de conexión).
5. En Service name (Nombre del servicio), ingrese el nombre del servicio y luego elija Verify service (Comprobar servicio).
6. En VPC, seleccione la VPC en la que desea crear el punto de conexión.
7. En Subnets (Subredes), seleccione la subred en la cual crear el punto de conexión.
8. En IP address type (Tipo de dirección IP), elija entre las siguientes opciones:
   - 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.
9. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
10. Seleccione 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-EC2Tagy 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)

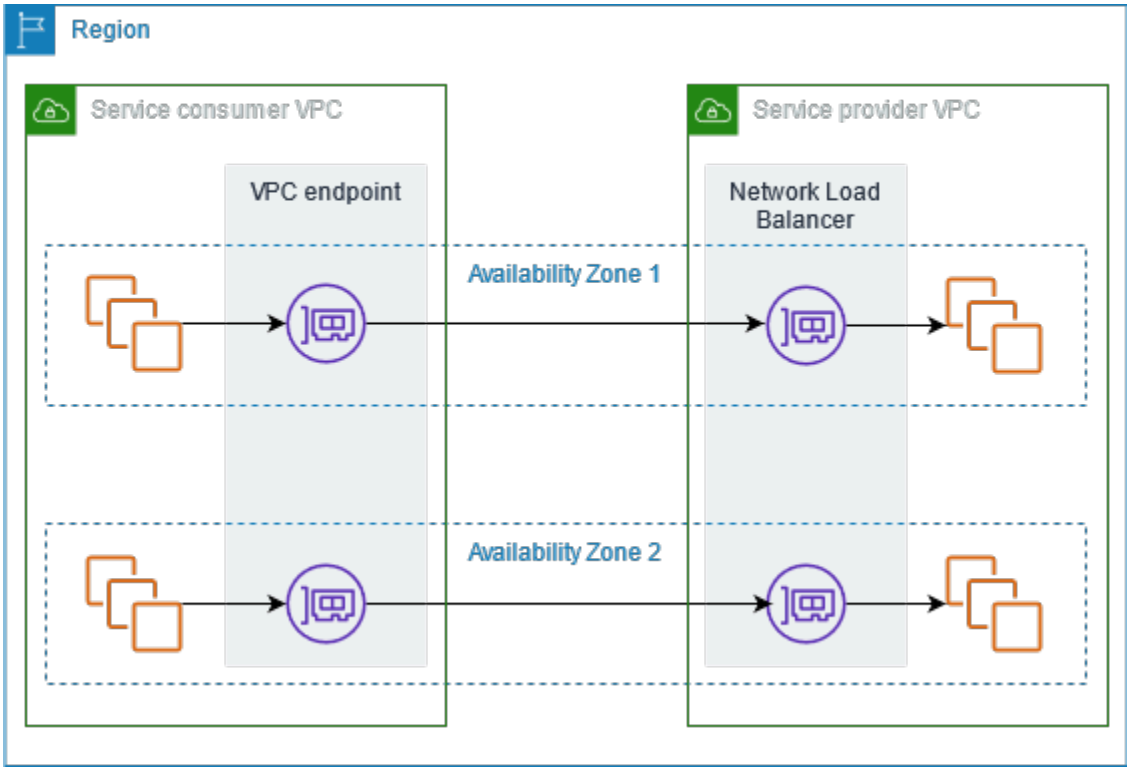
Comparta sus servicios a través de AWS PrivateLink

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

Contenido

Información 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 la 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.region.vpce.amazonaws.com
```

Los nombres de zona tienen la siguiente sintaxis:

```
endpoint_id-zone.endpoint_service_id.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.

Tipos de direcciones IP

Los proveedores de servicios pueden poner sus puntos de conexión de servicios a disposición de consumidores de servicios mediante IPv4, IPv6 o tanto IPv4 como IPv6, incluso si los servidores de backend 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 VPC de interfaz admite IPv4, las interfaces de red del punto de conexión tienen direcciones IPv4. Si un punto de conexión de VPC de interfaz 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.
- 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 direcciones IP de origen del encabezado Proxy Protocol versión 2, debe procesar direcciones IPv6.

Requisitos para habilitar IPv6 para un punto de conexión de interfaz

- El servicio de punto de conexión debe admitir solicitudes de IPv6.
- 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: 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.

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: se crean registros A para los nombres de DNS privados, regionales y de zonas. El tipo de dirección IP debe ser IPv4 o Dualstack.
- IPv6: se crean registros AAAA para los nombres de DNS privados, regionales y de zonas. El tipo de dirección IP debe ser IPv6 o Dualstack.
- 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 con tecnología de 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. Puede acceder al servicio de punto de conexión desde otras regiones mediante el emparejamiento de VPC.
- Un servicio de punto de conexión admite tráfico solo a través de TCP.
- 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 los ID de AZ en la Guía del usuario de Amazon EC2.
- 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 habilita el Proxy Protocol en el equilibrador de carga, puede obtener las direcciones de los consumidores del servicio y los ID de los puntos de conexión de interfaz del encabezado Proxy Protocol. Para obtener más información, consulte Proxy Protocol en la Guía del usuario de 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 AWS PrivateLink recursos. Para obtener más información, consulte AWS PrivateLink cuotas.

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 permitir que los consumidores de servicios creen puntos de conexión de VPC de interfaz IPv6 para el servicio de punto de conexión, la VPC y las subredes deben tener bloques de CIDR IPv6 asociados.
- 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 Network Load Balancer 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 entrante. AWS PrivateLink Para obtener más información, consulte los grupos de seguridad en la Guía del usuario de los balanceadores de carga de red.
- Para permitir que el servicio de punto de conexión acepte solicitudes de IPv6, los equilibradores de carga de red deben utilizar el tipo de dirección IP dualstack. 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 direcciones IP de origen del encabezado Proxy Protocol versión 2, verifique que pueda procesar direcciones IPv6.
- 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 los balanceadores 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 Available load balancers (Balanceadores de carga disponibles), seleccione los balanceadores de carga de red que desea asociar con el servicio de punto de enlace. Las zonas de disponibilidad incluidas muestran las zonas de disponibilidad que están habilitadas para los balanceadores de carga de red seleccionados. Su servicio de punto final estará disponible en estas zonas de disponibilidad.
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, estas solicitudes se aceptan de forma automática.
7. 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 del servicio 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.
8. 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.

9. (Opcional) Para agregar una etiqueta, elija Add new tag (Agregar etiqueta nueva) e ingrese la clave y el valor de la etiqueta.
10. 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 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 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”.

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 Service category (Categoría del servicio), elija Other endpoint services (Otros servicios de punto de conexión).
5. En Service name (Nombre del servicio), ingrese el nombre del servicio (por ejemplo, `com.amazonaws.vpce.us-east-1.vpce-svc-0e123abc123198abc`), y elija Verify service (Verificar servicio).
6. En VPC, seleccione la VPC en la que se va a crear el punto de conexión.
7. En Subnets (Subredes), seleccione las subredes (zonas de disponibilidad) desde las que se accederá al servicio de punto de conexión.
8. En IP address type (Tipo de dirección IP), elija entre las siguientes opciones:

   - 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 y el servicio de punto de conexión acepta solicitudes 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 solo subredes IPv6 y el servicio de punto de conexión acepta solicitudes 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 y el servicio de punto de conexión acepta solicitudes IPv4 e IPv6.
9. En DNS record IP type (Tipo de IP del registro DNS), elija entre las siguientes opciones:

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

10. En Grupo de seguridad, seleccione los grupos de seguridad que deban asociarse a las interfaces de red de punto de conexión.
11. Seleccione 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
- Aceptación o rechazo de solicitudes de conexión
- Administra los balanceadores de carga
- Asociación de un nombre de DNS privado
- Modificación de los tipos de direcciones IP compatibles
- Administración de etiquetas

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 las ARN de entidades principales de AWS .

ARN para los directores AWS

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

arn:aws:iam::*account_id*:root

Rol

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

Usuario

arn:aws:iam::*account_id*:user/*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, no afectará a las conexiones existentes entre el punto final 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-permissions (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.

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”.

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 rechaza una solicitud que ya se ha aceptado, esto no afecta a la conexión entre el punto final y el servicio.

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. Seleccione Save changes (Guardar cambios)

Para modificar la configuración de aceptación con la línea de comandos

- modify-vpc-endpoint-service-configuration (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-connections o reject-vpc-endpoint-connections (AWS CLI)
- Approve-EC2EndpointConnectiono Deny-EC2EndpointConnection(Herramientas para Windows PowerShell)

Administra los balanceadores de carga

Puede administrar los equilibradores de carga que están asociados a su servicio de punto final. 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 un Network Load Balancer, también puede habilitar la zona de disponibilidad para su servicio de punto final. Tras habilitar una zona de disponibilidad para

el servicio de puntos finales, los consumidores del servicio pueden añadir una subred de esa zona de disponibilidad a los puntos finales de la VPC de su interfaz.

Para administrar los balanceadores de carga de su servicio de punto final 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), Associate or disassociate load balancers (Asociar o desasociar equilibradores de carga).
5. Cambie la configuración del servicio de puntos finales según sea necesario. Por ejemplo:
   - Seleccione la casilla de verificación de un equilibrador de carga para asociarlo al servicio de puntos finales.
   - Desactive la casilla de verificación de un balanceador de cargas para desasociarlo del servicio de punto final. Debe mantener seleccionado al menos un equilibrador de carga.
   - Si has activado recientemente otra zona de disponibilidad para tu balanceador de cargas, aparecerá en Zonas de disponibilidad incluidas. Si guardas los cambios en el siguiente paso, se habilita el servicio de punto final para la nueva zona de disponibilidad.
6. Seleccione Save changes (Guardar cambios)

Para administrar los equilibradores de carga de su servicio de puntos finales mediante la línea de comandos

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

Para habilitar el servicio de punto final en una zona de disponibilidad que se habilitó recientemente para el balanceador de cargas, simplemente ejecute el comando con el ID del servicio de punto final.

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. Seleccione Save changes (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-configuration (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)

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 el servicio de punto de conexión acepte solicitudes de IPv6, los equilibradores de carga de red deben utilizar el tipo de dirección IP dualstack. 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: 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.
6. Seleccione Save changes (Guardar cambios).

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

- modify-vpc-endpoint-service-configuration (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 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 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 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 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. Cuando el proveedor de un servicio utiliza un nombre de DNS público existente como el nombre de DNS privado del servicio de punto de conexión, los consumidores del servicio no necesitan cambiar ninguna aplicación que utilice el nombre de DNS público existente. 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.
- No debe crear un registro A para el nombre de DNS privado, de modo que solo los servidores de la VPC del consumidor del servicio puedan resolver el nombre de DNS privado.
- Los nombres de DNS privados no son compatibles con los puntos de conexión del equilibrador de carga de puerta de enlace.
- 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 un máximo de 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.

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 AWS Management Console. 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.

Nombre	Tipo	Valor
_6e86v84tqgqubxbwi i1m.example.com	TXT	vpce:L6P0E 45jevfWOCP RxlTt

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. Use los siguientes valores:

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

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
Cloudflare	Administrar registros DNS
HostGator	Administre los registros DNS con /eNOM HostGator
Namecheap	¿Cómo agrego registros TXT/SPF/DKIM/DMARC 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 nslookup comando, que está disponible para Windows y Linux.

Consultarás los servidores DNS que sirven a tu dominio porque esos servidores contienen la mayor parte de la 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. Verifique que el registro TXT se publica correctamente mediante el siguiente comando, donde *name_server* es uno de los servidores de nombres que encontró 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 ha creado 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-notification (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.

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

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.

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

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-configurations (AWS CLI)
- Remove-EC2EndpointServiceConfiguration(Herramientas para Windows PowerShell)

Gestión 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 ayudarlo 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.

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como usuario de IAM o asumiendo una función de IAM. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte Firmar las solicitudes de la AWS API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS IAM Identity Center y Uso de la autenticación multifactor (MFA) en AWSen la Guía del usuario de IAM.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como 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, incluidos los que requieren acceso de administrador, 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 de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. 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 propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente una función de IAM en el AWS Management Console cambiando de función. Puede asumir un rol llamando a una operación de AWS API AWS CLI o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del usuario de IAM. Si utiliza IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un usuario o un rol de IAM para realizar acciones en ellas AWS, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los

permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

- Rol de servicio: un rol de servicio es un rol de IAM que adopta 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.
- Función vinculada al servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada 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.

- Aplicaciones que se ejecutan en Amazon EC2: puede usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una instancia EC2 y realizan AWS CLI solicitudes a la API. AWS Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar una AWS función a una instancia EC2 y ponerla a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del usuario de IAM.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre

la estructura y el contenido de los documentos de política JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

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.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

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.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS empresa. Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para más información sobre cómo elegir una política administrada o una política insertada, consulte Elegir 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 política JSON que se asocian a un recurso. 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

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.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios que admiten las ACL. AWS WAF Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): las SCP son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y gestionar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o a todas sus cuentas. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas

las de cada una. Usuario raíz de la cuenta de AWS Para obtener más información acerca de Organizations y las SCP, consulte Funcionamiento de las SCP en la Guía del usuario de AWS Organizations .

- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para 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 AWS determinar 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

Funciones de IAM que puede utilizar con 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
ACL	No

Característica de IAM	AWS PrivateLink soporte
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. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para 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 dentro de 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. 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. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para más información, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos 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

Admite acciones de política	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. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

AWS PrivateLink comparte su espacio de nombres de API con Amazon EC2. Las acciones políticas AWS PrivateLink utilizan el siguiente prefijo antes de la acción:

```
ec2
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
]
```

Puede utilizar caracteres comodín (*) para especificar varias acciones . Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

```
"Action": "ec2:Describe*"
```

Para ver una lista de AWS PrivateLink acciones, consulte las AWS PrivateLink acciones en la referencia de la API de Amazon EC2. Para obtener más información, consulte Acciones definidas por Amazon EC2 en la Referencia de autorizaciones de servicio.

Recursos de políticas para AWS PrivateLink

Admite 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. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica

recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, 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

Admite 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` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición mediante una `OR` operación lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Las siguientes claves de condición son específicas de: AWS PrivateLink

- `ec2:VpceServiceName`
- `ec2:VpceServiceOwner`
- `ec2:VpceServicePrivateDnsName`

Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por Amazon EC2.

ACL en AWS PrivateLink

Admite las ACL	No

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL 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. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es 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

Compatible con el uso de credenciales temporales	Sí

Algunas Servicios de AWS no funcionan cuando inicias sesión con credenciales temporales. Para obtener información adicional, incluida información sobre cuáles Servicios de AWS funcionan con credenciales temporales, consulta Cómo Servicios de AWS funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en ellas AWS Management Console mediante cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accedes AWS mediante el enlace de inicio de sesión único (SSO) de tu empresa, ese proceso crea automáticamente credenciales temporales. También crea credenciales temporales de forma automática cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Permisos principales entre servicios para AWS PrivateLink

Admite Forward access sessions (FAS)	Sí

Cuando utilizas un usuario o un rol de IAM para realizar acciones en él AWS, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. 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

Compatible 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 . Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o la AWS API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM 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 formato de los ARN para cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Amazon EC2 en la Referencia de autorización de servicios.

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.

```
{
    "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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc/*",
                "arn:aws:ec2:region:account-id:security-group/*",
                "arn:aws:ec2:region:account-id:subnet/*",
                "arn:aws:ec2:region:account-id:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id: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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifyVpcEndpointServiceConfiguration",
                "ec2:CreateVpcEndpointServiceConfiguration"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id: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.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc/*",
                "arn:aws:ec2:region:account-id:security-group/*",
                "arn:aws:ec2:region:account-id:subnet/*",
                "arn:aws:ec2:region:account-id:route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateVpcEndpoint",
            "Resource": [
                "arn:aws:ec2:region:account-id:vpc-endpoint/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:VpceServiceName": [
                        "com.amazonaws.region.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 conexión 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 conexión específicos o VPC específicas.

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.

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 admite 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 finales de las puertas de enlace, el `Principal` elemento debe estar * configurado en. Para especificar un principal, utilice la clave de `aws:PrincipalArn` condición.

```
"Condition": {
    "StringEquals": {
        "aws:PrincipalArn": "arn:aws:iam::123456789012:user/endpointuser"
    }
}
```

Si especifica el principal en el siguiente formato, el acceso se concede Usuario raíz de la cuenta de AWS únicamente a los usuarios y roles de la cuenta, no a todos.

```
"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 (Guardar).

Para actualizar una política de punto de conexión mediante la línea de comandos

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

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 puerta de enlace. 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 conexione s en los estados SYN_SENT y ESTABLISHED.

Métrica	Descripción
	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 direccion es. 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`

Métrica	Descripción
`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. 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 balanceador 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 Metrics (Métricas).
3. Seleccione el espacio de nombres de AWS/PrivateLinkEndpoints.
4. Seleccione el espacio de nombres de AWS/PrivateLinkServices.

Para ver métricas mediante 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 AWS Management Console 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 enlace.
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 AWS Management Console 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, elija Delete (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 PrivateLink cuotas

En las tablas siguientes, se muestran las cuotas, antes llamadas límites, para recursos de AWS PrivateLink por región para su cuenta. A no ser que se indique lo contrario, puede solicitar un aumento de estas cuotas. Para obtener más información, consulte Solicitud de un aumento de cuota en la Guía del usuario de Service Quotas.

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.

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
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 para AWS PrivateLink

En la siguiente tabla se describen las versiones de AWS PrivateLink.

Cambio	Descripción	Fecha
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 IPv6	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	Puedes usar las reglas integradas de Contributor Insights para identificar los puntos finales específicos en los que más contribuyen a las CloudWatch AWS PrivateLink métricas.	18 de agosto de 2022
Compatibilidad con IPv6	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	11 de mayo de 2022

	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.	
CloudWatch métricas	AWS PrivateLink publica CloudWatch métricas para los puntos finales de la interfaz, los puntos finales de Gateway Load Balancer y los servicios de puntos finales.	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 acceder a los servicios AWS PrivateLink basados desde su VPC mediante nombres DNS privados.	6 de enero de 2020
Servicios de punto de conexión de la 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 finales de VPC de interfaz para Servicios de AWS	Puede crear un punto final de interfaz para conectars e a Servicios de AWS ese punto de integración 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.