Guía del usuario

AWS Direct Connect

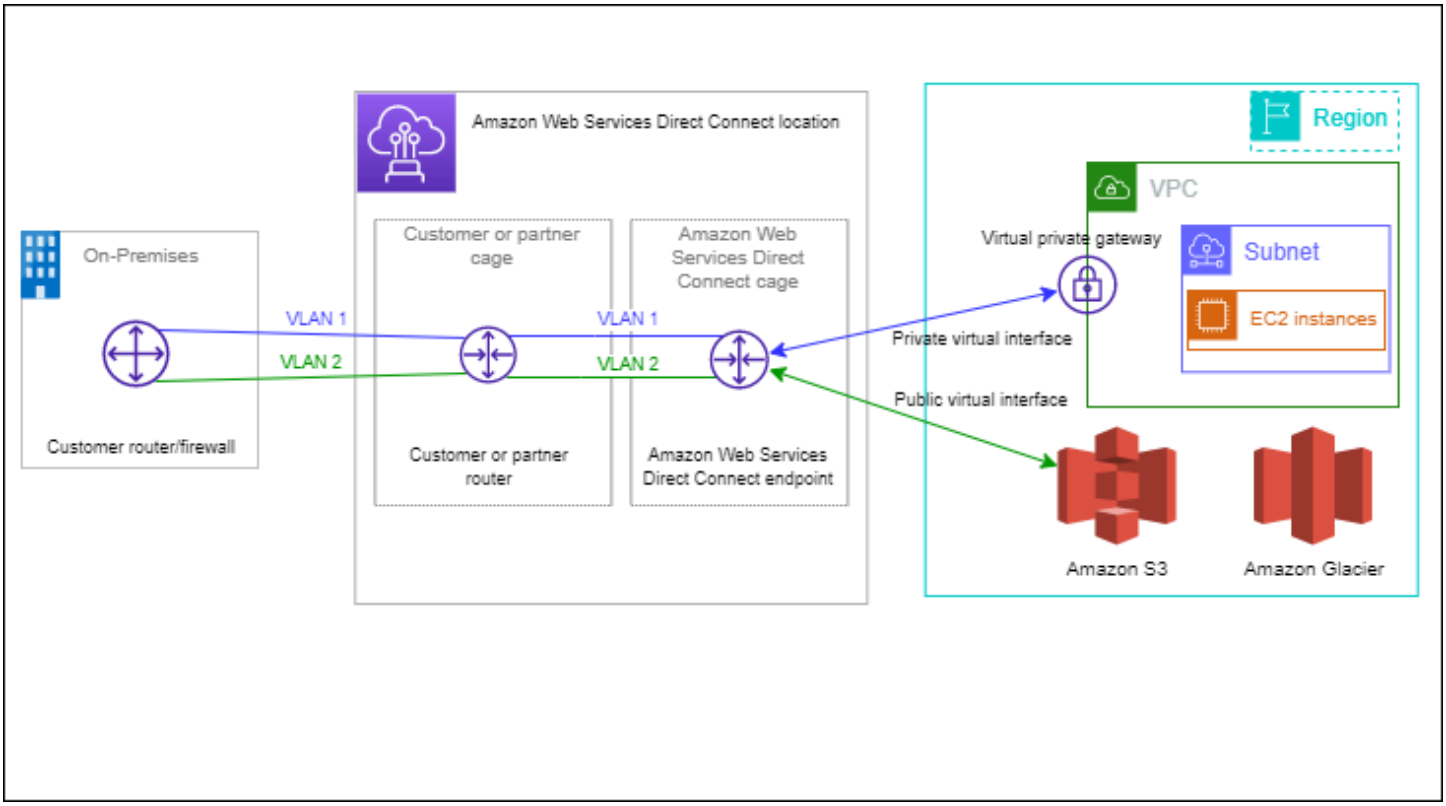
AWS Direct Connect: Guía del usuario

Table of Contents

¿Qué es AWS Direct Connect?

AWS Direct Connect conecta su red interna a una AWS Direct Connect ubicación a través de un cable Ethernet de fibra óptica estándar. Un extremo del cable se conecta a su router y el otro al router de AWS Direct Connect . Con esta conexión, puede crear interfaces virtuales directamente a los AWS servicios públicos (por ejemplo, a Amazon S3) o a Amazon VPC, sin tener en cuenta a los proveedores de servicios de Internet en su ruta de red. Una AWS Direct Connect ubicación proporciona acceso a la AWS región a la que está asociada. Puede usar una sola conexión en una región pública o AWS GovCloud (US) para acceder a los AWS servicios públicos en todas las demás regiones públicas.

El siguiente diagrama muestra una descripción general de alto nivel de cómo AWS Direct Connect interactúa con la red.



Contenido

- Acceso a una región de AWS remota
- Políticas de direccionamiento y comunidades de BGP

AWS Direct Connect componentes

Los componentes clave que se utilizan para AWS Direct Connect:

Conexiones

Cree una conexión en una AWS Direct Connect ubicación para establecer una conexión de red desde sus instalaciones a una AWS región. Para obtener más información, consulte AWS Direct Connect conexiones.

Interfaces virtuales

Cree una interfaz virtual para permitir el acceso a AWS los servicios. Una interfaz virtual pública lo habilita para acceder a servicios públicos, como Amazon S3. Una interfaz virtual privada permite el acceso a su VPC. Para obtener más información, consulte AWS Direct Connect interfaces virtuales y Requisitos previos de las interfaces virtuales.

Requisitos de red

Para usarla AWS Direct Connect en una AWS Direct Connect ubicación, la red debe cumplir una de las siguientes condiciones:

- Su red está ubicada junto a una AWS Direct Connect ubicación existente. Para obtener más información sobre AWS Direct Connect las ubicaciones disponibles, consulte los detalles del producto AWS Direct Connect.
- Está trabajando con un AWS Direct Connect socio que es miembro de la Red de AWS socios (APN). Para obtener información, consulte Socios de APN que trabajan con AWS Direct Connect.
- Está trabajando con un proveedor de servicios independientes para conectarse a AWS Direct Connect.

Además, la red debe cumplir las siguientes condiciones:

- Su red debe utilizar fibra monomodo con un transceptor 1000BASE-LX (1310 nm) para 1 gigabit Ethernet, un transceptor 10GBASE-LR (1310 nm) para 10 gigabit o un 100GBASE-LR4 para 100 gigabit Ethernet.

- La negociación automática de un puerto debe estar deshabilitada para una conexión con una velocidad de puerto superior a 1 Gbps. Sin embargo, según el punto final de AWS Direct Connect que dé servicio a su conexión, es posible que sea necesario activar o desactivar la negociación automática para las conexiones de 1 Gbps. Si la interfaz virtual permanece inactiva, consulte Solución de problemas de capa 2 (enlace de datos).
- La encapsulación de VLAN 802.1Q debe ser compatible en toda la conexión, incluidos los dispositivos intermedios.
- Su dispositivo debe ser compatible con el protocolo de puerta de enlace fronteriza (BGP) y la autenticación MD5 del BGP.
- (Opcional) Puede configurar la detección de reenvío bidireccional (BFD) en la red. La BFD asíncrona se habilita automáticamente para cada interfaz virtual. AWS Direct Connect Se habilita de forma automática en las interfaces virtuales de Direct Connect, pero no funcionará hasta que la configure en el enrutador. A fin de obtener más información, consulte Habilitar la BFD para una conexión de Direct Connect.

AWS Direct Connect admite los protocolos de comunicación IPv4 e IPv6. Se puede acceder a las direcciones IPv6 proporcionadas por AWS los servicios públicos a través de interfaces virtuales AWS Direct Connect públicas.

AWS Direct Connect admite un tamaño de la trama Ethernet de 1522 o 9023 bytes (encabezado de Ethernet de 14 bytes + etiqueta VLAN de 4 bytes + bytes para el datagrama IP + FCS de 4 bytes) en la capa de enlace. Puede establecer la MTU de sus interfaces virtuales privadas. Para obtener más información, consulte Establecer la MTU de red para interfaces virtuales privadas o de tránsito.

Precios para AWS Direct Connect

AWS Direct Connect tiene dos elementos de facturación: el horario de puerto y la transferencia de datos salientes. El precio de la hora de puerto está determinado por la capacidad y el tipo de conexión (conexión dedicada o conexión alojada).

Los gastos de transferencia de datos para las interfaces privadas y las interfaces virtuales de tránsito se asignan a la AWS cuenta responsable de la transferencia de datos. No se realizan cargos adicionales por usar una gateway de AWS Direct Connect con varias cuentas.

En el caso de AWS los recursos direccionables públicamente (por ejemplo, cubos de Amazon S3, instancias EC2 clásicas o tráfico EC2 que pasa por una puerta de enlace de Internet), si el

tráfico saliente se destina a prefijos públicos propiedad de la misma cuenta de AWS pagador y se anuncia activamente a AWS través de una interfaz virtual AWS Direct Connect pública, el uso de transferencia de datos salientes (DTO) se mide al propietario del recurso según la tasa de transferencia de datos. AWS Direct Connect

Para obtener más información, consulte Precios de AWS Direct Connect.

AWS Direct Connect Mantenimiento

AWS Direct Connect es un servicio totalmente gestionado en el que Direct Connect realiza periódicamente actividades de mantenimiento en una flota de hardware que respalda el servicio. Las conexiones Direct Connect se aprovisionan en dispositivos de hardware independientes, lo que le permite crear conexiones de red altamente resistentes entre su infraestructura local Amazon Virtual Private Cloud y su infraestructura local. Esta capacidad le permite acceder a sus AWS recursos de forma fiable, escalable y rentable. Para obtener más información, consulte Recomendaciones de resiliencia de AWS Direct Connect.

Existen dos tipos de mantenimiento de Direct Connect: mantenimiento planificado y de emergencia:

- Mantenimiento planificado. El mantenimiento planificado se programa con antelación para mejorar la disponibilidad y ofrecer características nuevas. Este tipo de mantenimiento se programa durante un período de mantenimiento en el que proporcionamos tres notificaciones: 14 días naturales, 7 días naturales y 1 día calendario.

  > **Note**
  >
  > Los días naturales incluyen los días no laborables y los feriados locales.

- Mantenimiento de emergencia. El mantenimiento de emergencia se inicia de forma crítica debido a una falla que afecta al servicio y requiere una acción inmediata por parte de AWS para restaurar los servicios. Este tipo de mantenimiento no se planifica con antelación. Los clientes afectados reciben una notificación sobre el mantenimiento de emergencia hasta 60 minutos antes del mantenimiento.

Le recomendamos que siga las Recomendaciones de resiliencia de AWS Direct Connect para poder transferir el tráfico de forma ágil y proactiva a su conexión redundante de Direct Connect durante el mantenimiento. También le recomendamos que pruebe de forma proactiva la resiliencia de sus conexiones redundantes de manera periódica para comprobar que la conmutación por error funciona

según lo previsto. Con esta the section called “Prueba de conmutación por error de AWS Direct Connect” funcionalidad, puede comprobar que el tráfico pasa por una de sus interfaces virtuales redundantes.

Para obtener información sobre los criterios de elegibilidad a fin de iniciar una solicitud de cancelación de mantenimiento planificada, consulte ¿Cómo cancelo un evento de mantenimiento de Direct Connect?.

> **Note**
>
> Las solicitudes de mantenimiento de emergencia no se pueden cancelar, ya que AWS hay que actuar de inmediato para restablecer el servicio.

Para obtener más información sobre los eventos de mantenimiento, consulte los eventos de mantenimiento en las AWS Direct Connect preguntas frecuentes.

Acceso a una región de AWS remota

Las ubicaciones de AWS Direct Connect de regiones públicas o de AWS GovCloud (US) pueden tener acceso a los servicios públicos de cualquier otra región pública (excepto China [Pekín y Ningxia]). Además, las conexiones de AWS Direct Connect de regiones públicas o de AWS GovCloud (US) pueden configurarse de modo que obtengan acceso a una VPC de la cuenta en cualquier otra región pública (excepto China [Pekín y Ningxia]). Por lo tanto, puede utilizar una única conexión de AWS Direct Connect para crear servicios en varias regiones. Todo el tráfico de red permanece en la red troncal global de AWS, independientemente de si obtiene acceso a los servicios de AWS públicos o a una VPC de otra región.

A cualquier transferencia de datos fuera de una región remota se le aplica la tasa de transferencia de datos de la región remota. Para obtener más información sobre los precios de transferencia de datos, consulte la sección de Precios de la página de detalles de AWS Direct Connect.

Para obtener más información sobre las políticas de direccionamiento y sobre las comunidades de BGP admitidas para las conexiones de AWS Direct Connect, consulte Políticas de direccionamiento y comunidades de BGP.

Acceso a servicios públicos en una región remota

Para obtener acceso a los recursos públicos de una región remota, debe configurar una interfaz virtual pública y establecer una sesión de protocolo de gateway fronteriza (BGP). Para obtener más información, consulte AWS Direct Connect interfaces virtuales.

Después de crear una interfaz virtual pública y establecer una sesión de BGP, el enrutador aprende las rutas de las demás regiones públicas de AWS. Para obtener más información sobre los prefijos anunciados por AWS en la actualidad, consulte Rangos de direcciones IP de AWS en la Referencia general de Amazon Web Services.

Acceso a una VPC en una región remota

Puede crear una gateway de Direct Connect en cualquier región pública. Utilícela para establecer la conexión de AWS Direct Connect a través de una interfaz virtual privada con las VPC de su cuenta que se encuentren en regiones diferentes o con una gateway de tránsito. Para obtener más información, consulte Uso de puertas de enlace de Direct Connect.

Si lo prefiere, puede crear una interfaz virtual pública para la conexión de AWS Direct Connect y, a continuación, establecer una conexión de VPN con la VPC en la región remota. A fin de obtener más información sobre la configuración de la conectividad de la VPN con una VPC, consulte Escenarios para el uso de Amazon Virtual Private Cloud en la Guía del usuario de Amazon VPC.

Opciones de conectividad de red a Amazon VPC

La siguiente configuración se puede utilizar para conectar redes remotas con su entorno de Amazon VPC. Estas opciones son útiles para integrar los recursos de AWS con sus servicios en el sitio existentes:

- Opciones de conectividad de Amazon Virtual Private Cloud

Políticas de direccionamiento y comunidades de BGP

AWS Direct Connect aplica políticas de enrutamiento entrantes (desde su centro de datos local) y salientes (desde su AWS región) para una conexión pública. AWS Direct Connect También puede utilizar las etiquetas de comunidad del protocolo de puerta de enlace fronteriza (BGP) en las rutas anunciadas por Amazon y aplicar etiquetas de comunidad del BGP en las que se anuncie en Amazon.

Políticas de direccionamiento de interfaces virtuales públicas

Si utilizas AWS servicios públicos AWS Direct Connect para acceder a ellos, debes especificar los prefijos públicos de IPv4 o IPv6 para anunciarte a través de BGP.

Se aplican las siguientes políticas de direccionamiento de entrada:

- Debe poseer los prefijos públicos y deben estar registrados como tales en el registro de Internet regional correspondiente.
- El tráfico debe estar destinado a los prefijos públicos de Amazon. No se admite el direccionamiento transitivo entre las conexiones.
- AWS Direct Connect filtra los paquetes entrantes para validar que la fuente del tráfico se originó en el prefijo anunciado.

Se aplican las siguientes políticas de direccionamiento de salida:

- AS_PATH y Longest Prefix Match se utilizan para determinar la ruta de enrutamiento. AWS recomienda anunciar rutas más específicas AWS Direct Connect si se anuncia el mismo prefijo tanto en Internet como en una interfaz virtual pública.
- AWS Direct Connect anuncia todos los prefijos regionales locales y remotos AWS cuando están disponibles e incluye prefijos en la red de otros puntos de presencia (PoP) AWS no regionales, cuando estén disponibles; por ejemplo, y de Route 53. CloudFront

  > **Note**
  >
  > - Los prefijos que figuran en el archivo JSON de rangos de direcciones AWS IP, ip-ranges.json, para las regiones de China solo se anuncian en las regiones de AWS China. AWS
  > - Los prefijos que figuran en el archivo JSON de intervalos de direcciones AWS IP, ip-ranges.json, para las regiones comerciales solo se anuncian en las regiones AWS comerciales. AWS
  >
  > Para obtener más información sobre el archivo ip-ranges.json, consulte los Rangos de direcciones IP de AWS en la Referencia general de AWS.

- AWS Direct Connect anuncia prefijos con una longitud de ruta mínima de 3.
- AWS Direct Connect anuncia todos los prefijos públicos en la conocida comunidad BGP. `NO_EXPORT`

- Si anuncias los mismos prefijos desde dos regiones diferentes mediante dos interfaces virtuales públicas diferentes y ambas tienen los mismos atributos de BGP y la longitud de prefijo más larga, se AWS dará prioridad a la región de origen para el tráfico saliente.
- Si tiene varias AWS Direct Connect conexiones, puede ajustar la distribución de la carga del tráfico entrante anunciando prefijos con los mismos atributos de ruta.
- Los prefijos anunciados por no AWS Direct Connect deben anunciarse más allá de los límites de la red de su conexión. Por ejemplo, estos prefijos no se deben incluir en ninguna tabla de direccionamiento de Internet pública.
- AWS Direct Connect conserva los prefijos anunciados por los clientes dentro de la red de Amazon. No volvemos a anunciar los prefijos de los clientes que se obtienen de una VIF pública en ninguno de los siguientes sitios:
  - Otros clientes AWS Direct Connect
  - Redes compatibles con la red AWS global
  - Proveedores de conexión de Amazon

Comunidades BGP de interfaces virtuales públicas

AWS Direct Connect admite las etiquetas de comunidad BGP de ámbito para ayudar a controlar el alcance (regional o global) y la preferencia de ruta del tráfico en las interfaces virtuales públicas. AWS trata todas las rutas recibidas de un VIF público como si estuvieran etiquetadas con la etiqueta de comunidad BGP NO_EXPORT, lo que significa que solo la AWS red utilizará esa información de enrutamiento.

Ámbito de las comunidades BGP

Puede aplicar las etiquetas de comunidad de BGP en los prefijos públicos que usted comunica en Amazon para indicar hasta qué punto se propagarán los prefijos en la red de Amazon, solo hasta la región de AWS local, a todas las regiones de un continente o a todas las regiones públicas.

Región de AWS comunidades

En el caso de las políticas de enrutamiento entrantes, puede utilizar las siguientes comunidades del BGP para los prefijos:

- `7224:9100`—Locales Regiones de AWS
- `7224:9200`—Todo Regiones de AWS para un continente:

  - En toda Norteamérica
  - Asia Pacífico
  - Europa, Medio Oriente y África
- `7224:9300`—Global (todas las regiones públicas) AWS

> **Note**
>
> Si no aplicas ninguna etiqueta de comunidad, los prefijos se anuncian en todas AWS las regiones públicas (globales) de forma predeterminada.
> Los prefijos marcados con las mismas comunidades y que tengan atributos AS_PATH idénticos son candidatos para las rutas de acceso múltiples.

Las comunidades `7224:1` a `7224:65535` están reservadas para AWS Direct Connect.

En el caso de las políticas de enrutamiento de salida, AWS Direct Connect aplica las siguientes comunidades de BGP a las rutas anunciadas:

- `7224:8100`—Rutas que se originan en la misma AWS región a la que está asociado el AWS Direct Connect punto de presencia.
- `7224:8200`—Rutas que se originan en el mismo continente al que está asociado el AWS Direct Connect punto de presencia.
- Sin etiqueta: rutas que se originan en otros continentes.

> **Note**
>
> Para recibir todos los prefijos AWS públicos no aplique ningún filtro.

Se eliminan las comunidades que no son compatibles con una conexión AWS Direct Connect pública.

Comunidad BGP de **`NO_EXPORT`**

En el caso de las políticas de enrutamiento salientes, la etiqueta de comunidad del BGP `NO_EXPORT` es compatible con las interfaces virtuales públicas.

AWS Direct Connect también proporciona etiquetas de comunidad BGP en las rutas de Amazon anunciadas. Si lo utilizas AWS Direct Connect para acceder a AWS los servicios públicos, puedes crear filtros basados en estas etiquetas de comunidad.

En el caso de las interfaces virtuales públicas, todas las rutas que AWS Direct Connect se anuncian a los clientes se etiquetan con la etiqueta comunitaria NO_EXPORT.

Políticas de direccionamiento de interfaces virtuales privadas e interfaces virtuales de tránsito

Si las utiliza AWS Direct Connect para acceder a sus AWS recursos privados, debe especificar los prefijos de IPv4 o IPv6 que desea anunciar a través de BGP. Estos prefijos pueden ser públicos o privados.

Las siguientes reglas de enrutamiento de salida se aplican en función de los prefijos anunciados:

- AWS evalúa primero la longitud más larga del prefijo. AWS recomienda anunciar rutas más específicas mediante varias interfaces virtuales de Direct Connect si las rutas de enrutamiento deseadas están destinadas a conexiones activas/pasivas. Para obtener más información, consulte Cómo influir en el tráfico en las redes híbridas mediante la coincidencia de prefijo más larga.
- La preferencia local es el atributo BGP que se recomienda usar cuando las rutas de enrutamiento deseadas estén destinadas a conexiones activas y pasivas y las longitudes de prefijo anunciadas sean las mismas. Este valor se establece por región para preferir las AWS Direct Connect ubicaciones que tengan lo mismo asociado Región de AWS mediante el valor de comunidad de preferencias locales `7224:7200` —Medium. Si la región local no está asociada a la ubicación de Direct Connect, se establece en un valor inferior. Esto se aplica solo si no se ha asignado ninguna etiqueta de comunidad de preferencias locales.
- La longitud AS_PATH se puede utilizar para determinar la ruta de enrutamiento cuando la longitud del prefijo y la preferencia local son las mismas.
- El discriminador de salidas múltiples (MED) se puede usar para determinar la ruta de enrutamiento cuando la longitud del prefijo, la preferencia local y el AS_PATH son iguales. AWS no recomienda el uso de valores MED debido a su menor prioridad en la evaluación.
- AWS compartirán la carga entre múltiples interfaces virtuales privadas o de tránsito cuando los prefijos tengan la misma longitud y los mismos atributos de BGP.

Comunidades BGP de interfaces virtuales privadas e interfaces virtuales de tránsito

Cuando una empresa Región de AWS enruta el tráfico a ubicaciones locales a través de interfaces virtuales privadas o de tránsito de Direct Connect, lo asociado a la ubicación Región de AWS de Direct Connect influye en la capacidad de utilizar el enrutamiento de rutas múltiples (ECMP) de igual costo. Regiones de AWS prefieren las ubicaciones de Direct Connect en las mismas ubicaciones asociadas Región de AWS de forma predeterminada. Consulte AWS Direct Connect Ubicaciones para identificar las ubicaciones asociadas a cualquier ubicación Región de AWS de Direct Connect.

Cuando no se han aplicado etiquetas de comunidad de preferencias locales, Direct Connect admite ECMP a través de interfaces virtuales privadas o de tránsito para prefijos con la misma longitud, longitud AS_PATH y valor MED en dos o más rutas en los siguientes escenarios:

- El tráfico de Región de AWS envío tiene dos o más rutas de interfaz virtual desde ubicaciones de la misma ubicación asociadas Región de AWS, ya sea en las mismas instalaciones de colocación o en diferentes.
- El tráfico de Región de AWS envío tiene dos o más rutas de interfaz virtual desde ubicaciones que no se encuentran en la misma región.

Para obtener más información, consulte ¿Cómo configuro una conexión Direct Connect activa/activa o activa/pasiva desde una interfaz AWS virtual privada o de tránsito?

> **Note**
>
> Esto no tiene ningún efecto en el ECMP hacia y desde las ubicaciones locales. Región de AWS

Para controlar las preferencias de ruta, Direct Connect admite etiquetas de comunidad BGP de preferencia local para las interfaces virtuales privadas y las interfaces virtuales de tránsito.

Comunidades de BGP de preferencia local

Puede utilizar las etiquetas de comunidad de BGP de preferencia local para lograr el equilibrio entre el balanceo de carga y las preferencias de ruta del tráfico entrante a la red. Para cada prefijo que usted comunica en una sesión de BGP, puede aplicar una etiqueta de comunidad para indicar la prioridad de la ruta asociada en el tráfico de retorno.

Se admiten las siguientes etiquetas de comunidad de BGP de preferencia local:

- `7224:7100`: preferencia baja
- `7224:7200`: preferencia intermedia
- `7224:7300`: preferencia alta

Las etiquetas de comunidad de BGP de preferencia local se excluyen mutuamente. Para equilibrar la carga del tráfico entre varias AWS Direct Connect conexiones (activas/activas) alojadas en la misma región o en AWS regiones diferentes, aplique la misma etiqueta de comunidad; por ejemplo, `7224:7200` (preferencia media) a los prefijos de las conexiones. Si se produce un error en una de las conexiones, se equilibrará la carga del tráfico mediante ECMP entre las conexiones activas restantes, independientemente de sus asociaciones regionales de origen. Para permitir la conmutación por error en varias conexiones de AWS Direct Connect (activa/pasiva), aplique una etiqueta de comunidad con una preferencia mayor a los prefijos de la interfaz virtual activa o principal y una preferencia menor a los prefijos de la interfaz virtual pasiva o de copia de seguridad. Por ejemplo, establezca las etiquetas de comunidad del BGP para sus interfaces virtuales principales o activas en `7224:7300` (preferencia alta) y `7224:7100` (preferencia baja) para sus interfaces virtuales pasivas.

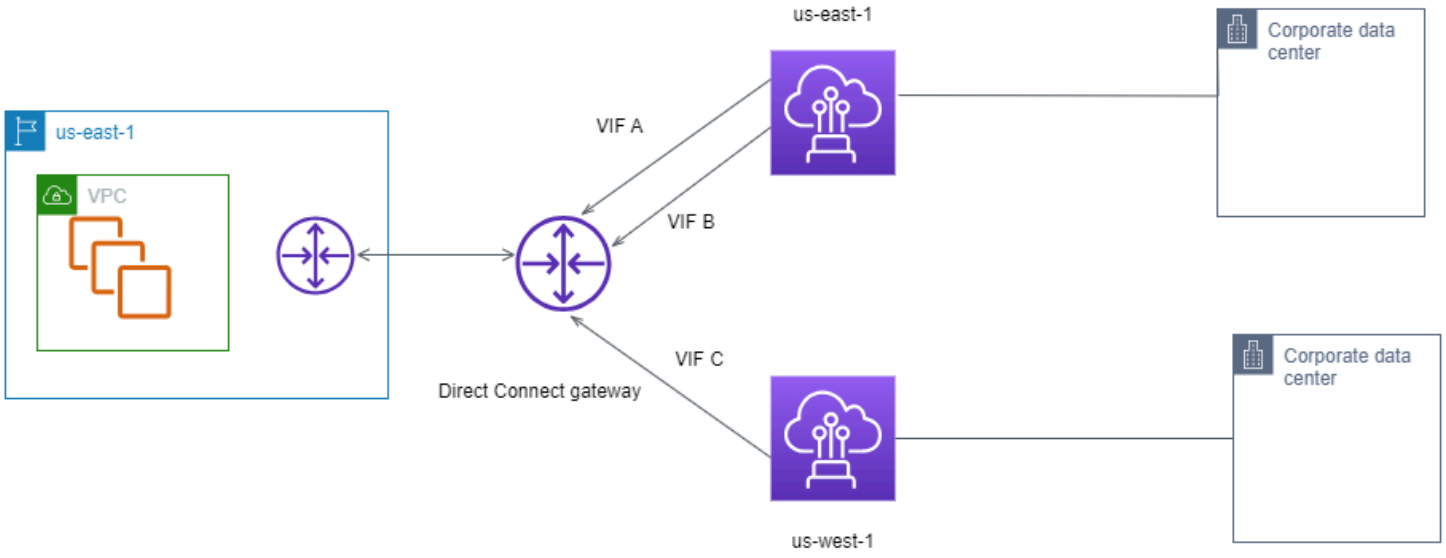
Las etiquetas de comunidad de BGP de preferencia local se evalúan antes que los atributos AS_PATH, y lo hacen por orden de preferencia, desde el valor más bajo hasta el valor más alto (se prefiere la preferencia más alta).

Ejemplo de enrutamiento de interfaz virtual privada

Considere la configuración en la que la región de origen de la AWS Direct Connect ubicación 1 es la misma que la región de origen de la VPC. Hay una AWS Direct Connect ubicación redundante en una región diferente. Hay dos VIF privados (VIF A y VIF B) desde la ubicación AWS Direct Connect 1 (us-east-1) hasta la puerta de enlace Direct Connect. Hay un VIF privado (VIF C) desde la AWS Direct Connect ubicación (us-west-1) hasta la puerta de enlace Direct Connect. Para que el tráfico de AWS ruta pase por el VIF B antes que por el VIF A, establezca el atributo AS_PATH del VIF B para que sea más corto que el atributo AS_PATH del VIF A.

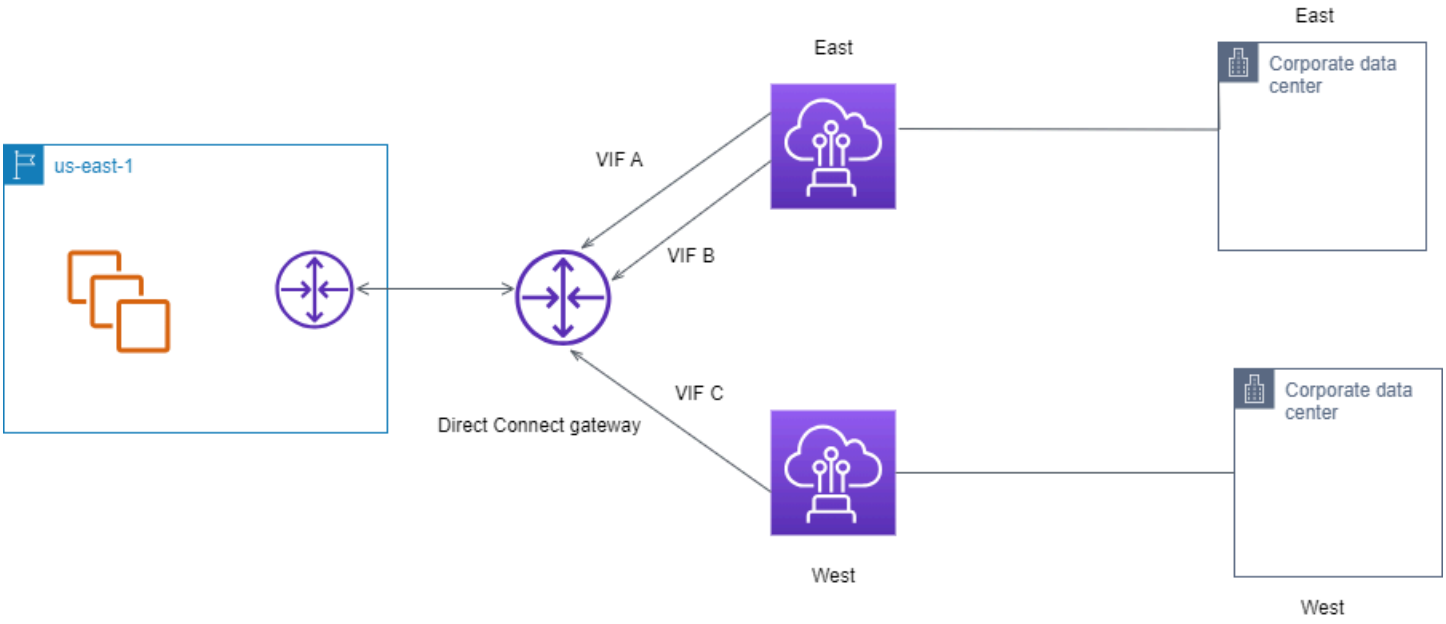
Las VIF tienen las siguientes configuraciones:

- La VIF A (en us-east-1) anuncia 172.16.0.0/16 y tiene un atributo AS_PATH de 65001, 65001, 65001
- La VIF B (en us-east-1) anuncia 172.16.0.0/16 y tiene un atributo AS_PATH de 65001, 65001
- La VIF C (en us-west-1) anuncia 172.16.0.0/16 y tiene un atributo AS_PATH de 65001



Si cambia la configuración del rango CIDR del VIF C, las rutas que se encuentran en el rango CIDR del VIF C utilizan el VIF C porque tiene la longitud de prefijo más larga.

- La VIF C (en us-west-1) anuncia 172.16.0.0/24 y tiene un atributo AS_PATH de 65001



Uso del kit de herramientas de AWS Direct Connect resiliencia para empezar

AWS ofrece a los clientes la posibilidad de lograr conexiones de red altamente resilientes entre Amazon Virtual Private Cloud (Amazon VPC) y su infraestructura local. El kit de herramientas AWS Direct Connect de resiliencia proporciona un asistente de conexión con varios modelos de resiliencia. Estos modelos le ayudan a determinar y, a continuación, realizar un pedido para el número de conexiones dedicadas para lograr su objetivo de SLA. Seleccione un modelo de resiliencia y, a continuación, el kit de herramientas de AWS Direct Connect resiliencia lo guiará a través del proceso específico de solicitud de conexiones. Los modelos de resiliencia están diseñados para garantizar que dispone del número adecuado de conexiones dedicadas en varias ubicaciones.

El kit de herramientas AWS Direct Connect de resiliencia tiene las siguientes ventajas:

- Proporciona directrices para determinar y después solicitar las conexiones dedicadas de AWS Direct Connect redundantes apropiadas.
- Garantiza que las conexiones dedicadas redundantes tengan la misma velocidad.
- Configura automáticamente los nombres de conexión dedicados.
- Aprueba automáticamente sus conexiones dedicadas cuando tiene una AWS cuenta existente y selecciona un socio conocido. AWS Direct Connect La Carta de autorización (LOA) está disponible para su descarga inmediata.
- Crea automáticamente un ticket de soporte para la aprobación de la conexión dedicada cuando eres un AWS cliente nuevo o seleccionas un socio desconocido (otro).
- Ofrece un resumen del pedido de las conexiones dedicadas, con el SLA que se puede alcanzar y el costo por hora de puerto para las conexiones dedicadas solicitadas.
- Crea grupos de agregación de enlaces (LAG) y agrega el número adecuado de conexiones dedicadas a los LAG cuando se elige una velocidad distinta de 1 Gbps, 10 Gbps o 100 Gbps.
- Ofrece un resumen del LAG con el SLA de conexión dedicada que puede alcanzar y el costo total por hora de puerto para cada conexión dedicada solicitada como parte del LAG.
- Impide que se terminen las conexiones dedicadas en el mismo dispositivo de AWS Direct Connect .
- Proporciona una forma de probar la resiliencia de su configuración. Puede trabajar con AWS para reducir la sesión de interconexión de BGP con el fin de comprobar que el tráfico se enruta a una

de sus interfaces virtuales redundantes. Para obtener más información, consulte the section called "Prueba de conmutación por error de AWS Direct Connect".

- Proporciona CloudWatch métricas de Amazon para conexiones e interfaces virtuales. Para obtener más información, consulte Supervisión.

Los siguientes modelos de resiliencia están disponibles en el kit de herramientas de AWS Direct Connect resiliencia:

- Maximum Resiliency (Resiliencia máxima): este modelo le ofrece una forma de solicitar conexiones dedicadas para conseguir un SLA del 99,99 %. Requiere que se cumplan todos los requisitos para alcanzar el SLA especificado en el Acuerdo de nivel de servicios de AWS Direct Connect.
- High-Resiliency (Alta resiliencia): este modelo le ofrece una forma de solicitar conexiones dedicadas para conseguir un SLA del 99,9 %. Requiere que se cumplan todos los requisitos para alcanzar el SLA especificado en el Acuerdo de nivel de servicios de AWS Direct Connect.
- Desarrollo y pruebas: este modelo le ofrece una forma de conseguir resiliencia de desarrollo y pruebas para cargas de trabajo no críticas mediante el uso de conexiones independientes que terminan en dispositivos independientes en una ubicación.
- Classic. Este modelo está destinado a aquellos usuarios que tengan conexiones existentes y que deseen añadir otras. Este modelo no proporciona un SLA.

La mejor práctica es utilizar el asistente de conexión del kit de herramientas de AWS Direct Connect resiliencia para ordenar las conexiones específicas a fin de lograr su objetivo de SLA.

Tras seleccionar el modelo de resiliencia, el kit de herramientas de AWS Direct Connect resiliencia le guiará por los siguientes procedimientos:

- Selección del número de conexiones dedicadas
- Selección de la capacidad de conexión y la ubicación de conexión dedicada
- Solicitud de las conexiones dedicadas
- Comprobación de que las conexiones dedicadas están listas para su uso
- Descarga de la Carta de autorización (LOA-CFA) para cada conexión dedicada
- Comprobación de que la configuración cumple con los requisitos de resiliencia

Requisitos previos

AWS Direct Connect admite las siguientes velocidades de puerto a través de fibra monomodo: transceptor 1000BASE-LX (1310 nm) para Ethernet de 1 gigabit, transceptor 10GBASE-LR (1310 nm) para 10 gigabits o 100GBASE-LR4 para Ethernet de 100 gigabit.

AWS Direct Connect Puede configurar una conexión de una de las siguientes maneras:

Modelo	Ancho de banda	Método
Conexión dedicada	1 Gbps, 10 Gbps y 100 Gbps	Trabaje con un AWS Direct Connect socio o un proveedor de red para conectar un router desde su centro de datos, oficina o entorno de colocación a una AWS Direct Connect ubicación. El proveedor de red no tiene que ser un Socio de AWS Direct Connect para conectarlo a una conexión dedicada. Las conexiones dedicadas de AWS Direct Connect admiten estas velocidades de puerto a través de fibra monomodo: 1 Gbps: 1000BASE-LX (1310 nm), 10 Gbps: 10GBASE-LR (1310 nm) y 100 Gbps: 100GBASE-LR4.
Conexión alojada	50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps y 10 Gbps	Trabaje con un AWS Direct Connect socio del Programa de Socios para conectar un router desde su centro de datos, oficina o entorno de colocación a una AWS Direct Connect ubicación.

Modelo	Ancho de banda	Método
		Solo algunos socios proporcionan las conexiones de mayor capacidad.

Para conexiones AWS Direct Connect con anchos de banda de 1 Gbps o más, asegúrese de que su red cumpla los siguientes requisitos:

- Su red debe utilizar fibra monomodo con un transceptor 1000BASE-LX (1310 nm) para 1 gigabit Ethernet, un transceptor 10GBASE-LR (1310 nm) para 10 gigabit o un 100GBASE-LR4 para 100 gigabit Ethernet.
- La negociación automática de un puerto debe estar deshabilitada para una conexión con una velocidad de puerto superior a 1 Gbps. Sin embargo, según el punto final de AWS Direct Connect que dé servicio a su conexión, es posible que sea necesario activar o desactivar la negociación automática para las conexiones de 1 Gbps. Si la interfaz virtual permanece inactiva, consulte Solución de problemas de capa 2 (enlace de datos).
- La encapsulación de VLAN 802.1Q debe ser compatible en toda la conexión, incluidos los dispositivos intermedios.
- Su dispositivo debe ser compatible con el protocolo de puerta de enlace fronteriza (BGP) y la autenticación MD5 del BGP.
- (Opcional) Puede configurar la detección de reenvío bidireccional (BFD) en la red. La BFD asíncrona se habilita automáticamente para cada interfaz virtual. AWS Direct Connect Se habilita de forma automática en las interfaces virtuales de Direct Connect, pero no funcionará hasta que la configure en el enrutador. A fin de obtener más información, consulte Habilitar la BFD para una conexión de Direct Connect.

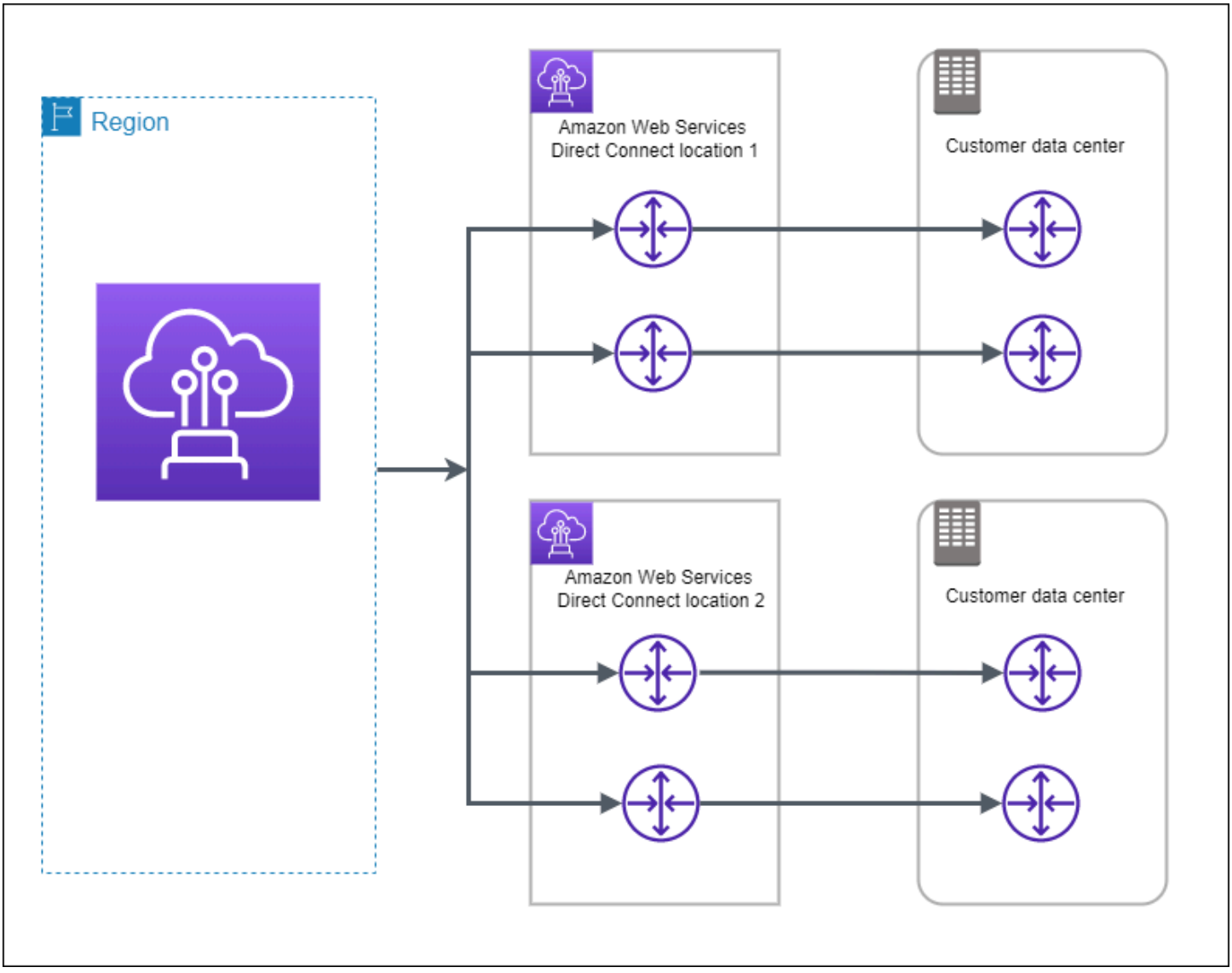
Asegúrese de que dispone de la siguiente información antes de comenzar la configuración:

- El modelo de resiliencia que desea utilizar.
- La velocidad, la ubicación y el socio de todas las conexiones.

  Solo necesita la velocidad para una conexión.

Resiliencia máxima

Puede conseguir la máxima resiliencia para cargas de trabajo críticas mediante el uso de conexiones independientes que terminan en dispositivos independientes en más de una ubicación (tal y como se muestra en la siguiente figura). Este modelo proporciona resistencia frente a errores de dispositivo, conectividad y ubicación completa. La siguiente figura muestra las dos conexiones de cada centro de datos del cliente que van a las mismas ubicaciones. AWS Direct Connect Si lo desea, puede hacer que cada conexión desde el centro de datos del cliente vaya a diferentes ubicaciones.



Los siguientes procedimientos muestran cómo utilizar el kit de herramientas de AWS Direct Connect resiliencia para configurar un modelo de máxima resiliencia.

Temas

Paso 1: Inscríbase en AWS

Para usarla AWS Direct Connect, necesitas una AWS cuenta si aún no la tienes.

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de registrarte en un usuario Cuenta de AWS, protege Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilita y crea un usuario administrativo para que no utilices el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Signing in as the root user en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Paso 2: Configurar el modelo de resiliencia

Para configurar un modelo de resiliencia máxima

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Conexiones y, a continuación, Crear una conexión.
3. En Connection ordering type (Tipo de solicitud de conexión), elija Connection wizard (Asistente de conexión).
4. En Resiliency level (Nivel de resiliencia), elija Maximum Resiliency (Resiliencia máxima) y, a continuación, elija Next (Siguiente).
5. En el panel Configure connections (Configurar conexiones), en Connection settings (Configuración de conexión), proceda del modo siguiente:

   a. En Bandwidth (Ancho de banda), elija el ancho de banda de la conexión dedicada.

      Este ancho de banda se aplica a todas las conexiones creadas.

   b. En el caso del proveedor de servicios de primera ubicación, seleccione la AWS Direct Connect ubicación adecuada para la conexión dedicada.

   c. Si procede, en First Sub location (Primera ubicación secundaria), elija el piso más cercano a usted o a su proveedor de red. Esta opción solo está disponible si la ubicación dispone de Meet-Me Rooms (MMR) en varios pisos del edificio.

   d. Si ha seleccionado Other (Otro) para First location service provider (Proveedor de servicios de la primera ubicación), en Name of other provider (Nombre de otro proveedor), escriba el nombre del socio que utiliza.

   e. En Proveedor de servicios de segunda ubicación, seleccione la AWS Direct Connect ubicación adecuada.

f. Si procede, en Second Sub location (Segunda ubicación secundaria), elija el piso más cercano a usted o a su proveedor de red. Esta opción solo está disponible si la ubicación dispone de Meet-Me Rooms (MMR) en varios pisos del edificio.

g. Si ha seleccionado Other (Otro) en Second location service provider, (Proveedor de servicios de la segunda ubicación), en Name of other provider (Nombre de otro proveedor), escriba el nombre del socio que utiliza.

h. (Opcional) Añada o elimine una etiqueta.

   [Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

   - En Key (Clave), escriba el nombre de la clave.
   - En Valor, escriba el valor de la clave.

   [Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

6. Elija Siguiente.
7. Revise las conexiones y, a continuación, elija Continue (Continuar).

   Si las LOA están listas, puede elegir Download LOA (Descargar LOA), y, a continuación, hacer clic en Continue (Continuar).

   La revisión de la solicitud y el aprovisionamiento de un puerto para la conexión pueden tardar hasta 72 horas. AWS Durante este tiempo, es posible que reciba un correo electrónico con una solicitud de información adicional sobre su caso de uso o sobre la ubicación especificada. El correo electrónico se envía a la dirección de correo electrónico que utilizaste cuando te registraste AWS. Si no responde en un plazo de 7 días, se eliminará la conexión.

Paso 3: Crear las interfaces virtuales

Puede crear una interfaz virtual privada para conectarla a la VPC. O bien, puede crear una interfaz virtual pública para conectarse a AWS servicios públicos que no estén en una VPC. Al crear una interfaz virtual privada con una VPC, necesita una interfaz virtual privada para cada VPC a la que se va a conectar. Por ejemplo, necesita tres interfaces virtuales privadas para conectarse a tres VPC.

Antes de comenzar, asegúrese de que dispone de la siguiente información:

Recurso	Información necesaria
Conexión	El grupo de AWS Direct Connect conexión o agregación de enlaces (LAG) para el que va a crear la interfaz virtual.
Nombre de la interfaz virtual	Un nombre para la interfaz virtual.
Propietario de la interfaz virtual	Si va a crear la interfaz virtual para otra cuenta, necesitará el ID de AWS cuenta de la otra cuenta.
(Solo para la interfaz virtual privada) Conexión	Para conectarse a una VPC de la misma AWS región, necesita la puerta de enlace privada virtual para su VPC. El ASN del lado de Amazon de la sesión del BGP se hereda de la puerta de enlace privada virtual. Al crear una puerta de enlace privada virtual, puede especificar su propio ASN privado. De lo contrario, Amazon proporciona un ASN predeterminado. Para obtener información, consulte Crear una puerta de enlace privada virtual en la Guía del usuario de Amazon VPC. Para conectarse a una VPC a través de una puerta de enlace de Direct Connect, se necesita la puerta de enlace de Direct Connect. Para obtener más información, consulte Gateways de Direct Connect.
VLAN	Una etiqueta de red de área local virtual (VLAN) única que aún no se encuentra en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de AWS Direct Connect . Si tiene una conexión alojada, su AWS Direct Connect socio le proporcionará este valor. No puede modificar el valor después de haber creado la interfaz virtual.
Direcciones IP de mismo nivel	Una interfaz virtual es compatible con una sesión de intercambio de tráfico del BGP para IPv4 e IPv6, o con uno de cada una (pila doble). No utilice direccion es IP elásticas (eIP) ni traiga sus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias sesiones de BGP para la misma familia de direccionamiento IP en la misma interfaz virtual. Los rangos de las direcciones IP que se asignan a cada extremo de la interfaz virtual para la sesión de intercambio de tráfico del BGP.

Recurso	Información necesaria
	• IPv4: • (Solo para la interfaz virtual pública) Debe especificar direcciones IPv4 públicas únicas que sean de su propiedad. El valor puede ser uno de los siguientes: • Un CIDR IPv4 propiedad del cliente Puede ser cualquier IP pública (propiedad del cliente o proporcionada por él AWS), pero se debe usar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del router. AWS Por ejemplo, si asigna un `/31` rango, por ejemplo, podría usarlo `203.0.113.0` para su IP homóloga y `203.0.113.1` para la AWS IP homóloga. `203.0.113.0/31` O bien, si asignas un `/24` rango, por ejemplo`198.51.100.0/24` , puedes usarlo `198.51.100.10` para tu IP homóloga y `198.51.100.20` para la IP AWS homóloga. • Un rango de IP propiedad de su AWS Direct Connect socio o ISP, junto con una autorización LOA-CFA • Un AWS CIDR /31 proporcionado. Póngase en contacto con AWS Asistencia para solicitar un CIDR IPv4 público (e indique un caso de uso en su solicitud) **Note** No podemos garantizar que podamos cumplir con todas las solicitudes de direcciones IPv4 públicas AWS proporcionadas. • (Solo para la interfaz virtual privada) Amazon puede generar direcciones IPv4 privadas en su nombre. Si especifica el suyo propio, asegúrese de especificar únicamente los CIDR privados para la interfaz de su router y la interfaz AWS Direct Connect. Por ejemplo, no especifique otras direcciones IP de su red local. Al igual que en una interfaz virtual pública, se debe usar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del AWS router. Por ejemplo, si asigna un `/30` rango, por ejemplo, podría usarlo `192.168.0.1` para su IP homóloga y `192.168.0.2` para la IP AWS homóloga. `192.168.0.0/30`

Recurso	Información necesaria
	• IPv6: Amazon le asigna un CIDR IPv6 /125 de forma automática. No puede especificar sus propias direcciones IPv6 de mismo nivel.
Familia de direcciones	Si la sesión de intercambio de tráfico del BGP se realizará a través de IPv4 o IPv6.
Información sobre el BGP	• Un número de sistema autónomo (ASN) para el protocolo de puerta de enlace fronteriza (BGP) público o privado en su lado de la sesión del BGP. Si utiliza un ASN público, debe tener uno propio. Si utiliza un ASN privado, puede establecer un valor de ASN personalizado. Para un ASN de 16 bits ASN, el valor debe estar dentro del rango de 64 512 a 65 534. En el caso de un ASN de 32 bits, el valor debe estar dentro del rango de 1 a 2147483647. El sistema autónomo (AS) que se antepone no funciona si utiliza un ASN privado para una interfaz virtual pública. • AWS habilita MD5 de forma predeterminada. Esta opción no se puede modificar. • Una clave de autenticación del BGP MD5. Puede proporcionar su propia clave o dejar que Amazon genere una en su nombre.

Recurso	Información necesaria

(Solo para la interfaz virtual pública) Prefijos que desea anunciar	Rutas IPv4 públicas o rutas IPv6 para anunciar a través del BGP. Debe comunicar al menos un prefijo a través del BGP, hasta un máximo de 1 000 prefijos.
	• IPv4: el CIDR de IPv4 puede superponerse con otro CIDR de IPv4 público que se haya anunciado que se utiliza AWS Direct Connect cuando se cumple alguna de las siguientes condiciones:
	  • Los CIDR provienen de distintas regiones. AWS Asegúrese de aplicar etiquetas de comunidad del BGP a los prefijos públicos.
	  • Utiliza AS_PATH cuando tiene un ASN público en una configuración activa/pasiva.
	  Para obtener más información, consulte Políticas de enrutamiento y comunidades del BGP.
	• IPv6: especifique una longitud de prefijo de /64 caracteres o menos.
	• Puede agregar prefijos adicionales a una VIF pública existente y anunciarl os si se pone en contacto con AWS Asistencia. En su caso de soporte, proporcione una lista de los prefijos de CIDR adicionales que desee agregar a la VIF pública y anunciar.
	• Puede especificar cualquier longitud de prefijo en una interfaz virtual pública de Direct Connect. IPv4 debería admitir cualquier valor entre /1 y /32, e IPv6 debería admitir cualquier valor entre /1 y /64.

Recurso	Información necesaria
(Solo para la interfaz virtual privada) Tramas gigantes	La unidad máxima de transmisión (MTU) de los paquetes superados. AWS Direct Connect El valor predeterminado es 1500. El establecimiento de la MTU de una interfaz virtual en 9001 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Las tramas gigantes solo se aplican a las rutas propagadas desde. AWS Direct Connect Si agrega rutas estáticas a una tabla de enrutamiento que apuntan a una gateway privada virtual, el tráfico enrutado a través de las rutas estáticas se envía utilizando 1500 MTU. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Jumbo Frame Capable en la página de configuración general de la interfaz virtual.
(Solo para la interfaz virtual de tránsito) Tramas gigantes	La unidad máxima de transmisión (MTU) de los paquetes superados. AWS Direct Connect El valor predeterminado es 1500. El establecimiento de la MTU de una interfaz virtual en 8500 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Se admiten tramas gigantes de hasta 8500 de MTU para Direct Connect. Las rutas estáticas y propagadas configuradas en la tabla de enrutamiento de puerta de enlace de tránsito admitirán tramas gigantes, incluso desde instancias de EC2 con entradas de la tabla de enrutamiento estáticas de VPC hasta la conexión de puerta de enlace de tránsito. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Capacidad para tramas gigantes en la página de configuración general de la interfaz virtual.

Si sus prefijos públicos o ASN pertenecen a un ISP o un operador de red, le solicitamos información adicional. Esta información puede ser un documento con un membrete oficial de la empresa o un correo electrónico proveniente del nombre de dominio de la empresa que confirme que usted puede utilizar el prefijo de red o el ASN.

Al crear una interfaz virtual pública, revisar y aprobar la solicitud AWS puede tardar hasta 72 horas.

Para aprovisionar una interfaz virtual pública a servicios que no sean de una VPC

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Virtual interface type (Tipo de interfaz virtual) en Type (Tipo), elija Public (Pública).
5. En Public virtual interface settings (Configuración de la interfaz virtual pública), haga lo siguiente:

   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

   c. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

   d. En BGP ASN, escriba el número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) de la gateway.

      Los valores válidos son 1-2.147.483.647.
6. En Additional settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

      [IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
      - En Amazon router peer IP (IP del mismo nivel del router de Amazon), escriba la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

      [IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

   b. Para utilizar su propia clave de BGP, introduzca su clave MD5 de BGP.

      Si no ingresa un valor, generamos una clave de BGP.

c. Para anunciar prefijos para Amazon, en Prefixes you want to advertise (Prefijos que desea anunciar), escriba las direcciones CIDR IPv4 de destino (separadas por comas) a las que debe redirigirse el tráfico a través de la interfaz virtual.

d. (Opcional) Añada o elimine una etiqueta.

[Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

- En Key (Clave), escriba el nombre de la clave.
- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

7. Elija Create virtual interface (Crear interfaz virtual).

Para aprovisionar una interfaz virtual privada a una VPC

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Tipo de interfaz virtual, en Tipo, elija Privada.
5. En Configuración de la interfaz virtual privada, realice lo siguiente:

a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

c. En Tipo de puerta de enlace, elija Puerta de enlace privada virtual o Puerta de enlace de Direct Connect.

d. En Propietario de la interfaz virtual, elija Otra AWS cuenta y, a continuación, introduzca la AWS cuenta.

e. En Puerta de enlace privada virtual, elija la puerta de enlace privada virtual para utilizar con esta interfaz.

f. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

g. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

Los valores válidos son 1 a 2147483647.

6. En Additional Settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

      [IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
      - En IP de mismo nivel del enrutador de Amazon, ingrese la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

      > **Important**
      >
      > Si permite la AWS asignación automática de direcciones IPv4, se asignará un CIDR /29 desde 169.254.0.0/16 IPv4 Link-Local de acuerdo con la RFC 3927 para la conectividad. point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP del mismo nivel del router del cliente como origen o destino del tráfico de VPC. En su lugar, debe utilizar la RFC 1918 u otro direccionamiento y especificar la dirección por su cuenta.
      >
      > - Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.
      > - Para obtener más información sobre la RFC 3927, consulte Dynamic Configuration of IPv4 Link-Local Addresses.

      [IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

   b. Para cambiar la unidad de transmisión máxima (MTU) de 1500 (predeterminada) a 9001 (tramas gigantes), seleccione MTU gigante (tamaño de MTU 9001).

   c. (Opcional) En Habilitar SiteLink, elija Habilitado para habilitar la conectividad directa entre los puntos de presencia de Direct Connect.

   d. (Opcional) Añada o elimine una etiqueta.

      [Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

      - En Key (Clave), escriba el nombre de la clave.

- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

7. Elija Create virtual interface (Crear interfaz virtual).

Paso 4: Compruebe la configuración de resiliencia de la interfaz virtual

Una vez que haya establecido las interfaces virtuales para la AWS nube o para Amazon VPC, realice una prueba de conmutación por error de la interfaz virtual para comprobar que la configuración cumple con los requisitos de resiliencia. Para obtener más información, consulte the section called "Prueba de conmutación por error de AWS Direct Connect".

Paso 5: Compruebe la conectividad de las interfaces virtuales

Una vez que haya establecido las interfaces virtuales con la AWS nube o con Amazon VPC, puede verificar la AWS Direct Connect conexión mediante los siguientes procedimientos.

Para verificar la conexión de su interfaz virtual a la nube AWS

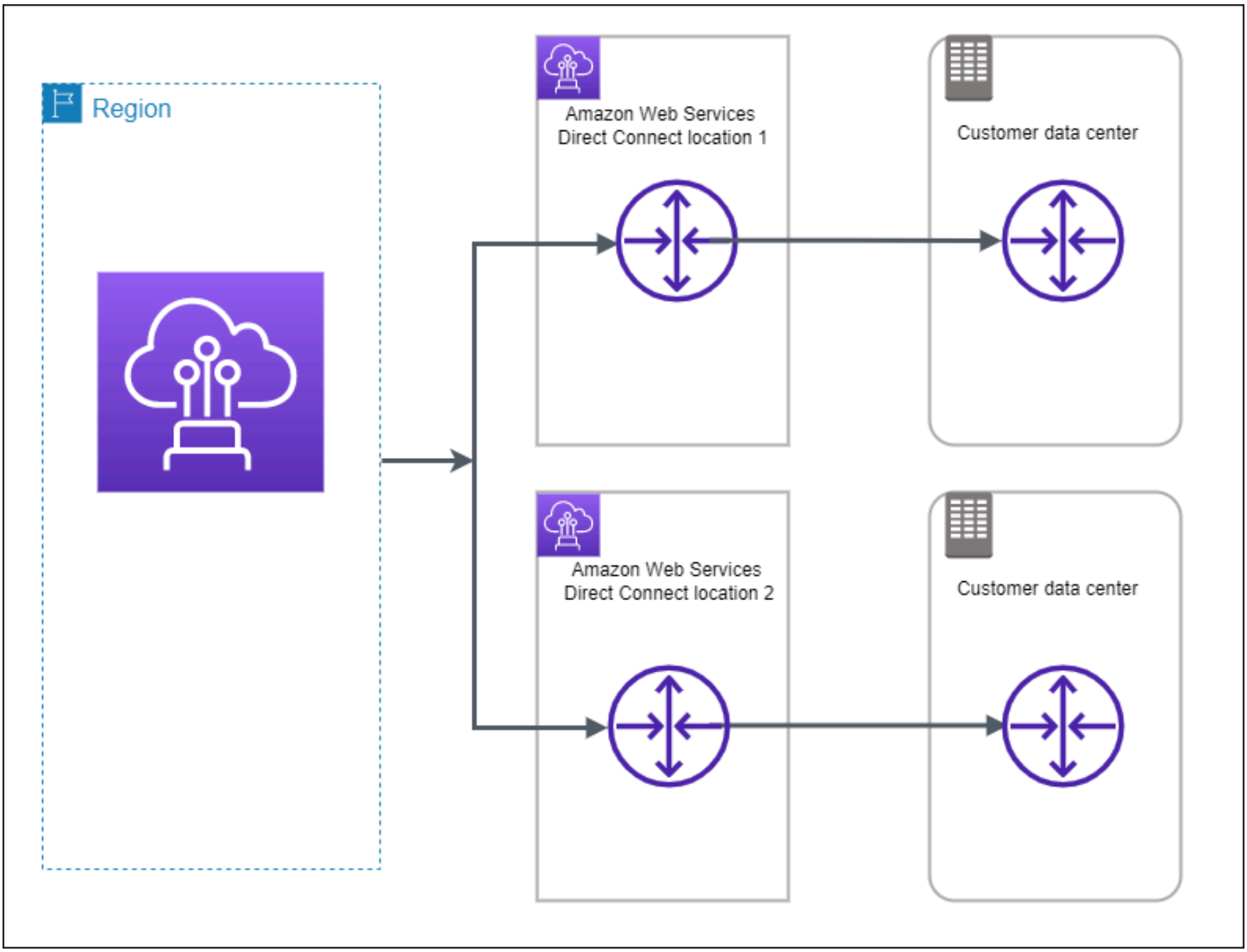
- Ejecute `traceroute` y verifique que el AWS Direct Connect identificador esté en el rastreo de la red.

Para verificar la conexión de la interfaz virtual a Amazon VPC

1. Mediante una AMI que permita hacer ping, como una AMI de Amazon Linux, lance una instancia de EC2 en la VPC adjunta a la puerta de enlace privada virtual. Las AMI de Amazon Linux se encuentran disponibles en la pestaña de Inicio rápido cuando utiliza el asistente de lanzamiento de instancias en la consola de Amazon EC2. Para obtener más información, consulte Lanzar una instancia en la Guía del usuario de Amazon EC2. Asegúrese de que el grupo de seguridad asociado a la instancia incluye una regla que permita el tráfico ICMP entrante (para la solicitud de ping).
2. Cuando la instancia se esté ejecutando, obtenga la dirección IPv4 privada (por ejemplo, 10.0.0.4). En la consola de Amazon EC2, se muestra la dirección en los datos de la instancia.
3. Haga ping a las direcciones IPv4 privadas y obtenga una respuesta.

Alta resiliencia

Puede conseguir una alta resiliencia para cargas de trabajo críticas mediante el uso de dos conexiones únicas a varias ubicaciones (tal y como se muestra en la siguiente figura). Este modelo proporciona resiliencia frente a errores de conectividad provocados por un corte de fibra o un error del dispositivo. También ayuda a evitar un error completo en la ubicación.



Los siguientes procedimientos muestran cómo utilizar el kit de herramientas de AWS Direct Connect resiliencia para configurar un modelo de alta resiliencia.

Temas

- Paso 1: Inscríbase en AWS
- Paso 2: Configurar el modelo de resiliencia

- Paso 3: Crear las interfaces virtuales
- Paso 4: Compruebe la configuración de resiliencia de la interfaz virtual
- Paso 5: Compruebe la conectividad de las interfaces virtuales

Paso 1: Inscríbase en AWS

Para usarla AWS Direct Connect, necesitas una AWS cuenta si aún no la tienes.

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de registrarte en un usuario Cuenta de AWS, protege Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilita y crea un usuario administrativo para que no utilices el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Signing in as the root user en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Paso 2: Configurar el modelo de resiliencia

Para configurar un modelo de alta resiliencia

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Conexiones y, a continuación, Crear una conexión.
3. En Connection ordering type (Tipo de solicitud de conexión), elija Connection wizard (Asistente de conexión).
4. En Resiliency level (Nivel de resiliencia), elija High Resiliency (Alta resiliencia), y, a continuación, elija Next (Siguiente).
5. En el panel Configure connections (Configurar conexiones), en Connection settings (Configuración de conexión), proceda del modo siguiente:

   a. En bandwidth (ancho de banda), elija el ancho de banda de la conexión.

      Este ancho de banda se aplica a todas las conexiones creadas.

   b. En el caso del proveedor de servicios de primera ubicación, seleccione la AWS Direct Connect ubicación adecuada.

   c. Si procede, en First Sub location (Primera ubicación secundaria), elija el piso más cercano a usted o a su proveedor de red. Esta opción solo está disponible si la ubicación dispone de Meet-Me Rooms (MMR) en varios pisos del edificio.

   d. Si ha seleccionado Other (Otro) para First location service provider (Proveedor de servicios de la primera ubicación), en Name of other provider (Nombre de otro proveedor), escriba el nombre del socio que utiliza.

   e. En Proveedor de servicios de segunda ubicación, seleccione la AWS Direct Connect ubicación adecuada.

f. Si procede, en Second Sub location (Segunda ubicación secundaria), elija el piso más cercano a usted o a su proveedor de red. Esta opción solo está disponible si la ubicación dispone de Meet-Me Rooms (MMR) en varios pisos del edificio.

g. Si ha seleccionado Other (Otro) en Second location service provider, (Proveedor de servicios de la segunda ubicación), en Name of other provider (Nombre de otro proveedor), escriba el nombre del socio que utiliza.

h. (Opcional) Añada o elimine una etiqueta.

   [Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

   - En Key (Clave), escriba el nombre de la clave.
   - En Valor, escriba el valor de la clave.

   [Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

6. Elija Siguiente.
7. Revise las conexiones y, a continuación, elija Continue (Continuar).

   Si las LOA están listas, puede elegir Download LOA (Descargar LOA), y, a continuación, hacer clic en Continue (Continuar).

   La revisión de la solicitud y el aprovisionamiento de un puerto para la conexión pueden tardar hasta 72 horas. AWS Durante este tiempo, es posible que reciba un correo electrónico con una solicitud de información adicional sobre su caso de uso o sobre la ubicación especificada. El correo electrónico se envía a la dirección de correo electrónico que utilizaste cuando te registraste AWS. Si no responde en un plazo de 7 días, se eliminará la conexión.

Paso 3: Crear las interfaces virtuales

Puede crear una interfaz virtual privada para conectarla a la VPC. O bien, puede crear una interfaz virtual pública para conectarse a AWS servicios públicos que no estén en una VPC. Al crear una interfaz virtual privada con una VPC, necesita una interfaz virtual privada para cada VPC a la que se va a conectar. Por ejemplo, necesita tres interfaces virtuales privadas para conectarse a tres VPC.

Antes de comenzar, asegúrese de que dispone de la siguiente información:

Recurso	Información necesaria
Conexión	El grupo de AWS Direct Connect conexión o agregación de enlaces (LAG) para el que va a crear la interfaz virtual.
Nombre de la interfaz virtual	Un nombre para la interfaz virtual.
Propietario de la interfaz virtual	Si va a crear la interfaz virtual para otra cuenta, necesitará el ID de AWS cuenta de la otra cuenta.
(Solo para la interfaz virtual privada) Conexión	Para conectarse a una VPC de la misma AWS región, necesita la puerta de enlace privada virtual para su VPC. El ASN del lado de Amazon de la sesión del BGP se hereda de la puerta de enlace privada virtual. Al crear una puerta de enlace privada virtual, puede especificar su propio ASN privado. De lo contrario, Amazon proporciona un ASN predeterminado. Para obtener información, consulte Crear una puerta de enlace privada virtual en la Guía del usuario de Amazon VPC. Para conectarse a una VPC a través de una puerta de enlace de Direct Connect, se necesita la puerta de enlace de Direct Connect. Para obtener más información, consulte Gateways de Direct Connect.
VLAN	Una etiqueta de red de área local virtual (VLAN) única que aún no se encuentra en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de AWS Direct Connect . Si tiene una conexión alojada, su AWS Direct Connect socio le proporcionará este valor. No puede modificar el valor después de haber creado la interfaz virtual.
Direcciones IP de mismo nivel	Una interfaz virtual es compatible con una sesión de intercambio de tráfico del BGP para IPv4 e IPv6, o con uno de cada una (pila doble). No utilice direccion es IP elásticas (eIP) ni traiga sus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias sesiones de BGP para la misma familia de direccionamiento IP en la misma interfaz virtual. Los rangos de las direcciones IP que se asignan a cada extremo de la interfaz virtual para la sesión de intercambio de tráfico del BGP.

Recurso	Información necesaria
	• IPv4: • (Solo para la interfaz virtual pública) Debe especificar direcciones IPv4 públicas únicas que sean de su propiedad. El valor puede ser uno de los siguientes: • Un CIDR IPv4 propiedad del cliente Puede ser cualquier IP pública (propiedad del cliente o proporcionada por él AWS), pero se debe usar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del router. AWS Por ejemplo, si asigna un `/31` rango, por ejemplo, podría usarlo `203.0.113.0` para su IP homóloga y `203.0.113.1` para la AWS IP homóloga. `203.0.113.0/31` O bien, si asignas un `/24` rango, por ejemplo`198.51.100.0/24` , puedes usarlo `198.51.100.10` para tu IP homóloga y `198.51.100.20` para la IP AWS homóloga. • Un rango de IP propiedad de su AWS Direct Connect socio o ISP, junto con una autorización LOA-CFA • Un AWS CIDR /31 proporcionado. Póngase en contacto con AWS Asistencia para solicitar un CIDR IPv4 público (e indique un caso de uso en su solicitud) **Note** No podemos garantizar que podamos cumplir con todas las solicitudes de direcciones IPv4 públicas AWS proporcionadas. • (Solo para la interfaz virtual privada) Amazon puede generar direcciones IPv4 privadas en su nombre. Si especifica el suyo propio, asegúrese de especificar únicamente los CIDR privados para la interfaz de su router y la interfaz AWS Direct Connect. Por ejemplo, no especifique otras direcciones IP de su red local. Al igual que en una interfaz virtual pública, se debe usar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del AWS router. Por ejemplo, si asigna un `/30` rango, por ejemplo, podría usarlo `192.168.0.1` para su IP homóloga y `192.168.0.2` para la IP AWS homóloga. `192.168.0.0/30`

Recurso	Información necesaria
	• IPv6: Amazon le asigna un CIDR IPv6 /125 de forma automática. No puede especificar sus propias direcciones IPv6 de mismo nivel.
Familia de direcciones	Si la sesión de intercambio de tráfico del BGP se realizará a través de IPv4 o IPv6.
Información sobre el BGP	• Un número de sistema autónomo (ASN) para el protocolo de puerta de enlace fronteriza (BGP) público o privado en su lado de la sesión del BGP. Si utiliza un ASN público, debe tener uno propio. Si utiliza un ASN privado, puede establecer un valor de ASN personalizado. Para un ASN de 16 bits ASN, el valor debe estar dentro del rango de 64 512 a 65 534. En el caso de un ASN de 32 bits, el valor debe estar dentro del rango de 1 a 2147483647. El sistema autónomo (AS) que se antepone no funciona si utiliza un ASN privado para una interfaz virtual pública. • AWS habilita MD5 de forma predeterminada. Esta opción no se puede modificar. • Una clave de autenticación del BGP MD5. Puede proporcionar su propia clave o dejar que Amazon genere una en su nombre.

Recurso	Información necesaria

(Solo para la interfaz virtual pública) Prefijos que desea anunciar	Rutas IPv4 públicas o rutas IPv6 para anunciar a través del BGP. Debe comunicar al menos un prefijo a través del BGP, hasta un máximo de 1 000 prefijos.
	• IPv4: el CIDR de IPv4 puede superponerse con otro CIDR de IPv4 público que se haya anunciado que se utiliza AWS Direct Connect cuando se cumple alguna de las siguientes condiciones:
	  • Los CIDR provienen de distintas regiones. AWS Asegúrese de aplicar etiquetas de comunidad del BGP a los prefijos públicos.
	  • Utiliza AS_PATH cuando tiene un ASN público en una configuración activa/pasiva.
	  Para obtener más información, consulte Políticas de enrutamiento y comunidades del BGP.
	• IPv6: especifique una longitud de prefijo de /64 caracteres o menos.
	• Puede agregar prefijos adicionales a una VIF pública existente y anunciarl os si se pone en contacto con AWS Asistencia. En su caso de soporte, proporcione una lista de los prefijos de CIDR adicionales que desee agregar a la VIF pública y anunciar.
	• Puede especificar cualquier longitud de prefijo en una interfaz virtual pública de Direct Connect. IPv4 debería admitir cualquier valor entre /1 y /32, e IPv6 debería admitir cualquier valor entre /1 y /64.

Recurso	Información necesaria
(Solo para la interfaz virtual privada) Tramas gigantes	La unidad máxima de transmisión (MTU) de los paquetes superados. AWS Direct Connect El valor predeterminado es 1500. El establecimiento de la MTU de una interfaz virtual en 9001 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Las tramas gigantes solo se aplican a las rutas propagadas desde. AWS Direct Connect Si agrega rutas estáticas a una tabla de enrutamiento que apuntan a una gateway privada virtual, el tráfico enrutado a través de las rutas estáticas se envía utilizando 1500 MTU. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Jumbo Frame Capable en la página de configuración general de la interfaz virtual.
(Solo para la interfaz virtual de tránsito) Tramas gigantes	La unidad máxima de transmisión (MTU) de los paquetes superados. AWS Direct Connect El valor predeterminado es 1500. El establecimiento de la MTU de una interfaz virtual en 8500 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Se admiten tramas gigantes de hasta 8500 de MTU para Direct Connect. Las rutas estáticas y propagadas configuradas en la tabla de enrutamiento de puerta de enlace de tránsito admitirán tramas gigantes, incluso desde instancias de EC2 con entradas de la tabla de enrutamiento estáticas de VPC hasta la conexión de puerta de enlace de tránsito. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Capacidad para tramas gigantes en la página de configuración general de la interfaz virtual.

Si sus prefijos públicos o ASN pertenecen a un ISP o a un operador de red, AWS le solicitará información adicional. Esta información puede ser un documento con un membrete oficial de la empresa o un correo electrónico proveniente del nombre de dominio de la empresa que confirme que usted puede utilizar el prefijo de red o el ASN.

Al crear una interfaz virtual pública, revisar y aprobar la solicitud AWS puede tardar hasta 72 horas.

Para aprovisionar una interfaz virtual pública a servicios que no sean de una VPC

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Virtual interface type (Tipo de interfaz virtual) en Type (Tipo), elija Public (Pública).
5. En Public virtual interface settings (Configuración de la interfaz virtual pública), haga lo siguiente:

   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

   c. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

   d. En BGP ASN, escriba el número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) de la gateway.

      Los valores válidos son 1-2.147.483.647.
6. En Additional settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

      [IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
      - En Amazon router peer IP (IP del mismo nivel del router de Amazon), escriba la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

      [IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

   b. Para utilizar su propia clave de BGP, introduzca su clave MD5 de BGP.

      Si no ingresa un valor, generamos una clave de BGP.

c. Para anunciar prefijos para Amazon, en Prefixes you want to advertise (Prefijos que desea anunciar), escriba las direcciones CIDR IPv4 de destino (separadas por comas) a las que debe redirigirse el tráfico a través de la interfaz virtual.

d. (Opcional) Añada o elimine una etiqueta.

   [Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

   - En Key (Clave), escriba el nombre de la clave.
   - En Valor, escriba el valor de la clave.

   [Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

7. Elija Create virtual interface (Crear interfaz virtual).

Para aprovisionar una interfaz virtual privada a una VPC

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Tipo de interfaz virtual, en Tipo, elija Privada.
5. En Configuración de la interfaz virtual privada, realice lo siguiente:

   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

   c. En Tipo de puerta de enlace, elija Puerta de enlace privada virtual o Puerta de enlace de Direct Connect.

   d. En Propietario de la interfaz virtual, elija Otra AWS cuenta y, a continuación, introduzca la AWS cuenta.

   e. En Puerta de enlace privada virtual, elija la puerta de enlace privada virtual para utilizar con esta interfaz.

   f. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

   g. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

      Los valores válidos son 1 a 2147483647.

6. En Additional Settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

      [IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
      - En IP de mismo nivel del enrutador de Amazon, ingrese la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

      > **Important**
      >
      > Si permite la AWS asignación automática de direcciones IPv4, se asignará un CIDR /29 desde 169.254.0.0/16 IPv4 Link-Local de acuerdo con la RFC 3927 para la conectividad. point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP del mismo nivel del router del cliente como origen o destino del tráfico de VPC. En su lugar, debe utilizar la RFC 1918 u otro direccionamiento y especificar la dirección por su cuenta.
      >
      > - Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.
      > - Para obtener más información sobre la RFC 3927, consulte Dynamic Configuration of IPv4 Link-Local Addresses.

      [IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

   b. Para cambiar la unidad de transmisión máxima (MTU) de 1500 (predeterminada) a 9001 (tramas gigantes), seleccione MTU gigante (tamaño de MTU 9001).

   c. (Opcional) En Habilitar SiteLink, elija Habilitado para habilitar la conectividad directa entre los puntos de presencia de Direct Connect.

   d. (Opcional) Añada o elimine una etiqueta.

      [Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

      - En Key (Clave), escriba el nombre de la clave.

- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

7. Elija Create virtual interface (Crear interfaz virtual).

Paso 4: Compruebe la configuración de resiliencia de la interfaz virtual

Una vez que haya establecido las interfaces virtuales para la AWS nube o para Amazon VPC, realice una prueba de conmutación por error de la interfaz virtual para comprobar que la configuración cumple con los requisitos de resiliencia. Para obtener más información, consulte the section called "Prueba de conmutación por error de AWS Direct Connect".

Paso 5: Compruebe la conectividad de las interfaces virtuales

Una vez que haya establecido las interfaces virtuales con la AWS nube o con Amazon VPC, puede verificar la AWS Direct Connect conexión mediante los siguientes procedimientos.

Para verificar la conexión de su interfaz virtual a la nube AWS

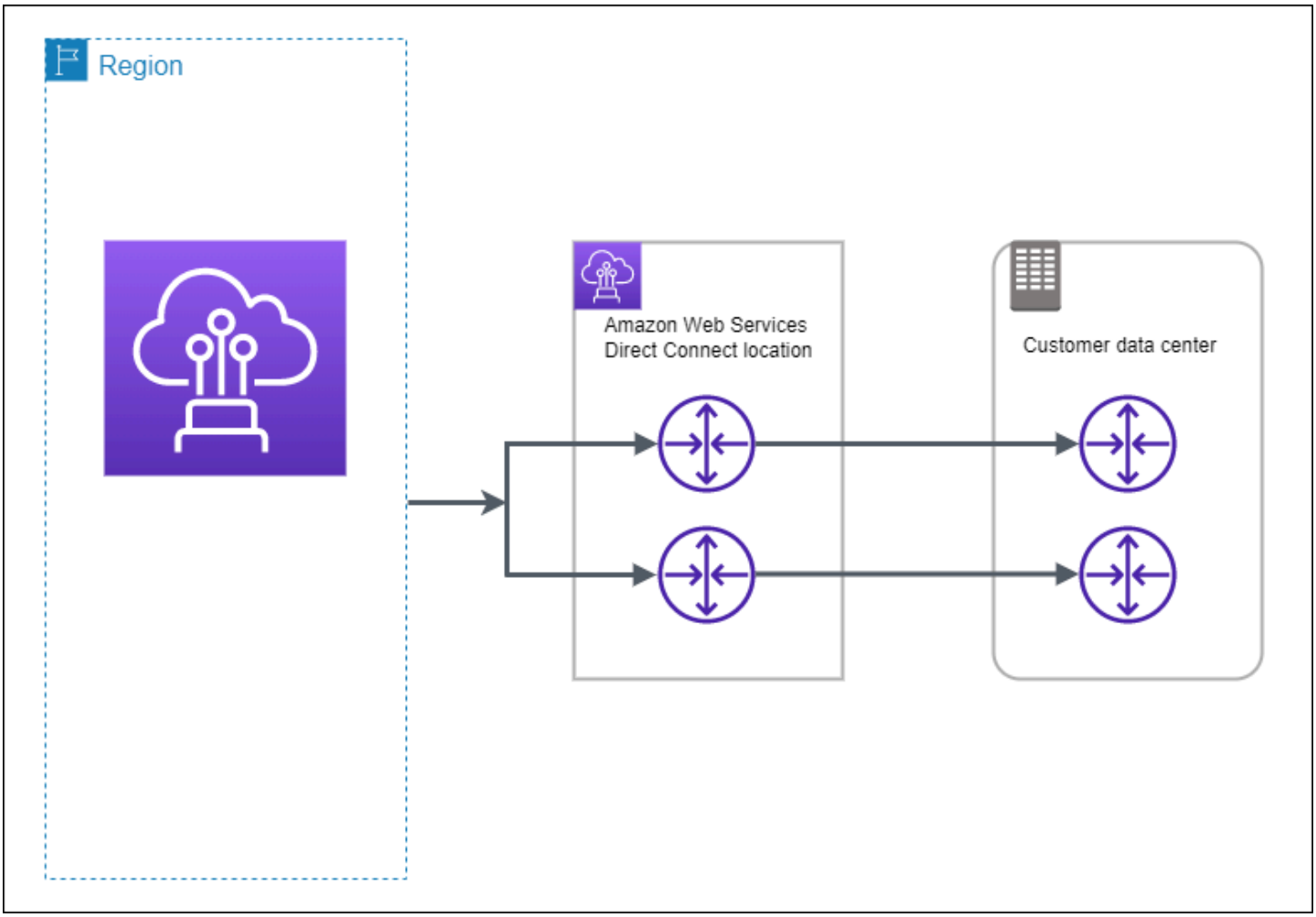
- Ejecute `traceroute` y verifique que el AWS Direct Connect identificador esté en el rastreo de la red.

Para verificar la conexión de la interfaz virtual a Amazon VPC

1. Mediante una AMI que permita hacer ping, como una AMI de Amazon Linux, lance una instancia de EC2 en la VPC adjunta a la puerta de enlace privada virtual. Las AMI de Amazon Linux se encuentran disponibles en la pestaña de Inicio rápido cuando utiliza el asistente de lanzamiento de instancias en la consola de Amazon EC2. Para obtener más información, consulte Lanzar una instancia en la Guía del usuario de Amazon EC2. Asegúrese de que el grupo de seguridad asociado a la instancia incluye una regla que permita el tráfico ICMP entrante (para la solicitud de ping).
2. Cuando la instancia se esté ejecutando, obtenga la dirección IPv4 privada (por ejemplo, 10.0.0.4). En la consola de Amazon EC2, se muestra la dirección en los datos de la instancia.
3. Haga ping a las direcciones IPv4 privadas y obtenga una respuesta.

Desarrollo y pruebas

Puede conseguir resiliencia de desarrollo y pruebas para cargas de trabajo no críticas mediante el uso de conexiones independientes que terminan en dispositivos independientes en una ubicación (tal y como se muestra en la siguiente figura). Este modelo proporciona resiliencia frente a errores de dispositivos, pero no ofrece resiliencia frente a errores de ubicación.



Los siguientes procedimientos muestran cómo utilizar el kit de herramientas de AWS Direct Connect resiliencia para configurar un modelo de resiliencia de desarrollo y prueba.

Temas

- Paso 1: Inscríbase en AWS
- Paso 2: Configurar el modelo de resiliencia
- Paso 3: Crear una interfaz virtual
- Paso 4: Compruebe la configuración de resiliencia de la interfaz virtual

- Paso 5: Compruebe la interfaz virtual

Paso 1: Inscríbase en AWS

Para usarla AWS Direct Connect, necesitas una AWS cuenta si aún no la tienes.

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en una Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea una. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de registrarte en un usuario Cuenta de AWS, protege Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilita y crea un usuario administrativo para que no utilices el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Signing in as the root user en la Guía del usuario de AWS Sign-In .

2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .

2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Paso 2: Configurar el modelo de resiliencia

Para configurar el modelo de resiliencia

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Conexiones y, a continuación, Crear una conexión.
3. En Connection ordering type (Tipo de solicitud de conexión), elija Connection wizard (Asistente de conexión).
4. En Resiliency level (Nivel de resiliencia), elija Development and test (Desarrollo y pruebas) y, a continuación, elija Next (Siguiente).
5. En el panel Configure connections (Configurar conexiones), en Connection settings (Configuración de conexión), proceda del modo siguiente:

   a. En bandwidth (ancho de banda), elija el ancho de banda de la conexión.

      Este ancho de banda se aplica a todas las conexiones creadas.

   b. En el caso del proveedor de servicios de primera ubicación, seleccione la AWS Direct Connect ubicación adecuada.

   c. Si procede, en First Sub location (Primera ubicación secundaria), elija el piso más cercano a usted o a su proveedor de red. Esta opción solo está disponible si la ubicación dispone de Meet-Me Rooms (MMR) en varios pisos del edificio.

   d. Si ha seleccionado Other (Otro) para First location service provider (Proveedor de servicios de la primera ubicación), en Name of other provider (Nombre de otro proveedor), escriba el nombre del socio que utiliza.

   e. (Opcional) Añada o elimine una etiqueta.

      [Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

      - En Key (Clave), escriba el nombre de la clave.
      - En Valor, escriba el valor de la clave.

      [Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

6. Elija Siguiente.

7. Revise las conexiones y, a continuación, elija Continue (Continuar).

   Si las LOA están listas, puede elegir Download LOA (Descargar LOA), y, a continuación, hacer clic en Continue (Continuar).

   La revisión de la solicitud y el aprovisionamiento de un puerto para la conexión pueden tardar hasta 72 horas. AWS Durante este tiempo, es posible que reciba un correo electrónico con una solicitud de información adicional sobre su caso de uso o sobre la ubicación especificada. El correo electrónico se envía a la dirección de correo electrónico que utilizaste cuando te registraste AWS. Si no responde en un plazo de 7 días, se eliminará la conexión.

Paso 3: Crear una interfaz virtual

Para empezar a utilizar AWS Direct Connect la conexión, debe crear una interfaz virtual. Puede crear una interfaz virtual privada para conectarla a la VPC. O bien, puede crear una interfaz virtual pública para conectarse a AWS servicios públicos que no estén en una VPC. Al crear una interfaz virtual privada con una VPC, necesita una interfaz virtual privada para cada VPC a la que se va a conectar. Por ejemplo, necesita tres interfaces virtuales privadas para conectarse a tres VPC.

Antes de comenzar, asegúrese de que dispone de la siguiente información:

Recurso	Información necesaria
Conexión	El grupo de AWS Direct Connect conexión o agregación de enlaces (LAG) para el que va a crear la interfaz virtual.
Nombre de la interfaz virtual	Un nombre para la interfaz virtual.
Propietario de la interfaz virtual	Si va a crear la interfaz virtual para otra cuenta, necesitará el ID de AWS cuenta de la otra cuenta.
(Solo para la interfaz virtual privada) Conexión	Para conectarse a una VPC de la misma AWS región, necesita la puerta de enlace privada virtual para su VPC. El ASN del lado de Amazon de la sesión del BGP se hereda de la puerta de enlace privada virtual. Al crear una puerta de enlace privada virtual, puede especificar su propio ASN privado. De lo contrario, Amazon proporciona un ASN predeterminado. Para obtener información, consulte Crear una puerta de enlace privada virtual en la Guía

Recurso	Información necesaria
	del usuario de Amazon VPC. Para conectarse a una VPC a través de una puerta de enlace de Direct Connect, se necesita la puerta de enlace de Direct Connect. Para obtener más información, consulte Gateways de Direct Connect.
VLAN	Una etiqueta de red de área local virtual (VLAN) única que aún no se encuentra en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de AWS Direct Connect . Si tiene una conexión alojada, su AWS Direct Connect socio le proporcionará este valor. No puede modificar el valor después de haber creado la interfaz virtual.

Recurso	Información necesaria

Direcciones IP de mismo nivel	Una interfaz virtual es compatible con una sesión de intercambio de tráfico del BGP para IPv4 e IPv6, o con uno de cada una (pila doble). No utilice direccion es IP elásticas (eIP) ni traiga sus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias sesiones de BGP para la misma familia de direccionamiento IP en la misma interfaz virtual. Los rangos de las direcciones IP que se asignan a cada extremo de la interfaz virtual para la sesión de intercambio de tráfico del BGP.
	
	• IPv4:
	  • (Solo para la interfaz virtual pública) Debe especificar direcciones IPv4 públicas únicas que sean de su propiedad. El valor puede ser uno de los siguientes:
	  • Un CIDR IPv4 propiedad del cliente
	
	Puede ser cualquier IP pública (propiedad del cliente o proporcio nada por él AWS), pero se debe usar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del router. AWS Por ejemplo, si asigna un `/31` rango, por ejemplo, podría usarlo `203.0.113.0` para su IP homóloga y `203.0.113.1` para la AWS IP homóloga. `203.0.113.0/31` O bien, si asignas un `/24` rango, por ejemplo`198.51.100.0/24` , puedes usarlo `198.51.100.10` para tu IP homóloga y `198.51.100.20` para la IP AWS homóloga.
	  • Un rango de IP propiedad de su AWS Direct Connect socio o ISP, junto con una autorización LOA-CFA
	  • Un AWS CIDR /31 proporcionado. Póngase en contacto con AWS Asistencia para solicitar un CIDR IPv4 público (e indique un caso de uso en su solicitud)
	
	Note
	No podemos garantizar que podamos cumplir con todas las solicitudes de direcciones IPv4 públicas AWS proporcionadas.
	  • (Solo para la interfaz virtual privada) Amazon puede generar direcciones IPv4 privadas en su nombre. Si especifica el suyo propio, asegúrese de

Recurso	Información necesaria
	especificar únicamente los CIDR privados para la interfaz de su router y la interfaz AWS Direct Connect. Por ejemplo, no especifique otras direcciones IP de su red local. Al igual que en una interfaz virtual pública, se debe usar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del AWS router. Por ejemplo, si asigna un `/30` rango, por ejemplo, podría usarlo `192.168.0.1` para su IP homóloga y `192.168.0.2` para la IP AWS homóloga. `192.168.0.0/30` • IPv6: Amazon le asigna un CIDR IPv6 /125 de forma automática. No puede especificar sus propias direcciones IPv6 de mismo nivel.
Familia de direcciones	Si la sesión de intercambio de tráfico del BGP se realizará a través de IPv4 o IPv6.
Información sobre el BGP	• Un número de sistema autónomo (ASN) para el protocolo de puerta de enlace fronteriza (BGP) público o privado en su lado de la sesión del BGP. Si utiliza un ASN público, debe tener uno propio. Si utiliza un ASN privado, puede establecer un valor de ASN personalizado. Para un ASN de 16 bits ASN, el valor debe estar dentro del rango de 64 512 a 65 534. En el caso de un ASN de 32 bits, el valor debe estar dentro del rango de 1 a 2147483647. El sistema autónomo (AS) que se antepone no funciona si utiliza un ASN privado para una interfaz virtual pública. • AWS habilita MD5 de forma predeterminada. Esta opción no se puede modificar. • Una clave de autenticación del BGP MD5. Puede proporcionar su propia clave o dejar que Amazon genere una en su nombre.

Recurso	Información necesaria

(Solo para la interfaz virtual pública) Prefijos que desea anunciar	Rutas IPv4 públicas o rutas IPv6 para anunciar a través del BGP. Debe comunicar al menos un prefijo a través del BGP, hasta un máximo de 1 000 prefijos.
	• IPv4: el CIDR de IPv4 puede superponerse con otro CIDR de IPv4 público que se haya anunciado que se utiliza AWS Direct Connect cuando se cumple alguna de las siguientes condiciones:
	  • Los CIDR provienen de distintas regiones. AWS Asegúrese de aplicar etiquetas de comunidad del BGP a los prefijos públicos.
	  • Utiliza AS_PATH cuando tiene un ASN público en una configuración activa/pasiva.
	  Para obtener más información, consulte Políticas de enrutamiento y comunidades del BGP.
	• IPv6: especifique una longitud de prefijo de /64 caracteres o menos.
	• Puede agregar prefijos adicionales a una VIF pública existente y anunciarl os si se pone en contacto con AWS Asistencia. En su caso de soporte, proporcione una lista de los prefijos de CIDR adicionales que desee agregar a la VIF pública y anunciar.
	• Puede especificar cualquier longitud de prefijo en una interfaz virtual pública de Direct Connect. IPv4 debería admitir cualquier valor entre /1 y /32, e IPv6 debería admitir cualquier valor entre /1 y /64.

Recurso	Información necesaria
(Solo para la interfaz virtual privada) Tramas gigantes	La unidad máxima de transmisión (MTU) de los paquetes superados. AWS Direct Connect El valor predeterminado es 1500. El establecimiento de la MTU de una interfaz virtual en 9001 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Las tramas gigantes solo se aplican a las rutas propagadas desde. AWS Direct Connect Si agrega rutas estáticas a una tabla de enrutamiento que apuntan a una gateway privada virtual, el tráfico enrutado a través de las rutas estáticas se envía utilizando 1500 MTU. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Jumbo Frame Capable en la página de configuración general de la interfaz virtual.
(Solo para la interfaz virtual de tránsito) Tramas gigantes	La unidad máxima de transmisión (MTU) de los paquetes superados. AWS Direct Connect El valor predeterminado es 1500. El establecimiento de la MTU de una interfaz virtual en 8500 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Se admiten tramas gigantes de hasta 8500 de MTU para Direct Connect. Las rutas estáticas y propagadas configuradas en la tabla de enrutamiento de puerta de enlace de tránsito admitirán tramas gigantes, incluso desde instancias de EC2 con entradas de la tabla de enrutamiento estáticas de VPC hasta la conexión de puerta de enlace de tránsito. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Capacidad para tramas gigantes en la página de configuración general de la interfaz virtual.

Si sus prefijos públicos o ASN pertenecen a un ISP o un operador de red, le solicitamos información adicional. Esta información puede ser un documento con un membrete oficial de la empresa o un correo electrónico proveniente del nombre de dominio de la empresa que confirme que usted puede utilizar el prefijo de red o el ASN.

Al crear una interfaz virtual pública, AWS puede tardar hasta 72 horas en revisar y aprobar la solicitud.

Para aprovisionar una interfaz virtual pública a servicios que no sean de una VPC

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Virtual interface type (Tipo de interfaz virtual) en Type (Tipo), elija Public (Pública).
5. En Public virtual interface settings (Configuración de la interfaz virtual pública), haga lo siguiente:

   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

   c. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

   d. En BGP ASN, escriba el número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) de la gateway.

      Los valores válidos son 1-2.147.483.647.
6. En Additional settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

      [IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
      - En Amazon router peer IP (IP del mismo nivel del router de Amazon), escriba la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

      [IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

   b. Para utilizar su propia clave de BGP, introduzca su clave MD5 de BGP.

Si no ingresa un valor, generamos una clave de BGP.

c. Para anunciar prefijos para Amazon, en Prefixes you want to advertise (Prefijos que desea anunciar), escriba las direcciones CIDR IPv4 de destino (separadas por comas) a las que debe redirigirse el tráfico a través de la interfaz virtual.

d. (Opcional) Añada o elimine una etiqueta.

[Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

- En Key (Clave), escriba el nombre de la clave.
- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

7. Elija Create virtual interface (Crear interfaz virtual).

Para aprovisionar una interfaz virtual privada a una VPC

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Tipo de interfaz virtual, en Tipo, elija Privada.
5. En Configuración de la interfaz virtual privada, realice lo siguiente:

a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

c. En Tipo de puerta de enlace, elija Puerta de enlace privada virtual o Puerta de enlace de Direct Connect.

d. En Propietario de la interfaz virtual, elija Otra AWS cuenta y, a continuación, introduzca la AWS cuenta.

e. En Puerta de enlace privada virtual, elija la puerta de enlace privada virtual para utilizar con esta interfaz.

f. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

g. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

Los valores válidos son 1 a 2147483647.

6. En Additional Settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

      [IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
      - En IP de mismo nivel del enrutador de Amazon, ingrese la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

      > **Important**
      >
      > Si permite la AWS asignación automática de direcciones IPv4, se asignará un CIDR /29 desde 169.254.0.0/16 IPv4 Link-Local de acuerdo con la RFC 3927 para la conectividad. point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP del mismo nivel del router del cliente como origen o destino del tráfico de VPC. En su lugar, debe utilizar la RFC 1918 u otro direccionamiento y especificar la dirección por su cuenta.
      >
      > - Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.
      > - Para obtener más información sobre la RFC 3927, consulte Dynamic Configuration of IPv4 Link-Local Addresses.

      [IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

   b. Para cambiar la unidad de transmisión máxima (MTU) de 1500 (predeterminada) a 9001 (tramas gigantes), seleccione MTU gigante (tamaño de MTU 9001).

   c. (Opcional) En Habilitar SiteLink, elija Habilitado para habilitar la conectividad directa entre los puntos de presencia de Direct Connect.

   d. (Opcional) Añada o elimine una etiqueta.

[Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

- En Key (Clave), escriba el nombre de la clave.
- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

7. Elija Create virtual interface (Crear interfaz virtual).

Paso 4: Compruebe la configuración de resiliencia de la interfaz virtual

Una vez que haya establecido las interfaces virtuales para la AWS nube o para Amazon VPC, realice una prueba de conmutación por error de la interfaz virtual para comprobar que la configuración cumple con los requisitos de resiliencia. Para obtener más información, consulte the section called “Prueba de conmutación por error de AWS Direct Connect”.

Paso 5: Compruebe la interfaz virtual

Una vez que haya establecido las interfaces virtuales con la AWS nube o con Amazon VPC, puede verificar la AWS Direct Connect conexión mediante los siguientes procedimientos.

Para verificar la conexión de su interfaz virtual a la nube AWS

- Ejecute `traceroute` y verifique que el AWS Direct Connect identificador esté en el rastreo de la red.

Para verificar la conexión de la interfaz virtual a Amazon VPC

1. Mediante una AMI que permita hacer ping, como una AMI de Amazon Linux, lance una instancia de EC2 en la VPC adjunta a la puerta de enlace privada virtual. Las AMI de Amazon Linux se encuentran disponibles en la pestaña de Inicio rápido cuando utiliza el asistente de lanzamiento de instancias en la consola de Amazon EC2. Para obtener más información, consulte Lanzar una instancia en la Guía del usuario de Amazon EC2. Asegúrese de que el grupo de seguridad asociado a la instancia incluye una regla que permita el tráfico ICMP entrante (para la solicitud de ping).
2. Cuando la instancia se esté ejecutando, obtenga la dirección IPv4 privada (por ejemplo, 10.0.0.4). En la consola de Amazon EC2, se muestra la dirección en los datos de la instancia.
3. Haga ping a las direcciones IPv4 privadas y obtenga una respuesta.

Classic

Seleccione Classic si tiene conexiones existentes.

Los siguientes procedimientos muestran los escenarios comunes para llevar a cabo la configuración de una conexión de AWS Direct Connect .

Contenido

Requisitos previos

Para conexiones AWS Direct Connect con velocidades de puerto de 1 Gbps o superiores, asegúrese de que la red cumpla los siguientes requisitos:

- Su red debe utilizar fibra monomodo con un transceptor 1000BASE-LX (1310 nm) para 1 gigabit Ethernet, un transceptor 10GBASE-LR (1310 nm) para 10 gigabit o un 100GBASE-LR4 para 100 gigabit Ethernet.
- La negociación automática de un puerto debe estar deshabilitada para una conexión con una velocidad de puerto superior a 1 Gbps. Sin embargo, según el punto final de AWS Direct Connect que dé servicio a su conexión, es posible que sea necesario activar o desactivar la negociación automática para las conexiones de 1 Gbps. Si la interfaz virtual permanece inactiva, consulte Solución de problemas de capa 2 (enlace de datos).
- La encapsulación de VLAN 802.1Q debe ser compatible en toda la conexión, incluidos los dispositivos intermedios.
- Su dispositivo debe ser compatible con el protocolo de puerta de enlace fronteriza (BGP) y la autenticación MD5 del BGP.

- (Opcional) Puede configurar la detección de reenvío bidireccional (BFD) en la red. La BFD asíncrona se habilita automáticamente para cada interfaz virtual. AWS Direct Connect Se habilita de forma automática en las interfaces virtuales de Direct Connect, pero no funcionará hasta que la configure en el enrutador. A fin de obtener más información, consulte Habilitar la BFD para una conexión de Direct Connect.

Paso 1: Inscríbase en AWS

Para usarla AWS Direct Connect, necesitas una cuenta si aún no la tienes.

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirte a una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Signing in as the root user en la Guía del usuario de AWS Sign-In .
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center .
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center .

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center .

Paso 2: Solicita una conexión AWS Direct Connect dedicada

En el caso de las conexiones dedicadas, puede enviar una solicitud de conexión mediante la AWS Direct Connect consola. En el caso de las conexiones alojadas, trabaje con un AWS Direct Connect socio para solicitar una conexión alojada. Asegúrese de que dispone de la siguiente información:

- La velocidad de puerto que necesita. No se puede cambiar la velocidad del puerto después de crear la solicitud de conexión.
- La AWS Direct Connect ubicación en la que se va a finalizar la conexión.

> **Note**
>
> No puede usar la AWS Direct Connect consola para solicitar una conexión alojada. En su lugar, póngase en contacto con un AWS Direct Connect socio, quien podrá crear una conexión alojada para usted, y luego usted la aceptará. Omita el siguiente procedimiento y vaya a Aceptación de la conexión alojada.

Para crear una AWS Direct Connect conexión nueva

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Conexiones y, a continuación, Crear una conexión.
3. Elija Classic.
4. En el panel Create Connection (Crear conexión), en Connection settings (Configuración de conexión) haga lo siguiente:

   a. En Name (Nombre), escriba un nombre para la conexión.

   b. En Location (Ubicación), seleccione la ubicación de AWS Direct Connect apropiada.

c. Si procede, en Sub Location (Sububicación), elija el piso más cercano a usted o a su proveedor de red. Esta opción solo está disponible si la ubicación dispone de Meet-Me Rooms (MMR) en varios pisos del edificio.

d. En Port Speed (Velocidad del puerto), elija el ancho de banda de la conexión.

e. En el caso de las instalaciones, seleccione Conectarse a través de un AWS Direct Connect socio cuando utilice esta conexión para conectarse a su centro de datos.

f. En el caso del proveedor de servicios, selecciona el AWS Direct Connect socio. Si utiliza un socio que no está en la lista, seleccione Other (Otro).

g. Si ha seleccionado Other (Otro) en Service provider (Proveedor de servicios), en Name of other provider (Nombre de otro proveedor), escriba el nombre del socio que utiliza.

h. (Opcional) Añada o elimine una etiqueta.

   [Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

   - En Key (Clave), escriba el nombre de la clave.
   - En Valor, escriba el valor de la clave.

   [Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

5. Elija Create Connection (Crear conexión).

La revisión de su solicitud y el aprovisionamiento de un puerto para su conexión pueden tardar hasta 72 horas. AWS Durante este tiempo, es posible que reciba un correo electrónico con una solicitud de información adicional sobre su caso de uso o sobre la ubicación especificada. El correo electrónico se envía a la dirección de correo electrónico que utilizaste cuando te registraste AWS. Si no responde en un plazo de 7 días, se eliminará la conexión.

Para obtener más información, consulte AWS Direct Connect conexiones.

Aceptación de la conexión alojada

Debe aceptar la conexión alojada en la AWS Direct Connect consola antes de poder crear una interfaz virtual. Este paso solo se aplica a las conexiones alojadas.

Para aceptar una interfaz virtual alojada

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Connections (Conexiones).
3. Seleccione la conexión alojada y, a continuación, elija Aceptar.

Elija Aceptar.

(Conexión dedicada) Paso 3: Descargar el documento LOA-CFA

Una vez que haya solicitado una conexión, ponemos a su disposición una Carta de autorización y asignación de instalaciones de conexión (LOA-CFA) que puede descargar, o le enviaremos un correo electrónico solicitándole más información. La LOA-CFA es la autorización para AWS conectarse y el proveedor de colocación o su proveedor de red la requieren para establecer la conexión entre redes (conexión cruzada).

Para descargar el documento LOA-CFA

1. Abra la consola en https://console.aws.amazon.com/directconnect/v2/home. AWS Direct Connect
2. En el panel de navegación, elija Connections (Conexiones).
3. Seleccione la conexión y elija View Details (Ver detalles).
4. Elija Download LOA-CFA (Descargar LOA-CFA).

   El documento LOA-CFA se descarga en su equipo como archivo PDF.

   > **Note**
   >
   > Si el enlace no está habilitado, significa que aún no puede descargar el documento LOA-CFA. Busque una solicitud para obtener más información el correo electrónico. Si todavía no está disponible o no ha recibido un correo electrónico transcurridas 72 horas, póngase en contacto con AWS Asistencia.

5. Después de descargar el documento LOA-CFA, realice una de las siguientes operaciones:

   - Si trabaja con un AWS Direct Connect socio o un proveedor de red, envíeles la LOA-CFA para que puedan solicitarle una conexión cruzada en esa ubicación. AWS Direct Connect Si no pueden solicitar la conexión cruzada para usted, puede ponerse en contacto con el proveedor de coubicación directamente.
   - Si tiene equipos en la AWS Direct Connect ubicación, póngase en contacto con el proveedor de colocación para solicitar una conexión entre redes. Debe ser un cliente del proveedor de coubicación. También debe presentarles la LOA-CFA que autoriza la conexión al AWS router y la información necesaria para conectarse a la red.

AWS Direct Connect las ubicaciones que figuran como sitios múltiples (por ejemplo, Equinix DC1-DC6 y DC10-DC11) se configuran como campus. Si su equipo o el de su proveedor de red está ubicado en cualquiera de estos sitios, puede solicitar una conexión cruzada con el puerto asignado aunque este se encuentre en otro edificio del campus.

> **Important**
>
> Un campus se considera una única ubicación. AWS Direct Connect Para conseguir un alto nivel de disponibilidad, configure conexiones con diferentes ubicaciones de AWS Direct Connect .

Si usted o su proveedor de red experimentan problemas al establecer una conexión física, consulte Solución de problemas de capa 1 (físicos).

Paso 4: Crear una interfaz virtual

Para empezar a utilizar AWS Direct Connect la conexión, debe crear una interfaz virtual. Puede crear una interfaz virtual privada para conectarla a la VPC. O bien, puede crear una interfaz virtual pública para conectarse a AWS servicios públicos que no estén en una VPC. Al crear una interfaz virtual privada a una VPC, necesita una interfaz virtual privada para cada VPC a la que se va a conectar. Por ejemplo, necesita tres interfaces virtuales privadas para conectarse a tres VPC.

Antes de comenzar, asegúrese de que dispone de la siguiente información:

Recurso	Información necesaria
Conexión	El grupo de AWS Direct Connect conexión o agregación de enlaces (LAG) para el que va a crear la interfaz virtual.
Nombre de la interfaz virtual	Un nombre para la interfaz virtual.
Propietario de la interfaz virtual	Si va a crear la interfaz virtual para otra cuenta, necesitará el ID de AWS cuenta de la otra cuenta.
(Solo para la interfaz	Para conectarse a una VPC de la misma AWS región, necesita la puerta de enlace privada virtual para su VPC. El ASN del lado de Amazon de la sesión del BGP se hereda de la puerta de enlace privada virtual. Al crear una

Recurso	Información necesaria
virtual privada) Conexión	puerta de enlace privada virtual, puede especificar su propio ASN privado. De lo contrario, Amazon proporciona un ASN predeterminado. Para obtener información, consulte Crear una puerta de enlace privada virtual en la Guía del usuario de Amazon VPC. Para conectarse a una VPC a través de una puerta de enlace de Direct Connect, se necesita la puerta de enlace de Direct Connect. Para obtener más información, consulte Gateways de Direct Connect.
VLAN	Una etiqueta de red de área local virtual (VLAN) única que aún no se encuentra en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de AWS Direct Connect . Si tiene una conexión alojada, su AWS Direct Connect socio le proporcionará este valor. No puede modificar el valor después de haber creado la interfaz virtual.

Recurso	Información necesaria

Direcciones IP de mismo nivel	Una interfaz virtual es compatible con una sesión de intercambio de tráfico del BGP para IPv4 e IPv6, o con uno de cada una (pila doble). No utilice direccion es IP elásticas (eIP) ni traiga sus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias sesiones de BGP para la misma familia de direccionamiento IP en la misma interfaz virtual. Los rangos de las direcciones IP que se asignan a cada extremo de la interfaz virtual para la sesión de intercambio de tráfico del BGP.
	
	• IPv4:
	  • (Solo para la interfaz virtual pública) Debe especificar direcciones IPv4 públicas únicas que sean de su propiedad. El valor puede ser uno de los siguientes:
	  • Un CIDR IPv4 propiedad del cliente
	
	Puede ser cualquier IP pública (propiedad del cliente o proporcio nada por él AWS), pero se debe usar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del router. AWS Por ejemplo, si asigna un `/31` rango, por ejemplo, podría usarlo `203.0.113.0` para su IP homóloga y `203.0.113.1` para la AWS IP homóloga. `203.0.113.0/31` O bien, si asignas un `/24` rango, por ejemplo`198.51.100.0/24` , puedes usarlo `198.51.100.10` para tu IP homóloga y `198.51.100.20` para la IP AWS homóloga.
	  • Un rango de IP propiedad de su AWS Direct Connect socio o ISP, junto con una autorización LOA-CFA
	  • Un AWS CIDR /31 proporcionado. Póngase en contacto con AWS Asistencia para solicitar un CIDR IPv4 público (e indique un caso de uso en su solicitud)
	
	Note
	No podemos garantizar que podamos cumplir con todas las solicitudes de direcciones IPv4 públicas AWS proporcionadas.
	  • (Solo para la interfaz virtual privada) Amazon puede generar direcciones IPv4 privadas en su nombre. Si especifica el suyo propio, asegúrese de

Recurso	Información necesaria
	especificar únicamente los CIDR privados para la interfaz de su router y la interfaz AWS Direct Connect. Por ejemplo, no especifique otras direcciones IP de su red local. Al igual que en una interfaz virtual pública, se debe usar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del AWS router. Por ejemplo, si asigna un `/30` rango, por ejemplo, podría usarlo `192.168.0.1` para su IP homóloga y `192.168.0.2` para la IP AWS homóloga. `192.168.0.0/30` • IPv6: Amazon le asigna un CIDR IPv6 /125 de forma automática. No puede especificar sus propias direcciones IPv6 de mismo nivel.
Familia de direcciones	Si la sesión de intercambio de tráfico del BGP se realizará a través de IPv4 o IPv6.
Información sobre el BGP	• Un número de sistema autónomo (ASN) para el protocolo de puerta de enlace fronteriza (BGP) público o privado en su lado de la sesión del BGP. Si utiliza un ASN público, debe tener uno propio. Si utiliza un ASN privado, puede establecer un valor de ASN personalizado. Para un ASN de 16 bits ASN, el valor debe estar dentro del rango de 64 512 a 65 534. En el caso de un ASN de 32 bits, el valor debe estar dentro del rango de 1 a 2147483647. El sistema autónomo (AS) que se antepone no funciona si utiliza un ASN privado para una interfaz virtual pública. • AWS habilita MD5 de forma predeterminada. Esta opción no se puede modificar. • Una clave de autenticación del BGP MD5. Puede proporcionar su propia clave o dejar que Amazon genere una en su nombre.

Recurso	Información necesaria

(Solo para la interfaz virtual pública) Prefijos que desea anunciar	Rutas IPv4 públicas o rutas IPv6 para anunciar a través del BGP. Debe comunicar al menos un prefijo a través del BGP, hasta un máximo de 1 000 prefijos.
	• IPv4: el CIDR de IPv4 puede superponerse con otro CIDR de IPv4 público que se haya anunciado que se utiliza AWS Direct Connect cuando se cumple alguna de las siguientes condiciones:
	  • Los CIDR provienen de distintas regiones. AWS Asegúrese de aplicar etiquetas de comunidad del BGP a los prefijos públicos.
	  • Utiliza AS_PATH cuando tiene un ASN público en una configuración activa/pasiva.
	  Para obtener más información, consulte Políticas de enrutamiento y comunidades del BGP.
	• IPv6: especifique una longitud de prefijo de /64 caracteres o menos.
	• Puede agregar prefijos adicionales a una VIF pública existente y anunciarl os si se pone en contacto con AWS Asistencia. En su caso de soporte, proporcione una lista de los prefijos de CIDR adicionales que desee agregar a la VIF pública y anunciar.
	• Puede especificar cualquier longitud de prefijo en una interfaz virtual pública de Direct Connect. IPv4 debería admitir cualquier valor entre /1 y /32, e IPv6 debería admitir cualquier valor entre /1 y /64.

Recurso	Información necesaria
(Solo para la interfaz virtual privada) Tramas gigantes	La unidad máxima de transmisión (MTU) de los paquetes superados. AWS Direct Connect El valor predeterminado es 1500. El establecimiento de la MTU de una interfaz virtual en 9001 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Las tramas gigantes solo se aplican a las rutas propagadas desde. AWS Direct Connect Si agrega rutas estáticas a una tabla de enrutamiento que apuntan a una gateway privada virtual, el tráfico enrutado a través de las rutas estáticas se envía utilizando 1500 MTU. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Jumbo Frame Capable en la página de configuración general de la interfaz virtual.
(Solo para la interfaz virtual de tránsito) Tramas gigantes	La unidad máxima de transmisión (MTU) de los paquetes superados. AWS Direct Connect El valor predeterminado es 1500. El establecimiento de la MTU de una interfaz virtual en 8500 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Se admiten tramas gigantes de hasta 8500 de MTU para Direct Connect. Las rutas estáticas y propagadas configuradas en la tabla de enrutamiento de puerta de enlace de tránsito admitirán tramas gigantes, incluso desde instancias de EC2 con entradas de la tabla de enrutamiento estáticas de VPC hasta la conexión de puerta de enlace de tránsito. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Capacidad para tramas gigantes en la página de configuración general de la interfaz virtual.

Solicitamos información adicional si sus prefijos públicos o ASN pertenecen a un ISP o un operador de red. Esta información puede ser un documento con un membrete oficial de la empresa o un correo electrónico proveniente del nombre de dominio de la empresa confirmando que usted puede utilizar el prefijo de red o el ASN.

En la interfaz virtual privada y las interfaces virtuales públicas, 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 la conexión. La MTU de una interfaz virtual privada puede ser 1500 o 9001 (tramas gigantes). La MTU de una interfaz virtual de tránsito puede ser 1500 o 8500 (tramas gigantes). Puede especificar la MTU al crear la interfaz o actualizarla tras crearla. El establecimiento de la MTU de una interfaz virtual en 8500 (tramas gigantes) o 9001 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Jumbo Frame Capable en la pestaña Resumen.

Al crear una interfaz virtual pública, revisar y aprobar la solicitud AWS puede tardar hasta 72 horas.

Para aprovisionar una interfaz virtual pública a servicios que no sean de una VPC

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Virtual interface type (Tipo de interfaz virtual) en Type (Tipo), elija Public (Pública).
5. En Public virtual interface settings (Configuración de la interfaz virtual pública), haga lo siguiente:

   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

   c. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

   d. En BGP ASN, introduzca el número de sistema autónomo para protocolo de gateway fronteriza del router del mismo nivel de sus instalaciones de la nueva interfaz virtual.

      Los valores válidos son 1-2.147.483.647.
6. En Additional settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

      [IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

- Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
- En Amazon router peer IP (IP del mismo nivel del router de Amazon), escriba la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

[IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

b. Para utilizar su propia clave de BGP, introduzca su clave MD5 de BGP.

Si no ingresa un valor, generamos una clave de BGP.

c. Para anunciar prefijos para Amazon, en Prefixes you want to advertise (Prefijos que desea anunciar), escriba las direcciones CIDR IPv4 de destino (separadas por comas) a las que debe redirigirse el tráfico a través de la interfaz virtual.

d. (Opcional) Añada o elimine una etiqueta.

[Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

- En Key (Clave), escriba el nombre de la clave.
- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

7. Elija Create virtual interface (Crear interfaz virtual).

Para aprovisionar una interfaz virtual privada a una VPC

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Tipo de interfaz virtual, en Tipo, elija Privada.
5. En Configuración de la interfaz virtual privada, realice lo siguiente:

a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

c. En Tipo de puerta de enlace, elija Puerta de enlace privada virtual o Puerta de enlace de Direct Connect.

d. En Propietario de la interfaz virtual, elija Otra AWS cuenta y, a continuación, introduzca la AWS cuenta.

e. En Puerta de enlace privada virtual, elija la puerta de enlace privada virtual para utilizar con esta interfaz.

f. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

g. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

   Los valores válidos son 1 a 2147483647.

6. En Additional Settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

      [IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
      - En IP de mismo nivel del enrutador de Amazon, ingrese la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

      > **Important**
      >
      > Si permite la AWS asignación automática de direcciones IPv4, se asignará un CIDR /29 desde 169.254.0.0/16 IPv4 Link-Local de acuerdo con la RFC 3927 para la conectividad. point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP del mismo nivel del router del cliente como origen o destino del tráfico de VPC. En su lugar, debe utilizar la RFC 1918 u otro direccionamiento y especificar la dirección por su cuenta.
      >
      > - Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.
      > - Para obtener más información sobre la RFC 3927, consulte Dynamic Configuration of IPv4 Link-Local Addresses.

[IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

b. Para cambiar la unidad de transmisión máxima (MTU) de 1500 (predeterminada) a 9001 (tramas gigantes), seleccione MTU gigante (tamaño de MTU 9001).

c. (Opcional) En Habilitar SiteLink, elija Habilitado para habilitar la conectividad directa entre los puntos de presencia de Direct Connect.

d. (Opcional) Añada o elimine una etiqueta.

[Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

- En Key (Clave), escriba el nombre de la clave.
- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

7. Elija Create virtual interface (Crear interfaz virtual).
8. Debe utilizar su dispositivo de BGP a fin de anunciar la red que utiliza para la conexión de VIF pública.

Paso 5: Descargar la configuración del enrutador

Después de crear una interfaz virtual para la AWS Direct Connect conexión, puede descargar el archivo de configuración del router. El archivo contiene los comandos necesarios para configurar el router para su uso con la interfaz virtual pública o privada.

Para descargar una configuración del router

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Seleccione la conexión y elija View Details (Ver detalles).
4. Elija Download router configuration (Descargar configuración del router).
5. En Download router configuration (Descargar configuración del router), haga lo siguiente:

   a. En Vendor (Proveedor), seleccione el fabricante del router.

   b. En Platform, seleccione el modelo del router.

   c. En Software, seleccione la versión de software del router.

6. Elija Download (Descargar) y, a continuación, utilice la configuración adecuada del router para garantizar de que puede conectarse a AWS Direct Connect.

Para ver archivos de configuración de ejemplo, consulte Ejemplos de archivos de configuración del router.

Una vez que haya configurado el router, el estado de la interfaz virtual pasa a UP. Si la interfaz virtual permanece inactiva y no puede hacer ping a la dirección IP homóloga del AWS Direct Connect dispositivo, consulteSolución de problemas de capa 2 (enlace de datos). Si puede hacer ping a la dirección IP de mismo nivel, consulte Solución de problemas de capa 3/4 (red/transporte). Si la sesión de intercambio de tráfico BGP se ha establecido, pero no puede dirigir el tráfico, consulte Solución de problemas de direccionamiento.

Paso 6: Verificar la interfaz virtual

Una vez que haya establecido las interfaces virtuales con la AWS nube o con Amazon VPC, puede verificar la AWS Direct Connect conexión mediante los siguientes procedimientos.

Para verificar la conexión de su interfaz virtual a la nube AWS

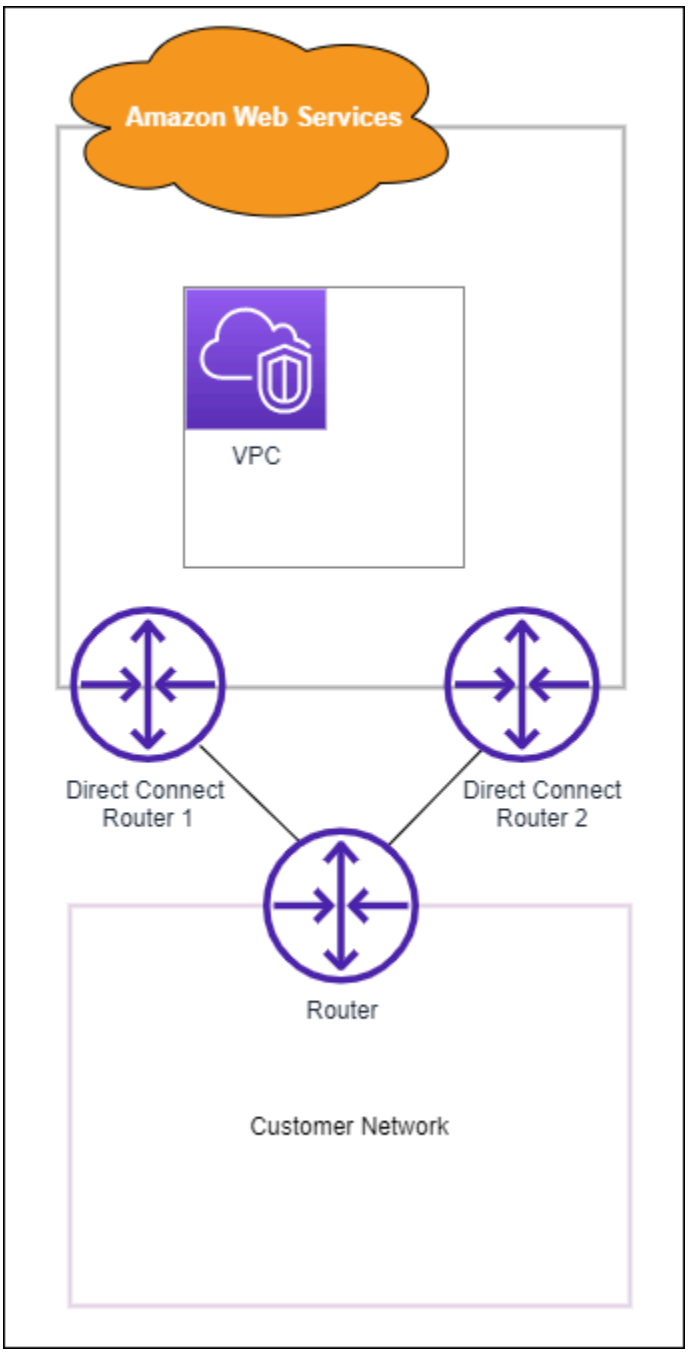
- Ejecute `traceroute` y verifique que el AWS Direct Connect identificador esté en el rastreo de la red.

Para verificar la conexión de la interfaz virtual a Amazon VPC

1. Mediante una AMI que permita hacer ping, como una AMI de Amazon Linux, lance una instancia de EC2 en la VPC adjunta a la puerta de enlace privada virtual. Las AMI de Amazon Linux se encuentran disponibles en la pestaña de Inicio rápido cuando utiliza el asistente de lanzamiento de instancias en la consola de Amazon EC2. Para obtener más información, consulte Lanzar una instancia en la Guía del usuario de Amazon EC2. Asegúrese de que el grupo de seguridad asociado a la instancia incluye una regla que permita el tráfico ICMP entrante (para la solicitud de ping).
2. Cuando la instancia se esté ejecutando, obtenga la dirección IPv4 privada (por ejemplo, 10.0.0.4). En la consola de Amazon EC2, se muestra la dirección en los datos de la instancia.
3. Haga ping a las direcciones IPv4 privadas y obtenga una respuesta.

(Recomendado) Paso 7: Configurar conexiones redundantes

Para permitir la conmutación por error, le recomendamos que solicite y configure dos conexiones dedicadas para AWS, tal y como se muestra en la siguiente figura. Estas conexiones pueden terminar en uno o dos router de la red.



Cuando se aprovisionan dos conexiones dedicadas, existen diferentes opciones de configuración disponibles:

- Activa/Activa (múltiples rutas de BGP). Esta es la configuración predeterminada, en la que ambas conexiones están activas. AWS Direct Connect admite múltiples rutas a múltiples interfaces virtuales dentro de la misma ubicación y la carga del tráfico se comparte entre las interfaces en función del flujo. Si una conexión no se encuentra disponible, todo el tráfico se redirige a través de la otra conexión.
- Activa/Pasiva (conmutación por error). Una conexión gestiona el tráfico mientas que la otra está en modo de espera. Si la conexión activa no se encuentra disponible, todo el tráfico se redirige a través de la conexión pasiva. Deberá colocar la ruta de AS delante de la ruta de uno de los enlaces para convertirlo en el enlace pasivo.

Cómo se configuren las conexiones no afecta a la redundancia, pero sí afecta a las políticas que determinan la forma en la que los datos se redirigen a través de ambas conexiones. Le recomendamos que configure las dos conexiones como activas.

Si utiliza una conexión de VPN para aportar redundancia, no olvide implementar un mecanismo de comprobación de estado y conmutación por error. Si utiliza una de las siguientes configuraciones, tendrá que comprobar el direccionamiento de la tabla de ruteo para direccionar a la nueva interfaz de red.

- Puede utilizar sus propias instancias para el direccionamiento; por ejemplo, la instancia es el firewall.
- Puede utilizar su propia instancia que termina una conexión de VPN.

Para lograr una alta disponibilidad, le recomendamos encarecidamente que configure las conexiones a diferentes ubicaciones. AWS Direct Connect

Para obtener más información sobre AWS Direct Connect la resiliencia, consulte las recomendaciones de AWS Direct Connect resiliencia.

Prueba de conmutación por error de AWS Direct Connect

Los modelos de resiliencia de AWS Direct Connect Resiliency Toolkit se han diseñado para garantizar que dispone del número adecuado de conexiones de interfaz virtual en varias ubicaciones. Después de completar el asistente, utilice la prueba de conmutación por error de AWS Direct Connect Resiliency Toolkit para reducir la sesión de intercambio de tráfico del BGP con el fin de comprobar que el tráfico se enruta a una de las interfaces virtuales redundantes y cumple los requisitos de resiliencia.

Utilice la prueba para asegurarse de que el tráfico se enruta a través de interfaces virtuales redundantes cuando una interfaz virtual está fuera de servicio. Para comenzar la prueba, seleccione una interfaz virtual, una sesión de interconexión de BGP y cuánto tiempo se ejecutará la prueba. AWS coloca la sesión de interconexión de BGP de interfaz virtual seleccionada en el estado descendente. Cuando la interfaz está en este estado, el tráfico debe pasar por una interfaz virtual redundante. Si la configuración no contiene las conexiones redundantes adecuadas, la sesión de interconexión de BGP produce un error y el tráfico no se enruta. Cuando se completa la prueba o se detiene manualmente la prueba, AWS restaura la sesión de BGP. Una vez finalizada la prueba, puede utilizar AWS Direct Connect Resiliency Toolkit para ajustar la configuración.

> **Note**
>
> No utilice esta función durante un período de mantenimiento de Direct Connect, ya que la sesión de BGP podría restaurarse prematuramente durante o después del mantenimiento.

Historial de pruebas

AWS elimina el historial de pruebas después de 365 días. El historial de pruebas incluye el estado de las pruebas que se ejecutaron en todos los BGP del mismo nivel. El historial incluye qué sesiones de intercambio de tráfico del BGP se han probado, las horas de inicio y finalización, además del estado de la prueba, que puede ser cualquiera de los siguientes valores:

- En curso: la prueba se está ejecutando actualmente.
- Completado: la prueba se ejecutó durante el tiempo especificado.
- Cancelado: la prueba se canceló antes de la hora especificada.
- Error: la prueba no se ejecutó durante el tiempo especificado. Esto puede suceder cuando hay un problema con el enrutador.

Para obtener más información, consulte the section called “Visualización del historial de pruebas de conmutación por error de interfaz virtual”.

Permisos de validación

La única cuenta que tiene permiso para ejecutar la prueba de conmutación por error es la cuenta propietaria de la interfaz virtual. El propietario de la cuenta recibe una indicación a través de AWS CloudTrail de que se ejecutó una prueba en una interfaz virtual.

Comienzo de la prueba de conmutación por error de interfaz virtual

Puede comenzar la prueba de conmutación por error de interfaz virtual utilizando la consola de AWS Direct Connect o la AWS CLI.

Para comenzar la prueba de conmutación por error de interfaz virtual desde la consola de AWS Direct Connect

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. Elija Interfaces virtuales.
3. Seleccione las interfaces virtuales y, a continuación, elija Acciones, Reducir BGP.

   Puede ejecutar la prueba en una interfaz virtual pública, privada o de tránsito.
4. En el cuadro de diálogo Iniciar la prueba de error, haga lo siguiente:

   a. En Interconexiones para reducir de prueba, elija qué sesiones de interconexiones probar, por ejemplo IPv4.
   b. En Tiempo máximo de la prueba, especifique el número de minutos que durará la prueba.

      El valor máximo es 4320 minutos (72 horas).

      El valor predeterminado es 180 minutos (3 horas).
   c. En Para confirmar la prueba, escriba Confirmar.
   d. Seleccione Confirmar.

   La sesión de interconexión de BGP se coloca en el estado DOWN. Puede enviar tráfico para verificar que no hay interrupciones. Si es necesario, puede detener la prueba inmediatamente.

Para comenzar la prueba de conmutación por error de interfaz virtual mediante la AWS CLI

Uso StartBgpFailoverTest.

Visualización del historial de pruebas de conmutación por error de interfaz virtual

Puede consultar el historial de pruebas de conmutación por error de interfaz virtual mediante la consola de AWS Direct Connect o la AWS CLI.

Para consultar el historial de pruebas de conmutación por error de interfaz virtual desde la consola de AWS Direct Connect

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. Elija Interfaces virtuales.
3. Seleccione la interfaz virtual y, a continuación, elija View details (Ver detalles).
4. Elija Historial de pruebas.

   La consola muestra las pruebas de interfaz virtual que realizó para la interfaz virtual.
5. Para consultar los detalles de una prueba específica, seleccione el ID de prueba.

Para consultar el historial de pruebas de conmutación por error de interfaz virtual mediante la AWS CLI

Uso ListVirtualInterfaceTestHistory.

Parar la prueba de conmutación por error de interfaz virtual

Puede detener la prueba de conmutación por error de interfaz virtual mediante la consola de AWS Direct Connect o la AWS CLI.

Para detener la prueba de conmutación por error de interfaz virtual desde la consola de AWS Direct Connect

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. Elija Interfaces virtuales.
3. Seleccione la interfaz virtual y, a continuación, elija Acciones, Cancelar prueba.
4. Seleccione Confirmar.

AWS restaura la sesión de intercambio de tráfico del BGP. El historial de pruebas muestra "cancelado" para la prueba.

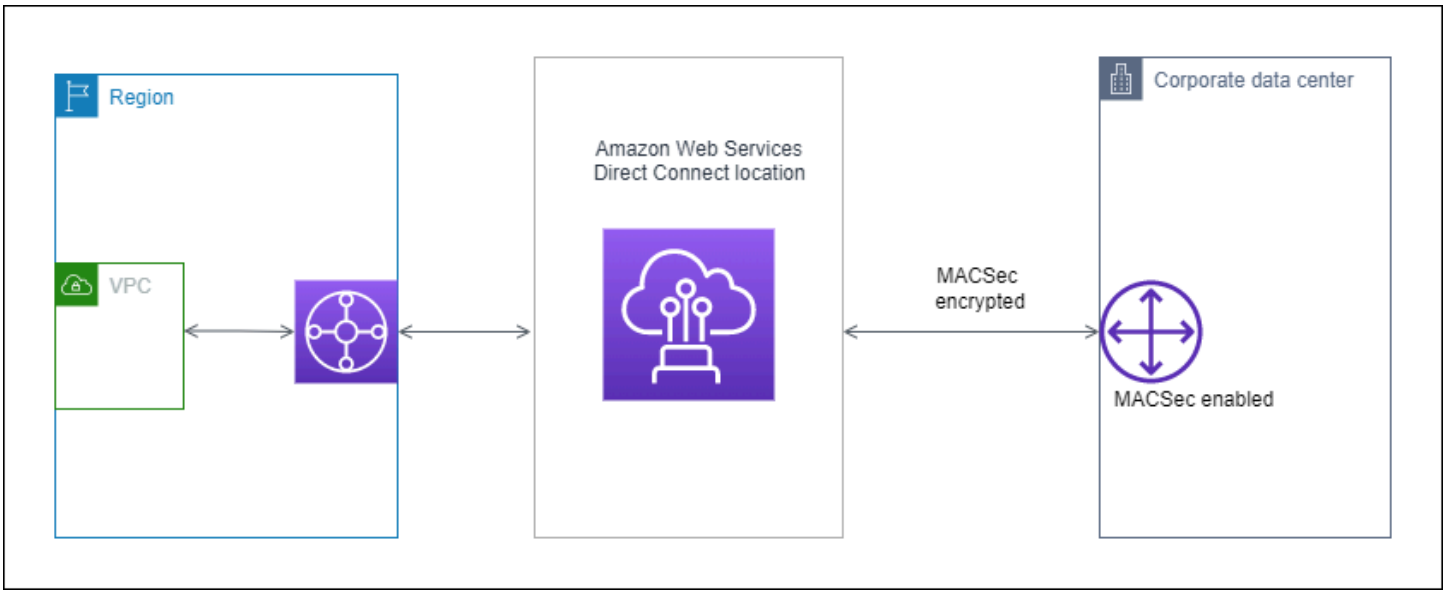
Para detener la prueba de conmutación por error de interfaz virtual mediante la AWS CLI

Uso StopBgpFailoverTest.

Seguridad de MAC

La seguridad de MAC (MACsec) es un estándar IEEE que proporciona confidencialidad, integridad y autenticidad del origen de los datos. MACsec proporciona point-to-point cifrado de capa 2 a través de la conexión cruzada a. AWS El MACSec funciona en la capa 2 entre dos enrutadores de capa 3 y proporciona cifrado en el dominio de capa 2. Todos los datos que circulan por la red AWS global que se interconecta con los centros de datos y las regiones se cifran automáticamente en la capa física antes de salir del centro de datos.

En el siguiente diagrama, tanto la conexión dedicada como los recursos en las instalaciones deben ser compatibles con MACsec. El tráfico de la capa 2 que viaja a través de la conexión dedicada hacia el centro de datos o desde este se encuentra cifrado.



Conceptos sobre MACsec

A continuación se enumeran los conceptos clave sobre MACsec:

- Seguridad de MAC (MACsec): estándar IEEE 802.1 de capa 2 que proporciona confidencialidad, integridad y autenticidad del origen de los datos. Para obtener más información sobre el protocolo, consulte 802.1AE: seguridad de MAC (MACsec).
- Clave secreta MACSec: clave previamente compartida que establece la conectividad MACSec entre el router local del cliente y el puerto de conexión de la ubicación. AWS Direct Connect Los dispositivos que se encuentran en los extremos de la conexión generan la clave mediante el par CKN/CAK que usted proporciona AWS y que también ha aprovisionado en el dispositivo.

- Nombre de clave de conexión (CKN) y clave de asociación de conectividad (CAK): los valores de este par se utilizan para generar la clave secreta de MACsec. Usted genera los valores de los pares, los asocia a una AWS Direct Connect conexión y los aprovisiona en el dispositivo perimetral al final de la conexión. AWS Direct Connect

Conexiones compatibles

MACsec se encuentra disponible en conexiones dedicadas. Para obtener información sobre cómo solicitar conexiones compatibles con MACsec, consulte AWS Direct Connect.

Comenzar a utilizar MACsec en conexiones dedicadas

Las siguientes tareas le ayudarán a familiarizarse con MACsec en conexiones AWS Direct Connect dedicadas. El uso de MACSec no conlleva cargos adicionales.

Antes de configurar MACSec en una conexión dedicada, tenga en cuenta lo siguiente:

- MACsec es compatible con conexiones de Direct Connect dedicadas de 10 Gbps y 100 Gbps en puntos de presencia seleccionados. Para estas conexiones, se admiten los siguientes conjuntos de cifrado MACSec:
  - Para conexiones de 10 Gbps, GCM-AES-256 y GCM-AES-XPN-256.
  - Para conexiones de 100 Gbps, GCM-AES-XPN-256.

- Solo se admiten claves MACsec de 256 bits.
- Se requiere la numeración de paquetes extendida (XPN) para las conexiones de 100 Gbps. Para conexiones de 10 Gbps, Direct Connect admite GCM-AES-256 y GCM-AES-XPN-256. Las conexiones de alta velocidad, como las conexiones dedicadas de 100 Gbps, pueden agotar rápidamente el espacio original de numeración de paquetes de 32 bits del MACSec, lo que requeriría rotar las claves de cifrado cada pocos minutos para establecer una nueva asociación de conectividad. Para evitar esta situación, la modificación de la norma IEEE 802.1AEBW-2013 introdujo una numeración de paquetes ampliada, aumentando el espacio de numeración a 64 bits y reduciendo el requisito de puntualidad para la rotación de claves.
- El identificador de canal seguro (SCI) es obligatorio y debe estar activado. Esta configuración no se puede ajustar.
- La etiqueta IEEE 802.1Q (dot1Q/VLAN) offset/dot1 no se admite para mover una etiqueta de VLAN fuera de q-in-clear una carga útil cifrada.

Para obtener información adicional sobre Direct Connect y MACsec, consulte la sección MACsec de las AWS Direct Connect preguntas frecuentes.

Temas

Requisitos previos de MACsec

Complete las siguientes tareas antes de configurar MACsec en una conexión dedicada.

- Cree un par de CKN/CAK para la clave secreta de MACsec.

  Puede crear el par con una herramienta estándar abierta. El par debe cumplir los requisitos especificados de the section called “Paso 4: Configurar su enrutador en las instalaciones”.
- Asegúrese de que cuenta con un dispositivo en su extremo de conexión que sea compatible con MACsec.
- El identificador de canal seguro (SCI) debe estar activado.
- Solo se admiten claves MACSec de 256 bits, lo que proporciona la protección de datos avanzada más reciente.

Roles vinculados a servicios

AWS Direct Connect utiliza funciones vinculadas al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS Direct Connect Los roles vinculados al servicio están predefinidos AWS Direct Connect e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre. Un rol vinculado a un servicio facilita la configuración AWS Direct Connect , ya que no es necesario añadir manualmente los permisos necesarios. AWS Direct Connect define los permisos

de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Direct Connect puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM. Para obtener más información, consulte the section called “Roles vinculados al servicio”.

Consideraciones clave sobre los pares de CKN/CAK previamente compartidos por MACsec

AWS Direct Connect usa CMK AWS administradas para las claves previamente compartidas que se asocian a las conexiones o los LAG. Secrets Manager guarda los pares de CKN y CAK previamente compartidos como un secreto que cifra la clave raíz de Secrets Manager. A fin de obtener más información, consulte CMK administradas por AWS en la Guía para desarrolladores de AWS Key Management Service .

Por diseño, la clave almacenada es de solo lectura, pero puede programar una eliminación de siete a treinta días mediante la consola o la API de AWS Secrets Manager. Al programar una eliminación, no se puede leer el CKN y esto podría afectar a la conectividad de la red. Cuando esto ocurre, aplicamos las siguientes reglas:

- Si la conexión se encuentra en estado pendiente, desasociamos el CKN de la conexión.
- Si la conexión se encuentra en un estado disponible, se lo notificamos al propietario de la conexión por correo electrónico. Si no realiza ninguna acción en un plazo de 30 días, desasociaremos el CKN de su conexión.

Cuando desasociamos el último CKN de su conexión y el modo de cifrado de la conexión se establece en “debe cifrarse”, configuramos el modo en “should_encrypt” para evitar la pérdida repentina de paquetes.

Paso 1: Crear una conexión

Para comenzar a utilizar MACsec, debe activar la característica al crear una conexión dedicada. Para obtener más información, consulte the section called “Crear una conexión mediante el asistente de conexión”.

(Opcional) Paso 2: Crear un grupo de agregación de enlaces (LAG)

Si utiliza varias conexiones para obtener redundancia, puede crear un LAG que admita MACsec. Para obtener más información, consulte the section called “Consideraciones de MACsec” y the section called “Crear un LAG”.

Paso 3: Asociar el par de CKN/CAK a la conexión o LAG

Después de crear la conexión o LAG compatible con MACsec, puede asociar un par de CKN/CAK a la conexión. Para obtener más información, consulte una de las siguientes:

- the section called “Asociar un par de CKN/CAK de MACsec a una conexión”
- the section called “Asociar un par de CKN/CAK de MACsec a un LAG”

Paso 4: Configurar su enrutador en las instalaciones

Actualice su enrutador en las instalaciones con la clave secreta de MACsec. La clave secreta MACSec del router local y la de la ubicación deben coincidir. AWS Direct Connect Para obtener más información, consulte the section called “Descargar el archivo de configuración del enrutador”.

Paso 5: (Opcional) Eliminar la asociación entre el par de CKN/CAK y la conexión o LAG

Si necesita eliminar la asociación entre la clave de MACsec y la conexión o LAG, consulte una de las siguientes alternativas:

- the section called “Eliminar la asociación entre una clave secreta de MACsec y una conexión”
- the section called “Eliminar la asociación entre una clave secreta de MACsec y un LAG”

AWS Direct Connect conexiones

AWS Direct Connect le permite establecer una conexión de red dedicada entre su red y una de las AWS Direct Connect ubicaciones.

Existen dos tipos de conexiones:

- Conexión dedicada: conexión Ethernet física asociada a un único cliente. Los clientes pueden solicitar una conexión dedicada a través de la AWS Direct Connect consola, la CLI o la API. Para obtener más información, consulte the section called “Conexiones dedicadas”.
- Conexión alojada: conexión Ethernet física que un AWS Direct Connect socio proporciona en nombre de un cliente. A fin de solicitar una conexión alojada, los clientes se ponen en contacto con un socio del programa para socios de AWS Direct Connect , que aprovisiona la conexión. Para obtener más información, consulte the section called “Conexiones alojadas”.

Conexiones dedicadas

Para crear una conexión dedicada de AWS Direct Connect , necesita la siguiente información:

AWS Direct Connect location

Trabaje con un AWS Direct Connect socio del Programa de Socios para que le ayude a establecer circuitos de red entre una AWS Direct Connect ubicación y su centro de datos, oficina o entorno de colocación. También pueden contribuir a proporcionar una sala técnica de coubicación en las mismas instalaciones que la ubicación. Para obtener más información, consulte Socios de APN que trabajan con AWS Direct Connect.

Velocidad del puerto

Los valores posibles son 1 Gbps, 10 Gbps y 100 Gbps.

No puede cambiar la velocidad del puerto después de crear la solicitud de conexión. Para cambiar la velocidad de puerto, debe crear y configurar una conexión nueva.

Puede crear una conexión mediante el asistente de conexión o crear una conexión clásica. Con el asistente de conexión, puede configurar las conexiones al seguir las recomendaciones de resiliencia. Se recomienda utilizar el asistente si va a configurar las conexiones por primera vez. Si lo prefiere, puede usar Classic para crear conexiones one-at-a-time. Se recomienda la versión clásica si ya

cuenta con una configuración existente a la que desea agregar conexiones. Puede crear una conexión independiente o puede crear una conexión para asociarla a un LAG en su cuenta. Si asocia una conexión a un LAG, se crea con la misma velocidad del puerto y ubicación especificados en el LAG.

Una vez que haya solicitado la conexión, ponemos a su disposición una Carta de autorización y asignación de instalaciones de conexión (LOA-CFA) que puede descargar, o le enviaremos un correo electrónico solicitándole más información. Si recibe una solicitud para obtener más información, deberá responder en un plazo de 7 días o se eliminará la conexión. La LOA-CFA es la autorización para AWS conectarse y su proveedor de red la necesita para solicitarle una conexión cruzada. Si no tiene equipo en la AWS Direct Connect ubicación, no puede solicitar una conexión cruzada para usted en esa ubicación.

A continuación, se muestran las operaciones disponibles para las conexiones dedicadas:

- the section called “Crear una conexión mediante el asistente de conexión”
- the section called “Crear una conexión clásica”
- the section called “Ver los detalles de la conexión”
- the section called “Actualizar una conexión”
- the section called “Asociar un par de CKN/CAK de MACsec a una conexión”
- the section called “Eliminar la asociación entre una clave secreta de MACsec y una conexión”
- the section called “Eliminar conexiones”

Puede agregar una conexión dedicada a un grupo de agregación de enlaces (LAG), lo que le permite tratar varias conexiones como una sola. Para obtener más información, consulte Asociar una conexión a un LAG.

Una vez que crea una conexión, cree una interfaz virtual para conectarse a los recursos públicos y privados de AWS . Para obtener más información, consulte AWS Direct Connect interfaces virtuales.

Si no tiene equipo en una AWS Direct Connect sucursal, póngase primero en contacto con un AWS Direct Connect AWS Direct Connect socio del Programa de Socios. Para obtener más información, consulte Socios de APN que trabajan con AWS Direct Connect.

Si desea crear una conexión que utilice la seguridad de MAC (MACsec), revise los requisitos previos antes de crear la conexión. Para obtener más información, consulte the section called “Requisitos previos de MACsec ”.

Crear una conexión mediante el asistente de conexión

En esta sección se describe la creación de una conexión mediante el asistente de conexión. Si prefiere crear una conexión clásica, consulte los pasos que se indican en the section called “Paso 2: Solicita una conexión AWS Direct Connect dedicada”.

Para crear una conexión mediante el asistente de conexión

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Conexiones y, a continuación, elija Crear conexión.
3. En la página Crear conexión, en Tipo de orden de conexión, elija Asistente de conexión.
4. Elija un Nivel de resiliencia para sus conexiones de red. Un nivel de resiliencia puede ser uno de los siguientes:

   - Resiliencia máxima
   - Alta resiliencia
   - Desarrollo y pruebas

   Para obtener descripciones e información más detallada sobre estos niveles de resiliencia, consulte ¿Cómo usar el kit de herramientas AWS Direct Connect de resiliencia para empezar.
5. Elija Siguiente.
6. En la página Configurar conexiones, proporcione los siguientes detalles.

   a. En la lista desplegable de Ancho de banda, elija el ancho de banda necesario para la conexión. Puede oscilar entre 1 Gbps y 100 Gbps.
   b. En Ubicación, elija la AWS Direct Connect ubicación adecuada y, a continuación, elija el proveedor de servicios de primera ubicación y, a continuación, seleccione el proveedor de servicios que proporciona conectividad para la conexión en esta ubicación.
   c. En Segunda ubicación, elija la ubicación adecuada AWS Direct Connect en la segunda ubicación y, a continuación, elija el proveedor de servicios de segunda ubicación y, a continuación, seleccione el proveedor de servicios que proporciona conectividad para la conexión en esta segunda ubicación.
   d. (Opcional) Configure la seguridad de MAC (MACsec) para la conexión. En Configuración adicional, seleccione Solicitar un puerto compatible con MACsec.

      MACsec solo se encuentra disponible en conexiones dedicadas.

e. (Opcional) Seleccione Agregar etiqueta para agregar pares clave/valor que ayuden a identificar aún más esta conexión.

   - En Clave, escriba el nombre de la clave.
   - En Valor, escriba el valor de la clave.

   Para eliminar una etiqueta existente, selecciónela y, a continuación, elija Eliminar etiqueta. No puede tener etiquetas vacías.

7. Elija Siguiente.
8. En la página Revisar y crear, verifique la conexión. En esta página también se muestran los costos estimados del uso del puerto y los cargos adicionales por transferencia de datos.
9. Seleccione Crear.
10. Descargue su Carta de autorización y asignación de instalaciones de conexión (LOA-CFA). Para obtener más información, consulte the section called “Descargar la LOA-CFA”.

Utilice uno de los siguientes comandos.

- create-connection (AWS CLI)
- CreateConnection(AWS Direct Connect API)

Crear una conexión clásica

En el caso de las conexiones dedicadas, puede enviar una solicitud de conexión mediante la AWS Direct Connect consola. En el caso de las conexiones alojadas, trabaje con un AWS Direct Connect socio para solicitar una conexión alojada. Asegúrese de que dispone de la siguiente información:

- La velocidad de puerto que necesita. En el caso de las conexiones dedicadas, no puede cambiar la velocidad del puerto después de crear la solicitud de conexión. En el caso de las conexiones alojadas, su socio de AWS Direct Connect puede cambiar la velocidad.
- La AWS Direct Connect ubicación en la que se va a finalizar la conexión.

> **Note**
>
> No puede usar la AWS Direct Connect consola para solicitar una conexión alojada. En su lugar, póngase en contacto con un AWS Direct Connect socio, quien podrá crear una

conexión alojada para usted, y luego usted la aceptará. Omita el siguiente procedimiento y vaya a Aceptación de la conexión alojada.

Para crear una AWS Direct Connect conexión nueva

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En la pantalla AWS Direct Connect, en Get started (Empezar), seleccione Create a connection (Crear una conexión).
3. Elija Classic.
4. En Name (Nombre), escriba un nombre para la conexión.
5. En Location (Ubicación), seleccione la ubicación de AWS Direct Connect apropiada.
6. Si procede, en Sub Location (Sububicación), elija el piso más cercano a usted o a su proveedor de red. Esta opción solo está disponible si la ubicación dispone de Meet-Me Rooms (MMR) en varios pisos del edificio.
7. En Port Speed (Velocidad del puerto), elija el ancho de banda de la conexión.
8. En En las instalaciones, seleccione Conectar a través de un socio de AWS Direct Connect si utiliza esta conexión para conectarse a su centro de datos.
9. En el caso del proveedor de servicios, seleccione el AWS Direct Connect socio. Si utiliza un socio que no está en la lista, seleccione Other (Otro).
10. Si ha seleccionado Other (Otro) en Service provider (Proveedor de servicios), en Name of other provider (Nombre de otro proveedor), escriba el nombre del socio que utiliza.
11. (Opcional) Seleccione Agregar etiqueta para agregar pares clave/valor que ayuden a identificar aún más esta conexión.

    - En Clave, escriba el nombre de la clave.
    - En Valor, escriba el valor de la clave.

    Para eliminar una etiqueta existente, selecciónela y, a continuación, elija Eliminar etiqueta. No puede tener etiquetas vacías.
12. Elija Create Connection (Crear conexión).

La revisión de su solicitud y el aprovisionamiento de un puerto para su conexión pueden tardar hasta 72 horas. AWS Durante este tiempo, es posible que reciba un correo electrónico con una

solicitud de información adicional sobre su caso de uso o sobre la ubicación especificada. El correo electrónico se envía a la dirección de correo electrónico que utilizaste cuando te registraste AWS. Si no responde en un plazo de 7 días, se eliminará la conexión.

Para obtener más información, consulte AWS Direct Connect conexiones.

Descargar la LOA-CFA

Una vez que hayamos procesado su solicitud de conexión, puede descargar la LOA-CFA. Si el enlace no está habilitado, significa que aún no puede descargar el documento LOA-CFA. Compruebe su correo electrónico para ver si hay una solicitud de información.

La facturación comienza de forma automática cuando el puerto se encuentra activo o 90 días después de la emisión de la LOA, lo que ocurra primero. Para evitar los cargos de facturación, elimine el puerto antes de la activación o en un plazo de 90 días a partir de la emisión de la LOA.

Si su conexión no funciona después de 90 días y no se ha emitido la LOA-CFA, le enviaremos un correo electrónico informándole de que el puerto se eliminará en 10 días. Si no activa el puerto dentro del periodo adicional de 10 días, el puerto se eliminará de forma automática y tendrá que reiniciar el proceso de creación del puerto.

> **Note**
>
> Para obtener más información sobre los precios, consulte Precios de AWS Direct Connect. Si después de la nueva emisión del documento LOA-CFA ya no desea la conexión, debe eliminarla usted mismo. Para obtener más información, consulte Eliminar conexiones.

Console

Para descargar el documento LOA-CFA

1. Abre la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Connections (Conexiones).
3. Seleccione la conexión y, a continuación, elija Ver detalles.
4. Elija Download LOA-CFA (Descargar LOA-CFA).

> **Note**
>
> Si el enlace no está habilitado, significa que aún no puede descargar el documento LOA-CFA. Se creará un caso de Asistencia al solicitar información adicional. Una vez que haya respondido a la solicitud y se haya procesado, la LOA-CFA se encontrará disponible para su descarga. Si sigue sin estar disponible, póngase en contacto con AWS Asistencia.

5. Envíe el documento LOA-CFA al proveedor de red o proveedor de coubicación para que pueda solicitar una conexión cruzada para usted. El proceso de contacto puede variar en función del proveedor de coubicación. Para obtener más información, consulte Solicitud de conexiones cruzadas en AWS Direct Connect ubicaciones.

Command line

Para descargar el documento LOA-CFA mediante la línea de comandos o la API

- describe-loa (AWS CLI)
- DescribeLoa(AWS Direct Connect API)

Actualizar una conexión

Puede actualizar los siguientes atributos de conexión:

- El nombre de la conexión.
- El modo de cifrado de MACsec de la conexión.

> **Note**
>
> MACsec solo se encuentra disponible en conexiones dedicadas.

Los valores válidos son:

- `should_encrypt`
- `must_encrypt`

Al establecer el modo de cifrado en este valor, la conexión se desactiva cuando el cifrado se encuentra inactivo.

- `no_encrypt`

Console

Para actualizar una conexión

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Connections (Conexiones).
3. Seleccione la conexión y, a continuación, elija Editar.
4. Modifique la conexión:

   [Cambiar el nombre] En Name (Nombre), escriba un nombre nuevo para la conexión.

   [Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

   - En Key (Clave), escriba el nombre de la clave.
   - En Valor, escriba el valor de la clave.

   [Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).
5. Elija Edit connection (Editar conexión).

Command line

Para agregar y eliminar una etiqueta con la línea de comandos

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

Para actualizar una conexión mediante la línea de comandos o la API

- update-connection (AWS CLI)
- UpdateConnection(AWS Direct Connect API)

Asociar un par de CKN/CAK de MACsec a una conexión

Después de crear la conexión compatible con MACsec, puede asociar un par de CKN/CAK a la conexión.

> **Note**
>
> No puede modificar una clave secreta de MACsec después de asociarla a una conexión. Si necesita modificar la clave, desasocie la clave de la conexión y, a continuación, asocie una clave nueva a la conexión. Para obtener información sobre cómo quitar una asociación, consulte the section called “Eliminar la asociación entre una clave secreta de MACsec y una conexión”.

Console

Para asociar una clave de MACsec a una conexión

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel izquierdo, elija Connections (Conexiones).
3. Seleccione una conexión y, a continuación, elija Ver detalles.
4. Elija Asociar clave.
5. Ingrese la clave de MACsec.

   [Utilizar el par de CAK/CKN] Elija el Par de claves y, a continuación, realice lo siguiente:

   - En Clave de asociación de conectividad (CAK), ingrese la CAK.
   - En Nombre de clave de asociación de conectividad (CKN), ingrese el CKN.

   [Utilizar el secreto] Elija Secreto de Secrets Manager existente y, a continuación, en Secreto, seleccione la clave secreta de MACsec.
6. Elija Asociar clave.

Command line

Para asociar una clave de MACsec a una conexión

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey(AWS Direct Connect API)

Eliminar la asociación entre una clave secreta de MACsec y una conexión

Puede eliminar la asociación entre la conexión y la clave de MACsec.

Console

Para eliminar una asociación entre una conexión y una clave de MACsec

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2.
3. En el panel izquierdo, elija Connections (Conexiones).
4. Seleccione una conexión y, a continuación, elija Ver detalles.
5. Seleccione el secreto de MACsec que desee eliminar y, a continuación, elija Desasociar clave.
6. En el cuadro de diálogo de confirmación, ingrese disociar y, a continuación, elija Desasociar.

Command line

Para eliminar una asociación entre una conexión y una clave de MACsec

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey(AWS Direct Connect API)

Conexiones alojadas

Para crear una conexión AWS Direct Connect alojada, necesita la siguiente información:

AWS Direct Connect location

Trabaje con un AWS Direct Connect AWS Direct Connect socio del programa de socios para que le ayude a establecer circuitos de red entre una AWS Direct Connect ubicación y su centro de datos, oficina o entorno de colocación. También pueden contribuir a proporcionar una sala técnica de coubicación en las mismas instalaciones que la ubicación. Para obtener más información, consulte Socios de entrega de AWS Direct Connect.

> **Note**
>
> No puede solicitar una conexión alojada a través de la AWS Direct Connect consola. Sin embargo, un AWS Direct Connect socio puede crear y configurar una conexión alojada para usted. Una vez que se haya configurado, la conexión aparece en el panel de Conexiones de la consola.
> Antes de empezar a utilizar una conexión alojada, debe aceptarla. Para obtener más información, consulte the section called “Aceptar una conexión alojada”.

Velocidad del puerto

Para las conexiones alojadas, los valores posibles son 50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps y 25 Gbps. Tenga en cuenta que solo los AWS Direct Connect socios que cumplan requisitos específicos pueden crear una conexión alojada de 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps o 25 Gbps. Las conexiones de 25 Gbps solo están disponibles en ubicaciones de Direct Connect donde estén disponibles velocidades de puerto de 100 Gbps.

Tenga en cuenta lo siguiente:

- Solo su socio puede cambiar las velocidades de los puertos de conexión. AWS Direct Connect Ya no es necesario que elimine y, a continuación, vuelva a crear una conexión para actualizar o reducir el ancho de banda de una conexión alojada existente. Para cambiar la velocidad de su puerto, póngase en contacto con el AWS Direct Connect socio que administra su conexión alojada.
- AWS utiliza la regulación del tráfico en las conexiones alojadas, lo que significa que cuando la velocidad de tráfico alcanza la velocidad máxima configurada, se elimina el exceso de tráfico. Esto puede provocar que el tráfico en ráfagas tenga un rendimiento menor que el tráfico sin ráfagas.

- Las tramas gigantes solo se pueden habilitar en las conexiones si se habilitaron originalmente en la conexión principal alojada de AWS Direct Connect . Si las tramas gigantes no se encuentran habilitadas en esa conexión principal, no podrá habilitarlas en ninguna conexión.

Las siguientes operaciones de consola se encontrará disponibles una vez que haya solicitado una conexión alojada y la haya aceptado:

- the section called “Ver los detalles de la conexión”
- the section called “Actualizar una conexión”
- the section called “Eliminar conexiones”

Una vez que acepte una conexión, cree una interfaz virtual para conectarse a los recursos públicos y privados de AWS . Para obtener más información, consulte AWS Direct Connect interfaces virtuales.

Aceptar una conexión alojada

Si está interesado en adquirir una conexión alojada, debe ponerse en contacto con un AWS Direct Connect AWS Direct Connect socio del Programa de socios. El socio creará la conexión por usted. Una vez que la conexión se haya configurado, aparece en el panel Connections (Conexiones) de la consola de AWS Direct Connect .

Antes de empezar a utilizar una conexión alojada, debe aceptar la conexión.

Console

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Connections (Conexiones).
3. Seleccione la conexión alojada y elija Ver detalles.
4. Seleccione la casilla de verificación de confirmación y elija Aceptar.

Command line

Para aceptar una conexión alojada mediante la línea de comandos o la API

- confirm-connection (AWS CLI)
- ConfirmConnection(AWS Direct Connect API)

Ver los detalles de la conexión

Puede ver el estado actual de su conexión. También puede ver el ID de conexión (por ejemplo, `dxcon-12nikabc`) y comprobar que coincide con el ID de conexión que aparece en el documento LOA-CFA que ha recibido o descargado.

Para obtener información sobre la supervisión de conexiones, consulte Supervisión.

Console

Para ver los detalles de una conexión

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel izquierdo, elija Connections (Conexiones).
3. Seleccione una conexión y, a continuación, elija Ver detalles.

Command line

Para describir una conexión mediante la línea de comandos o la API

- describe-connections (AWS CLI)
- DescribeConnections(AWS Direct Connect API)

Eliminar conexiones

Puede eliminar una conexión siempre y cuando no tenga interfaces virtuales adjuntas. Al eliminar tu conexión, se detendrán todos los cargos por hora de puerto de esta conexión, pero es posible que sigas incurriendo en cargos por conexiones cruzadas o por circuitos de red (ver más abajo). AWS Direct Connect los gastos de transferencia de datos están asociados a las interfaces virtuales. Para obtener más información sobre cómo eliminar una interfaz virtual, consulte Eliminar interfaces virtuales.

Antes de eliminar una conexión, descargue la LOA de la conexión que contiene la información de las cuentas cruzadas para disponer de la información pertinente sobre los circuitos que se van a desconectar. Para conocer los pasos a fin de descargar la LOA de conexión, consulte the section called “Descargar la LOA-CFA”.

Al eliminar una conexión, AWS indicará al proveedor de colocación que desconecte el dispositivo de red del router Direct Connect quitando el cable de conexión cruzada de fibra óptica del panel de conexiones correspondiente. AWS Sin embargo, es posible que su proveedor de ubicación o circuito le siga cobrando los cargos de conexión cruzada o de circuito de red, ya que es posible que el cable de conexión cruzada siga conectado a su dispositivo de red. Estos cargos por la conexión cruzada son independientes de Direct Connect y deben cancelarse con el proveedor de colocación o circuito utilizando la información de la LOA.

Si la conexión es parte de un grupo de agregación de enlaces (LAG), no puede eliminarla si al hacerlo provoca que el número mínimo de conexiones operativas del LAG caiga por debajo del umbral establecido.

Console

Para eliminar una conexión

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Connections (Conexiones).
3. Seleccione la conexión y elija Delete (Eliminar).
4. En el cuadro de diálogo Delete confirmation (Confirmación de eliminación), elija Delete (Eliminar).

Command line

Para eliminar una conexión de mediante la línea de comandos o la API

- delete-connection (AWS CLI)
- DeleteConnection(AWS Direct Connect API)

Solicitud de conexiones cruzadas en AWS Direct Connect ubicaciones

Una vez que haya descargado la Carta de autorización y Asignación de instalaciones de conexión (LOA-CFA), debe completar la conexión de red cruzada, también conocida como conexión cruzada. Si ya tiene el equipo ubicado en una AWS Direct Connect ubicación, póngase en contacto con el proveedor correspondiente para completar la conexión cruzada. Para obtener instrucciones específicas sobre cada proveedor, consulte la tabla que aparece a continuación. Póngase en contacto con el proveedor para conocer los precios de las conexiones. Una vez que se haya establecido la conexión puede crear las interfaces virtuales mediante la consola de AWS Direct Connect .

Algunas ubicaciones están configuradas como un campus. Para obtener más información, incluidas las velocidades disponibles en cada ubicación, consulte Ubicaciones de AWS Direct Connect.

Si aún no tiene el equipo ubicado en una AWS Direct Connect ubicación, puede trabajar con uno de los socios de la red de AWS socios (APN). Le ayudarán a conectarse a una ubicación de AWS Direct Connect . Para obtener más información, consulte el soporte de los socios de APN. AWS Direct Connect Debe compartir el documento LOA-CFA con el proveedor seleccionado para que realice la solicitud de conexión cruzada.

Una AWS Direct Connect conexión puede proporcionar acceso a recursos en otras regiones. Para obtener más información, consulte Acceso a una región de AWS remota.

> **Note**
>
> Si pasados 90 días la conexión no se ha completado la autoridad que concede el documento LOA-CFA caduca. Para renovar un documento LOA-CFA caducado, puede volver a descargarlo desde la consola de AWS Direct Connect . Para obtener más información, consulte Descargar la LOA-CFA.

Coubicaciones

- Este de EE. UU. (Ohio)
- Este de EE. UU. (Norte de Virginia)
- Oeste de EE. UU. (Norte de California)

- Oeste de EE. UU. (Oregón)
- África (Ciudad del Cabo)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Bombay)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Tokio)
- Canadá (centro)
- China (Pekín)
- China (Ningxia)
- Europa (Fráncfort)
- Europa (Irlanda)
- Europa (Milán)
- Europa (Londres)
- Europa (París)
- Europa (Estocolmo)
- Europa (Zúrich)
- Israel (Tel Aviv)
- Medio Oriente (Baréin)
- Medio Oriente (EAU)
- América del Sur (São Paulo)
- AWS GovCloud (Este de EE. UU.)
- AWS GovCloud (Estados Unidos-Oeste)

Este de EE. UU. (Ohio)

Ubicación	Cómo solicitar una conexión
Cologix COL2, Columbus	Póngase en contacto con Cologix en sales@cologix.com.

Ubicación	Cómo solicitar una conexión
Cologix MIN3, Minneapolis	Póngase en contacto con Cologix en sales@cologix.com.
CyrusOne West III, Houston	Envíe una solicitud mediante el portal del cliente.
Equinix CH2, Chicago	Póngase en contacto con Equinix en awsdealreg@equinix.com.
QTS, Chicago	Póngase en contacto con QTS en AConnect@qtsdatacenters.com.
Centros de datos de Netrality, 1102 Grand, Kansas City	Póngase en contacto con los Centros de datos de Netrality en support@netrality.com.

Este de EE. UU. (Norte de Virginia)

Ubicación	Cómo solicitar una conexión
165 Halsey Street, Newark	Póngase en contacto con operations@165halsey.com.
CoreSite 32k, Nueva York	Realice un pedido a través del Portal de CoreSite Clientes. Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web.
CoreSite VA1-VA2, Reston	Realice un pedido en el portal del cliente. CoreSite Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web.
Digital Realty ATL1 y ATL2, Atlanta	Póngase en contacto con Digital Realty en amazon.orders@digitalrealty.com.
Digital Realty IAD38, Ashburn	Póngase en contacto con Digital Realty en amazon.orders@digitalrealty.com.
Equinix DC1-DC6 y DC10-D12, Ashburn	Póngase en contacto con Equinix en awsdealreg@equinix.com.

Ubicación	Cómo solicitar una conexión
Equinix DAA1-DC3 y DC6, Dallas	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix MI1, Miami	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix NY5, Seacaucus	Póngase en contacto con Equinix en awsdealreg@equinix.com.
KIO Networks QRO1, Querétaro, MX	Póngase en contacto con KIO Networks».
Markley, One Summer Street, Boston	Para los clientes actuales, cree una solicitud mediante el portal de clientes. Para nuevas consultas, póngase en contacto con sales@markleygroup.com.
Neutrality Data Centers, segundo piso, MMR, Filadelfia	Póngase en contacto con los Centros de datos de Netrality en support@netrality.com.
QTS ATL1, Atlanta	Póngase en contacto con QTS en AConnect@qtsdatacenters.com.

Oeste de EE. UU. (Norte de California)

Ubicación	Cómo solicitar una conexión
CoreSite, LA1, Los Ángeles	Realice un pedido a través del portal de CoreSite clientes. Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web.
CoreSite SV2, Milpitas	Realice un pedido a través del portal de clientes. CoreSite Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web.
CoreSite SV4, Santa Clara	Realice un pedido a través del portal de CoreSite clientes. Después de completar el formulario, revise el pedido para comprobar que es correcto y, a continuación, apruebelo en el MyCoreSite sitio web.

Ubicación	Cómo solicitar una conexión
EdgeConneX, Phoenix	Haga un pedido con el Portal del cliente de EdgeOS. Una vez que haya enviado el formulario, EdgeConne X le proporcionará un formulario de solicitud de servicio para su aprobación. Puede enviar preguntas a cloudaccess@edgeconnex.com.
Equinix LA3, El Segundo	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix SV1 y SV5, San José	Póngase en contacto con Equinix en awsdealreg@equinix.com.
PhoenixNAP, Phoenix	Póngase en contacto con phoenixNAP Provisioning en provisioning@phoenixnap.com.

Oeste de EE. UU. (Oregón)

Ubicación	Cómo solicitar una conexión
CoreSite DE1, Denver	Realice un pedido a través del portal de CoreSite clientes. Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web.
Digital Realty SEA10, edificio Westin, Seattle	Póngase en contacto con Digital Realty en amazon.orders@digitalrealty.com.
EdgeConneX, Portland	Haga un pedido con el Portal del cliente de EdgeOS. Una vez que haya enviado el formulario, EdgeConne X le proporcionará un formulario de solicitud de servicio para su aprobación. Puede enviar preguntas a cloudaccess@edgeconnex.com.
Equinix SE2, Seattle	Póngase en contacto con Equinix en support@equinix.com.
Pittock Block, Portland	Envíe las solicitudes por correo electrónico a crossconnect@pittock.com o llame por teléfono al +1 503 226 6777.
Switch SUPERNAP 8, Las Vegas	Póngase en contacto con Switch SUPERNAP en orders@supernap.com.

Ubicación	Cómo solicitar una conexión
TierPoint Seattle	Póngase TierPoint en contacto con nosotros en sales@tierpoint.com.

África (Ciudad del Cabo)

Ubicación	Cómo solicitar una conexión
Centros de datos de Cape Town Internet Exchange/ Teraco	Póngase en contacto con Teraco en support@teraco.co.za (si es cliente de Teraco) o en connect@teraco.co.za (para nuevos clientes).
Teraco JB1, Johannesburgo, Sudáfrica	Póngase en contacto con Teraco en support@teraco.co.za (si es cliente de Teraco) o en connect@teraco.co.za (para nuevos clientes).

Asia-Pacífico (Yakarta)

Ubicación	Cómo solicitar una conexión
DCI JK3, Yakarta	Póngase en contacto con DCI Indonesia en jessie.w@dci-indonesia.com.com.
Centro de datos NTT 2, Yakarta	Póngase en contacto con NTT en tps.cms.presales@global.ntt.

Asia-Pacífico (Bombay)

Ubicación	Cómo solicitar una conexión
Equinix, Bombay	Póngase en contacto con Equinix en awsdealreg@equinix.com.

Ubicación	Cómo solicitar una conexión
NetMagic DC2, Bangalore	Póngase en contacto con NetMagic Ventas y Marketing llamando al número gratuito 18001033130 o enviando un correo electrónico a marketing@netmagicsolutions.com.
Sify Rabale, Mumbai	Póngase en contacto con Sify en aws.directconnect@sifycorp.com.
STT Delhi DC2, Delhi	Póngase en contacto con STT si tiene alguna consulta. AWSDX@sttelemediagdc .in.
STT GDC Pvt. Ltd. VSB, Chennai	Póngase en contacto con STT si tiene alguna consulta. AWSDX@sttelemediagdc .in.
STT Hyderabad DC1, Hyderabad	Póngase en contacto con STT si tiene alguna consulta. AWSDX@sttelemediagdc .in.

Asia-Pacífico (Seúl)

Ubicación	Cómo solicitar una conexión
Digital Realty ICN1, Seúl	Póngase en contacto con Digital Realty en amazon.orders@digitalrealty.com.
Centro de datos de Gasan de KINX, Seúl	Póngase en contacto con KINX en sales@kinx.net.
LG U+ Pyeong-Chon Mega Center, Seúl	Envíe el documento LOA a kidcadmin@lguplus.co.kr y center8@kidc.net.

Asia-Pacífico (Singapur)

Ubicación	Cómo solicitar una conexión
Equinix HK1, Tsuen Wan N. T., RAE de Hong Kong	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix SG2, Singapur	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Global Switch, Singapur	Póngase en contacto con Global Switch en salessingapore@globalswitch.com.
GPX, Mumbai	Póngase en contacto con GPX (Equinix) en awsdealreg@equinix.com.
iAdvantage Mega-i, Hong Kong	Póngase en contacto con iAdvantage en cs@iadvantage.net o haga un pedido con el iAdvantage Cabling Order e-Form (formulario electrónico de solicitud de cableado de iAdvantage).
Menara AIMS, Kuala Lumpur	Los clientes de AIMS existentes pueden solicitar una orden X-Connect en el portal del servicio de atención al cliente al completar el formulario de solicitud de orden de trabajo de ingeniería. Póngase en contacto con service.delivery@aims.com.my si hay problemas para enviar la solicitud.
Centro de datos TCC, Bangkok	Póngase en contacto con TCC Technology Co., Ltd en gateway.ne@tcc-technology.com.

Asia-Pacífico (Sídney)

Ubicación	Cómo solicitar una conexión
CDC Hume 2, Canberra	Inicie sesión en el portal de clientes del Portal de clientes de los CDC.
Datacom DH6, Auckland	Póngase en contacto con Datacom en Datacom Orbit, Auckland.

Ubicación	Cómo solicitar una conexión
Equinix ME2, Melbourne	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix SY3, Sídney	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Global Switch, Sídney	Póngase en contacto con Global Switch en salessydney@globalswitch.com.
NEXTDC C1, Canberra	Póngase en contacto con NEXTDC en nxtops@nextdc.com.
NEXTDC M1, Melbourne	Póngase en contacto con NEXTDC en nxtops@nextdc.com.
NEXTDC P1, Perth	Póngase en contacto con NEXTDC en nxtops@nextdc.com.
NEXTDC S2, Sídney	Póngase en contacto con NEXTDC en nxtops@nextdc.com.

Asia-Pacífico (Tokio)

Ubicación	Cómo solicitar una conexión
Centro de datos AT Tokyo Chuo, Tokio	Póngase en contacto con el servicio de TOKIO en at-sales@attokyo.co.jp.
Chief Telecom LY, Taipei	Póngase en contacto con Chief Telecom en vicky_chan@chief.com.tw.
Chunghwa Telecom, Taipei	Póngase en contacto con CHT Taipei IDC NOC en taipei_idc@cht.com.tw.
Equinix OS1, Osaka	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix TY2, Tokio	Póngase en contacto con Equinix en awsdealreg@equinix.com.
NEC Inzai, Inzai	Póngase en contacto con NEC Inzai en connection_support@ices.jp.nec.com.

Canadá (centro)

Ubicación	Cómo solicitar una conexión
Allied 250 Front St W, Toronto	Póngase en contacto con driches@alliedreit.com.
Cologix MTL3, Montreal	Póngase en contacto con Cologix en sales@cologix.com.
Cologix VAN2, Vancouver	Póngase en contacto con Cologix en sales@cologix.com.
eStruxture, Montreal	Póngase en contacto con eStruxture en directconnect@estruxture.com.

China (Pekín)

Ubicación	Cómo solicitar una conexión
CIDS Jiachuang IDC, Pekín	Póngase en contacto con dx-order@sinnet.com.cn.
Sinnet Jiuxianqiao IDC, Pekín	Póngase en contacto con dx-order@sinnet.com.cn.
GDS No. 3 Data Center, Shanghái	Póngase en contacto con dx@nwcdcloud.cn.
GDS No. 3 Data Center, Shenzhen	Póngase en contacto con dx@nwcdcloud.cn.

China (Ningxia)

Ubicación	Cómo solicitar una conexión
Industrial Park IDC, Ningxia	Póngase en contacto con dx@nwcdcloud.cn.
Shapotou IDC, Ningxia	Póngase en contacto con dx@nwcdcloud.cn.

Europa (Fráncfort)

Ubicación	Cómo solicitar una conexión
CE Colo, Praga, República Checa	Póngase en contacto con CE Colo en info@cecolo.com.
DigiPlex Ulven, Oslo, Noruega	Póngase en contacto con nosotros DigiPlex en helpme@digiplex.com.
Equinix AM3, Ámsterdam, Países Bajos	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix FR5, Fráncfort	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix HE6, Helsinki	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix MU1, Múnich	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix WA1, Varsovia	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Interxion AMS7, Ámsterdam	Póngase en contacto con Interxion en customer.services@interxion.com.
Interxion CPH2, Copenhague	Póngase en contacto con Interxion en customer.services@interxion.com.
Interxion FRA6, Fráncfort	Póngase en contacto con Interxion en customer.services@interxion.com.
Interxion MAD2, Madrid	Póngase en contacto con Interxion en customer.services@interxion.com.
Interxion VIE2, Viena	Póngase en contacto con Interxion en customer.services@interxion.com.
Interxion ZUR1, Zúrich	Póngase en contacto con Interxion en customer.services@interxion.com.
IPB, Berlín	Póngase en contacto con IPB en kontakt@ipb.de.

Ubicación	Cómo solicitar una conexión
Equinix ITConic MD2, Madrid	Póngase en contacto con Equinix en awsdealreg@equinix.com.

Europa (Irlanda)

Ubicación	Cómo solicitar una conexión
Digital Realty (Reino Unido), Docklands	Póngase en contacto con Digital Realty (Reino Unido) en amazon.orders@digitalrealty.com.
Eircom Clonshaugh	Póngase en contacto con Eircom en awsorders@eircom.ie.
Equinix DX1, Dublín	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix LD5, Londres (Slough)	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Interxion DUB2, Dublín	Póngase en contacto con Interxion en customer.services@interxion.com.
Interxion MRS1, Marsella	Póngase en contacto con Interxion en customer.services@interxion.com.

Europa (Milán)

Ubicación	Cómo solicitar una conexión
CDLAN srl Via Caldera 21, Milán	Contacte con CDLAN en sales@cdlan.it.
Equinix, ML2, Milán, Italia	Póngase en contacto con Equinix en awsdealreg@equinix.com.

Europa (Londres)

Ubicación	Cómo solicitar una conexión
Digital Realty (Reino Unido), Docklands	Póngase en contacto con Digital Realty (Reino Unido) en amazon.orders@digitalrealty.com.
Equinix LD5, Londres (Slough)	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix MA3, Mánchester	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Telehouse West, Londres	Póngase en contacto con Telehouse UK en sales.support@uk.telehouse.net.

Europa (París)

Ubicación	Cómo solicitar una conexión
Equinix PA3, París	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Interxion PAR7, París	Póngase en contacto con Interxion en customer.services@interxion.com.
Telehouse Voltaire, París	Póngase en contacto con Telehouse Paris Voltaire a través de la página de contacto.

Europa (Estocolmo)

Ubicación	Cómo solicitar una conexión
Interxion STO1, Estocolmo	Póngase en contacto con Interxion en customer.services@interxion.com.

Europa (Zúrich)

Ubicación	Cómo solicitar una conexión
Equinix ZRH51, Oberengstringen, Suiza	Póngase en contacto con Equinix en awsdealreg@equinix.com.

Israel (Tel Aviv)

Ubicación	Cómo solicitar una conexión
MedOne, Haifa	Póngase en contacto con nosotros MedOne en support@Medone.co.il
EdgeConnex, Herzliya	Póngase en contacto con nosotros en info@edgeconnecx.com EdgeConnect

Medio Oriente (Baréin)

Ubicación	Cómo solicitar una conexión
AWS Bahréin DC53, Manama	Para realizar la conexión, puede colaborar con uno de nuestros socios proveedores de red de la ubicación para establecer la conectividad. Luego, entregará una carta de autorización (LOA) del proveedor de la red a AWS través del AWS Support Center. AWS completa la conexión cruzada en esta ubicación.
AWS Bahréin DC52, Manama	Para realizar la conexión, puede colaborar con uno de nuestros socios proveedores de red de la ubicación para establecer la conectividad. Luego, entregará una carta de autorización (LOA) del proveedor de la red a AWS través del AWS Support Center. AWS completa la conexión cruzada en esta ubicación.

Medio Oriente (EAU)

Ubicación	Cómo solicitar una conexión
Equinix DX1, Dubái, EAU	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Centro de SmartHub datos de Etisalat, Fujairah (Emiratos Árabes Unidos)	Póngase en contacto con el centro de datos de Etisalat en -C& WS@etisalat.ae. SmartHub IntlSales

América del Sur (São Paulo)

Ubicación	Cómo solicitar una conexión
Equinix RJ2, Río de Janeiro	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix SP4, São Paulo	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Tivit	Póngase en contacto con Tivit en aws@tivit.com.br.

AWS GovCloud (Este de EE. UU.)

No puede solicitar conexiones en esta región.

AWS GovCloud (Estados Unidos-Oeste)

Ubicación	Cómo solicitar una conexión
Equinix SV5, San José	Póngase en contacto con Equinix en awsdealreg@equinix.com.

AWS Direct Connect interfaces virtuales

Debe crear una de las siguientes interfaces virtuales (VIF) para empezar a utilizar la conexión. AWS Direct Connect

- Interfaz virtual privada: una interfaz virtual privada se debe utilizar para acceder a una Amazon VPC mediante direcciones IP privadas.
- Interfaz virtual pública: una interfaz virtual pública puede acceder a todos los servicios AWS públicos mediante direcciones IP públicas.
- Interfaz virtual de tránsito: una interfaz virtual de tránsito se debe utilizar para acceder a una o varias puertas de enlace de tránsito de Amazon VPC asociadas a las puertas de enlace de Direct Connect. Puede utilizar las interfaces virtuales de tránsito con cualquier conexión AWS Direct Connect dedicada o alojada de cualquier velocidad. Para obtener información acerca de las configuraciones de gateway de Direct Connect, consulte the section called “Gateways de Direct Connect”.

Para conectarse a otros AWS servicios mediante direcciones IPv6, consulte la documentación del servicio para comprobar que se admite el direccionamiento IPv6.

Reglas de anuncio de prefijo de interfaz virtual pública

Te anunciamos los prefijos de Amazon adecuados para que puedas acceder a tus VPC o a otros AWS servicios. Puede acceder a todos los AWS prefijos a través de esta conexión; por ejemplo, Amazon EC2, Amazon S3 y Amazon.com. No tiene acceso a los prefijos que no son de Amazon. Para ver una lista actualizada de los prefijos anunciados por AWS, consulte Intervalos de AWS direcciones IP en. Referencia general de Amazon Web Services AWS no vuelve a anunciar a otros clientes los prefijos de los clientes que se recibieron a través de las interfaces virtuales públicas de Direct AWS Connect. Para obtener más información sobre las interfaces virtuales públicas y las políticas de enrutamiento, consulte the section called “Políticas de direccionamiento de interfaces virtuales públicas”.

> **Note**
>
> Le recomendamos que utilice un filtro de firewall (en función de la dirección de origen/destino de los paquetes) para controlar el tráfico que envía a algunos prefijos o que procede de ellos. Si utiliza un filtro de prefijo (mapeado de ruta), asegúrese de que acepta prefijos con una

coincidencia exacta o mayor. Los prefijos anunciados AWS Direct Connect pueden estar agregados y pueden diferir de los prefijos definidos en el filtro de prefijos.

Interfaces virtuales alojadas

Para usar su AWS Direct Connect conexión con otra cuenta, puede crear una interfaz virtual alojada para esa cuenta. El propietario de la otra cuenta debe aceptar la interfaz virtual alojada para empezar a utilizarla. Una interfaz virtual alojada funciona igual que una interfaz virtual estándar y puede conectarse a los recursos públicos o a una VPC.

Puede usar interfaces virtuales de tránsito con conexiones alojadas o dedicadas de Direct Connect de cualquier velocidad. Las conexiones alojadas solo son compatibles con una interfaz virtual.

Para crear una interfaz virtual, necesita la siguiente información:

Recurso	Información necesaria
Conexión	La AWS Direct Connect conexión o el grupo de agregación de enlaces (LAG) para el que va a crear la interfaz virtual.
Nombre de la interfaz virtual	Un nombre para la interfaz virtual.
Propietario de la interfaz virtual	Si va a crear la interfaz virtual para otra cuenta, necesitará el ID de AWS cuenta de la otra cuenta.
(Solo para la interfaz virtual privada) Conexión	Para conectarse a una VPC de la misma AWS región, necesita la puerta de enlace privada virtual para su VPC. El ASN del lado de Amazon de la sesión del BGP se hereda de la puerta de enlace privada virtual. Al crear una puerta de enlace privada virtual, puede especificar su propio ASN privado. De lo contrario, Amazon proporciona un ASN predeterminado. Para obtener información, consulte Crear una puerta de enlace privada virtual en la Guía del usuario de Amazon VPC. Para conectarse a una VPC a través de una puerta de enlace de Direct Connect, se necesita la puerta de enlace de Direct Connect. Para obtener más información, consulte Gateways de Direct Connect.

Recurso	Información necesaria
VLAN	Una etiqueta de red de área local virtual (VLAN) única que aún no se encuentra en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de AWS Direct Connect . Si tiene una conexión alojada, su AWS Direct Connect socio le proporcionará este valor. No puede modificar el valor después de haber creado la interfaz virtual.

Recurso	Información necesaria

Direcciones IP de mismo nivel	Una interfaz virtual es compatible con una sesión de intercambio de tráfico del BGP para IPv4 e IPv6, o con uno de cada una (pila doble). No utilice direccion es IP elásticas (eIP) ni traiga sus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias sesiones de BGP para la misma familia de direccionamiento IP en la misma interfaz virtual. Los rangos de las direcciones IP que se asignan a cada extremo de la interfaz virtual para la sesión de intercambio de tráfico del BGP.
	
	• IPv4:
	  • (Solo para la interfaz virtual pública) Debe especificar direcciones IPv4 públicas únicas que sean de su propiedad. El valor puede ser uno de los siguientes:
	  • Un CIDR IPv4 propiedad del cliente
	
	Puede ser cualquier IP pública (propiedad del cliente o proporcio nada por él AWS), pero se debe utilizar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del router. AWS Por ejemplo, si asigna un `/31` rango, por ejemplo, podría usarlo `203.0.113.0` para su IP homóloga y `203.0.113.1` para la AWS IP homóloga. `203.0.113.0/31` O bien, si asignas un `/24` rango, por ejemplo`198.51.100.0/24` , puedes usarlo `198.51.100.10` para tu IP homóloga y `198.51.100.20` para la IP AWS homóloga.
	  • Un rango de IP propiedad de su AWS Direct Connect socio o ISP, junto con una autorización LOA-CFA
	  • Un AWS CIDR /31 proporcionado. Póngase en contacto con AWS Asistencia para solicitar un CIDR IPv4 público (e indique un caso de uso en su solicitud)
	
	Note
	No podemos garantizar que podamos cumplir con todas las solicitudes de direcciones IPv4 públicas AWS proporcionadas.
	  • (Solo para la interfaz virtual privada) Amazon puede generar direcciones IPv4 privadas en su nombre. Si especifica el suyo propio, asegúrese de

Recurso	Información necesaria
	especificar únicamente los CIDR privados para la interfaz de su router y la interfaz AWS Direct Connect. Por ejemplo, no especifique otras direcciones IP de su red local. Al igual que en una interfaz virtual pública, se debe utilizar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del AWS router. Por ejemplo, si asigna un `/30` rango, por ejemplo, podría usarlo `192.168.0.1` para su IP homóloga y `192.168.0.2` para la IP AWS homóloga. `192.168.0.0/30` • IPv6: Amazon le asigna un CIDR IPv6 /125 de forma automática. No puede especificar sus propias direcciones IPv6 de mismo nivel.
Familia de direcciones	Si la sesión de intercambio de tráfico del BGP se realizará a través de IPv4 o IPv6.
Información sobre el BGP	• Un número de sistema autónomo (ASN) para el protocolo de puerta de enlace fronteriza (BGP) público o privado en su lado de la sesión del BGP. Si utiliza un ASN público, debe tener uno propio. Si utiliza un ASN privado, puede establecer un valor de ASN personalizado. Para un ASN de 16 bits ASN, el valor debe estar dentro del rango de 64 512 a 65 534. En el caso de un ASN de 32 bits, el valor debe estar dentro del rango de 1 a 2147483647. El sistema autónomo (AS) que se antepone no funciona si utiliza un ASN privado para una interfaz virtual pública. • AWS habilita MD5 de forma predeterminada. Esta opción no se puede modificar. • Una clave de autenticación del BGP MD5. Puede proporcionar su propia clave o dejar que Amazon genere una en su nombre.

Recurso	Información necesaria

(Solo para la interfaz virtual pública) Prefijos que desea anunciar	Rutas IPv4 públicas o rutas IPv6 para anunciar a través del BGP. Debe comunicar al menos un prefijo a través del BGP, hasta un máximo de 1 000 prefijos.
	• IPv4: el CIDR de IPv4 puede superponerse con otro CIDR de IPv4 público que se haya anunciado que se utiliza AWS Direct Connect cuando se cumple alguna de las siguientes condiciones:
	  • Los CIDR provienen de distintas regiones. AWS Asegúrese de aplicar etiquetas de comunidad del BGP a los prefijos públicos.
	  • Utiliza AS_PATH cuando tiene un ASN público en una configuración activa/pasiva.
	  Para obtener más información, consulte Políticas de enrutamiento y comunidades del BGP.
	• IPv6: especifique una longitud de prefijo de /64 caracteres o menos.
	• Puede agregar prefijos adicionales a una VIF pública existente y anunciarl os si se pone en contacto con AWS Asistencia. En su caso de soporte, proporcione una lista de los prefijos de CIDR adicionales que desee agregar a la VIF pública y anunciar.
	• Puede especificar cualquier longitud de prefijo en una interfaz virtual pública de Direct Connect. IPv4 debería admitir cualquier valor entre /1 y /32, e IPv6 debería admitir cualquier valor entre /1 y /64.

Recurso	Información necesaria
(Solo para la interfaz virtual privada) Tramas gigantes	La unidad máxima de transmisión (MTU) de los paquetes superados. AWS Direct Connect El valor predeterminado es 1500. El establecimiento de la MTU de una interfaz virtual en 9001 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Las tramas gigantes solo se aplican a las rutas propagadas desde. AWS Direct Connect Si agrega rutas estáticas a una tabla de enrutamiento que apuntan a una gateway privada virtual, el tráfico enrutado a través de las rutas estáticas se envía utilizando 1500 MTU. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Jumbo Frame Capable en la página de configuración general de la interfaz virtual.
(Solo para la interfaz virtual de tránsito) Tramas gigantes	La unidad máxima de transmisión (MTU) de los paquetes superados. AWS Direct Connect El valor predeterminado es 1500. El establecimiento de la MTU de una interfaz virtual en 8500 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Se admiten tramas gigantes de hasta 8500 de MTU para Direct Connect. Las rutas estáticas y propagadas configuradas en la tabla de enrutamiento de puerta de enlace de tránsito admitirán tramas gigantes, incluso desde instancias de EC2 con entradas de la tabla de enrutamiento estáticas de VPC hasta la conexión de puerta de enlace de tránsito. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Capacidad para tramas gigantes en la página de configuración general de la interfaz virtual.

SiteLink

Si va a crear una interfaz virtual privada o de tránsito, puede utilizarla. SiteLink

SiteLink es una función opcional de Direct Connect para las interfaces privadas virtuales que permite la conectividad entre dos puntos de presencia de Direct Connect (PoPs) de la misma AWS partición mediante la ruta más corta disponible a través de la AWS red. Esto le permite conectar la red en las instalaciones a través de la red global de AWS sin necesidad de enrutar el tráfico a través de una región. Para obtener más información al respecto, SiteLink consulte Introducción AWS Direct Connect SiteLink.

> **Note**
>
> SiteLink no está disponible en AWS GovCloud (US) las regiones de China.

Hay una tarifa de precio diferente por su uso SiteLink. Para obtener más información, consulte Precios de AWS Direct Connect.

SiteLink no es compatible con todos los tipos de interfaz virtual. En la siguiente tabla, se muestra el tipo de interfaz y si se admite.

Tipo de interfaz virtual	Admitido/No admitido
Interfaz virtual de tránsito	Compatible
Interfaz virtual privada adjunta a una puerta de enlace de Direct Connect con una puerta de enlace virtual	Compatible
Interfaz virtual privada adjunta a una puerta de enlace de Direct Connect no asociada a una puerta de enlace virtual o de tránsito	Compatible
Interfaz virtual privada adjunta a una puerta de enlace virtual	No compatible
Interfaz virtual privada	No compatible

El comportamiento del enrutamiento del tráfico desde Regiones de AWS (puertas de enlace virtuales o de tránsito) a ubicaciones locales a través de una interfaz virtual SiteLink habilitada varía ligeramente del comportamiento predeterminado de la interfaz virtual Direct Connect con un prefijo de AWS ruta. Cuando SiteLink está habilitada, las interfaces virtuales de an Región de AWS prefieren una ruta BGP con una longitud de ruta AS inferior desde una ubicación de Direct Connect, independientemente de la región asociada. Por ejemplo, se anuncia una región asociada para cada ubicación de Direct Connect. Si SiteLink está deshabilitado, de forma predeterminada, el tráfico que proviene de una puerta de enlace virtual o de tránsito prefiere una ubicación de Direct Connect asociada a esa ubicación Región de AWS, incluso si el enrutador de las ubicaciones de Direct Connect asociadas a diferentes regiones anuncia una ruta con una longitud de ruta AS más corta. La puerta de enlace virtual o de tránsito sigue prefiriendo la ruta desde las ubicaciones de Direct Connect locales a la Región de AWS asociada.

SiteLink admite un tamaño máximo de MTU de trama gigante de 8500 o 9001, según el tipo de interfaz virtual. Para obtener más información, consulte the section called “Establecer la MTU de red para interfaces virtuales privadas o de tránsito”.

Requisitos previos de las interfaces virtuales

Antes de crear una interfaz virtual, haga lo siguiente:

- Cree una conexión. Para obtener más información, consulte the section called “Crear una conexión mediante el asistente de conexión”.
- Cree un grupo de agregación de enlaces (LAG) cuando tenga varias conexiones que desea tratar como una sola. Para obtener más información, consulte Asociar una conexión a un LAG.

Para crear una interfaz virtual, necesita la siguiente información:

Recurso	Información necesaria
Conexión	El grupo de AWS Direct Connect conexión o agregación de enlaces (LAG) para el que va a crear la interfaz virtual.
Nombre de la interfaz virtual	Un nombre para la interfaz virtual.

Recurso	Información necesaria
Propietario de la interfaz virtual	Si va a crear la interfaz virtual para otra cuenta, necesitará el ID de AWS cuenta de la otra cuenta.
(Solo para la interfaz virtual privada) Conexión	Para conectarse a una VPC de la misma AWS región, necesita la puerta de enlace privada virtual para su VPC. El ASN del lado de Amazon de la sesión del BGP se hereda de la puerta de enlace privada virtual. Al crear una puerta de enlace privada virtual, puede especificar su propio ASN privado. De lo contrario, Amazon proporciona un ASN predeterminado. Para obtener información, consulte Crear una puerta de enlace privada virtual en la Guía del usuario de Amazon VPC. Para conectarse a una VPC a través de una puerta de enlace de Direct Connect, se necesita la puerta de enlace de Direct Connect. Para obtener más información, consulte Gateways de Direct Connect.
VLAN	Una etiqueta de red de área local virtual (VLAN) única que aún no se encuentra en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de AWS Direct Connect . Si tiene una conexión alojada, su AWS Direct Connect socio le proporcionará este valor. No puede modificar el valor después de haber creado la interfaz virtual.

Recurso	Información necesaria

Direcciones IP de mismo nivel	Una interfaz virtual es compatible con una sesión de intercambio de tráfico del BGP para IPv4 e IPv6, o con uno de cada una (pila doble). No utilice direccion es IP elásticas (eIP) ni traiga sus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias sesiones de BGP para la misma familia de direccionamiento IP en la misma interfaz virtual. Los rangos de las direcciones IP que se asignan a cada extremo de la interfaz virtual para la sesión de intercambio de tráfico del BGP.
	
	• IPv4:
	  • (Solo para la interfaz virtual pública) Debe especificar direcciones IPv4 públicas únicas que sean de su propiedad. El valor puede ser uno de los siguientes:
	  • Un CIDR IPv4 propiedad del cliente
	
	Puede ser cualquier IP pública (propiedad del cliente o proporcio nada por él AWS), pero se debe utilizar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del router. AWS Por ejemplo, si asigna un `/31` rango, por ejemplo, podría usarlo `203.0.113.0` para su IP homóloga y `203.0.113.1` para la AWS IP homóloga. `203.0.113.0/31` O bien, si asignas un `/24` rango, por ejemplo`198.51.100.0/24` , puedes usarlo `198.51.100.10` para tu IP homóloga y `198.51.100.20` para la IP AWS homóloga.
	  • Un rango de IP propiedad de su AWS Direct Connect socio o ISP, junto con una autorización LOA-CFA
	  • Un AWS CIDR /31 proporcionado. Póngase en contacto con AWS Asistencia para solicitar un CIDR IPv4 público (e indique un caso de uso en su solicitud)
	
	Note
	No podemos garantizar que podamos cumplir con todas las solicitudes de direcciones IPv4 públicas AWS proporcionadas.
	  • (Solo para la interfaz virtual privada) Amazon puede generar direcciones IPv4 privadas en su nombre. Si especifica el suyo propio, asegúrese de

Recurso	Información necesaria
	especificar únicamente los CIDR privados para la interfaz de su router y la interfaz AWS Direct Connect. Por ejemplo, no especifique otras direcciones IP de su red local. Al igual que en una interfaz virtual pública, se debe utilizar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del AWS router. Por ejemplo, si asigna un `/30` rango, por ejemplo, podría usarlo `192.168.0.1` para su IP homóloga y `192.168.0.2` para la IP AWS homóloga. `192.168.0.0/30` • IPv6: Amazon le asigna un CIDR IPv6 /125 de forma automática. No puede especificar sus propias direcciones IPv6 de mismo nivel.
Familia de direcciones	Si la sesión de intercambio de tráfico del BGP se realizará a través de IPv4 o IPv6.
Información sobre el BGP	• Un número de sistema autónomo (ASN) para el protocolo de puerta de enlace fronteriza (BGP) público o privado en su lado de la sesión del BGP. Si utiliza un ASN público, debe tener uno propio. Si utiliza un ASN privado, puede establecer un valor de ASN personalizado. Para un ASN de 16 bits ASN, el valor debe estar dentro del rango de 64 512 a 65 534. En el caso de un ASN de 32 bits, el valor debe estar dentro del rango de 1 a 2147483647. El sistema autónomo (AS) que se antepone no funciona si utiliza un ASN privado para una interfaz virtual pública. • AWS habilita MD5 de forma predeterminada. Esta opción no se puede modificar. • Una clave de autenticación del BGP MD5. Puede proporcionar su propia clave o dejar que Amazon genere una en su nombre.

Recurso	Información necesaria

(Solo para la interfaz virtual pública) Prefijos que desea anunciar	Rutas IPv4 públicas o rutas IPv6 para anunciar a través del BGP. Debe comunicar al menos un prefijo a través del BGP, hasta un máximo de 1 000 prefijos.
	• IPv4: el CIDR de IPv4 puede superponerse con otro CIDR de IPv4 público que se haya anunciado que se utiliza AWS Direct Connect cuando se cumple alguna de las siguientes condiciones:
	  • Los CIDR provienen de distintas regiones. AWS Asegúrese de aplicar etiquetas de comunidad del BGP a los prefijos públicos.
	  • Utiliza AS_PATH cuando tiene un ASN público en una configuración activa/pasiva.
	  Para obtener más información, consulte Políticas de enrutamiento y comunidades del BGP.
	• IPv6: especifique una longitud de prefijo de /64 caracteres o menos.
	• Puede agregar prefijos adicionales a una VIF pública existente y anunciarl os si se pone en contacto con AWS Asistencia. En su caso de soporte, proporcione una lista de los prefijos de CIDR adicionales que desee agregar a la VIF pública y anunciar.
	• Puede especificar cualquier longitud de prefijo en una interfaz virtual pública de Direct Connect. IPv4 debería admitir cualquier valor entre /1 y /32, e IPv6 debería admitir cualquier valor entre /1 y /64.

Recurso	Información necesaria
(Solo para la interfaz virtual privada) Tramas gigantes	La unidad máxima de transmisión (MTU) de los paquetes superados. AWS Direct Connect El valor predeterminado es 1500. El establecimiento de la MTU de una interfaz virtual en 9001 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Las tramas gigantes solo se aplican a las rutas propagadas desde. AWS Direct Connect Si agrega rutas estáticas a una tabla de enrutamiento que apuntan a una gateway privada virtual, el tráfico enrutado a través de las rutas estáticas se envía utilizando 1500 MTU. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Jumbo Frame Capable en la página de configuración general de la interfaz virtual.
(Solo para la interfaz virtual de tránsito) Tramas gigantes	La unidad máxima de transmisión (MTU) de los paquetes superados. AWS Direct Connect El valor predeterminado es 1500. El establecimiento de la MTU de una interfaz virtual en 8500 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Se admiten tramas gigantes de hasta 8500 de MTU para Direct Connect. Las rutas estáticas y propagadas configuradas en la tabla de enrutamiento de puerta de enlace de tránsito admitirán tramas gigantes, incluso desde instancias de EC2 con entradas de la tabla de enrutamiento estáticas de VPC hasta la conexión de puerta de enlace de tránsito. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Capacidad para tramas gigantes en la página de configuración general de la interfaz virtual.

Al crear una interfaz virtual, puede especificar la cuenta a la que pertenece. Cuando eliges una AWS cuenta que no es la tuya, se aplican las siguientes reglas:

- En interfaces virtuales privadas y en tránsito, la cuenta se usa para la interfaz virtual y el destino de la gateway privada virtual o de Direct Connect.
- En interfaces virtuales públicas, la cuenta se usa para la facturación de las interfaces virtuales. El uso de transferencia de datos salientes (DTO) se calcula en beneficio del propietario del recurso según la velocidad de transferencia de AWS Direct Connect datos.

> **Note**
>
> Los prefijos de 31 bits se admiten en todos los tipos de interfaz virtual de Direct Connect. Consulte RFC 3021: Using 31-Bit Prefixes on IPv4 Point-to-Point Links para obtener más información.

Crear una interfaz virtual

Puede crear una interfaz virtual de tránsito para conectarse a una gateway de tránsito, una interfaz virtual pública para conectarse a los recursos públicos (servicios que no sean de la VPC) o una interfaz virtual privada para conectarse a una VPC.

Para crear una interfaz virtual para las cuentas propias AWS Organizations o AWS Organizations distintas de la suya, cree una interfaz virtual alojada. Para obtener más información, consulte the section called “Crear una interfaz virtual alojada”.

Requisitos previos

Antes de comenzar, asegúrese de que ha leído la información que aparece en Requisitos previos de las interfaces virtuales.

Crear una interfaz virtual pública

Al crear una interfaz virtual pública, podemos tardar hasta 72 horas en revisar y aprobar la solicitud.

Para aprovisionar una interfaz virtual pública

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).

4. En Virtual interface type (Tipo de interfaz virtual) en Type (Tipo), elija Public (Pública).
5. En Public virtual interface settings (Configuración de la interfaz virtual pública), haga lo siguiente:

   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

   c. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

   d. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

      Los valores válidos son 1-2.147.483.647.
6. En Additional settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

      [IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
      - En Amazon router peer IP (IP del mismo nivel del router de Amazon), escriba la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

      [IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

   b. Para utilizar su propia clave de BGP, introduzca su clave MD5 de BGP.

      Si no ingresa un valor, generamos una clave de BGP. Si proporcionó su propia clave o si la generamos nosotros, ese valor aparece en la columna de Clave de autenticación del BGP de la página de detalles de interfaz virtual de Interfaces virtuales.

   c. Para anunciar prefijos para Amazon, en Prefixes you want to advertise (Prefijos que desea anunciar), escriba las direcciones CIDR IPv4 de destino (separadas por comas) a las que debe redirigirse el tráfico a través de la interfaz virtual.

> **Important**
>
> Puede agregar prefijos adicionales a una VIF pública existente y anunciarlos si se pone en contacto con AWS Asistencia. En su caso de soporte, proporcione una lista de los prefijos de CIDR adicionales que desee agregar a la VIF pública y anunciar.

d. (Opcional) Añada o elimine una etiqueta.

[Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

- En Key (Clave), escriba el nombre de la clave.
- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

7. Elija Create virtual interface (Crear interfaz virtual).
8. Descargue la configuración del router para su dispositivo. Para obtener más información, consulte Descargar el archivo de configuración del enrutador.

Para crear una interfaz virtual pública mediante la línea de comandos o la API

- create-public-virtual-interface (AWS CLI)
- CreatePublicVirtualInterface(AWS Direct Connect API)

Crear una interfaz virtual privada

Puede aprovisionar una interfaz virtual privada a una puerta de enlace privada virtual en la misma región que su AWS Direct Connect conexión. Para obtener más información sobre el aprovisionamiento de una interfaz virtual privada a una AWS Direct Connect puerta de enlace, consulteUso de puertas de enlace de Direct Connect.

Si utiliza el asistente de VPC para crear una VPC, la propagación de rutas se activa automáticamente. Gracias a la propagación de rutas, estas aparecen automáticamente en las tablas de ruteo de la VPC. Si lo prefiere, puede deshabilitar la propagación de rutas. Para obtener más información, consulte Habilitar la propagación de ruta en su tabla de enrutamiento en la Guía del usuario de Amazon VPC.

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 la conexión. La MTU de una interfaz virtual privada puede ser 1500 o 9001 (tramas gigantes). La MTU de una interfaz virtual de tránsito puede ser 1500 o 8500 (tramas gigantes). Puede especificar la MTU al crear la interfaz o actualizarla tras crearla. El establecimiento de la MTU de una interfaz virtual en 8500 (tramas gigantes) o 9001 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la consola de AWS Direct Connect y busque Jumbo Frame Capable (Con capacidad de tramas gigantes) en la pestaña Summary (Resumen).

Para aprovisionar una interfaz virtual privada a una VPC

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Tipo de interfaz virtual, elija Privada.
5. En Configuración de la interfaz virtual privada, realice lo siguiente:

   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

   c. Como propietario de la interfaz virtual, elija Mi AWS cuenta si la interfaz virtual es para su AWS cuenta.

   d. En Direct Connect gateway (Gateway de Direct Connect), seleccione la gateway de Direct Connect.

   e. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

   f. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

      Los valores válidos son 1 a 2147483647.
6. En Additional Settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

[IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

- Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
- En IP de mismo nivel del enrutador de Amazon, ingrese la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

> **Important**
>
> Si permite la AWS asignación automática de direcciones IPv4, se asignará un CIDR /29 desde 169.254.0.0/16 IPv4 Link-Local de acuerdo con la RFC 3927 para la conectividad. point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP del mismo nivel del router del cliente como origen o destino del tráfico de VPC. En su lugar, debe utilizar el RFC 1918 u otro direccionamiento (que no sea el RFC 1918) y especificar la dirección usted mismo.
>
> - Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.
> - Para obtener más información sobre la RFC 3927, consulte Dynamic Configuration of IPv4 Link-Local Addresses.

[IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

b. Para cambiar la unidad de transmisión máxima (MTU) de 1500 (predeterminada) a 9001 (tramas gigantes), seleccione MTU gigante (tamaño de MTU 9001).

c. (Opcional) En Habilitar SiteLink, elija Habilitado para habilitar la conectividad directa entre los puntos de presencia de Direct Connect.

d. (Opcional) Añada o elimine una etiqueta.

[Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

- En Key (Clave), escriba el nombre de la clave.
- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

7. Elija Create virtual interface (Crear interfaz virtual).
8. Descargue la configuración del router para su dispositivo. Para obtener más información, consulte Descargar el archivo de configuración del enrutador.

Para crear una interfaz virtual privada mediante la línea de comandos o la API

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface(AWS Direct Connect API)

Crear una interfaz virtual de tránsito en la puerta de enlace de Direct Connect

Para conectar tu AWS Direct Connect conexión a la pasarela de tránsito, debes crear una interfaz de tránsito para tu conexión. Especifique la gateway de Direct Connect a la que se va a conectar.

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 la conexión. La MTU de una interfaz virtual privada puede ser 1500 o 9001 (tramas gigantes). La MTU de una interfaz virtual de tránsito puede ser 1500 o 8500 (tramas gigantes). Puede especificar la MTU al crear la interfaz o actualizarla tras crearla. El establecimiento de la MTU de una interfaz virtual en 8500 (tramas gigantes) o 9001 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la consola de AWS Direct Connect y busque Jumbo Frame Capable (Con capacidad de tramas gigantes) en la pestaña Summary (Resumen).

> **Important**
>
> Si asocia su puerta de enlace de tránsito a una o más puertas de enlace de Direct Connect, el número de sistema autónomo (ASN) que utilizan la puerta de enlace de tránsito y de Direct Connect deben ser diferentes. Por ejemplo, si utiliza el ASN 64512 predeterminado tanto para la puerta de enlace de tránsito como para la de Direct Connect, la solicitud de asociación fallará.

Para aprovisionar una interfaz virtual de tránsito en una gateway de Direct Connect

1. Abre la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Virtual interface type (Tipo de interfaz virtual) en Type (Tipo), elija Transit (Tránsito).
5. En Transit virtual interface settings (Configuración de la interfaz virtual de tránsito), haga lo siguiente:

   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

   c. Como propietario de la interfaz virtual, elija Mi AWS cuenta si la interfaz virtual es para su AWS cuenta.

   d. En Direct Connect gateway (Gateway de Direct Connect), seleccione la gateway de Direct Connect.

   e. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

   f. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

      Los valores válidos son 1 a 2147483647.
6. En Additional Settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

      [IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
      - En IP de mismo nivel del enrutador de Amazon, ingrese la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

> **Important**
>
> Si permite la AWS asignación automática de direcciones IPv4, se asignará un CIDR /29 desde 169.254.0.0/16 IPv4 Link-Local de acuerdo con la RFC 3927 para la conectividad. point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP del mismo nivel del router del cliente como origen o destino del tráfico de VPC. En su lugar, debe utilizar el RFC 1918 u otro direccionamiento (que no sea el RFC 1918) y especificar la dirección usted mismo.
>
> - Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.
> - Para obtener más información sobre la RFC 3927, consulte Dynamic Configuration of IPv4 Link-Local Addresses.

[IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

b. Para cambiar la unidad de transmisión máxima (MTU) de 1500 (predeterminada) a 8500 (tramas gigantes), seleccione Jumbo MTU (MTU size 8500) [MTU gigante (tamaño de MTU 8500)].

c. (Opcional) En Habilitar SiteLink, elija Habilitado para habilitar la conectividad directa entre los puntos de presencia de Direct Connect.

d. (Opcional) Añada o elimine una etiqueta.

   [Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

   - En Key (Clave), escriba el nombre de la clave.
   - En Valor, escriba el valor de la clave.

   [Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

7. Elija Create virtual interface (Crear interfaz virtual).

Una vez que cree la interfaz virtual, puede descargar la configuración del router de su dispositivo. Para obtener más información, consulte Descargar el archivo de configuración del enrutador.

Para crear una interfaz virtual de tránsito mediante la línea de comandos o la API

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface(AWS Direct Connect API)

Para ver las interfaces virtuales que se han adjuntado a una gateway de Direct Connect mediante la línea de comandos o la API

- describe-direct-connect-gateway-attachments (AWS CLI)
- DescribeDirectConnectGatewayAdjuntos (AWS Direct Connect API)

Descargar el archivo de configuración del enrutador

Después de crear la interfaz virtual y cuando el estado de la interfaz esté activo, puede descargar el archivo de configuración del router para su router.

Si utiliza alguno de los siguientes enrutadores para las interfaces virtuales con MACsec activado, crearemos el archivo de configuración para su enrutador de forma automática:

- Switches Nexus de Cisco serie 9000 que ejecutan el software NX-OS 9.3 o posterior
- Enrutadores de la serie M/MX de Juniper Networks que ejecutan el software JunOS 9.5 o posterior

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Seleccione la interfaz virtual y, a continuación, elija View details (Ver detalles).
4. Elija Download router configuration (Descargar configuración del router).
5. En Download router configuration (Descargar configuración del router), haga lo siguiente:
    a. En Vendor (Proveedor), seleccione el fabricante del router.
    b. En Platform, seleccione el modelo del router.
    c. En Software, seleccione la versión de software del router.
6. Elija Download (Descargar) y, a continuación, utilice la configuración adecuada del router para garantizar de que puede conectarse a AWS Direct Connect.

Consideraciones de MACsec

Si necesita configurar de forma manual su enrutador para MACsec, utilice la siguiente tabla como guía.

Parámetro	Descripción
Longitud del CKN	Se trata de una cadena de 64 caracteres hexadecimales (0–9, A–E). Utilice la longitud completa para maximizar la compatibilidad multiplataforma.
Longitud de la CAK	Se trata de una cadena de 64 caracteres hexadecimales (0–9, A–E). Utilice la longitud completa para maximizar la compatibilidad multiplataforma.
Algoritmo criptográfico	AES_256_CMAC
Conjunto de cifrado de SAK	• Para conexiones de 100 Gbps: GCM_AES_XPN_256 • Para conexiones de 10 Gbps: GCM_AES_XPN_256 o GCM_AES _256
Conjunto de cifrado de claves	16
Desplazamiento de confidenc ialidad	0
Indicador de ICV	No
Tiempo de cambio de clave de SAK	Sustitución de PN>

Ver los detalles de la interfaz virtual

Puede consultar el estado actual de la interfaz virtual. Los detalles incluyen:

- Estado de la conexión
- Nombre
- Ubicación
- VLAN
- Detalles de BGP
- Direcciones IP de mismo nivel

Para ver los detalles de una interfaz virtual

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel izquierdo, elija Virtual Interfaces (Interfaces virtuales).
3. Seleccione la interfaz virtual y, a continuación, elija View details (Ver detalles).

Para describir interfaces virtuales mediante la línea de comandos o la API

- describe-virtual-interfaces (AWS CLI)
- DescribeVirtualInterfaces (AWS Direct Connect API)

Adición o eliminación de un BGP de mismo nivel

Añada o elimine una sesión de intercambio de tráfico BGP IPv4 o IPv6 a la interfaz virtual.

Una interfaz virtual puede ser compatible con una única sesión de intercambio de tráfico BGP IPv4 y con única sesión de intercambio de tráfico BGP IPv6.

No puede especificar sus propias direcciones IPv6 de mismo nivel para una sesión de intercambio de tráfico BGP IPv6. Amazon le asigna automáticamente una /125 CIDR IPv6.

No hay compatibilidad con el BGP multiprotocolo. IPv4 e IPv6 operan en modo de pila doble en la interfaz virtual.

AWS habilita MD5 de forma predeterminada. Esta opción no se puede modificar.

Agregar un BGP de mismo nivel

Utilice el siguiente procedimiento para añadir un BGP de mismo nivel.

Para añadir un BGP de mismo nivel

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Seleccione la interfaz virtual y, a continuación, elija View details (Ver detalles).
4. Elija Add peering (Añadir intercambio).
5. (Interfaz virtual privada) Para añadir BGP IPv4 del mismo nivel, haga lo siguiente:
   - Elija IPv4.
   - Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico. En IP de mismo nivel del enrutador de Amazon, ingrese la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.
6. (Interfaz virtual pública) Para añadir BGP IPv4 del mismo nivel, haga lo siguiente:
   - En Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que se debe enviar el tráfico.
   - En Amazon router peer IP (IP del mismo nivel del router de Amazon), escriba la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

   > **Important**
   >
   > Si permite la AWS asignación automática de direcciones IP, se asignará un CIDR /29 a partir de 169.254.0.0/16. AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen y destino del tráfico. En su lugar, debe utilizar la RFC 1918 u otro direccionamiento y especificar la dirección por su cuenta. Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.
7. (Interfaz virtual pública o privada) Para añadir BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignan automáticamente desde el grupo de direcciones IPv6 de Amazon; no puede especificar direcciones IPv6 personalizadas.
8. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

   En el caso de una interfaz virtual pública, el ASN debe ser privado o ya estar habilitado para la interfaz virtual.

Los valores válidos son 1-2.147.483.647.

Tenga en cuenta que si no ingresa un valor, le asignaremos uno de forma automática.

9. Para utilizar su propia clave de BGP, en BGP Authentication Key (Clave de autenticación de BGP), escriba su clave MD5 de BGP.
10. Elija Add peering (Añadir intercambio).

Para crear un BGP de mismo nivel mediante la línea de comandos o la API

- create-bgp-peer (AWS CLI)
- CreateBGPPeer (API)AWS Direct Connect

Eliminar un BGP de mismo nivel

Si la interfaz virtual tiene una sesión de intercambio de tráfico BGP IPv4 e IPv6, puede eliminar una de las sesiones de intercambio de tráfico BGP (pero no ambas).

Para eliminar un BGP de mismo nivel

1. Abra la consola en https://console.aws.amazon.com/directconnect/v2/home AWS Direct Connect.
2. En el panel de navegación, elija Virtual Interfaces.
3. Seleccione la interfaz virtual y, a continuación, elija View details (Ver detalles).
4. En Peerings (Intercambios), seleccione el intercambio que desea eliminar y, a continuación, elija Delete (Eliminar).
5. En el cuadro de diálogo Remove peering from virtual interface (Eliminar un intercambio de tráfico de la interfaz virtual), elija Delete (Eliminar).

Para eliminar un BGP de mismo nivel mediante la línea de comandos o la API

- delete-bgp-peer (AWS CLI)
- DeleteBGPPeer (API)AWS Direct Connect

Establecer la MTU de red para interfaces virtuales privadas o de tránsito

AWS Direct Connect admite un tamaño de trama Ethernet de 1522 o 9023 bytes (encabezado Ethernet de 14 bytes + etiqueta VLAN de 4 bytes + bytes para el datagrama IP + 4 bytes FCS) en la capa de enlace.

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 la conexión. La MTU de una interfaz virtual privada puede ser 1500 o 9001 (tramas gigantes). La MTU de una interfaz virtual de tránsito puede ser 1500 o 8500 (tramas gigantes). Puede especificar la MTU al crear la interfaz o actualizarla tras crearla. El establecimiento de la MTU de una interfaz virtual en 8500 (tramas gigantes) o 9001 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Jumbo Frame Capable en la pestaña Resumen.

Una vez que habilite tramas gigantes para su interfaz virtual privada o de tránsito, solo podrá asociarla con una conexión o LAG que sea compatible con tramas gigantes. Las tramas gigantes se admiten en una interfaz virtual privada asociada a una puerta de enlace privada virtual o de Direct Connect, o en una interfaz virtual de tránsito asociada a una puerta de enlace de Direct Connect. Si tiene dos interfaces virtuales privadas que anuncian la misma ruta, pero utilizan otros valores de MTU, o si tiene una Site-to-Site VPN que anuncia la misma ruta, se utilizará una MTU de 1500.

Important

Los marcos gigantes solo se aplicarán a las rutas propagadas AWS Direct Connect y a las rutas estáticas a través de pasarelas de tránsito. Las tramas gigantes de las puertas de enlace de tránsito solo admiten 8500 bytes.

Si una instancia de EC2 no admite tramas gigantes, elimina las tramas gigantes de Direct Connect. Todos los tipos de instancia EC2 admiten tramas gigantes salvo en el caso de C1, CC1, T1 y M1. Para obtener más información, consulte la Unidad de transmisión máxima de red (MTU) para su instancia EC2 en la Guía del usuario de Amazon EC2.

En el caso de las conexiones alojadas, las tramas gigantes solo se pueden habilitar si se habilitaron originalmente en la conexión principal alojada de Direct Connect. Si las tramas

gigantes no se encuentran habilitadas en esa conexión principal, no podrá habilitarlas en ninguna conexión.

Para establecer la MTU de una interfaz virtual privada

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Seleccione la interfaz virtual y, a continuación, elija Edit (Editar).
4. En Jumbo MTU (MTU size 9001) [MTU gigante (tamaño de MTU 9001)] o Jumbo MTU (MTU size 8500) [MTU gigante (tamaño de MTU 8500)], seleccione Enabled (Habilitada).
5. En Acknowledge (Confirmación), seleccione I understand the selected connection(s) will go down for a brief period (Entiendo que las conexiones seleccionadas dejarán de funcionar durante un breve periodo de tiempo). El estado de la interfaz virtual es `pending` hasta que se haya completado la actualización.

Para establecer la MTU de una interfaz virtual privada alojada mediante la línea de comandos o la API

- update-virtual-interface-attributes (AWS CLI)
- UpdateVirtualInterfaceAttributes(AWS Direct Connect API)

Agregar o eliminar etiquetas de interfaz virtual

Las etiquetas proporcionan un método para identificar la interfaz virtual. Puede agregar o eliminar una etiqueta si es el propietario de la cuenta de la interfaz virtual.

Para añadir o eliminar una etiqueta de interfaz virtual

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Seleccione la interfaz virtual y, a continuación, elija Edit (Editar).
4. Añada o elimine una etiqueta.

   [Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

- En Key (Clave), escriba el nombre de la clave.
- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

5. Elija Edit virtual interface (Editar interfaz virtual).

Para agregar y eliminar una etiqueta con la línea de comandos

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

Eliminar interfaces virtuales

Puede eliminar una o varias interfaces virtuales. Antes de poder eliminar una conexión, debe eliminar la interfaz virtual. Al eliminar una interfaz virtual, se detienen AWS Direct Connect los cargos de transferencia de datos asociados a la interfaz virtual.

Para eliminar una interfaz virtual

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel izquierdo, elija Virtual Interfaces (Interfaces virtuales).
3. Seleccione las interfaces virtuales y, a continuación, elija Delete (eliminar).
4. En el cuadro de diálogo Delete confirmation (Confirmación de eliminación), elija Delete (Eliminar).

Para eliminar una interfaz virtual mediante la línea de comandos o la API

- delete-virtual-interface (AWS CLI)
- DeleteVirtualInterfaz (AWS Direct Connect API)

Crear una interfaz virtual alojada

Puede crear una interfaz virtual alojada pública, de tránsito o privada. Antes de comenzar, asegúrese de que ha leído la información que aparece en Requisitos previos de las interfaces virtuales.

Crear una interfaz virtual privada alojada

Para crear una interfaz virtual privada alojada

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Tipo de interfaz virtual, en Tipo, elija Privada.
5. En Configuración de la interfaz virtual privada, realice lo siguiente:

   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

   c. En Propietario de la interfaz virtual, elija Otra cuenta de AWS y, a continuación, en Propietario de la interfaz virtual, ingrese el ID de la cuenta propietaria de esta interfaz virtual.

   d. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

   e. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

      Los valores válidos son 1-2.147.483.647.
6. En Additional Settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

      [IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
      - En IP de mismo nivel del enrutador de Amazon, ingrese la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

> **Important**
>
> Si permite la AWS asignación automática de direcciones IP, se asignará un CIDR /29 a partir de 169.254.0.0/16. AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen y destino del tráfico. En su lugar, debe utilizar el RFC 1918 u otro direccionamiento (que no sea el RFC 1918) y especificar la dirección usted mismo. Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.

[IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

b. Para cambiar la unidad de transmisión máxima (MTU) de 1500 (predeterminada) a 9001 (tramas gigantes), seleccione MTU gigante (tamaño de MTU 9001).

c. (Opcional) Añada o elimine una etiqueta.

[Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

- En Key (Clave), escriba el nombre de la clave.
- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

7. Una vez que el propietario de la otra cuenta de AWS haya aceptado la interfaz virtual alojada, puede descargar el archivo de configuración del enrutador.

Para crear una interfaz virtual privada alojada mediante la línea de comandos o la API

- allocate-private-virtual-interface (AWS CLI)
- AllocatePrivateVirtualInterface(API)AWS Direct Connect

Crear una interfaz virtual pública alojada

Para crear una interfaz virtual privada pública

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.

3. Elija Create virtual interface (Crear interfaz virtual).
4. En Virtual interface type (Tipo de interfaz virtual) en Type (Tipo), elija Public (Pública).
5. En Public Virtual Interface Settings (Configuración de la interfaz virtual pública), haga lo siguiente:

   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

   c. En Propietario de la interfaz virtual, elija Otra AWS cuenta y, a continuación, en Propietario de la interfaz virtual, introduzca el ID de la cuenta propietaria de esta interfaz virtual.

   d. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

   e. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

      Los valores válidos son 1-2.147.483.647.

6. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

   [IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

   - Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
   - En IP de mismo nivel del enrutador de Amazon, ingrese la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

   > **Important**
   >
   > Si permite la AWS asignación automática de direcciones IP, se asignará un CIDR /29 a partir de 169.254.0.0/16. AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen y destino del tráfico. En su lugar, debe utilizar la RFC 1918 u otro direccionamiento y especificar la dirección por su cuenta. Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.

[IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

7. Para anunciar prefijos para Amazon, en Prefixes you want to advertise (Prefijos que desea anunciar), escriba las direcciones CIDR IPv4 de destino (separadas por comas) a las que debe redirigirse el tráfico a través de la interfaz virtual.
8. Para proporcionar su propia clave para autenticar la sesión de BGP, en Additional Settings (Configuración adicional), para BGP authentication key (Clave de autenticación de BGP), introduzca la clave.

   Si no ingresa un valor, luego generamos una clave de BGP.
9. (Opcional) Añada o elimine una etiqueta.

   [Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

   - En Key (Clave), escriba el nombre de la clave.
   - En Valor, escriba el valor de la clave.

   [Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).
10. Elija Create virtual interface (Crear interfaz virtual).
11. Una vez que el propietario de la otra cuenta de AWS haya aceptado la interfaz virtual alojada, puede descargar el archivo de configuración del enrutador.

Para crear una interfaz virtual pública alojada mediante la línea de comandos o la API

- allocate-public-virtual-interface (AWS CLI)
- AllocatePublicVirtualInterface(AWS Direct Connect API)

Crear una interfaz virtual de tránsito alojada

Para crear una interfaz virtual de tránsito alojada

> **Important**
>
> Si asocia su puerta de enlace de tránsito a una o más puertas de enlace de Direct Connect, el número de sistema autónomo (ASN) que utilizan la puerta de enlace de tránsito y de

Direct Connect deben ser diferentes. Por ejemplo, si utiliza el ASN 64512 predeterminado tanto para la puerta de enlace de tránsito como para la de Direct Connect, la solicitud de asociación fallará.

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Virtual interface type (Tipo de interfaz virtual) en Type (Tipo), elija Transit (Tránsito).
5. En Transit virtual interface settings (Configuración de la interfaz virtual de tránsito), haga lo siguiente:

   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

   c. En Propietario de la interfaz virtual, elija Otra AWS cuenta y, a continuación, en Propietario de la interfaz virtual, introduzca el ID de la cuenta propietaria de esta interfaz virtual.

   d. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

   e. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

      Los valores válidos son 1-2.147.483.647.

6. En Additional Settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

      [IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
      - En IP de mismo nivel del enrutador de Amazon, ingrese la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

> **Important**
>
> Si permite la AWS asignación automática de direcciones IP, se asignará un CIDR /29 a partir de 169.254.0.0/16. AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen y destino del tráfico. En su lugar, debe utilizar la RFC 1918 u otro direccionamiento y especificar la dirección por su cuenta. Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.

[IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

b. Para cambiar la unidad de transmisión máxima (MTU) de 1500 (predeterminada) a 8500 (tramas gigantes), seleccione Jumbo MTU (MTU size 8500) [MTU gigante (tamaño de MTU 8500)].

c. [Opcional] Añada una etiqueta. Haga lo siguiente:

[Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

- En Key (Clave), escriba el nombre de la clave.
- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

7. Elija Create virtual interface (Crear interfaz virtual).
8. Una vez que el propietario de la otra cuenta de AWS haya aceptado la interfaz virtual alojada, puede descargar el archivo de configuración del enrutador.

Para crear una interfaz virtual de tránsito alojada mediante la línea de comandos o la API

- allocate-transit-virtual-interface (AWS CLI)
- AllocateTransitVirtualInterface(AWS Direct Connect API)

Aceptar una interfaz virtual alojada

Para poder empezar a usar una interfaz virtual alojada, debe aceptar la interfaz virtual. En una interfaz virtual privada, también debe tener una gateway privada virtual o de Direct Connect. En una interfaz virtual de tránsito, debe tener una gateway de Direct Connect o una gateway de tránsito existente.

Para aceptar una interfaz virtual alojada

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Seleccione la interfaz virtual y, a continuación, elija View details (Ver detalles).
4. Elija Aceptar.
5. Esto se aplica a las interfaces virtuales privadas y a las interfaces virtuales de tránsito.

   (Interfaz virtual de tránsito) En el cuadro de diálogo Accept virtual interface (Aceptar interfaz virtual), seleccione una gateway de Direct Connect y, a continuación, elija Accept virtual interface (Aceptar interfaz virtual).

   (Interfaz virtual privada) En el cuadro de diálogo Accept virtual interface (Aceptar interfaz virtual), seleccione una gateway privada virtual o de Direct Connect y, a continuación, elija Accept (Aceptar).
6. Una vez que acepte la interfaz virtual alojada, el propietario de la conexión de AWS Direct Connect puede descargar el archivo de configuración del router. La opción Download router configuration (Descargar configuración del router) no está disponible para la cuenta que acepta la interfaz virtual alojada.

Para aceptar una interfaz virtual privada alojada mediante la línea de comandos o la API

- confirm-private-virtual-interface (AWS CLI)
- ConfirmPrivateVirtualInterface(AWS Direct Connect API)

Para aceptar una interfaz virtual pública alojada mediante la línea de comandos o la API

- confirm-public-virtual-interface (AWS CLI)
- ConfirmPublicVirtualInterface(AWS Direct Connect API)

Para aceptar una interfaz virtual de tránsito alojada mediante la línea de comandos o la API

- confirm-transit-virtual-interface (AWS CLI)
- ConfirmTransitVirtualInterface(AWS Direct Connect API)

Migrar una interfaz virtual

Utilice este procedimiento cuando desee realizar cualquiera de las siguientes operaciones de migración de interfaz virtual:

- Migrar una interfaz virtual existente asociada con una conexión a otro LAG.
- Migrar una interfaz virtual existente asociada con un LAG existente a un LAG nuevo.
- Migrar una interfaz virtual existente asociada con una conexión a otra conexión.

> **Note**
>
> - Puede migrar una interfaz virtual a una conexión nueva dentro de la misma región, pero no puede migrarla de una región a otra. Al migrar o asociar una interfaz virtual existente a una conexión nueva, los parámetros de configuración asociados con esas interfaces virtuales son los mismos. Para solucionar este problema, puede preparar la configuración en la conexión y, a continuación, actualizar la configuración de BGP.
> - No puede migrar una VIF de una conexión alojada a otra conexión alojada. Los ID de VLAN son únicos; por lo tanto, si se migra una VIF de esta manera, las VLAN no coinciden. Es necesario eliminar la conexión o la VIF y, a continuación, volver a crearla mediante una VLAN que sea igual para la conexión y la VIF.

> **Important**
>
> La interfaz virtual estará inactiva durante un periodo breve. Le recomendamos que realice este procedimiento durante un periodo de mantenimiento.

Para migrar una interfaz virtual

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.

2. En el panel de navegación, elija Virtual Interfaces.
3. Seleccione la interfaz virtual y, a continuación, elija Edit (Editar).
4. En Connection (Conexión), seleccione el LAG o la conexión.
5. Elija Edit virtual interface (Editar interfaz virtual).

Para migrar una interfaz virtual mediante la línea de comandos o la API

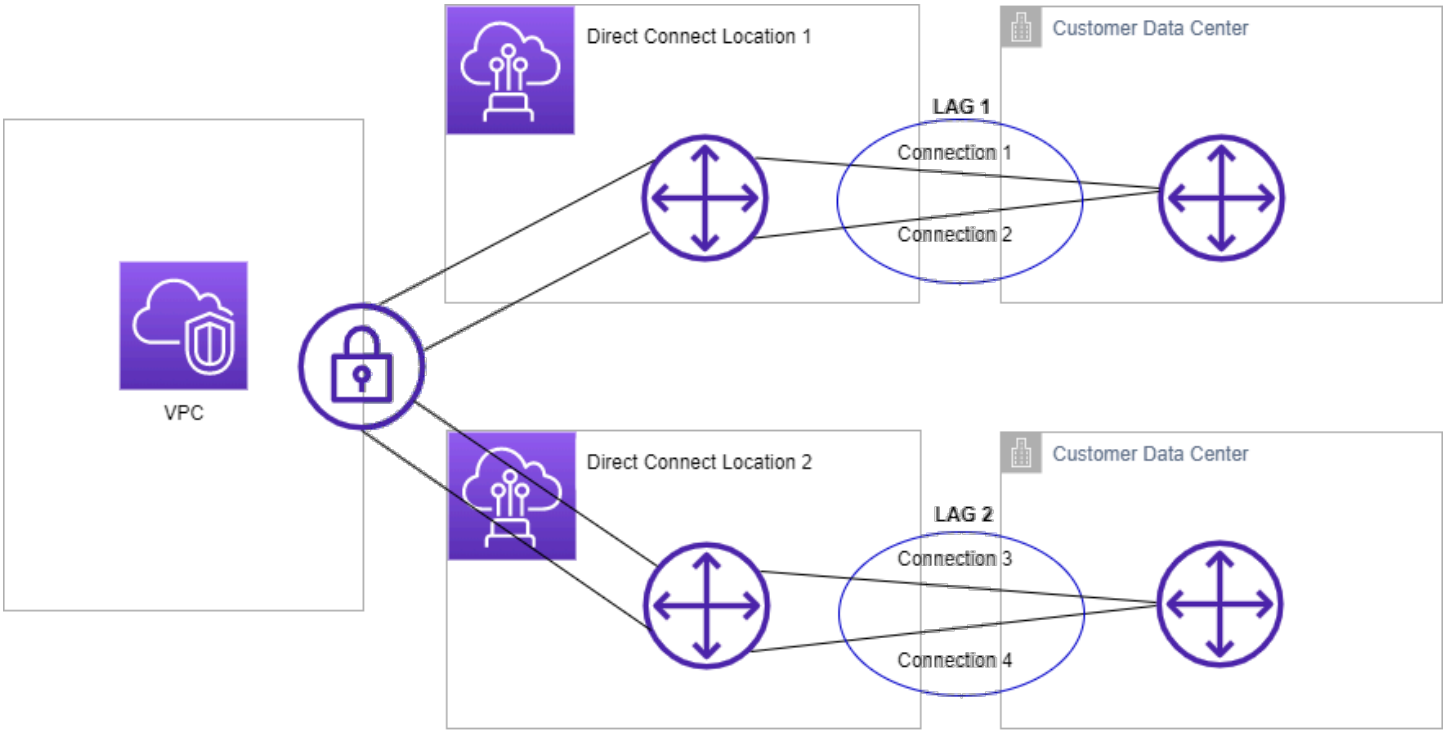
- associate-virtual-interface (AWS CLI)
- AssociateVirtualInterfaz (AWS Direct Connect API)

Grupos de agregación de enlaces (LAG)

Puede utilizar varias conexiones para aumentar el ancho de banda disponible. Un grupo de agregación de enlaces (LAG) es una interfaz lógica que utiliza el Protocolo de control de adición de enlaces (LACP) para agregar varias conexiones a un único punto de enlace de AWS Direct Connect, lo que permite tratarlos como una única conexión gestionada. Los LAG optimizan la configuración porque la configuración de LAG se aplica a todas las conexiones del grupo.

> **Note**
>
> El LAG multichasis (MLAG) no es compatible con AWS.

En el siguiente diagrama, tiene cuatro conexiones, con dos conexiones a cada ubicación. Puede crear un LAG para las conexiones que terminen en el mismo AWS dispositivo y en la misma ubicación y, a continuación, usar los dos LAG en lugar de las cuatro conexiones para la configuración y la administración.



Puede crear un LAG desde las conexiones existentes o puede aprovisionar nuevas conexiones. Una vez que haya creado el LAG, puede asociar las conexiones existentes (ya sea de forma independiente como parte de otro LAG) al LAG.

Se aplican las siguientes reglas:

- Todas las conexiones deben ser conexiones dedicadas y tener una velocidad de puerto de 1 Gbps, 10 Gbps o 100 Gbps.
- Todas las conexiones del LAG deben utilizar el mismo ancho de banda.
- Puede tener un máximo de dos conexiones de 100 G o cuatro conexiones con una velocidad de puerto inferior a 100 G en un LAG. Cada conexión del LAG cuenta para el límite de conexión global de la región.
- Todas las conexiones del LAG deben terminar en el mismo punto de enlace de AWS Direct Connect.
- Los LAG son compatibles con todos los tipos de interfaces virtuales: públicas, privadas y de tránsito.

Al crear un LAG, puede descargar de forma individual desde la consola la Carta de autorización y Asignación de instalaciones de conexión (LOA-CFA) de cada nueva conexión física de AWS Direct Connect. Para obtener más información, consulte Descargar la LOA-CFA.

Todos los LAG tienen un atributo que determina el número mínimo de conexiones del LAG que deben estar operativas para que el LAG funcione. De forma predeterminada, los LAG nuevos tienen este atributo establecido en 0. Puede actualizar el LAG para especificar un valor diferente, pero si lo hace, el LAG completo dejará de funcionar si el número de conexiones operativas es inferior a este umbral. Este atributo se puede utilizar para evitar la utilización excesiva de las otras conexiones.

Todas las conexiones de un LAG deben funcionar en modo Active/Activo.

> **Note**
>
> Al crear un LAG, o al asociarle más conexiones, es posible que no podamos garantizar puertos disponibles suficientes en un determinado punto de enlace de AWS Direct Connect.

Consideraciones de MACsec

Tenga en cuenta lo siguiente cuando desee configurar MACsec en los LAG:

- Al crear un LAG a partir de conexiones existentes, desasociamos todas las claves de MACsec de las conexiones. Luego, agregamos las conexiones al LAG y asociamos la clave de MACsec del LAG a las conexiones.

- Al asociar una conexión existente a un LAG, las claves de MACsec que se encuentran asociadas actualmente al LAG se asocian a la conexión. Por lo tanto, desasociamos las claves de MACsec de la conexión, agregamos la conexión al LAG y, a continuación, asociamos la clave de MACsec del LAG a la conexión.

Crear un LAG

Puede crear un LAG aprovisionando nuevas conexiones o añadiendo conexiones existentes.

No puede crear un LAG con conexiones nuevas si esto hace que supere el límite de conexiones global de la región.

Para crear un LAG desde conexiones existentes, las conexiones deben estar en el mismo dispositivo de AWS (deben finalizar en el mismo punto de conexión de AWS Direct Connect). También deben utilizar el mismo ancho de banda. No puede migrar una conexión desde un LAG existente si el hecho de eliminar la conexión provoca que el número mínimo de conexiones operativas del LAG caiga por debajo del umbral establecido.

> **Important**
>
> En el caso de las conexiones existentes, la conectividad a AWS se interrumpe durante la creación del LAG.

Create a LAG with new connections using the console

Para crear un LAG con nuevas conexiones

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija LAGs (LAG).
3. Seleccione Create LAG (Crear LAG).
4. En Lag creation type (Tipo de creación de LAG), elija Request new connections (Solicitar conexiones nuevas) y proporcione la información siguiente:
   - LAG Name (Nombre del LAG): un nombre para el LAG.
   - Location (Ubicación): la ubicación del LAG.
   - Port speed (Velocidad del puerto): la velocidad del puerto para las conexiones.

- Number of new connections (Número de conexiones nuevas): el número de conexiones nuevas que se van a crear. Puede tener un máximo de cuatro conexiones cuando la velocidad del puerto es de 1 G o 10 G, o dos cuando la velocidad del puerto es de 100 G.
- (Opcional) Configure la seguridad de MAC (MACsec) para la conexión. En Configuración adicional, seleccione Solicitar un puerto compatible con MACsec.

  MACsec solo se encuentra disponible en conexiones dedicadas.
- (Opcional) Añada o elimine una etiqueta.

  [Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:
  - En Key (Clave), escriba el nombre de la clave.
  - En Valor, escriba el valor de la clave.

  [Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

5. Seleccione Create LAG (Crear LAG).

Create a LAG with existing connections using the console

Para crear un LAG desde conexiones existentes

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija LAGs (LAG).
3. Seleccione Create LAG (Crear LAG).
4. En Lag creation type (Tipo de creación de LAG), elija Use existing connections (Usar conexiones existentes) y proporcione la información siguiente:
   - LAG Name (Nombre del LAG): un nombre para el LAG.
   - Conexión existente: la conexión de Direct Connect que se va a utilizar para el LAG.
   - (Opcional) Número de conexiones nuevas: el número de conexiones nuevas que se van a crear. Puede tener un máximo de cuatro conexiones cuando la velocidad del puerto es de 1 G o 10 G, o dos cuando la velocidad del puerto es de 100 G.
   - Minimum links (Mínimo de enlaces): el número mínimo de conexiones que deben estar operativas para que el LAG funcione. Si no especifica un valor, se asignará el valor predeterminado (0).
5. (Opcional) Añada o elimine una etiqueta.

[Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

- En Key (Clave), escriba el nombre de la clave.
- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

6. Seleccione Create LAG (Crear LAG).

Command line

Para crear un LAG mediante la línea de comandos o la API

- create-lag (AWS CLI)
- CreateLag(AWS Direct ConnectAPI)

Para describir los LAG mediante la línea de comandos o la API

- describe-lags (AWS CLI)
- DescribeLags(AWS Direct ConnectAPI)

Para descargar el documento LOA-CFA mediante la línea de comandos o la API

- describe-loa (AWS CLI)
- DescribeLoa(AWS Direct ConnectAPI)

Una vez que crea un LAG, puede asociar o desasociar conexiones. Para obtener más información, consulte Asociar una conexión a un LAG y Desasociar una conexión de un LAG.

Ver los detalles del LAG

Una vez que crea un LAG, puede ver sus detalles.

Console

Para ver la información de los LAG

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija LAGs (LAG).
3. Seleccione el LAG y elija View details (Ver detalles).
4. Puede ver información sobre el LAG, incluido su ID y el punto de conexión de AWS Direct Connect en el que terminan las conexiones.

Command line

Para ver información sobre su LAG con la línea de comandos o la API

- describe-lags (AWS CLI)
- DescribeLags(AWS Direct ConnectAPI)

Actualizar un LAG

Puede actualizar los siguientes atributos del grupo de agregación de enlaces (LAG):

- El nombre del LAG.
- El valor del número mínimo de conexiones que deben estar operativas para que el LAG funcione.
- El modo de cifrado de MACsec del LAG.

  MACsec solo se encuentra disponible en conexiones dedicadas.

  AWS asigna este valor a cada conexión que forma parte del LAG.

  Los valores válidos son:

  - `should_encrypt`
  - `must_encrypt`

    Al establecer el modo de cifrado en este valor, las conexiones se desactivan cuando el cifrado se encuentra inactivo.
  - `no_encrypt`

- Las etiquetas.

> **Note**
>
> Si ajusta el umbral del número mínimo de conexiones operativas, asegúrese de que el nuevo valor no provoque que el LAG caiga por debajo del umbral y deje de funcionar.

Console

Para actualizar un LAG

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija LAGs (LAG).
3. Seleccione el LAG y, a continuación, elija Editar.
4. Modifique el LAG.

   [Cambiar el nombre] En LAG Name (Nombre del LAG), escriba un nombre nuevo para el LAG.

   [Ajustar el número mínimo de conexiones] En Mínimo de enlaces, ingrese el número mínimo de conexiones operativas.

   [Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

   - En Key (Clave), escriba el nombre de la clave.
   - En Valor, escriba el valor de la clave.

   [Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).
5. Elija Edit LAG (Editar LAG).

Command line

Para actualizar un LAG mediante la línea de comandos o la API

- update-lag (AWS CLI)
- UpdateLag(AWS Direct ConnectAPI)

Para agregar y eliminar una etiqueta con la línea de comandos

- tag-resource (AWS CLI)
- untag-resource (AWS CLI)

Asociar una conexión a un LAG

Puede asociar una conexión existente a un LAG. La conexión puede ser independiente o puede ser parte de otro LAG. La conexión debe estar en el mismo dispositivo de AWS y utilizar el mismo ancho de banda que el LAG. Si la conexión ya está asociada a otro LAG, no puede volver a asociarla si el hecho de eliminar la conexión provoca que el número mínimo de conexiones operativas del LAG caiga por debajo del umbral establecido.

La asociación de una conexión con un nuevo LAG automáticamente vuelve a asociar sus interfaces virtuales al LAG.

> **Important**
>
> La conectividad a AWS a través de la conexión se interrumpe durante la asociación.

Console

Para asociar una conexión a un LAG

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija LAGs (LAG).
3. Seleccione el LAG y, a continuación, elija Ver detalles.
4. En Connections (Conexiones), elija Associate connection (Asociar conexión).
5. En Connection (Conexión), elija la conexión de Direct Connect que se va a utilizar para el LAG.
6. Elija Associate Connection (Asociar conexión).

Command line

Para asociar una conexión mediante la línea de comandos o la API

- associate-connection-with-lag (AWS CLI)
- AssociateConnectionWithLag(AWS Direct ConnectAPI)

Desasociar una conexión de un LAG

Convierta una conexión en independiente separándola de un LAG. No puede desasociar una conexión si al hacerlo provoca que el número mínimo de conexiones operativas del LAG caiga por debajo del umbral establecido.

Desasociar una conexión de un LAG no anula automáticamente las interfaces virtuales.

> **Important**
>
> Su conexión a AWS se interrumpe durante la desasociación.

Console

Para desasociar una conexión de un LAG

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel izquierdo, elija LAGs.
3. Seleccione el LAG y, a continuación, elija Ver detalles.
4. En Connections (Conexiones), seleccione la conexión en la lista de conexiones disponibles y elija Disassociate (Desasociar).
5. En el cuadro de diálogo de confirmación, elija Desasociar.

Command line

Para desasociar una conexión mediante la línea de comandos o la API

- disassociate-connection-from-lag (AWS CLI)

- DisassociateConnectionFromLag(AWS Direct ConnectAPI)

Asociar un par de CKN/CAK de MACsec a un LAG

Después de crear el LAG compatible con MACsec, puede asociar un par de CKN/CAK a la conexión.

> **Note**
>
> No puede modificar una clave secreta de MACsec después de asociarla a un LAG. Si necesita modificar la clave, desasocie la clave de la conexión y, a continuación, asocie una clave nueva a la conexión. Para obtener información sobre cómo quitar una asociación, consulte the section called “Eliminar la asociación entre una clave secreta de MACsec y un LAG”.

Console

Para asociar una clave de MACsec a un LAG

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija LAGs (LAG).
3. Seleccione el LAG y elija View details (Ver detalles).
4. Elija Asociar clave.
5. Ingrese la clave de MACsec.

   [Utilizar el par de CAK/CKN] Elija el Par de claves y, a continuación, realice lo siguiente:

   - En Clave de asociación de conectividad (CAK), ingrese la CAK.
   - En Nombre de clave de asociación de conectividad (CKN), ingrese el CKN.

   [Utilizar el secreto] Elija Secreto de Secrets Manager existente y, a continuación, en Secreto, seleccione la clave secreta de MACsec.
6. Elija Asociar clave.

Command line

Para asociar una clave de MACsec a un LAG

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey(AWS Direct ConnectAPI)

Eliminar la asociación entre una clave secreta de MACsec y un LAG

Puede eliminar la asociación entre el LAG y la clave de MACsec.

Console

Para eliminar una asociación entre un LAG y una clave de MACsec

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija LAGs (LAG).
3. Seleccione el LAG y elija View details (Ver detalles).
4. Seleccione el secreto de MACsec que desee eliminar y, a continuación, elija Desasociar clave.
5. En el cuadro de diálogo de confirmación, ingrese disociar y, a continuación, elija Desasociar.

Command line

Para eliminar una asociación entre un LAG y una clave de MACsec

- disassociate-mac-sec-key (AWS CLI)
- DisassociateMacSecKey(AWS Direct ConnectAPI)

Eliminar LAG

Puede eliminar los LAG que no necesite. No puede eliminar un LAG si tiene interfaces virtuales asociadas. Primero debe eliminar las interfaces virtuales o asociarlas a otro LAG u otra conexión.

Eliminar un LAG no elimina las conexiones del LAG; debe eliminar las conexiones usted mismo. Para obtener más información, consulte Eliminar conexiones.

Console

Para eliminar un LAG

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija LAGs (LAG).
3. Seleccione los LAG y, a continuación, elija Eliminar.
4. En el cuadro de diálogo de confirmación, elija Eliminar.

Command line

Para eliminar un LAG mediante la línea de comandos o la API

- delete-lag (AWS CLI)
- DeleteLag(AWS Direct ConnectAPI)

Uso de puertas de enlace de Direct Connect

Puede trabajar con AWS Direct Connect puertas de enlace mediante la consola de Amazon VPC o la. AWS CLI

Contenidos

Gateways de Direct Connect

Utilice la AWS Direct Connect puerta de enlace para conectar sus VPC. Puede asociar una puerta de enlace de AWS Direct Connect con cualquiera de las siguientes puertas de enlace:

- Una puerta de enlace de tránsito cuando tiene varias VPC en la misma región
- Una gateway privada virtual

También puede utilizar una puerta de enlace privada virtual para ampliar su zona local. Esta configuración permite que la VPC asociada con la zona local se conecte a una puerta de enlace de Direct Connect. La puerta de enlace de Direct Connect se conecta a una ubicación de Direct Connect en una región. El centro de datos en las instalaciones tiene una conexión de Direct Connect con la ubicación de Direct Connect. Para obtener más información, consulte Acceso a las zonas locales mediante una puerta de enlace de Direct Connect en la Guía del usuario de Amazon VPC.

Una gateway de Direct Connect es un recurso disponible en todo el mundo. Puede conectarse a cualquier región del mundo mediante una puerta de enlace de Direct Connect. Esto incluye AWS GovCloud (US) , pero no incluye, las regiones de AWS China.

Los clientes que utilicen Direct Connect con las VPC que actualmente omitan una zona de disponibilidad principal no podrán migrar sus conexiones de Direct Connect ni sus interfaces virtuales.

A continuación se describen escenarios en los que puede utilizar una puerta de enlace de Direct Connect.

Una gateway de Direct Connect no permite que las asociaciones de gateway que se encuentran en la misma gateway de Direct Connect se envíen tráfico entre sí (por ejemplo, una gateway privada virtual a otra gateway privada virtual). Una excepción a esta regla, implementada en noviembre de 2021, es cuando se anuncia una superred en dos o más VPC, que tienen sus puertas de enlace privadas virtuales (VGW) asociadas a la misma puerta de enlace de Direct Connect y en la misma interfaz virtual. En este caso, las VPC pueden comunicarse entre sí a través del punto de conexión de Direct Connect. Por ejemplo, si anuncia una superred (por ejemplo, 10.0.0.0/8 o 0.0.0.0/0) que se superpone con las VPC conectadas a una puerta de enlace de Direct Connect (por ejemplo, 10.0.0.0/24 y 10.0.1.0/24) y, en la misma interfaz virtual, desde la red en las instalaciones, las VPC se pueden comunicar entre sí.

Si desea bloquear la comunicación de VPC a VPC dentro de una puerta de enlace de Direct Connect, realice lo siguiente:

1. Configure grupos de seguridad en las instancias y otros recursos de la VPC para bloquear el tráfico entre las VPC; utilícelos también como parte del grupo de seguridad predeterminado de la VPC.
2. Evite anunciar una superred desde su red en las instalaciones que se superponga con sus VPC. En su lugar, puede anunciar rutas más específicas desde su red en las instalaciones que no se superpongan con sus VPC.
3. Aprovisione una sola puerta de enlace de Direct Connect para cada VPC que desee conectar a la red en las instalaciones en lugar de utilizar la misma puerta de enlace de Direct Connect para varias VPC. Por ejemplo, en lugar de utilizar una sola puerta de enlace de Direct Connect para las VPC de desarrollo y producción, utilice puertas de enlace de Direct Connect independientes para cada una de estas VPC.

Una puerta de enlace de Direct Connect no impide que el tráfico se envíe desde una asociación de puerta de enlace a la propia asociación de puerta de enlace (por ejemplo, cuando tiene una ruta de superred en las instalaciones que contiene los prefijos de la asociación de puerta de enlace). Si tiene una configuración con varias VPC conectadas a puertas de enlace de tránsito asociadas a la misma puerta de enlace de Direct Connect, las VPC podrían comunicarse. Para evitar que las VPC se comuniquen, asocie una tabla de enrutamiento a los adjuntos de la VPC que tengan configurada la opción Blackhole.

A continuación se describen escenarios en los que puede utilizar una puerta de enlace de Direct Connect.

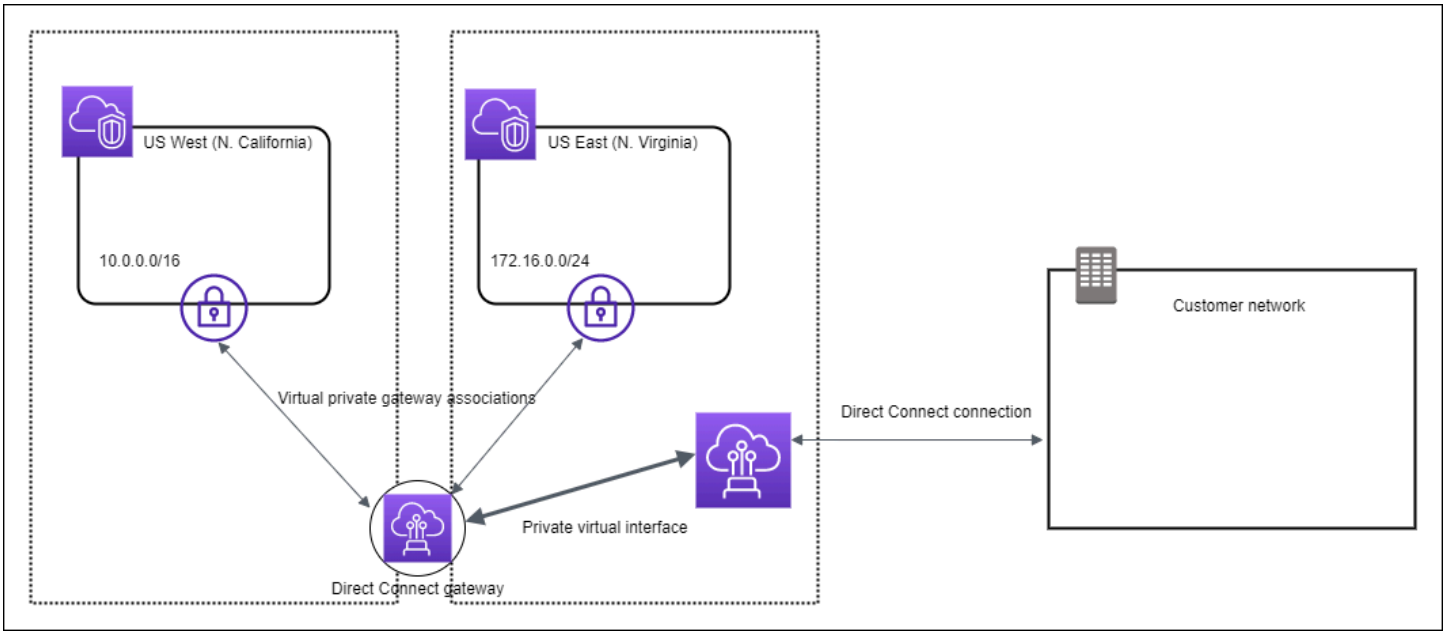
Escenarios

- Asociaciones de la gateway privada virtual
- Asociaciones de gateways privadas virtuales entre cuentas
- Asociaciones de la puerta de enlace de tránsito
- Asociaciones de gateways de tránsito entre cuentas
- Creación de una gateway de Direct Connect
- Eliminación de gateways de Direct Connect
- Migración desde una gateway privada virtual a una gateway de Direct Connect

Asociaciones de la gateway privada virtual

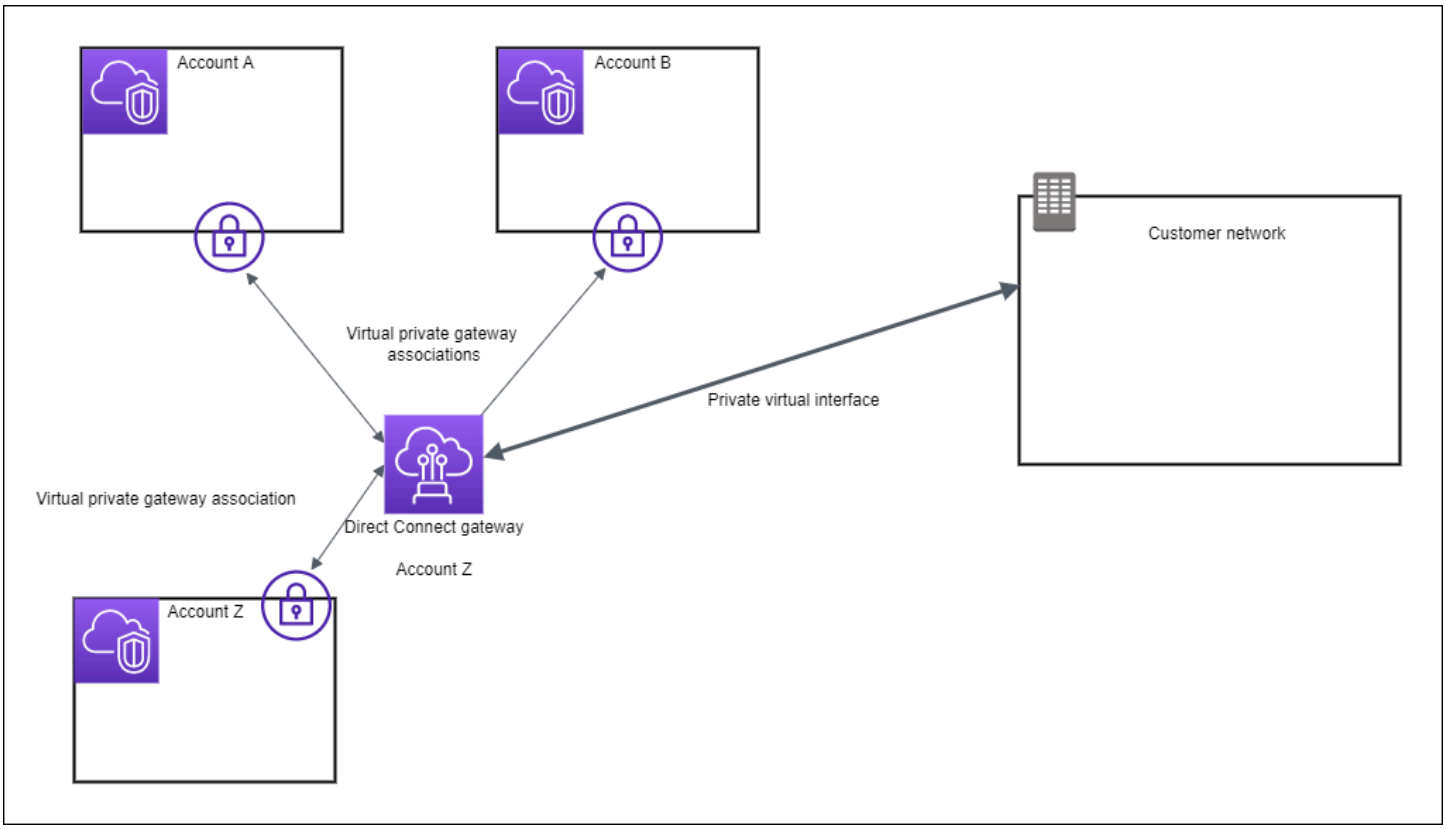
En el siguiente diagrama, la puerta de enlace de Direct Connect lo habilita para utilizar su conexión de AWS Direct Connect en la región Este de EE. UU. (Norte de Virginia) para acceder a las VPC de su cuenta en las regiones Este de EE. UU. (Norte de Virginia) y Oeste de EE. UU. (Norte de California).

Cada VPC tiene una puerta de enlace privada virtual que se conecta a la puerta de enlace de Direct Connect mediante una asociación de puerta de enlace privada virtual. La puerta de enlace Direct Connect utiliza una interfaz virtual privada para la conexión a la AWS Direct Connect ubicación. Hay una conexión de AWS Direct Connect desde la ubicación hasta el centro de datos del cliente.



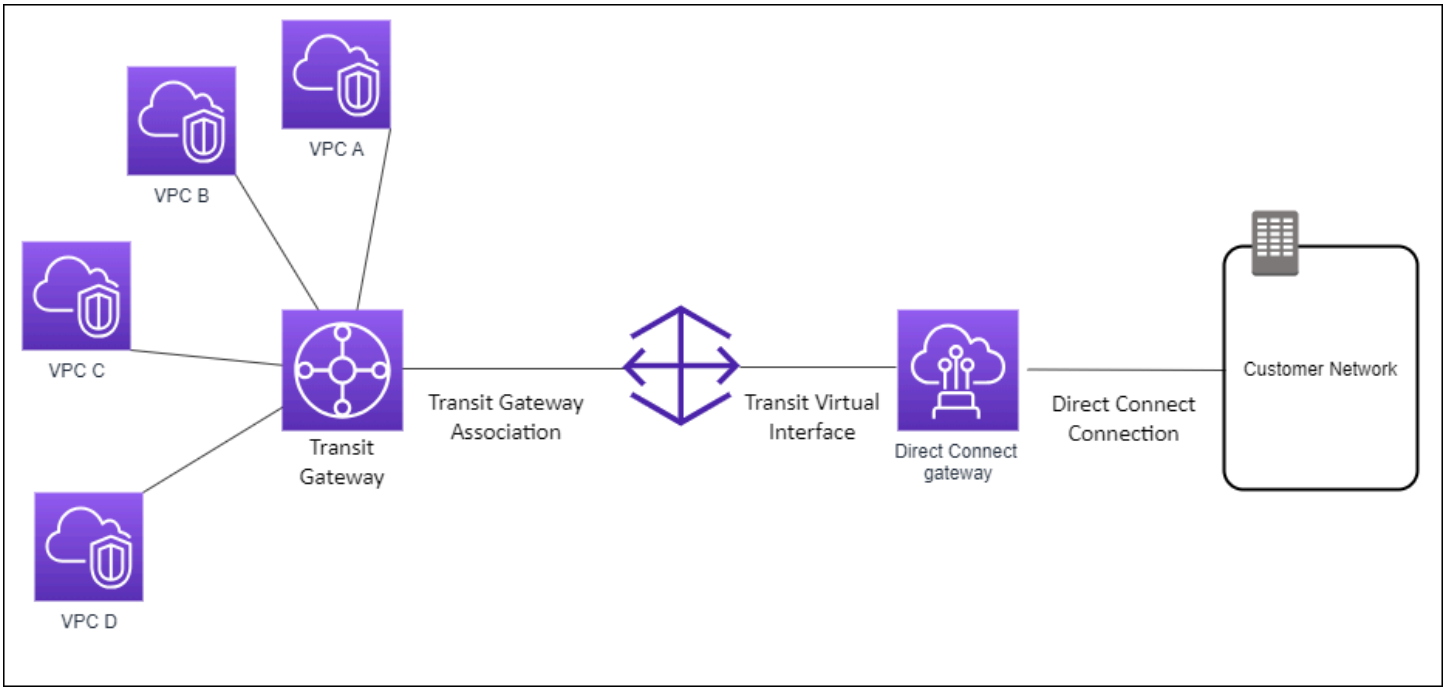
Asociaciones de gateways privadas virtuales entre cuentas

Considere este escenario en el que el propietario de una gateway de Direct Connect es la cuenta Z (account Z). Las cuentas A y B desean utilizar la gateway de Direct Connect. Las cuentas A y B envían sus respectivas propuestas de asociación a la cuenta Z. La cuenta Z acepta las propuestas de asociación y, si lo desea, puede actualizar los prefijos permitidos desde la gateway privada virtual de la cuenta A o desde la gateway privada virtual de la cuenta B. Cuando la cuenta Z acepta las propuestas, la cuenta A y la cuenta B pueden dirigir tráfico desde su gateway privada virtual a la gateway de Direct Connect. La cuenta Z también es propietaria del direccionamiento a los clientes, ya que la cuenta Z es la propietaria de la gateway.



Asociaciones de la puerta de enlace de tránsito

El siguiente diagrama muestra cómo le permite la gateway de Direct Connect crear una única conexión con su conexión de Direct Connect que todas las VPC pueden utilizar.



La solución implica los siguientes componentes:

- Una puerta de enlace de tránsito que tiene asociaciones de VPC.
- Una gateway de Direct Connect.
- Una asociación entre la gateway de Direct Connect y la gateway de tránsito.
- Una interfaz virtual de tránsito vinculada a la gateway de Direct Connect.

Esta configuración ofrece los siguientes beneficios. Puede hacer lo siguiente:

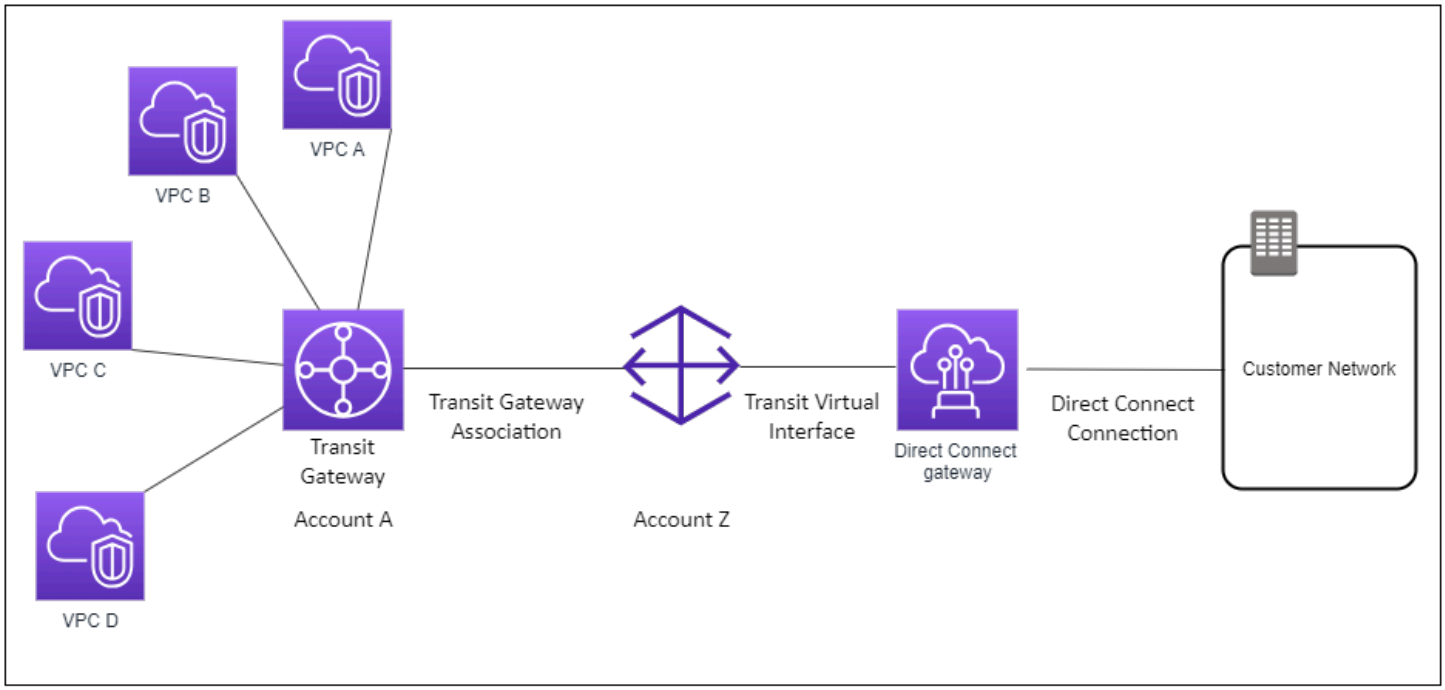
- Administrar una única conexión para las distintas VPC o VPN que haya en la misma región.
- Anuncie los prefijos desde las instalaciones locales hacia AWS y desde AWS las instalaciones locales.

Para obtener información sobre la configuración de puertas de enlace de tránsito, consulte Trabajo con puertas de enlace de tránsito en la Guía de puertas de enlace de tránsito de Amazon VPC.

Asociaciones de gateways de tránsito entre cuentas

Considere este escenario en el que el propietario de una gateway de Direct Connect es la cuenta Z (account Z). La cuenta A posee la puerta de enlace de tránsito y desea utilizar la puerta de enlace de Direct Connect. La cuenta Z acepta las propuestas de asociación y puede actualizar de forma

opcional los prefijos permitidos de la puerta de enlace de tránsito de la cuenta A. Después de que la cuenta Z acepte las propuestas, las VPC adjuntas a la puerta de enlace de tránsito pueden dirigir el tráfico desde la puerta de enlace de tránsito hasta la puerta de enlace de Direct Connect. La cuenta Z también es propietaria del direccionamiento a los clientes, ya que la cuenta Z es la propietaria de la gateway.



Contenidos

Creación de una gateway de Direct Connect

Puede crear una puerta de enlace de Direct Connect en cualquier región compatible.

Para crear una gateway de Direct Connect

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Direct Connect Gateways.
3. Elija Create Direct Connect gateway (Crear gateway de Direct Connect).

4. Especifique la información siguiente y elija Create Direct Connect gateway (Crear gateway de Direct Connect).

   - Name (Nombre): escriba un nombre que le ayude a identificar la gateway de Direct Connect.
   - Amazon side ASN (ASN del lado de Amazon): especifique el ASN del lado de Amazon de la sesión de BGP. El ASN debe estar comprendido entre 64 512 y 65 534 o entre 4 200 000 000 y 4 294 967 294.
   - Virtual private gateway (Gateway privada virtual): para asociar una gateway privada virtual, elija la gateway privada virtual.

Para crear una gateway de Direct Connect mediante la línea de comando o API

- create-direct-connect-gateway (AWS CLI)
- CreateDirectConnectGateway(AWS Direct Connect API)

Eliminación de gateways de Direct Connect

Si ya no necesita una gateway de Direct Connect, puede eliminarla. En primer lugar, debe desasociar todas las gateways privadas virtuales asociadas y eliminar la interfaz virtual privada adjunta.

Para eliminar una gateway de Direct Connect

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Direct Connect Gateways.
3. Seleccione las gateways y elija Delete (Eliminar).

Para eliminar una gateway de Direct Connect mediante la línea de comandos o la API

- delete-direct-connect-gateway (AWS CLI)
- DeleteDirectConnectGateway(AWS Direct Connect API)

Migración desde una gateway privada virtual a una gateway de Direct Connect

Si tenía una gateway privada virtual asociada a una interfaz virtual y desea migrar a una gateway de Direct Connect, siga estos pasos:

Para migrar a una gateway de Direct Connect

1. Cree una gateway de Direct Connect. Para obtener más información, consulte the section called “Creación de una gateway de Direct Connect”.
2. Cree una interfaz virtual para la gateway de Direct Connect. Para obtener más información, consulte the section called “Crear una interfaz virtual”.
3. Asocie cada gateway privada virtual con la gateway de Direct Connect. Para obtener más información, consulte the section called “Asociación y disociación de gateways privadas virtuales”.
4. Elimine la interfaz virtual que estaba asociada a la gateway privada virtual. Para obtener más información, consulte the section called “Eliminar interfaces virtuales”.

Asociaciones de la gateway privada virtual

Puede utilizar una gateway de AWS Direct Connect para establecer la conexión de AWS Direct Connect a través de una interfaz virtual privada con una o varias VPC de su cuenta que se encuentren en la misma región o en regiones diferentes. Asocia una gateway de Direct Connect con la gateway privada virtual de la VPC. A continuación, crea una interfaz virtual privada para la AWS Direct Connect conexión a la puerta de enlace Direct Connect. Puede adjuntar varias interfaces virtuales privadas a su gateway de Direct Connect.

Las siguientes reglas se aplican a las asociaciones de puerta de enlace privada virtual:

- No habilite la propagación de rutas hasta que haya asociado una puerta de enlace virtual a una puerta de enlace de Direct Connect. Si habilita la propagación de rutas antes de asociar las puertas de enlace, es posible que las rutas se propaguen incorrectamente.
- Existen límites para la creación y el uso de gateways de Direct Connect. Para obtener más información, consulte Cuotas.
- No puede adjuntar una puerta de enlace de Direct Connect en una puerta de enlace privada virtual cuando la puerta de enlace de Direct Connect ya se encuentra asociada a una puerta de enlace de tránsito.
- La VPC a la que se conecte mediante una gateway de Direct Connect no puede tener bloques de CIDR solapados. Si agrega un bloque de CIDR IPv4 a una VPC que está asociada a la gateway de Direct Connect, asegúrese de que el bloque de CIDR no se solape con un bloque de CIDR existente de cualquier otra VPC asociada. Para obtener más información, consulte Agregar bloques de CIDR IPv4 a una VPCen la Guía del usuario de Amazon VPC.

- No se puede crear una interfaz virtual pública a una gateway de Direct Connect.
- Una puerta de enlace de Direct Connect solo admite la comunicación entre interfaces virtuales privadas adjuntas y puertas de enlace privadas virtuales asociadas; puede habilitar una puerta de enlace privada virtual a otra puerta de enlace privada. No se admiten los siguientes flujos de tráfico:
  - Comunicación directa entre las VPC que están asociadas con una sola gateway de Direct Connect. Esto incluye el tráfico desde una VPC a otra mediante un enganche mediante una red en las instalaciones a través de una única puerta de enlace de Direct Connect.
  - Comunicación directa entre las interfaces virtuales que están asociadas a la gateway única de Direct Connect.
  - Comunicación directa entre las interfaces virtuales asociadas a una gateway única de Direct Connect y una conexión de VPN en una gateway privada virtual que está asociada con la misma gateway de Direct Connect.
- No se puede asociar una gateway privada virtual con más de una gateway de Direct Connect ni tampoco se puede adjuntar una interfaz virtual privada a más de una gateway de Direct Connect.
- Una gateway privada virtual que se asocia con una gateway de Direct Connect se debe adjuntar a una VPC.
- Una propuesta de asociación de gateways privadas virtuales caduca 7 días después de crearla.
- Una propuesta de gateway privada virtual aceptada o eliminada permanece visible durante 3 días.
- Una gateway privada virtual se puede asociar a una gateway de Direct Connect y también se puede asociar a una interfaz virtual.
- Al separar una puerta de enlace privada virtual de una VPC también se desasocia la puerta de enlace privada virtual de una puerta de enlace de Direct Connect.

Para conectar su AWS Direct Connect conexión a una VPC de la misma región únicamente, puede crear una puerta de enlace Direct Connect. O bien, puede crear una interfaz virtual privada y asociarla a la gateway privada virtual para la VPC. Para obtener más información, consulte Crear una interfaz virtual privada una VPN CloudHub.

Para usar la AWS Direct Connect conexión con una VPC en otra cuenta, puede crear una interfaz virtual privada alojada para esa cuenta. Cuando el propietario de la otra cuenta acepte la interfaz virtual alojada, puede optar por asociarla a una gateway privada virtual o a una gateway de Direct Connect de su cuenta. Para obtener más información, consulte AWS Direct Connect interfaces virtuales.

Contenidos

Creación de una puerta de enlace privada virtual

La gateway privada virtual se debe adjuntar a la VPC a la que desea conectarse.

> **Note**
>
> Si tiene previsto utilizar la gateway privada virtual para una gateway de Direct Connect y una conexión de VPN dinámica, defina el ASN de la gateway privada virtual en el valor que necesite para la conexión de VPN. De lo contrario, el ASN de la gateway privada virtual se puede configurar en cualquier valor admitido. La gateway de Direct Connect anuncia todas las VPC conectadas a través del ASN que tiene asignado.

Después de crear una gateway privada virtual, debe adjuntarla a su VPC.

Para crear una gateway privada virtual y adjuntarla a su VPC.

1. Abre la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Puertas de enlace privadas virtuales y, a continuación, elija Crear una puerta de enlace privada virtual.
3. (Opcional) Escriba un nombre para la gateway privada virtual. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
4. Para ASN, deje la selección predeterminada para utilizar el ASN de Amazon predeterminado. De lo contrario, elija Custom ASN (ASN personalizado) y escriba un valor. Para un ASN de 16 bits ASN, el valor debe estar dentro del rango de 64 512 a 65 534. Para un ASN de 32 bits ASN, el valor debe estar dentro del rango de 4 200 000 000 a 4 294 967 294.
5. Elija Create Virtual Private Gateway.
6. Seleccione la gateway privada virtual que ha creado y, a continuación, elija Actions, Attach to VPC.
7. Seleccione la VPC en la lista y elija Yes, Attach.

Para crear una gateway privada virtual mediante la línea de comando o API

- CreateVpnGateway(API de consultas de Amazon EC2)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

Para adjuntar una gateway privada virtual a una VPC mediante la línea de comando o API

- AttachVpnGateway(API de consultas de Amazon EC2)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Asociación y disociación de gateways privadas virtuales

Puede asociar o desasociar una puerta de enlace privada virtual y una puerta de enlace de Direct Connect. El propietario de la cuenta de la puerta de enlace privada virtual realiza estas operaciones.

Para asociar una gateway privada virtual

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Puertas de enlace de Direct Connect y, a continuación, elija la puerta de enlace de Direct Connect.
3. Elija Ver detalles.
4. Elija Asociaciones de puerta de enlace y, a continuación, elija Asociar puerta de enlace.
5. En Gateways, elija las gateways privadas virtuales que desea asociar y, a continuación, elija Associate gateway (Asociar gateway).

Puede ver todas las gateways privadas virtuales que están asociados con la gateway de Direct Connect. Para ello, elija Gateway Associations (Asociaciones de gateways).

Para desasociar una gateway privada virtual

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Direct Connect Gateways (Gateways de Direct Connect) y, a continuación, seleccione la gateway de Direct Connect.

3. Elija Ver detalles.
4. Elija Gateway associations (Asociaciones de gateway) y, a continuación, seleccione la gateway privada virtual.
5. Elija Desasociar.

Para asociar una gateway privada virtual mediante la línea de comandos o la API

- create-direct-connect-gateway-asociación ()AWS CLI
- CreateDirectConnectGatewayAssociation(AWS Direct Connect API)

Para ver las gateways privadas virtuales asociadas con una gateway de Direct Connect mediante la línea de comandos o la API

- describe-direct-connect-gateway-asociaciones ()AWS CLI
- DescribeDirectConnectGatewayAssociations(AWS Direct Connect API)

Para desasociar una gateway privada virtual mediante la línea de comandos o la API

- delete-direct-connect-gateway-asociación ()AWS CLI
- DeleteDirectConnectGatewayAssociation(AWS Direct Connect API)

Creación de una interfaz virtual privada ara la gateway de Direct Connect

Para conectar la AWS Direct Connect conexión a la VPC remota, debe crear una interfaz virtual privada para la conexión. Especifique la gateway de Direct Connect a la que se va a conectar.

> **Note**
>
> Si acepta una interfaz virtual privada alojada, puede asociarla a una gateway de Direct Connect de su cuenta. Para obtener más información, consulte Aceptar una interfaz virtual alojada.

Para provisionar una interfaz virtual privada en una gateway de Direct Connect

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.

2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Tipo de interfaz virtual, elija Privada.
5. En Configuración de la interfaz virtual privada, realice lo siguiente:

   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

   c. Como propietario de la interfaz virtual, elija Mi AWS cuenta si la interfaz virtual es para su AWS cuenta.

   d. En Direct Connect gateway (Gateway de Direct Connect), seleccione la gateway de Direct Connect.

   e. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

   f. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

      Los valores válidos son 1 a 2147483647.

6. En Additional Settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

      [IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
      - En IP de mismo nivel del enrutador de Amazon, ingrese la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

      > **Important**
      >
      > Si permite la AWS asignación automática de direcciones IPv4, se asignará un CIDR /29 desde 169.254.0.0/16 IPv4 Link-Local de acuerdo con la RFC 3927 para la conectividad. point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP del mismo nivel del router del cliente como origen o destino del tráfico

de VPC. En su lugar, debe utilizar el RFC 1918 u otro direccionamiento (que no sea el RFC 1918) y especificar la dirección usted mismo.

- Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.
- Para obtener más información sobre la RFC 3927, consulte Dynamic Configuration of IPv4 Link-Local Addresses.

[IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

b. Para cambiar la unidad de transmisión máxima (MTU) de 1500 (predeterminada) a 9001 (tramas gigantes), seleccione MTU gigante (tamaño de MTU 9001).

c. (Opcional) En Habilitar SiteLink, elija Habilitado para habilitar la conectividad directa entre los puntos de presencia de Direct Connect.

d. (Opcional) Añada o elimine una etiqueta.

[Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

- En Key (Clave), escriba el nombre de la clave.
- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

7. Elija Create virtual interface (Crear interfaz virtual).

Una vez que haya creado la interfaz virtual, puede descargar la configuración del router de su dispositivo. Para obtener más información, consulte Descargar el archivo de configuración del enrutador.

Para crear una interfaz virtual privada mediante la línea de comandos o la API

- create-private-virtual-interface (AWS CLI)
- CreatePrivateVirtualInterface(AWS Direct Connect API)

Para ver las interfaces virtuales que se han adjuntado a una gateway de Direct Connect mediante la línea de comandos o la API

- describe-direct-connect-gateway-archivos adjuntos ()AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct Connect API)

Asociación de una gateway privada virtual entre cuentas

Puede asociar una puerta de enlace de Direct Connect a una puerta de enlace privada virtual que sea propiedad de cualquier AWS cuenta. La gateway de Direct Connect puede ser una gateway existente o puede crear una nueva gateway. El propietario de la gateway privada virtual crea una propuesta de asociación y el propietario de la gateway de Direct Connect debe aceptar la propuesta.

Una propuesta de asociación puede contener los prefijos que se permitirán desde la gateway privada virtual. El propietario de la gateway de Direct Connect puede anular cualquiera de los prefijos solicitados en la propuesta de asociación.

Prefijos permitidos

Al asociar una gateway privada virtual a una gateway de Direct Connect, debe especificar una lista de prefijos de Amazon VPC que se deben anunciar a la gateway de Direct Connect. La lista de prefijos actúa como un filtro que permite anunciar los mismos CIDR o unos CIDR más pequeños a la gateway de Direct Connect. En Allowed prefixes (Prefijos permitidos), debe definir un rango que coincida o que sea más amplio que el CIDR de la VPC porque aprovisionamos CIDR de VPC completos en la gateway privada virtual.

Por ejemplo, supongamos que el CIDR de la VPC es 10.0.0.0/16. Puede definir Allowed prefixes (Prefijos permitidos) en 10.0.0.0/16 (el valor del CIDR de la VPC) o en 10.0.0.0/15 (un valor que es más amplio que el del CIDR de la VPC).

Cualquier interfaz virtual incluida en los prefijos de red anunciados a través de Direct Connect solo se propaga a las pasarelas de tránsito de todas las regiones, no dentro de la misma región. Para obtener más información sobre cómo interactúan los prefijos permitidos con las puertas de enlace privadas virtuales y las puertas de enlace de tránsito, consulte the section called “Interacciones de prefijos permitidos”.

Tareas

- Creación de una propuesta de asociación

- Aceptación o rechazo de una propuesta de asociación
- Actualización de los prefijos permitidos para una asociación
- Eliminación de una propuesta de asociación

Creación de una propuesta de asociación

Si es el propietario de la gateway privada virtual, debe crear una propuesta de asociación. La puerta de enlace privada virtual debe estar conectada a una VPC de su AWS cuenta. El propietario de la puerta de enlace de Direct Connect debe compartir el ID de la puerta de enlace de Direct Connect y el ID de su AWS cuenta. Después de crear la propuesta, el propietario de la gateway de Direct Connect debe aceptarla, para que usted pueda tener acceso a la red local a través de AWS Direct Connect.

Para crear una propuesta de asociación

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual private gateways (Gateways privadas virtuales) y seleccione la gateway privada virtual.
3. Elija Ver detalles.
4. Elija Direct Connect gateway associations (Asociaciones de gateways de Direct Connect) y elija Associate Direct Connect gateway (Asociar gateway de Direct Connect).
5. En Association account type (Tipo de cuenta para la asociación), en Account owner (Propietario de la cuenta), elija Another account (Otra cuenta).
6. En Propietario de la puerta de enlace de Direct Connect, ingrese el ID de la cuenta de AWS a la que pertenece la puerta de enlace de Direct Connect.
7. En Association settings (Configuración de la asociación), haga lo siguiente:

   a. En Direct Connect gateway ID (ID de la gateway de Direct Connect), escriba el ID de la gateway de Direct Connect.

   b. Para el propietario de la puerta de enlace Direct Connect, introduzca el ID de la AWS cuenta propietaria de la puerta de enlace Direct Connect de la asociación.

   c. (Opcional) Para especificar una lista de los prefijos que se permitirán desde la gateway privada virtual, agregue los prefijos a Allowed prefixes (Prefijos permitidos) utilizando comas para separarlos o introduciéndolos en diferentes líneas.
8. Elija Associate Direct Connect gateway (Asociar gateway de Direct Connect).

Para crear una propuesta de asociación mediante la línea de comandos o la API

- create-direct-connect-gateway-propuesta de asociación ()AWS CLI
- CreateDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Aceptación o rechazo de una propuesta de asociación

Si es el propietario de la gateway de Direct Connect, debe aceptar la propuesta de asociación para crear la asociación. De lo contrario, puede rechazar la propuesta de asociación.

Para aceptar una propuesta de asociación

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Direct Connect gateways (Gateways de Direct Connect).
3. Seleccione la gateway de Direct Connect que tiene propuestas pendientes y elija View details (Ver detalles).
4. En la pestaña Pending proposals (Propuestas pendientes), seleccione la propuesta y elija Accept proposal (Aceptar propuesta).
5. (Opcional) Para especificar una lista de los prefijos que se permitirán desde la gateway privada virtual, agregue los prefijos a Allowed prefixes (Prefijos permitidos) utilizando comas para separarlos o introduciéndolos en diferentes líneas.
6. Elija Accept proposal (Aceptar propuesta).

Para rechazar una propuesta de asociación

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Direct Connect gateways (Gateways de Direct Connect).
3. Seleccione la gateway de Direct Connect que tiene propuestas pendientes y elija View details (Ver detalles).
4. En la pestaña Pending proposals (Propuestas pendientes), seleccione la gateway privada virtual y elija Reject proposal (Rechazar propuesta).
5. En el cuadro de diálogo Reject proposal (Rechazar propuesta), escriba Delete y elija Reject proposal (Rechazar propuesta).

Para ver las propuestas de asociación mediante la línea de comandos o la API

- describe-direct-connect-gateway-propuestas de asociación ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposals(API)AWS Direct Connect

Para aceptar una propuesta de asociación mediante la línea de comandos o la API

- accept-direct-connect-gateway-asociación-propuesta ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Para rechazar una propuesta de asociación mediante la línea de comandos o la API

- delete-direct-connect-gateway-asociación-propuesta ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Actualización de los prefijos permitidos para una asociación

Puede actualizar los prefijos permitidos para el tráfico desde la gateway privada virtual a través de la gateway de Direct Connect.

Si es el propietario de la gateway privada virtual, cree una propuesta de asociación para la misma gateway de Direct Connect y la misma gateway privada virtual, especificando los prefijos permitidos.

Si es el propietario de la gateway de Direct Connect, actualice los prefijos permitidos cuando acepte la propuesta de asociación o actualice los prefijos permitidos para una asociación existente, tal y como se indica a continuación.

Para actualizar los prefijos permitidos para una asociación existente mediante la línea de comandos o la API

- update-direct-connect-gateway-asociación ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Eliminación de una propuesta de asociación

El propietario de la gateway privada virtual puede eliminar la propuesta de asociación de la gateway de Direct Connect si todavía está pendiente de aceptación. Una vez aceptada una propuesta de asociación, no es posible eliminarla, pero se puede desasociar la gateway privada virtual de la

gateway de Direct Connect. Para obtener más información, consulte the section called “Asociación y disociación de gateways privadas virtuales”.

Para eliminar una propuesta de asociación

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual private gateways (Gateways privadas virtuales) y seleccione la gateway privada virtual.
3. Elija Ver detalles.
4. Elija Pending Direct Connect gateway associations (Asociaciones pendientes de la gateway de Direct Connect), seleccione la asociación y elija Delete association (Eliminar asociación).
5. En el cuadro de diálogo Delete association proposal (Eliminar propuesta de asociación), escriba Delete y elija Delete (Eliminar).

Para eliminar una propuesta de asociación pendiente mediante la línea de comandos o la API

- delete-direct-connect-gateway-propuesta de asociación ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Asociaciones de la puerta de enlace de tránsito

Puede utilizar una puerta de enlace de AWS Direct Connect para conectar su conexión de AWS Direct Connect a través de una interfaz virtual de tránsito a las VPC o VPN vinculadas a la puerta de enlace de tránsito. Asocie una puerta de enlace de Direct Connect con la puerta de enlace de tránsito. A continuación, cree una interfaz virtual de tránsito para su AWS Direct Connect conexión a la puerta de enlace Direct Connect.

Las siguientes reglas se aplican a las asociaciones de puerta de enlace de tránsito:

- No puede adjuntar una puerta de enlace de Direct Connect en una puerta de enlace de tránsito cuando la puerta de enlace de Direct Connect ya se encuentra asociada a una puerta de enlace privada virtual o adjunta a una interfaz virtual privada.
- Existen límites para la creación y el uso de gateways de Direct Connect. Para obtener más información, consulte Cuotas.
- Una puerta de enlace Direct Connect admite la comunicación entre las interfaces virtuales de tránsito conectadas y las puertas de enlace de tránsito asociadas.

- Si se conecta a varias puertas de enlace de tránsito que se encuentran en diferentes regiones, utilice ASN únicos para cada puerta de enlace de tránsito.
- Cualquier interfaz virtual incluida en los prefijos de red anunciados a través de Direct Connect solo se propaga a las pasarelas de tránsito de todas las regiones, pero no dentro de la misma región

Asociación y disociación de gateways de tránsito

Para asociar una puerta de enlace de tránsito

1. Abra la consola en https://console.aws.amazon.com/directconnect/v2/home AWS Direct Connect.
2. En el panel de navegación, elija Direct Connect Gateways (Gateways de Direct Connect) y, a continuación, seleccione la gateway de Direct Connect.
3. Elija Ver detalles.
4. Elija Gateway associations (Asociaciones de gateway) y, a continuación, elija Associate gateway (Asociar gateway).
5. En Puertas de enlace, elija la puerta de enlace de tránsito que desee asociar.
6. En Prefijos permitidos, ingrese los prefijos (separados por una coma o en una línea nueva) que la puerta de enlace de Direct Connect anuncia en el centro de datos en las instalaciones. Para obtener más información sobre los prefijos permitidos, consulte the section called “Interacciones de prefijos permitidos”.
7. Elija Asociar puerta de enlace

Puede ver todas las gateways que están asociadas con la gateway de Direct Connect. Para ello, elija Gateway associations (Asociaciones de gateways).

Desasociación de una puerta de enlace de tránsito

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Direct Connect gateways (Gateways de Direct Connect) y, a continuación, seleccione la gateway de Direct Connect.
3. Elija Ver detalles.
4. Elija Gateway associations (Asociaciones de gateway) y, a continuación, seleccione la gateway de tránsito.
5. Elija Desasociar.

Actualización de los prefijos permitidos para una puerta de enlace de tránsito

Puede agregar o eliminar prefijos permitidos en la puerta de enlace de tránsito.

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Puertas de enlace de Direct Connect y, a continuación, elija la puerta de enlace de Direct Connect para la que desee agregar o eliminar los prefijos permitidos.
3. Seleccione la pestaña de Asociaciones de puerta de enlace.
4. Elija la puerta de enlace que desee modificar y, a continuación, elija Editar.
5. En Prefijos permitidos, ingrese los prefijos que la puerta de enlace de Direct Connect anuncia en el centro de datos en las instalaciones. En el caso de varios prefijos, separe cada prefijo con una coma o coloque cada prefijo en una línea nueva. Los prefijos que agregue deben coincidir con los CIDR de Amazon VPC de todas las puertas de enlace privadas virtuales. Para obtener más información sobre los prefijos permitidos, consulte the section called “Interacciones de prefijos permitidos”.
6. Elija Edit association.

   En la sección de Asociación de puerta de enlace, el Estado muestra actualizando. Al finalizar, el Estado cambia a asociado.
7. Elija Desasociar.
8. Vuelva a elegir Desasociar para confirmar que desea desasociar la puerta de enlace.

   En la sección de Asociación de puerta de enlace, el Estado muestra desasociando. Al finalizar, aparece un mensaje de confirmación y la puerta de enlace se elimina de la sección. Esto puede tardar varios minutos o más tiempo en completarse.

Para asociar una puerta de enlace de tránsito mediante la línea de comandos o la API

- create-direct-connect-gateway-asociación ()AWS CLI
- CreateDirectConnectGatewayAssociation(AWS Direct Connect API)

Para ver las puertas de enlace de tránsito asociadas con una puerta de enlace de Direct Connect mediante la línea de comandos o la API

- describe-direct-connect-gateway-asociaciones ()AWS CLI
- DescribeDirectConnectGatewayAssociations(AWS Direct Connect API)

Para desasociar una puerta de enlace de tránsito mediante la línea de comandos o la API

- delete-direct-connect-gateway-asociación ()AWS CLI
- DeleteDirectConnectGatewayAssociation(AWS Direct Connect API)

A fin de actualizar los prefijos permitidos para una puerta de enlace de tránsito mediante la línea de comando o API

- update-direct-connect-gateway-asociación ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Creación de una interfaz virtual de tránsito en la gateway de Direct Connect

Para conectar tu AWS Direct Connect conexión a la pasarela de tránsito, debes crear una interfaz de tránsito para tu conexión. Especifique la gateway de Direct Connect a la que se va a conectar.

> **Important**
>
> Si asocia su puerta de enlace de tránsito a una o más puertas de enlace de Direct Connect, el número de sistema autónomo (ASN) que utilizan la puerta de enlace de tránsito y de Direct Connect deben ser diferentes. Por ejemplo, si utiliza el ASN 64512 predeterminado tanto para la puerta de enlace de tránsito como para la de Direct Connect, la solicitud de asociación fallará.

Para aprovisionar una interfaz virtual de tránsito en una gateway de Direct Connect

1. Abre la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Virtual interface type (Tipo de interfaz virtual) en Type (Tipo), elija Transit (Tránsito).
5. En Transit virtual interface settings (Configuración de la interfaz virtual de tránsito), haga lo siguiente:

   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.

b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.

c. Como propietario de la interfaz virtual, elija Mi AWS cuenta si la interfaz virtual es para su AWS cuenta.

d. En Direct Connect gateway (Gateway de Direct Connect), seleccione la gateway de Direct Connect.

e. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

f. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

   Los valores válidos son 1 a 2147483647.

6. En Additional Settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un BGP IPv4 o IPv6 del mismo nivel, haga lo siguiente:

      [IPv4] Para configurar un BGP IPv4 de mismo nivel, elija IPv4 y realice una de las siguientes operaciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip (IP del mismo nivel de su router), escriba la dirección CIDR IPv4 de destino a la que Amazon debe enviar el tráfico.
      - En IP de mismo nivel del enrutador de Amazon, ingrese la dirección CIDR IPv4 que se va a utilizar para enviar tráfico a AWS.

      > **Important**
      >
      > Si permite la AWS asignación automática de direcciones IPv4, se asignará un CIDR /29 desde 169.254.0.0/16 IPv4 Link-Local de acuerdo con la RFC 3927 para la conectividad. point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP del mismo nivel del router del cliente como origen o destino del tráfico de VPC. En su lugar, debe utilizar el RFC 1918 u otro direccionamiento (que no sea el RFC 1918) y especificar la dirección usted mismo.
      >
      > - Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.
      > - Para obtener más información sobre la RFC 3927, consulte Dynamic Configuration of IPv4 Link-Local Addresses.

[IPv6] Para configurar un BGP IPv6 del mismo nivel, elija IPv6. Las direcciones IPv6 de mismo nivel se asignarán automáticamente desde el grupo de direcciones IPv6 de Amazon. No puede especificar direcciones IPv6 personalizadas.

b. Para cambiar la unidad de transmisión máxima (MTU) de 1500 (predeterminada) a 8500 (tramas gigantes), seleccione Jumbo MTU (MTU size 8500) [MTU gigante (tamaño de MTU 8500)].

c. (Opcional) En Habilitar SiteLink, elija Habilitado para habilitar la conectividad directa entre los puntos de presencia de Direct Connect.

d. (Opcional) Añada o elimine una etiqueta.

[Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

- En Key (Clave), escriba el nombre de la clave.
- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).

7. Elija Create virtual interface (Crear interfaz virtual).

Una vez que haya creado la interfaz virtual, puede descargar la configuración del router de su dispositivo. Para obtener más información, consulte Descargar el archivo de configuración del enrutador.

Para crear una interfaz virtual de tránsito mediante la línea de comandos o la API

- create-transit-virtual-interface (AWS CLI)
- CreateTransitVirtualInterface(AWS Direct Connect API)

Para ver las interfaces virtuales que se han adjuntado a una gateway de Direct Connect mediante la línea de comandos o la API

- describe-direct-connect-gateway-archivos adjuntos ()AWS CLI
- DescribeDirectConnectGatewayAttachments(AWS Direct Connect API)

Asociación de una gateway de tránsito entre cuentas

Puede asociar una puerta de enlace Direct Connect existente o una nueva puerta de enlace de Direct Connect a una puerta de enlace de tránsito que sea propiedad de cualquier AWS cuenta. El propietario de la puerta de enlace de tránsito crea una propuesta de asociación y el propietario de la puerta de enlace de Direct Connect debe aceptar la propuesta de asociación.

Una propuesta de asociación puede contener los prefijos que se permitirán desde la puerta de enlace de tránsito. El propietario de la gateway de Direct Connect puede anular cualquiera de los prefijos solicitados en la propuesta de asociación.

Prefijos permitidos

En el caso de una asociación de puerta de enlace de tránsito, aprovisione la lista de prefijos permitidos de la puerta de enlace de Direct Connect. La lista se usa para enrutar el tráfico desde las instalaciones AWS hasta la puerta de enlace de tránsito, incluso si las VPC conectadas a la puerta de enlace de tránsito no tienen CIDR asignados. Los prefijos de la lista de prefijos permitidos de la gateway de Direct Connect se originan en la gateway de Direct Connect y se publican en la red local. Para obtener más información sobre cómo interactúan los prefijos permitidos con las puertas de enlace de tránsito y las puertas de enlace privadas virtuales, consulte the section called “Interacciones de prefijos permitidos”.

Tareas

- Creación de una propuesta de asociación de la gateway de tránsito
- Aceptación o rechazo de una propuesta de asociación de la gateway de tránsito
- Actualización de los prefijos permitidos para una asociación de la gateway de tránsito
- Eliminación de una propuesta de asociación de la gateway de tránsito

Creación de una propuesta de asociación de la gateway de tránsito

Si es el propietario de la puerta de enlace de tránsito, debe crear la propuesta de asociación. La pasarela de tránsito debe estar conectada a una VPC o VPN de tu AWS cuenta. El propietario de la puerta de enlace de Direct Connect debe compartir el ID de la puerta de enlace de Direct Connect y el ID de su cuenta de AWS . Después de crear la propuesta, el propietario de la gateway de Direct Connect debe aceptarla, para que usted pueda tener acceso a la red local a través de AWS Direct Connect.

Para crear una propuesta de asociación

1. Abre la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Puertas de enlace de tránsito y, a continuación, seleccione la puerta de enlace de tránsito.
3. Elija Ver detalles.
4. Elija Direct Connect gateway associations (Asociaciones de gateways de Direct Connect) y, a continuación, elija Associate Direct Connect gateway (Asociar gateway de Direct Connect).
5. En Association account type (Tipo de cuenta para la asociación), en Account owner (Propietario de la cuenta), elija Another account (Otra cuenta).
6. En Propietario de la puerta de enlace de Direct Connect, ingrese el ID de la cuenta a la que pertenece la puerta de enlace de Direct Connect.
7. En Association settings (Configuración de la asociación), haga lo siguiente:

   a. En Direct Connect gateway ID (ID de la gateway de Direct Connect), escriba el ID de la gateway de Direct Connect.
   b. En Propietario de la interfaz virtual, ingrese el ID de la cuenta a la que pertenece la interfaz virtual para la asociación.
   c. (Opcional) Para especificar una lista de los prefijos que se permitirán desde la puerta de enlace de tránsito, agregue los prefijos a Prefijos permitidos utilizando comas a fin de separarlos o introduciéndolos en diferentes líneas.
8. Elija Associate Direct Connect gateway (Asociar gateway de Direct Connect).

Para crear una propuesta de asociación mediante la línea de comandos o la API

- create-direct-connect-gateway-propuesta de asociación ()AWS CLI
- CreateDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Aceptación o rechazo de una propuesta de asociación de la gateway de tránsito

Si es el propietario de la gateway de Direct Connect, debe aceptar la propuesta de asociación para crear la asociación. También tiene la opción de rechazar la propuesta de asociación.

Para aceptar una propuesta de asociación

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.

2. En el panel de navegación, elija Direct Connect gateways (Gateways de Direct Connect).
3. Seleccione la gateway de Direct Connect que tiene propuestas pendientes y, a continuación, elija View details (Ver detalles).
4. En la pestaña Pending proposals (Propuestas pendientes), seleccione la propuesta y, a continuación, elija Accept proposal (Aceptar propuesta).
5. (Opcional) Para especificar una lista de los prefijos que se permitirán desde la puerta de enlace de tránsito, agregue los prefijos a Prefijos permitidos utilizando comas para separarlos o introduciéndolos en diferentes líneas.
6. Elija Accept proposal (Aceptar propuesta).

Para rechazar una propuesta de asociación

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Direct Connect gateways (Gateways de Direct Connect).
3. Seleccione la gateway de Direct Connect que tiene propuestas pendientes y, a continuación, elija View details (Ver detalles).
4. En la pestaña Pending proposals (Propuestas pendientes), seleccione la gateway de tránsito y, a continuación, elija Reject proposal (Rechazar propuesta).
5. En el cuadro de diálogo Reject proposal (Rechazar propuesta), escriba Delete y, a continuación, elija Reject proposal (Rechazar propuesta).

Para ver las propuestas de asociación mediante la línea de comandos o la API

- describe-direct-connect-gateway-propuestas de asociación ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposals(API)AWS Direct Connect

Para aceptar una propuesta de asociación mediante la línea de comandos o la API

- accept-direct-connect-gateway-asociación-propuesta ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Para rechazar una propuesta de asociación mediante la línea de comandos o la API

- delete-direct-connect-gateway-asociación-propuesta ()AWS CLI

- DeleteDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Actualización de los prefijos permitidos para una asociación de la gateway de tránsito

Puede actualizar los prefijos permitidos para el tráfico desde la puerta de enlace de tránsito a través de la puerta de enlace de Direct Connect.

Si es el propietario de la puerta de enlace de tránsito, cree una propuesta de asociación para la misma puerta de enlace de Direct Connect y puerta de enlace privada virtual, al especificar los prefijos permitidos.

Si es el propietario de la gateway de Direct Connect, actualice los prefijos permitidos cuando acepte la propuesta de asociación o actualice los prefijos permitidos para una asociación existente, tal y como se indica a continuación.

Para actualizar los prefijos permitidos para una asociación existente mediante la línea de comandos o la API

- update-direct-connect-gateway-asociación ()AWS CLI
- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

Eliminación de una propuesta de asociación de la gateway de tránsito

El propietario de la puerta de enlace de tránsito puede eliminar la propuesta de asociación de la puerta de enlace de Direct Connect si todavía se encuentra pendiente de aceptación. Una vez aceptada una propuesta de asociación, no es posible eliminarla, pero se puede desasociar la gateway de tránsito de la gateway de Direct Connect. Para obtener más información, consulte the section called “Creación de una propuesta de asociación de la gateway de tránsito”.

Para eliminar una propuesta de asociación

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Puertas de enlace de tránsito y, a continuación, seleccione la puerta de enlace de tránsito.
3. Elija Ver detalles.
4. Elija Pending gateway associations (Asociaciones pendientes de la gateway), seleccione la asociación y, a continuación, elija Delete association (Eliminar asociación).

5. En el cuadro de diálogo Delete association proposal (Eliminar propuesta de asociación), escriba Delete y, a continuación, elija Delete (Eliminar).

Para eliminar una propuesta de asociación pendiente mediante la línea de comandos o la API

- delete-direct-connect-gateway-propuesta de asociación ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Interacciones de prefijos permitidos

Aprenda cómo interactúan los prefijos permitidos con las puertas de enlace de tránsito y las puertas de enlace privadas virtuales. Para obtener más información, consulte the section called “Políticas de direccionamiento y comunidades de BGP”.

Asociaciones de la gateway privada virtual

La lista de prefijos (IPv4 e IPv6) actúa como un filtro que permite anunciar los mismos CIDR, o un rango más pequeño de CIDR, a la puerta de enlace de Direct Connect. Debe establecer los prefijos en el mismo rango, o en uno más amplio, que el bloque CIDR de VPC.

> **Note**
>
> La lista de permitidos solo funciona como un filtro y solo el CIDR de VPC asociado se anunciará en la puerta de enlace de cliente.

Piense en una situación en la que tiene una VPC con el CIDR 10.0.0.0/16 adjunta a una gateway privada virtual.

- Cuando la lista de prefijos permitidos se establece en 22.0.0.0/24, no recibe ninguna ruta porque 22.0.0.0/24 es diferente o más amplia que 10.0.0.0/16.
- Cuando la lista de prefijos permitidos se establece en 10.0.0.0/24, no recibe ninguna ruta porque 10.0.0.0/24 es diferente o más amplia que 10.0.0.0/16.
- Cuando la lista de prefijos permitidos se establece en 10.0.0.0/15, no recibe 10.0.0.0/16 porque la dirección IP es más amplia que 10.0.0.0/16.

Cuando elimina o agrega un prefijo permitido, el tráfico que no lo utiliza no se ve afectado. Durante las actualizaciones, el estado cambia de `associated` a `updating`. La modificación de un prefijo existente solo puede retrasar el tráfico que utiliza ese prefijo.

Asociaciones de la puerta de enlace de tránsito

En el caso de una asociación de puerta de enlace de tránsito, aprovisione la lista de prefijos permitidos de la puerta de enlace de Direct Connect. La lista enruta el tráfico en las instalaciones hacia o desde una puerta de enlace de Direct Connect, incluso cuando las VPC conectadas a la puerta de enlace de tránsito no tengan CIDR asignados. Los prefijos permitidos funcionan de forma diferente en función del tipo de puerta de enlace:

- En el caso de las asociaciones de puerta de enlace de tránsito, solo se anunciarán en las instalaciones los prefijos permitidos ingresados. Se mostrarán como originarios del ASN de la puerta de enlace de Direct Connect.
- En el caso de las puertas de enlace privadas virtuales, los prefijos permitidos ingresados actúan como un filtro para admitir CIDR iguales o menores.

Considere el escenario en que tiene una VPC con un CIDR 10.0.0.0/16 asociado a una puerta de enlace de tránsito.

- Cuando la lista de prefijos permitidos se establece en 22.0.0.0/24, recibe 22.0.0.0/24 a través de BGP en su interfaz virtual de tránsito. No recibe 10.0.0.0/16 porque aprovisionamos directamente los prefijos que se encuentran en la lista de prefijos permitidos.
- Cuando la lista de prefijos permitidos se establece en 10.0.0.0/24, recibe 10.0.0.0/24 a través de BGP en su interfaz virtual de tránsito. No recibe 10.0.0.0/16 porque aprovisionamos directamente los prefijos que se encuentran en la lista de prefijos permitidos.
- Cuando la lista de prefijos permitidos se establece en 10.0.0.0/8, recibe 10.0.0.0/8 a través de BGP en su interfaz virtual de tránsito.

No se permiten las superposiciones de prefijos permitidos cuando hay varias puertas de enlace de tránsito asociadas a una puerta de enlace de Direct Connect. Por ejemplo, si tiene una puerta de enlace de tránsito con una lista de prefijos permitidos que incluye 10.1.0.0/16 y una segunda puerta de enlace de tránsito con una lista de prefijos permitidos que incluye 10.2.0.0/16 y 0.0.0.0/0, no puede establecer las asociaciones de la segunda puerta de enlace de tránsito en 0.0.0.0/0. Como 0.0.0.0/0 incluye todas las redes IPv4, no puede configurar 0.0.0.0/0 si hay varias puertas de enlace

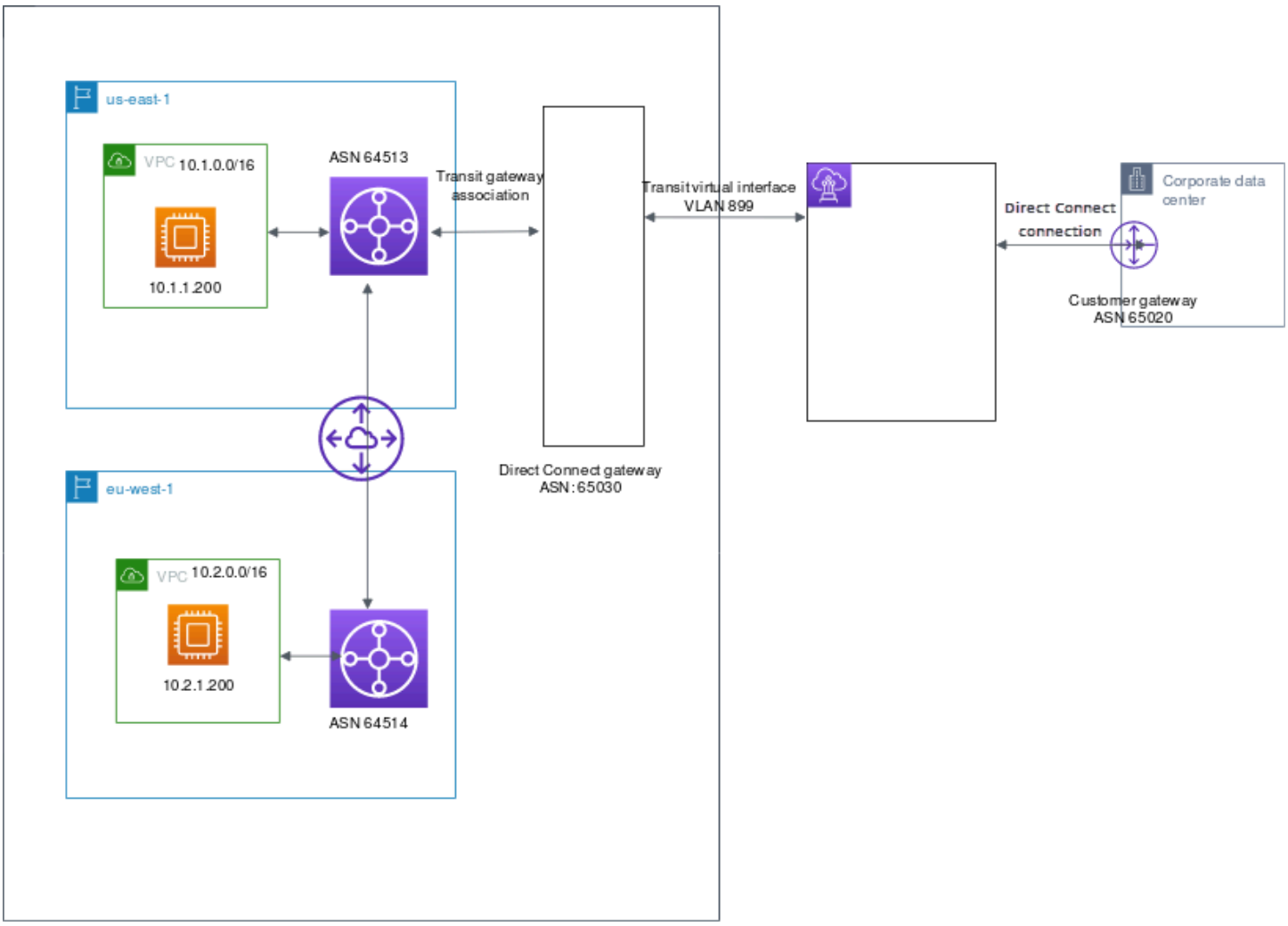
de tránsito asociadas a una puerta de enlace de Direct Connect. Se devuelve un error que indica que las rutas permitidas se superponen a una o más rutas permitidas existentes en la puerta de enlace de Direct Connect.

Cuando elimina o agrega un prefijo permitido, el tráfico que no lo utiliza no se ve afectado. Durante las actualizaciones, el estado cambia de `associated` a `updating`. La modificación de un prefijo existente solo puede retrasar el tráfico que utiliza ese prefijo.

Ejemplo: Prefijos permitidos en una configuración de puerta de enlace de tránsito

Considere la configuración en la que hay instancias en dos regiones de AWS diferentes que necesitan acceder al centro de datos corporativo. Puede utilizar los siguientes recursos para esta configuración:

- Una puerta de enlace de tránsito en cada región.
- Una conexión de intercambio de tráfico de puerta de enlace de tránsito.
- Una puerta de enlace de Direct Connect.
- Una asociación de puerta de enlace de tránsito entre una de las puertas de enlace de tránsito (la de us-east-1) y la puerta de enlace de Direct Connect.
- Una interfaz virtual de tránsito desde la ubicación en las instalaciones y la ubicación de AWS Direct Connect.



Configure las siguientes opciones para los recursos.

- Puerta de enlace de Direct Connect: establezca el ASN en 65030. Para más información, consulte the section called “Creación de una gateway de Direct Connect”.
- Interfaz virtual de tránsito: establezca la VLAN en 899 y el ASN en 65020. Para más información, consulte the section called “Crear una interfaz virtual de tránsito en la puerta de enlace de Direct Connect”.
- Asociación de la puerta de enlace de Direct Connect con la puerta de enlace de tránsito: establezca los prefijos permitidos en 10.0.0.0/8.

  Este bloque de CIDR cubre ambos bloques de CIDR de la VPC. Para más información, consulte the section called “Asociación y disociación de gateways de tránsito”.
- Ruta de la VPC: para enrutar el tráfico desde la VPC 10.2.0.0, cree una ruta en la tabla de enrutamiento de la VPC que tenga un destino de 0.0.0.0/0 y el ID de la puerta de enlace de tránsito

como destino. Para obtener más información sobre el enrutamiento a la puerta de enlace de tránsito, consulte Enrutamiento de una puerta de enlace en la Guía del usuario de Amazon VPC.

Etiquetado de recursos de AWS Direct Connect

Una etiqueta es un elemento que el propietario de un recurso asigna a sus recursos de AWS Direct Connect. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario. Las etiquetas permiten al propietario del recurso clasificar los recursos de AWS Direct Connect de diversas maneras, por ejemplo, según su finalidad o entorno. Esto es útil cuando tiene muchos recursos del mismo tipo, ya que puede identificar rápidamente un recurso específico en función de las etiquetas que le haya asignado.

Por ejemplo, si tiene dos conexiones de AWS Direct Connect en una región y cada una está en una ubicación diferente. La conexión `dxcon-11aa22bb` es una conexión que sirve tráfico de producción y que está asociada a la interfaz virtual `dxvif-33cc44dd`. La conexión `dxcon-abcabcab` es una conexión redundante (backup) asociada a la interfaz virtual `dxvif-12312312`. Para ayudar a distinguirlas, puede etiquetar las conexiones e interfaces virtuales tal y como se indica a continuación:

ID de recurso	Clave de etiqueta	Valor de etiqueta
`dxcon-11aa22bb`	Finalidad	Producción
	Location	Ámsterdam
`dxvif-33cc44dd`	Finalidad	Producción
`dxcon-abcabcab`	Finalidad	Copia de seguridad
	Location	Fráncfort
`dxvif-12312312`	Finalidad	Copia de seguridad

Recomendamos que idee un conjunto de claves de etiqueta que cumpla sus necesidades para cada tipo de recurso. Mediante el uso de un conjunto coherente de claves de etiquetas, podrá administrar los recursos más fácilmente. Las etiquetas no tienen ningún significado semántico para AWS Direct Connect, por lo que se interpretan estrictamente como cadenas de caracteres. Además, las etiquetas no se asignan a los recursos automáticamente. Puede editar las claves y los valores de las etiquetas y también puede eliminar etiquetas de un recurso en cualquier momento. Puede establecer el valor de una etiqueta como una cadena vacía, pero no puede asignarle un valor nulo. Si añade una

etiqueta con la misma clave que una etiqueta existente en ese recurso, el nuevo valor sobrescribirá al antiguo. Si elimina un recurso, también se eliminará cualquier etiqueta asignada a dicho recurso.

Puede etiquetar los siguientes recursos de AWS Direct Connect mediante la consola de AWS Direct Connect, la API de AWS Direct Connect, la AWS CLI, las AWS Tools for Windows PowerShell o un AWS SDK. Cuando se utilizan estas herramientas para administrar etiquetas, es preciso especificar el nombre de recurso de Amazon (ARN) del recurso. Para obtener más información acerca de los ARN, consulte Nombres de recurso de Amazon (ARN) en la Referencia general de Amazon Web Services.

Recurso	Admite etiquetas	Admite etiquetas en la creación	Admite etiquetas que controlan el acceso y la asignación de recursos	Admite la asignación de costos
Conexiones	Sí	Sí	Sí	Sí
Interfaces virtuales	Sí	Sí	Sí	No
Grupos de agregación de enlaces (LAG)	Sí	Sí	Sí	Sí
Interconexiones	Sí	Sí	Sí	Sí
Gateways de Direct Connect	No	No	No	No

Restricciones de las etiquetas

Las siguientes reglas y restricciones se aplican a las etiquetas:

- Número máximo de etiquetas por recurso: 50
- Longitud máxima de la clave: 128 caracteres Unicode
- Longitud máxima del valor: 265 caracteres Unicode

- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
- El prefijo `aws:` se reserva para uso de AWS. No puede editar ni eliminar la clave o el valor de una etiqueta cuando la etiqueta tiene una clave de etiqueta con el prefijo `aws:`. Las etiquetas con una clave de etiqueta con el prefijo `aws:` no cuentan para el límite de etiquetas por recurso.
- Los caracteres permitidos son letras, espacios y números representables en UTF-8, además de los siguientes caracteres especiales: + - = . _ : / @
- Solo el propietario del recurso puede añadir o eliminar etiquetas. Por ejemplo, si hay una conexión alojada, el socio no podrá añadir, eliminar ni ver las etiquetas.
- Las etiquetas de asignación de costos solo se admiten para conexiones, interconexiones y LAG. Para obtener información sobre cómo utilizar etiquetas con la administración de costos, consulte Uso de etiquetas de asignación de costos en la Guía del usuario de AWS Billing and Cost Management.

Uso de etiquetas mediante la CLI o la API

Utilice lo siguiente para añadir, actualizar, listar y eliminar las etiquetas de los recursos.

Tarea	API	CLI
Agregar o sobrescribir una o varias etiquetas.	TagResource	tag-resource
Eliminar una o varias etiquetas .	UntagResource	untag-resource
Describir una o varias etiquetas.	DescribeTags	describe-tags

Ejemplos

Utilice el comando tag-resource para etiquetar la conexión `dxcon-11aa22bb`.

```
aws directconnect tag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tags "key=Purpose,value=Production"
```

Utilice el comando describe-tags para describir las etiquetas `dxcon-11aa22bb` de la conexión.

```
aws directconnect describe-tags --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb
```

Utilice el comando untag-resource para eliminar una etiqueta de la conexión `dxcon-11aa22bb`.

```
aws directconnect untag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tag-keys Purpose
```

Seguridad en AWS Direct Connect

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad que se aplican a AWS Direct Connect, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad se determina según el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Direct Connect. En los siguientes temas, se le mostrará cómo configurar AWS Direct Connect para satisfacer sus objetivos de seguridad y conformidad. También puede aprender a utilizar otros servicios de AWS que lo ayuden a monitorear y proteger los recursos de AWS Direct Connect.

Temas

Protección de los datos en AWS Direct Connect

El modelo de responsabilidad compartida, y de AWS se aplica a la protección de datos de AWS Direct Connect. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Para proteger los datos, recomendamos proteger las credenciales de Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. reSe recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no ingresar nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye las situaciones en las que debe trabajar con la AWS Direct Connect u otros Servicios de AWS a través de la consola, la API, la AWS CLI o los SDK de AWS. Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para nombres

se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Para obtener más información sobre la protección de datos, consulte la entrada de blog relativa al modelo de responsabilidad compartida de AWS y GDPR en el blog de seguridad de AWS.

Temas

- Privacidad del tráfico entre redes en AWS Direct Connect
- Cifrado en tránsito AWS Direct Connect

Privacidad del tráfico entre redes en AWS Direct Connect

Tráfico entre el servicio y las aplicaciones y clientes locales

Tiene dos opciones de conectividad entre su red privada y AWS:

- Una asociación a un AWS Site-to-Site VPN. Para obtener más información, consulte the section called “Seguridad de infraestructuras”.
- Una asociación a VPC. Para obtener más información, consulte the section called “Asociaciones de la gateway privada virtual” y the section called “Asociaciones de la puerta de enlace de tránsito”.

Tráfico entre recursos de AWS en la misma región

Tiene dos opciones de conectividad:

- Una asociación a un AWS Site-to-Site VPN. Para obtener más información, consulte the section called “Seguridad de infraestructuras”.
- Una asociación a VPC. Para obtener más información, consulte the section called “Asociaciones de la gateway privada virtual” y the section called “Asociaciones de la puerta de enlace de tránsito”.

Cifrado en tránsito AWS Direct Connect

AWS Direct Connect no cifra el tráfico que está en tránsito de forma predeterminada. Para cifrar los datos en tránsito que los atraviesan AWS Direct Connect, debe utilizar las opciones de cifrado de tránsito de ese servicio. Para obtener más información sobre el cifrado del tráfico de instancias EC2, consulte Encryption in Transit en la Guía del usuario de Amazon EC2.

Con AWS Direct Connect y AWS Site-to-Site VPN, puede combinar una o más conexiones de red AWS Direct Connect dedicadas con la VPN de Amazon VPC. Esta combinación proporciona una conexión privada cifrada con IPsec que también reduce los costos de red, aumenta el rendimiento del ancho de banda y proporciona una experiencia de red más coherente que las conexiones de VPN basadas en Internet. Para obtener más información, consulte las Opciones de conectividad entre Amazon VPC y Amazon VPC.

La seguridad de MAC (MACsec) es un estándar IEEE que proporciona confidencialidad, integridad y autenticidad del origen de los datos. Puede utilizar AWS Direct Connect conexiones compatibles con MacSec para cifrar los datos desde el centro de datos corporativo hasta la ubicación. AWS Direct Connect Para obtener más información, consulte Seguridad de MAC.

Identity and Access Management para Direct Connect

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Direct Connect. IAM es un servicio de AWS que se puede utilizar sin cargo adicional.

Temas

Público

La forma en que utilice AWS Identity and Access Management (IAM) difiere en función del trabajo que realice en Direct Connect.

Usuario de servicio: si utiliza el servicio de Direct Connect para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Direct Connect para realizar su trabajo, es posible que necesite otros permisos. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Direct Connect, consulte Solución de problemas de identidad y acceso de Direct Connect.

Administrador de servicio: si está a cargo de los recursos de Direct Connect de su empresa, es probable que tenga acceso completo a Direct Connect. Su trabajo consiste en determinar a qué características y recursos de Direct Connect 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. Para obtener más información sobre cómo su empresa puede utilizar IAM con Direct Connect, consulte Funcionamiento de Direct Connect con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera obtener más detalles sobre cómo escribir políticas para administrar el acceso a Direct Connect. Para consultar ejemplos de las políticas basadas en identidades de Direct Connect que puede utilizar en IAM, consulte Ejemplos de políticas basadas en identidades de Direct Connect.

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como el Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad de AWS IAM Identity Center. Los usuarios (del 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 accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

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

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de la línea de comandos (CLI) para firmar criptográficamente las solicitudes mediante el uso de las credenciales. Si no usa las herramientas de AWS, debe firmar usted mismo las solicitudes. Para obtener más información sobre la firma de solicitudes, consulte Firma de solicitudes API de AWS 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, AWS le recomienda el uso de 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 Single Sign-On y Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

Usuario raíz de cuenta de AWS

Cuando se crea una cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los servicios y recursos de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó 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, solicite que los usuarios humanos, incluidos los que requieren acceso de administrador, utilicen la federación con un proveedor de identidades para acceder a los servicios de AWS utilizando credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidad web, el AWS Directory Service, el directorio del Identity Center, o cualquier usuario que acceda a los Servicios de AWS utilizando credenciales proporcionadas a través de una fuente de identidad. Cuando identidades federadas acceden a las Cuentas de AWS, asumen roles y los roles proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS Single Sign-On. Puede crear usuarios y grupos en el IAM Identity Center o puede conectarse y sincronizar con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus

aplicaciones y Cuentas de AWS. 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 en su Cuenta de AWS que dispone de 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 de tu cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la AWS Management Consolecambiando de roles. Puede asumir un rol llamando a una operación de AWS CLI o de la API de AWS, 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 el IAM Identity Center, debe configurar un conjunto de permisos. El 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. No obstante, con algunos Servicios de AWS se puede asociar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información sobre 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 características de 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 a servicios.
  - Reenviar sesiones de acceso (FAS): cuando utiliza un rol o un usuario de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o 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.
  - Rol vinculado a servicios: un rol vinculado a servicios 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 a servicios aparecen en la 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 utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de 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

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario raíz) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de las políticas JSON en la Guía del Usuario de IAM.

Los administradores pueden utilizar las políticas JSON de AWS 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. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. 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 dicha política puede obtener información del usuario de la consola, AWS CLI o la API de AWS.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede vincular a una identidad, como un usuario, grupo o rol de IAM. 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 en función de identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidad 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 asociar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas de AWS y las políticas administradas por el cliente. Para obtener más información acerca de cómo elegir una política administrada o una política insertada, consulte Elección 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. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Las entidades 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 se puede utilizar políticas de IAM administradas por AWS 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 política JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. 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 otros tipos de políticas adicionales menos frecuentes. 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 en función de 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 servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada rootlong. 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 identidad 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 obtener información sobre cómo AWS decide si permite o no una solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

Funcionamiento de Direct Connect con IAM

Antes de utilizar IAM para administrar el acceso a Direct Connect, conozca qué características de IAM se pueden utilizar con Direct Connect.

Características de IAM que puede utilizar con Direct Connect

Características de IAM	Compatibilidad de Direct Connect
Políticas basadas en identidad	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	Sí
Roles vinculados al servicio	No

Para obtener una perspectiva general sobre cómo funcionan Direct Connect y otros servicios de AWS con las características de IAM, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidades de Direct Connect

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 identidad 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 obtener más información sobre los elementos que puede utilizar en una política JSON, consulte Referencia de los elementos de las políticas JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades de Direct Connect

Para ver ejemplos de políticas basadas en identidades de Direct Connect, consulte Ejemplos de políticas basadas en identidades de Direct Connect.

Políticas basadas en recursos en Direct Connect

Compatibilidad con las políticas basadas en recursos	No

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Las entidades 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 la entidad principal y el recurso se encuentran en Cuentas de AWS diferentes, un 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 en función de 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.

Acciones de políticas de Direct Connect

Admite acciones de política	Sí

Los administradores pueden utilizar las políticas JSON de AWS 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 permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS 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.

Para ver una lista de las acciones de Direct Connect, consulte Acciones definidas por Direct Connect en la Referencia de autorización del servicio.

Las acciones de políticas de Direct Connect utilizan el siguiente prefijo antes de la acción:

```
Direct Connect
```

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

```
"Action": [
      "Direct Connect:action1",
      "Direct Connect:action2"
         ]
```

Recursos de políticas de Direct Connect

Admite recursos de políticas	Sí

Los administradores pueden utilizar las políticas JSON de AWS 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": "*"
```

Para ver una lista de los tipos de recursos de Direct Connect y sus ARN, consulte Recursos definidos por Direct Connect en la Referencia de la API de AWS Direct Connect. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por Direct Connect.

Para ver ejemplos de políticas basadas en identidades de Direct Connect, consulte Ejemplos de políticas basadas en identidades de Direct Connect.

Para ver ejemplos de políticas basadas en recursos de Direct Connect, consulte Ejemplos de políticas basadas en identidades de Direct Connect que utilizan condiciones basadas en etiquetas.

Claves de condición de políticas de Direct Connect

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden utilizar las políticas JSON de AWS 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 lógica `AND`. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación `OR` 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 globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del Usuario de IAM.

Para ver una lista de claves de condición de Direct Connect, consulte Claves de condición de Direct Connect en la Referencia de la API de AWS Direct Connect. Para saber con qué acciones y recursos puede usar una clave de condición, consulte Acciones, recursos y claves de condición de Direct Connect en la Referencia de autorización de servicio.

Para ver ejemplos de políticas basadas en identidades de Direct Connect, consulte Ejemplos de políticas basadas en identidades de Direct Connect.

ACL en Direct Connect

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 Direct Connect

Admite ABAC (etiquetas en las políticas)	Parcial

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 entidades de IAM (usuarios o roles) y a muchos recursos de AWS. 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.

Uso de credenciales temporales con Direct Connect

Admite el uso de credenciales temporales	Sí

Algunos Servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre qué Servicios de AWS funcionan con credenciales temporales, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

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

Puede crear credenciales temporales de forma manual mediante la AWS CLI o la API de AWS. A continuación, puede usar esas credenciales temporales para acceder a AWS. AWS recomienda

generar credenciales temporales de forma dinámica en lugar de usar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Permisos de entidad principal entre servicios de Direct Connect

Admite Forward access sessions (FAS)	Sí

Cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o 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.

Roles de servicio de Direct Connect

Compatible con roles de servicio	Sí

Un rol del servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Direct Connect. Edite los roles de servicio solo cuando Direct Connect proporcione orientación para hacerlo.

Roles vinculados a servicios para Direct Connect

Admite roles vinculados a servicios	No

Un rol vinculado a servicios 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 a servicios aparecen en la cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidades de Direct Connect

De forma predeterminada, los usuarios y los roles no tienen permiso para crear ni modificar los recursos de Direct Connect. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API de AWS. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles, y los usuarios pueden asumirlos.

Para obtener información sobre cómo crear una política basada en identidad 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.

A fin de obtener más información sobre las acciones y los tipos de recursos definidos por Direct Connect, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Direct Connect en la Referencia de autorizaciones de servicio.

Temas

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, abrir o eliminar los recursos de Direct Connect de la cuenta. Estas acciones pueden generar costes adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas administradas de AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas administradas de AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para los casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las políticas administradas de AWS o las políticas administradas de AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía de usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado, como por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Use el Analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el Analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El Analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. xPara más información, consulte la política de validación del Analizador de acceso de IAM en la Guía de usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus

políticas. Para obtener más información, consulte Configuración de acceso a una API protegida por MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Acciones, recursos y condiciones de Direct Connect

Con las políticas basadas en identidad 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. Direct Connect admite acciones, claves de condiciones y recursos específicos. Para obtener información sobre todos los elementos que utiliza en una política JSON, consulte Referencia de los elementos de las políticas JSON de IAM en la Guía del usuario de IAM.

Acciones

Los administradores pueden utilizar las políticas JSON de AWS 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 permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS 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.

Las acciones de políticas de Direct Connect utilizan el siguiente prefijo antes de la acción: `directconnect:`. Por ejemplo, para conceder a alguien permiso para ejecutar una instancia de Amazon EC2 con la operación `DescribeVpnGateways` de la API de Amazon EC2, debe incluir la acción `ec2:DescribeVpnGateways` en la política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. Direct Connect define su propio conjunto de acciones que describen las tareas que se pueden realizar con este servicio.

El siguiente ejemplo de política concede acceso de lectura a AWS Direct Connect.

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

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

El siguiente ejemplo de política concede acceso total a AWS Direct Connect.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

Para ver una lista de las acciones de Direct Connect, consulte Acciones definidas por Direct Connect en la Guía del usuario de IAM.

Recursos

Los administradores pueden utilizar las políticas JSON de AWS 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": "*"
```

Direct Connect utiliza los siguientes ARN:

ARN de recursos de Direct Connect

Tipo de recurso	ARN
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`
dx-vif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`

Para obtener más información acerca del formato de los ARN, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de servicios de AWS.

Por ejemplo, para especificar la interfaz `dxcon-11aa22bb` en su instrucción, utilice el siguiente ARN:

```
"Resource": "arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb
```

Para especificar todas las interfaces virtuales que pertenecen a una cuenta específica, utilice el carácter comodín (*):

```
"Resource": "arn:aws:directconnect:*:*:dxvif/*"
```

Algunas acciones de Direct Connect, como las empleadas para la creación de recursos, no se pueden llevar a cabo en un recurso específico. En dichos casos, debe utilizar el carácter comodín (*).

```
"Resource": "*"
```

Para ver una lista de los tipos de recursos de Direct Connect y sus ARN, consulte Tipos de recursos definidos por AWS Direct Connect en la Guía del usuario de IAM. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte SERVICE-ACTIONS-URL;.

Claves de condición

Los administradores pueden utilizar las políticas JSON de AWS 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 lógica `AND`. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación `OR` 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 globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del Usuario de IAM.

Direct Connect define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Puede utilizar claves de condición con el recurso de etiqueta. Para obtener más información, consulte Ejemplo: restricción del acceso a una región específica.

Para ver una lista de claves de condición de Direct Connect, consulte Claves de condición de Direct Connect en la Guía del usuario de IAM. Para obtener información sobre las acciones y los recursos con los que puede utilizar una clave de condición, consulte SERVICE-ACTIONS-URL;.

Uso de la consola de Direct Connect

Para acceder a la consola de Direct Connect, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle registrar y consultar los detalles acerca de los recursos de Direct Connect en su cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

Para asegurarse de que esas entidades puedan seguir utilizando la consola de Direct Connect, asocie también la siguiente política administrada de AWS a las entidades. Para obtener más información, consulte Agregar de permisos a un usuario en la Guía del usuario de IAM.

```
directconnect
```

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para realizar esta acción en la consola o mediante programación con la AWS CLI o la API de AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
```

```
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Acceso de solo lectura a AWS Direct Connect

El siguiente ejemplo de política concede acceso de lectura a AWS Direct Connect.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

Acceso completo a AWS Direct Connect

El siguiente ejemplo de política concede acceso total a AWS Direct Connect.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

Ejemplos de políticas basadas en identidades de Direct Connect que utilizan condiciones basadas en etiquetas

Puede controlar el acceso a los recursos y las solicitudes mediante condiciones de clave de etiqueta. También puede utilizar una condición en su política de IAM para controlar si se pueden utilizar claves de etiqueta específicas en un recurso o en una solicitud.

Para obtener información sobre el uso de etiquetas con políticas de IAM, consulte Control del acceso con etiquetas en la Guía del usuario de IAM.

Asociación de interfaces virtuales de Direct Connect basada en etiquetas

En el ejemplo siguiente se muestra cómo puede crear una política que permita asociar una interfaz virtual solo si la etiqueta contiene la clave de entorno y los valores preprod o production.

```
       {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Action": [
            "directconnect:AssociateVirtualInterface"
          ],
```

```
        "Resource": "arn:aws:directconnect:*:*:dxvif/*",
        "Condition": {
          "StringEquals": {
            "aws:ResourceTag/environment": [
              "preprod",
              "production"
            ]
          }
        }
      },
      {
        "Effect": "Allow",
        "Action": "directconnect:DescribeVirtualInterfaces",
        "Resource": "*"
      }
    ]
}
```

Control del acceso a solicitudes basado en etiquetas

Puede utilizar condiciones en sus políticas de IAM para controlar qué pares de clave-valor de etiqueta se pueden pasar en una solicitud que etiquete un recurso de AWS. En el siguiente ejemplo, se muestra cómo se puede crear una política que permita utilizar la AWS Direct Connect TagResource acción para adjuntar etiquetas a una interfaz virtual únicamente si la etiqueta contiene la clave de entorno y los valores de preproducción o producción. Le recomendamos que utilice el modificador `ForAllValues` con la clave de condición `aws:TagKeys` para indicar que solo se permite la clave environment en la solicitud.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "directconnect:TagResource",
        "Resource": "arn:aws:directconnect:*:*:dxvif/*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/environment": [
                    "preprod",
                    "production"
                ]
            },
```

```
                "ForAllValues:StringEquals": {"aws:TagKeys": "environment"}
            }
        }
    }
```

Control de claves de etiqueta

Puede utilizar una condición en sus políticas de IAM para controlar si se pueden utilizar claves de etiqueta específicas en un recurso o en una solicitud.

En el ejemplo siguiente se muestra cómo puede crear una política que le permita etiquetar recursos, pero solo con la clave de etiqueta environment.

```
 {
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "directconnect:TagResource",
    "Resource": "*",
    "Condition": {
      "ForAllValues:StringEquals": {
        "aws:TagKeys": [
          "environment"
        ]
      }
    }
  }
}
```

Roles vinculados a servicios de AWS Direct Connect

AWS Direct Connect utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a AWS Direct Connect. Los roles vinculados a servicios están predefinidos por AWS Direct Connect e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

Con una función vinculada a servicios, resulta más sencillo configurar AWS Direct Connect, porque no es preciso agregar los permisos necesarios manualmente. AWS Direct Connect define los permisos de las funciones vinculadas con su propio servicio y, a menos que esté definido de otra

manera, solo AWS Direct Connect puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo puede eliminar una función vinculada a un servicio después de eliminar sus recursos relacionados. De esta forma, se protegen los recursos de AWS Direct Connect, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Yes (Sí) en la columna Service Linked Role (Rol vinculado a servicios). Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios de AWS Direct Connect

AWS Direct Connect utiliza el rol vinculado al servicio denominado `AWSServiceRoleForDirectConnect`. Esto permite a AWS Direct Connect recuperar los secretos de MACSec almacenados en AWS Secrets Manager en su nombre.

El rol vinculado a servicios `AWSServiceRoleForDirectConnect` confía en los siguientes servicios para asumir el rol:

- `directconnect.amazonaws.com`

El rol vinculado al servicio `AWSServiceRoleForDirectConnect` utiliza la política administrada `AWSDirectConnectServiceRolePolicy`.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para que el rol vinculado al servicio `AWSServiceRoleForDirectConnect` se cree correctamente, la identidad de IAM con la que se utiliza AWS Direct Connect debe tener los permisos necesarios. Para conceder los permisos necesarios, asocie la siguiente política a la identidad de IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Condition": {
```

```
                "StringLike": {
                    "iam:AWSServiceName": "directconnect.amazonaws.com"
                }
            },
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "iam:GetRole",
            "Effect": "Allow",
            "Resource": "*"
       }
    ]
}
```

Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado a un servicio de AWS Direct Connect

No es necesario que cree de forma manual un rol vinculado al servicio. AWS Direct Connect crea el rol vinculado al servicio en su nombre. Al ejecutar el comando `associate-mac-sec-key`, AWS crea un rol vinculado al servicio que permite a AWS Direct Connect recuperar los secretos de MACSec que se encuentran almacenados en su nombre en AWS Secrets Manager en la AWS Management Console, la AWS CLI o la API de AWS.

> **Important**
>
> Este rol vinculado al servicio puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. AWS Direct Connect vuelve a crear el rol vinculado al servicio en su nombre.

También puede utilizar la consola de IAM para crear un rol vinculado al servicio con el caso de uso de AWS Direct Connect. En la AWS CLI o la API de AWS, cree un rol vinculado al servicio con el nombre de servicio `directconnect.amazonaws.com`. Para obtener más información, consulte

Creación de un rol vinculado a un servicio en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Modificación de un rol vinculado a un servicio de AWS Direct Connect

AWS Direct Connect no le permite editar el rol vinculado a servicios `AWSServiceRoleForDirectConnect`. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción del rol utilizando IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio de AWS Direct Connect

No es necesario eliminar manualmente el rol de `AWSServiceRoleForDirectConnect`. Al eliminar el rol vinculado al servicio, debe eliminar todos los recursos asociados que se encuentran almacenados en el servicio web de AWS Secrets Manager. Si utiliza la AWS Management Console, la AWS CLI o la API de AWS, AWS Direct Connect elimina los recursos y el rol vinculado al servicio de forma automática.

También puede utilizar la consola de IAM para eliminar el rol vinculado al servicio. Para ello, primero debe eliminar de forma manual los recursos del rol vinculado al servicio y luego podrá eliminarlo.

> **Note**
>
> Si el servicio AWS Direct Connect está utilizando el rol cuando intenta eliminar los recursos, la eliminación puede producir un error. En ese caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de AWS Direct Connect que se utilizan en **`AWSServiceRoleForDirectConnect`**

1. Elimine la asociación entre todas las claves y conexiones de MACSec. Para obtener más información, consultar the section called “Eliminar la asociación entre una clave secreta de MACsec y una conexión”
2. Elimine la asociación entre todas las claves de MACSec y LAG. Para obtener más información, consultar the section called “Eliminar la asociación entre una clave secreta de MACsec y un LAG”

Para eliminar manualmente el rol vinculado al servicio mediante IAM

Puede usar la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado a un servicio `AWSServiceRoleForDirectConnect`. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a un servicio de AWS Direct Connect

AWS Direct Connect admite el uso de roles vinculados al servicio en todas las Regiones de AWS en las que se encuentra disponible la característica de seguridad de MAC. Para obtener más información, consulte Ubicaciones de AWS Direct Connect.

Políticas administradas de AWS para AWS Direct Connect

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes, por lo que puede empezar a asignar permisos a los usuarios, grupos y roles.

Considere que es posible que las políticas administradas por AWS no concedan permisos de privilegio mínimo para los casos de uso concretos, ya que están disponibles para que las utilicen todos los clientes de AWS. Se recomienda definir políticas administradas por el cliente específicas para los casos de uso a fin de reducir aún más los permisos.

No puede cambiar los permisos definidos en las políticas administradas de AWS. Si AWS actualiza los permisos definidos en una política administrada de AWS, la actualización afecta a todas las identidades de entidades principales (usuarios, grupos y roles) a las que está adjunta la política. Lo más probable es que AWS actualice una política administrada de AWS cuando se lance un nuevo Servicio de AWS o las operaciones de la API nuevas estén disponibles para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AWSpolítica gestionada: AWSDirectConnectFullAccess

Puede adjuntar la política de `AWSDirectConnectFullAccess` a las identidades de IAM. Esta política otorga permisos que brindan acceso completo a AWS Direct Connect.

Para ver los permisos de esta política, consulte AWSDirectConnectFullAccess en la AWS Management Console.

AWSpolítica gestionada: AWSDirectConnectReadOnlyAccess

Puede adjuntar la política de `AWSDirectConnectReadOnlyAccess` a las identidades de IAM. Esta política otorga permisos que brindan acceso de solo lectura a AWS Direct Connect.

Para ver los permisos de esta política, consulte AWSDirectConnectReadOnlyAccess en la AWS Management Console.

AWSpolítica gestionada: AWSDirectConnectServiceRolePolicy

Esta política se adjunta a la función vinculada al servicio denominada AWSServiceRoleForDirectConnectAWS Direct Connectpara permitir recuperar los secretos de seguridad de MAC en su nombre. Para más información, consulte the section called “Roles vinculados a servicios”.

Para ver los permisos de esta política, consulte AWSDirectConnectServiceRolePolicy en la AWS Management Console.

Actualizaciones de AWS Direct Connect a las políticas administradas de AWS

Consulte los detalles relativos a las actualizaciones de las políticas administradas de AWS para AWS Direct Connect desde que este servicio empezara a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre cambios en esta página, suscríbase a la fuente RSS en la página de historial de documentos AWS Direct Connect.

Cambio	Descripción	Fecha
AWSDirectConnectServiceRolePolicy: política nueva	Para respaldar la seguridad de MAC, se agregó la AWSServiceRoleForDirectConnectfunción vinculada al servicio.	31 de marzo de 2021
AWS Direct Connect comenzó el seguimiento de los cambios	AWS Direct Connect comenzó el seguimiento de los cambios de las políticas administradas de AWS.	31 de marzo de 2021

Solución de problemas de identidad y acceso de Direct Connect

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Direct Connect e IAM.

Temas

No tengo autorización para realizar una acción en Direct Connect

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `directconnect:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 directconnect:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `directconnect:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar iam: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas se deben actualizar para permitirle pasar un rol a Direct Connect.

Algunos Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado a servicios. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Direct Connect. Sin embargo, la acción requiere que el servicio cuente con permisos que concede un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de Direct Connect

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulte lo siguiente:

- Para obtener información acerca de si Direct Connect admite estas características, consulte Funcionamiento de Direct Connect con IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte Cómo proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos a Cuentas de AWS de terceros, consulte Cómo proporcionar acceso a Cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Cómo proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del usuario de IAM.

- Para obtener información sobre 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.

Registro y monitoreo en AWS Direct Connect

Puede utilizar las siguientes herramientas de monitorización automatizado para vigilar AWS Direct Connect e informar cuando haya algún problema:

- Alarmas de Amazon CloudWatch: vea una sola métrica determinada durante el periodo especificado. Realiza una o varias acciones según el valor de la métrica con respecto a un umbral dado durante varios períodos de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS. Las alarmas de CloudWatch no invocan acciones tan solo por tener un estado determinado; es necesario que el estado haya cambiado y se mantenga durante un número específico de periodos. Para obtener más información, consulte Monitorización con Amazon CloudWatch.
- Monitoreo de registros de AWS CloudTrail: comparta archivos de registro entre cuentas y monitoree archivos de registro de CloudTrail en tiempo real mediante su envío a Registros de CloudWatch. También puede escribir aplicaciones de procesamiento de registros en Java y validar que los archivos de registro no hayan cambiado después de la entrega de CloudTrail. Para obtener más información, consulte Registro de llamadas a la API de AWS Direct Connect mediante AWS CloudTrail y Trabajo con archivos de registro de CloudTrail en la Guía del usuario de AWS CloudTrail.

Para obtener más información, consulte Supervisión.

Validación de conformidad para AWS Direct Connect

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

  > **Note**
  >
  > No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.

- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en AWS Direct Connect

La infraestructura global de AWS se compone de regiones de AWS y zonas de disponibilidad de AWS. Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las regiones y zonas de disponibilidad de AWS, consulte Infraestructura global de AWS.

Además de la infraestructura global de AWS, AWS Direct Connect ofrece varias características que le ayudan con sus necesidades de resiliencia y copia de seguridad de los datos.

Para obtener información sobre cómo utilizar la VPN con AWS Direct Connect, consulte AWS Direct Connect más VPN.

Conmutación por error

AWS Direct Connect Resiliency Toolkit proporciona un asistente de conexión con varios modelos de resiliencia que lo ayuda a solicitar conexiones dedicadas para alcanzar su objetivo de SLA. Seleccione un modelo de resiliencia y AWS Direct Connect Resiliency Toolkit lo guiará a través del proceso de solicitud de conexiones dedicadas. Los modelos de resiliencia están diseñados para garantizar que dispone del número adecuado de conexiones dedicadas en varias ubicaciones.

- Resiliencia máxima: puede conseguir la resiliencia máxima para cargas de trabajo críticas mediante el uso de conexiones independientes que terminan en dispositivos independientes en más de una ubicación. Este modelo proporciona resistencia frente a errores de dispositivo, conectividad y ubicación completa.
- Alta resiliencia: puede conseguir una resiliencia alta para cargas de trabajo críticas mediante el uso de dos conexiones únicas a varias ubicaciones. Este modelo proporciona resiliencia frente a

errores de conectividad provocados por un corte de fibra o un error del dispositivo. También ayuda a evitar un error completo en la ubicación.

- Desarrollo y pruebas: puede conseguir resiliencia de desarrollo y pruebas para cargas de trabajo no críticas mediante el uso de conexiones independientes que terminan en dispositivos independientes en una ubicación. Este modelo proporciona resiliencia frente a errores de dispositivos, pero no ofrece resiliencia frente a errores de ubicación.

Para obtener más información, consulte ¿Cómo usar el kit de herramientas AWS Direct Connect de resiliencia para empezar.

Seguridad de la infraestructura en AWS Direct Connect

Como se trata de un servicio administrado, AWS Direct Connect se encuentra protegido por los procedimientos de seguridad de la red global de AWS. Puede utilizar llamadas a la API publicadas en AWS para obtener acceso a AWS Direct Connect a través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.2 o una versión posterior. Nosotros recomendamos TLS 1.3. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad de seguridad de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Puede llamar a estas operaciones de la API desde cualquier ubicación de red, pero AWS Direct Connect admite políticas de acceso basadas en recursos, que pueden incluir restricciones en función de la dirección IP de origen. También puede utilizar políticas de AWS Direct Connect para controlar el acceso desde puntos de enlace específicos de Amazon Virtual Private Cloud (Amazon VPC) o VPC específicas. Este proceso aísla con eficacia el acceso de red a un recurso de AWS Direct Connect determinado únicamente desde la VPC específica de la red de AWS. Por ejemplo, consulte the section called “Ejemplos de políticas basadas en identidades”.

Seguridad del protocolo de puerta de enlace fronteriza (BGP)

La Internet depende en gran medida del BGP para enrutar la información entre los sistemas de red. El enrutamiento del BGP a veces puede ser susceptible a ataques maliciosos o al secuestro del

BGP. Para conocer cómo AWS protege su red de forma más segura contra el secuestro del BGP, consulte Cómo AWS ayuda a proteger el enrutamiento de Internet.

Utilización de la AWS CLI

Puede utilizar la AWS CLI para crear y trabajar con los recursos de AWS Direct Connect.

El ejemplo siguiente utiliza los comandos de la AWS CLI para crear una conexión de AWS Direct Connect. También puede descargar la Carta de autorización y Asignación de instalaciones de conexión (LOA-CFA) o aprovisionar una interfaz virtual pública o privada.

Antes de comenzar, asegúrese de que ha instalado y configurado la AWS CLI. Para obtener más información, consulte la Guía del usuario de AWS Command Line Interface.

Contenido

Paso 1: Crear una conexión

El primer paso es enviar una solicitud de conexión. Asegúrese de que conoce la velocidad de puerto que necesita y la ubicación de AWS Direct Connect. Para obtener más información, consulte AWS Direct Connect conexiones.

Para crear una solicitud de conexión

1. Describa las ubicaciones de AWS Direct Connect de su región actual. En el documento de salida devuelto, busque el código de ubicación de la ubicación en la que desea establecer la conexión.

```
aws directconnect describe-locations
```

```
{
    "locations": [
        {
            "locationName": "City 1, United States",
            "locationCode": "Example Location 1"
        },
        {
            "locationName": "City 2, United States",
            "locationCode": "Example location"
```

```
        }
    ]
}
```

2. Cree la conexión y especifique un nombre, la velocidad de puerto y el código de ubicación. En el documento de salida devuelto, busque y anote el ID de la conexión. Necesitará el ID para obtener el documento LOA-CFA en el siguiente paso.

```
aws directconnect create-connection --location Example location --bandwidth 1Gbps
 --connection-name "Connection to AWS"
```

```
{
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-EXAMPLE",
    "connectionState": "requested",
    "bandwidth": "1Gbps",
    "location": "Example location",
    "connectionName": "Connection to AWS",
    "region": "sa-east-1"
}
```

Paso 2: Descargar el documento LOA-CFA

Una vez que haya solicitado la conexión, podrá obtener el documento LOA-CFA mediante el comando `describe-loa`. El resultado aparece codificado en base64. Debe extraer el contenido relevante de la LOA, decodificarlo y generar un archivo PDF.

Para obtener el documento LOA-CFA a través de Linux o macOS

En este ejemplo, la última parte del comando decodifica el contenido mediante la utilidad base64 y envía el resultado a un archivo PDF.

```
aws directconnect describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent|base64 --decode > myLoaCfa.pdf
```

Para obtener el documento LOA-CFA mediante Windows

En este ejemplo, el resultado se extrae a un archivo llamado myLoaCfa.base64. El segundo comando utiliza la utilidad `certutil` para decodificar el archivo y enviar el resultado a un archivo PDF.

```
aws directconneawsct describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent > myLoaCfa.base64
```

```
certutil -decode myLoaCfa.base64 myLoaCfa.pdf
```

Una vez que haya descargado el documento LOA-CFA, envíeselo a su proveedor de red o de coubicación.

Paso 3: Crear una interfaz virtual y obtener la configuración del enrutador

Una vez que haya solicitado una conexión de AWS Direct Connect, deberá crear una interfaz virtual para empezar a utilizarla. Puede crear una interfaz virtual privada para conectarla a la VPC. O bien, puede crear una interfaz virtual pública para conectarse a los servicios de AWS que no están incluidos en una VPC. Puede crear una interfaz virtual compatible con el tráfico IPv6 o IPv4.

Antes de comenzar, asegúrese de que ha leído todos los requisitos previos que detallan en Requisitos previos de las interfaces virtuales.

Al crear una interfaz virtual mediante la AWS CLI, el resultado incluye información genérica sobre la configuración del router. Para crear una configuración de router específica para su dispositivo, utilice la consola de AWS Direct Connect. Para obtener más información, consulte Descargar el archivo de configuración del enrutador.

Para crear una interfaz virtual privada

1. Obtenga el ID de la gateway privada virtual (vgw-xxxxxxxx) adjunta a la VPC. Necesita el ID para crear la interfaz virtual en el siguiente paso.

   ```
   aws ec2 describe-vpn-gateways
   ```

   ```
   {
       "VpnGateways": [
           {
               "State": "available",
               "Tags": [
                   {
                       "Value": "DX_VGW",
   ```

```
                    "Key": "Name"
                }
            ],
            "Type": "ipsec.1",
            "VpnGatewayId": "vgw-ebaa27db",
            "VpcAttachments": [
                {
                    "State": "attached",
                    "VpcId": "vpc-24f33d4d"
                }
            ]
        }
    ]
}
```

2. Cree una interfaz virtual privada. Debe especificar un nombre, un ID de VLAN y un número de sistema autónomo (ASN) de BGP.

   Para el tráfico IPv4, necesita direcciones IPv4 privadas para cada extremo de la sesión de intercambio de tráfico BGP. Puede especificar sus propias direcciones IPv4 o de dejar que Amazon genera las direcciones por usted. En el siguiente ejemplo, las direcciones IPv4 se generan por usted.

```
aws directconnect create-private-virtual-interface --
connection-id dxcon-fg31dyv6 --new-private-virtual-interface
 virtualInterfaceName=PrivateVirtualInterface,vlan=101,asn=65000,virtualGatewayId=vgw-
ebaa27db,addressFamily=ipv4
```

```
{
    "virtualInterfaceState": "pending",
    "asn": 65000,
    "vlan": 101,
    "customerAddress": "192.168.1.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "vgw-ebaa27db",
    "virtualInterfaceId": "dxvif-ffhhk74f",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [],
    "location": "Example location",
    "bgpPeers": [
```

```
        {
            "bgpStatus": "down",
            "customerAddress": "192.168.1.2/30",
            "addressFamily": "ipv4",
            "authKey": "asdf34example",
            "bgpPeerState": "pending",
            "amazonAddress": "192.168.1.1/30",
            "asn": 65000
        }
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=
\"UTF-8\"?>\n<logical_connection id=\"dxvif-ffhhk74f\">\n  <vlan>101</
vlan>\n  <customer_address>192.168.1.2/30</customer_address>\n
 <amazon_address>192.168.1.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>private</connection_type>\n</
logical_connection>\n",
    "amazonAddress": "192.168.1.1/30",
    "virtualInterfaceType": "private",
    "virtualInterfaceName": "PrivateVirtualInterface"
}
```

Para crear una interfaz virtual privada que sea compatible con el tráfico IPv6, utilice el mismo comando que antes y defina en `ipv6` el parámetro `addressFamily`. No puede especificar sus propias direcciones IPv6 para la sesión de intercambio de tráfico BGP; Amazon es quien le asigna las direcciones IPv6.

3. Para ver la información de configuración del router en formato XML, describa la interfaz virtual que ha creado. Utilice el parámetro `--query` para extraer la información `customerRouterConfig` y el parámetro `--output` para organizar el texto en líneas delimitadas por tabulaciones.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-ffhhk74f
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-ffhhk74f">
  <vlan>101</vlan>
  <customer_address>192.168.1.2/30</customer_address>
  <amazon_address>192.168.1.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
```

```
  <connection_type>private</connection_type>
</logical_connection>
```

Para crear una interfaz virtual pública

1. Para crear una interfaz virtual pública, debe especificar un nombre, un ID de VLAN y un número de sistema autónomo (ASN) de BGP.

   Para el tráfico IPv4, debe especificar direcciones IPv4 públicas para cada extremo de la sesión de intercambio de tráfico BGP y las rutas IPv4 públicas que comunicará a través de BGP. El siguiente ejemplo crea una interfaz virtual pública para el tráfico IPv4.

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,amazonAddress=203.0.113.1/
{cidr=203.0.113.4/30}]
```

```
{
    "virtualInterfaceState": "verifying",
    "asn": 65000,
    "vlan": 2000,
    "customerAddress": "203.0.113.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "",
    "virtualInterfaceId": "dxvif-fgh0hcrk",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [
        {
            "cidr": "203.0.113.0/30"
        },
        {
            "cidr": "203.0.113.4/30"
        }
    ],
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
            "customerAddress": "203.0.113.2/30",
```

```
            "addressFamily": "ipv4",
            "authKey": "asdf34example",
            "bgpPeerState": "verifying",
            "amazonAddress": "203.0.113.1/30",
            "asn": 65000
        }
    ],
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>\n<logical_connection id=\"dxvif-fgh0hcrk\">\n  <vlan>2000</
vlan>\n  <customer_address>203.0.113.2/30</customer_address>\n
 <amazon_address>203.0.113.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>public</connection_type>\n</logical_connection>
\n",
    "amazonAddress": "203.0.113.1/30",
    "virtualInterfaceType": "public",
    "virtualInterfaceName": "PublicVirtualInterface"
}
```

Para crear una interfaz virtual pública que sea compatible con el tráfico IPv6, puede especificar las rutas IPv6 que comunicará a través de BGP. No puede especificar direcciones IPv6 para la sesión de intercambio de tráfico BGP; Amazon es quien le asigna las direcciones IPv6. El siguiente ejemplo crea una interfaz virtual pública para el tráfico IPv6.

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,addressFamily=ipv6,routeFi
{cidr=2001:db8:64ce:ba01::/64}]
```

2. Para ver la información de configuración del router en formato XML, describa la interfaz virtual que ha creado. Utilice el parámetro `--query` para extraer la información `customerRouterConfig` y el parámetro `--output` para organizar el texto en líneas delimitadas por tabulaciones.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-fgh0hcrk
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-fgh0hcrk">
  <vlan>2000</vlan>
```

```
  <customer_address>203.0.113.2/30</customer_address>
  <amazon_address>203.0.113.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>public</connection_type>
</logical_connection>
```

Registro de llamadas a la API de AWS Direct Connect mediante AWS CloudTrail

AWS Direct Connect se integra con AWS CloudTrail, un servicio que proporciona un registro de las acciones hechas por un usuario, un rol o un servicio de AWS en AWS Direct Connect. CloudTrail captura las llamadas a la API de AWS Direct Connect como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de AWS Direct Connect y las llamadas desde el código a las operaciones de la API de AWS Direct Connect. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos para AWS Direct Connect. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a AWS Direct Connect, la dirección IP desde la que se realizó, quién la realizó y cuándo, etc.

Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Información de AWS Direct Connect en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad en AWS Direct Connect, esa actividad se registra en un evento de CloudTrail junto con otros eventos de servicio de AWS en Event history (Historial de eventos). Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de eventos en la cuenta de AWS, incluidos los eventos de AWS Direct Connect, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail

- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail de varias regiones y Recibir archivos de registro de CloudTrail de varias cuentas

Todas las acciones de AWS Direct Connect las registra CloudTrail y se documentan en la Referencia de la API de AWS Direct Connect. Por ejemplo, las llamadas a las acciones `CreateConnection` y `CreatePrivateVirtualInterface` generan entradas en los archivos de registros de CloudTrail.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de AWS Identity and Access Management (usuario de IAM) o de usuario raíz.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte Elemento `userIdentity` de CloudTrail.

Descripción de las entradas de los archivos de registro de AWS Direct Connect

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

A continuación se muestran ejemplos de registros de CloudTrail para AWS Direct Connect.

Example Ejemplo: CreateConnection

```
{
    "Records": [
    {
        "eventVersion": "1.0",
```

```
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:28:16Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreateConnection",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "location": "EqSE2",
            "connectionName": "MyExampleConnection",
            "bandwidth": "1Gbps"
        },
        "responseElements": {
            "location": "EqSE2",
            "region": "us-west-2",
            "connectionState": "requested",
            "bandwidth": "1Gbps",
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-fhajolyy",
            "connectionName": "MyExampleConnection"
        }
    },
    ...
  ]
}
```

Example Ejemplo: CreatePrivateVirtualInterface

```
{
    "Records": [
```

```
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:39:55Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreatePrivateVirtualInterface",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy",
            "newPrivateVirtualInterface": {
                "virtualInterfaceName": "MyVirtualInterface",
                "customerAddress": "[PROTECTED]",
                "authKey": "[PROTECTED]",
                "asn": -1,
                "virtualGatewayId": "vgw-bb09d4a5",
                "amazonAddress": "[PROTECTED]",
                "vlan": 123
            }
        },
        "responseElements": {
            "virtualInterfaceId": "dxvif-fgq61m6w",
            "authKey": "[PROTECTED]",
            "virtualGatewayId": "vgw-bb09d4a5",
            "customerRouterConfig": "[PROTECTED]",
            "virtualInterfaceType": "private",
            "asn": -1,
            "routeFilterPrefixes": [],
            "virtualInterfaceName": "MyVirtualInterface",
            "virtualInterfaceState": "pending",
```

```
            "customerAddress": "[PROTECTED]",
            "vlan": 123,
            "ownerAccount": "123456789012",
            "amazonAddress": "[PROTECTED]",
            "connectionId": "dxcon-fhajolyy",
            "location": "EqSE2"
        }
    },
    ...
  ]
}
```

Example Ejemplo: DescribeConnections

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:27:28Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeConnections",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": null,
        "responseElements": null
    },
    ...
  ]
```

```
}
```

Example Ejemplo: DescribeVirtualInterfaces

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:37:53Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeVirtualInterfaces",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy"
        },
        "responseElements": null
    },
    ...
  ]
}
```

AWS Direct Connect Recursos de monitoreo

La supervisión es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de los recursos de Direct Connect. Debe recopilar datos de supervisión de todas las partes de la AWS solución para poder depurar más fácilmente una falla multipunto en caso de que se produzca. Sin embargo, antes de empezar a monitorear Direct Connect, debe crear un plan de monitoreo que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la supervisión?
- ¿Qué recursos deben monitorizarse?
- ¿Con qué frecuencia debe monitorizar estos recursos?
- ¿Qué herramientas de monitorización puede utilizar?
- ¿Quién se encarga de realizar las tareas de monitorización?
- ¿Quién debería recibir una notificación cuando surjan problemas?

El siguiente paso es establecer una línea base para el rendimiento normal de Direct Connect en su entorno, midiendo el rendimiento en distintos momentos y bajo diferentes condiciones de carga. Mientras supervisa Direct Connect, almacene los datos históricos de supervisión. De este modo, puede compararlos con los datos de rendimiento actuales, identificar patrones de rendimiento normal y anomalías en el rendimiento, así como desarrollar métodos para la resolución de problemas.

Para establecer una línea base, debe supervisar el uso, el estado y el estado de las conexiones físicas de Direct Connect.

Contenido

Herramientas de monitoreo

AWS proporciona varias herramientas que puede utilizar para supervisar una AWS Direct Connect conexión. Puede configurar algunas de estas herramientas para que monitoricen por usted, pero otras herramientas requieren intervención manual. Le recomendamos que automatice las tareas de monitorización en la medida de lo posible.

Herramientas de monitoreo automatizadas

Puede usar las siguientes herramientas de monitoreo automatizadas para ver Direct Connect e informar cuando algo vaya mal:

- Amazon CloudWatch Alarms: observa una única métrica durante un período de tiempo que especifiques. Realiza una o varias acciones según el valor de la métrica con respecto a un umbral dado durante varios períodos de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS. CloudWatch las alarmas no invocan acciones simplemente porque se encuentran en un estado determinado; el estado debe haber cambiado y se ha mantenido durante un número específico de períodos. Para obtener información sobre las métricas y dimensiones disponibles, consulte Monitorización con Amazon CloudWatch.
- AWS CloudTrail Supervisión de registros: comparta archivos de registro entre cuentas y supervise los archivos de CloudTrail registro en tiempo real enviándolos a CloudWatch Logs. También puede escribir aplicaciones de procesamiento de registros en Java y validar que los archivos de registro no hayan cambiado después de la entrega por CloudTrail. Para obtener más información, consulte Registro de llamadas a la API de AWS Direct Connect mediante AWS CloudTrail y Trabajar con archivos de CloudTrail registro en la Guía del AWS CloudTrail usuario.

Herramientas de monitoreo manuales

Otra parte importante de la supervisión de una AWS Direct Connect conexión implica la supervisión manual de los elementos que CloudWatch las alarmas no cubren. Los paneles de Direct Connect y de la CloudWatch consola proporcionan una at-a-glance vista del estado de su AWS entorno.

- La AWS Direct Connect consola muestra:
  - Estado de la conexión (consulte la columna State)
  - Estado de la interfaz virtual (consulte la columna State)
- La página de CloudWatch inicio muestra:
  - Alarmas y estado actual
  - Gráficos de alarmas y recursos
  - Estado de los servicios

  Además, puede CloudWatch hacer lo siguiente:
  - Cree paneles personalizados para monitorizar los servicios que le interesen.

- Realizar un gráfico con los datos de las métricas para resolver problemas y descubrir tendencias.
- Busca y examina todas tus métricas AWS de recursos.
- Crear y editar las alarmas de notificación de problemas.

Monitorización con Amazon CloudWatch

Puede monitorear AWS Direct Connect las conexiones físicas y las interfaces virtuales mediante CloudWatch. CloudWatch recopila datos sin procesar de Direct Connect y los procesa para convertirlos en métricas legibles. De forma predeterminada, CloudWatch proporciona datos de métricas de Direct Connect en intervalos de 5 minutos.

Para obtener información detallada al respecto CloudWatch, consulta la Guía del CloudWatch usuario de Amazon. También puedes monitorear tus servicios CloudWatch para ver cuáles están consumiendo recursos. Para obtener más información, consulte AWS Servicios que publican CloudWatch métricas.

Contenido

AWS Direct Connect métricas y dimensiones

Las métricas están disponibles para las conexiones AWS Direct Connect físicas y las interfaces virtuales.

AWS Direct Connect Métricas de conexión

Las siguientes métricas están disponibles en las conexiones dedicadas de Direct Connect.

Métrica	Descripción
`ConnectionState`	El estado de la conexión.1 indica activa y 0 indica inactiva.

Métrica	Descripción
	Esta métrica está disponible para conexiones dedicadas y alojadas. **Note** Esta métrica también se encuentra disponibl e en las cuentas de propietario de la interfaz virtual alojada, al igual que en las cuentas de propietario de la conexión. Unidades: booleano
`ConnectionBpsEgress`	La velocidad de bits de los datos salientes desde el AWS lado de la conexión. El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especific ado (5 minutos de forma predeterminada y 1 minuto como mínimo). Puede cambiar el valor acumulado predeterminado. Es posible que esta métrica no esté disponible para una nueva conexión o cuando se reinicie un dispositi vo. La métrica se inicia cuando la conexión se utiliza para enviar o recibir tráfico. Unidades: bits por segundo

Métrica	Descripción
`ConnectionBpsIngress`	La velocidad de bits de los datos entrantes al AWS lado de la conexión. Es posible que esta métrica no esté disponible para una nueva conexión o cuando se reinicie un dispositivo. La métrica se inicia cuando la conexión se utiliza para enviar o recibir tráfico. Unidades: bits por segundo
`ConnectionPpsEgress`	La velocidad de paquetes de los datos salientes desde el AWS lado de la conexión. El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especificado (5 minutos de forma predeterminada y 1 minuto como mínimo). Puede cambiar el valor acumulado predeterminado. Es posible que esta métrica no esté disponible para una nueva conexión o cuando se reinicie un dispositivo. La métrica se inicia cuando la conexión se utiliza para enviar o recibir tráfico. Unidades: paquetes por segundo

Métrica	Descripción
`ConnectionPpsIngress`	La velocidad de paquetes de datos entrantes al AWS lado de la conexión. El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especific ado (5 minutos de forma predeterminada y 1 minuto como mínimo). Puede cambiar el valor acumulado predeterminado. Es posible que esta métrica no esté disponible para una nueva conexión o cuando se reinicie un dispositi vo. La métrica se inicia cuando la conexión se utiliza para enviar o recibir tráfico. Unidades: paquetes por segundo
`ConnectionCRCErrorCount`	Este recuento ya no está en uso. En su lugar, use `ConnectionErrorCount` .

Métrica	Descripción
`ConnectionErrorCount`	El recuento total de errores de todos los tipos de errores de nivel de MAC en el dispositivo de AWS . El total incluye errores de comprobación de redundancia cíclica (CRC). Esta métrica es el recuento de errores que se han producido desde el último punto de datos registrado. Cuando hay errores en la interfaz, la métrica muestra valores distintos de cero. Para obtener el recuento total de todos los errores del intervalo seleccionado en CloudWatch, por ejemplo, 5 minutos, aplique la estadística de «suma». Para obtener más informaci ón sobre cómo obtener la estadística de suma, consulta Cómo obtener estadísticas para una métrica en la Guía del CloudWatch usuario de Amazon. El valor de la métrica se establece en 0 cuando se detienen los errores en la interfaz. **Note** Esta métrica sustituye a `ConnectionCRCErrorCount` , que ya no se encuentra en uso. Unidades: recuento

Métrica	Descripción
`ConnectionLightLevelTx`	Indica el estado de la conexión de fibra para el tráfico saliente (de salida) procedente del AWS lado de la conexión. Hay dos dimensiones para esta métrica. Para obtener más información, consulte the section called “AWS Direct Connect dimensiones disponibles”. Unidades: dBm
`ConnectionLightLevelRx`	Indica el estado de la conexión de fibra para el tráfico entrante (de entrada) al AWS lado de la conexión. Hay dos dimensiones para esta métrica. Para obtener más información, consulte the section called “AWS Direct Connect dimensiones disponibles”. Unidades: dBm
`ConnectionEncryptionState`	Indica el estado del cifrado de la conexión. 1 indica que el cifrado de la conexión es up y 0 indica que es down. Cuando esta métrica se aplica a un LAG, 1 indica que todas las conexiones del LAG se encuentran cifradas up. 0 indica que al menos una conexión LAG se encuentra cifrada down.

AWS Direct Connect métricas de la interfaz virtual

Las siguientes métricas están disponibles en las interfaces AWS Direct Connect virtuales.

Métrica	Descripción
`VirtualInterfaceBpsEgress`	La velocidad de bits de los datos salientes desde el AWS lateral de la interfaz virtual.

Métrica	Descripción
	El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especificado (5 minutos de forma predeterminada). Unidades: bits por segundo
`VirtualInterfaceBpsIngress`	La velocidad de bits de los datos entrantes al AWS lateral de la interfaz virtual. El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especificado (5 minutos de forma predeterminada). Unidades: bits por segundo
`VirtualInterfacePpsEgress`	La velocidad de paquetes de los datos salientes desde el AWS lado de la interfaz virtual. El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especificado (5 minutos de forma predeterminada). Unidades: paquetes por segundo
`VirtualInterfacePpsIngress`	La velocidad de paquetes de los datos entrantes al AWS lado de la interfaz virtual. El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especificado (5 minutos de forma predeterminada). Unidades: paquetes por segundo

AWS Direct Connect dimensiones disponibles

Puede filtrar los AWS Direct Connect datos utilizando las siguientes dimensiones.

Dimensión	Descripción
`ConnectionId`	Esta dimensión está disponible en las métricas de la conexión Direct Connect y la interfaz virtual. Esta dimensión filtra los datos por conexión.
`OpticalLaneNumber`	Esta dimensión filtra los `ConnectionLightLevelTx` datos y los `ConnectionLightLevelRx` datos, y filtra los datos por el número de carril óptico de la conexión Direct Connect.
`VirtualInterfaceId`	Esta dimensión está disponible en las métricas de la interfaz virtual Direct Connect y filtra los datos por la interfaz virtual.

Visualización de AWS Direct Connect CloudWatch las métricas

AWS Direct Connect envía las siguientes métricas sobre sus conexiones de Direct Connect. CloudWatchA continuación, Amazon agrega estos puntos de datos en intervalos de 1 o 5 minutos. De forma predeterminada, los datos de las métricas de Direct Connect se escriben CloudWatch en intervalos de 5 minutos.

> **Note**
>
> Si estableces un intervalo de 1 minuto, Direct Connect hará todo lo posible por escribir las métricas para CloudWatch usar este intervalo, pero no siempre se puede garantizar.

Puede usar los siguientes procedimientos para ver las métricas de las conexiones de Direct Connect.

Para ver las métricas mediante la CloudWatch consola

Las métricas se agrupan en primer lugar por el espacio de nombres de servicio y, a continuación, por las diversas combinaciones de dimensiones dentro de cada espacio de nombres. Para obtener más información sobre cómo Amazon CloudWatch ver las métricas de Direct Connect, incluida la adición de funciones matemáticas o consultas prediseñadas, consulte Uso de Amazon CloudWatch métricas en la Guía del CloudWatch usuario de Amazon.

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.

2. En el panel de navegación, elija Metrics (Métricas) y, a continuación, All metrics (Todas las métricas).
3. En la sección de Métricas, elija DX.
4. Elija un ConnectionIdnombre de métrica y, a continuación, elija una de las siguientes opciones para definir mejor la métrica:

   - Agregar a la búsqueda: agrega esta métrica a los resultados de la búsqueda.
   - Solo buscar esta: solo busca esta métrica.
   - Eliminar del gráfico: elimina esta métrica del gráfico.
   - Solo graficar esta métrica: solo grafica esta métrica.
   - Graficar todos los resultados de la búsqueda: grafica todas las métricas.
   - Graficar con una consulta de SQL: abre Información de métricas: generador de consultas, que le permite elegir lo que desea graficar mediante la creación de una consulta de SQL. Para obtener más información sobre el uso de Metric Insights, consulta Consulta tus métricas con CloudWatch Metrics Insights en la Guía del CloudWatch usuario de Amazon.

Para ver las métricas mediante la AWS Direct Connect consola

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Connections (Conexiones).
3. Seleccione la conexión.
4. Elija la pestaña de Monitoreo para visualizar las métricas de su conexión.

Para ver las métricas mediante el AWS CLI

En el símbolo del sistema, ejecute el siguiente comando.

```
aws cloudwatch list-metrics --namespace "AWS/DX"
```

Crear CloudWatch alarmas para monitorear AWS Direct Connect las conexiones

Puede crear una CloudWatch alarma que envíe un mensaje de Amazon SNS cuando la alarma cambie de estado. Una alarma vigila una métrica determinada durante el periodo especificado. Envía

una notificación a un tema de Amazon SNS en función del valor de la métrica con respecto a un umbral determinado durante varios periodos de tiempo.

Por ejemplo, puede crear una alarma que monitorice el estado de una conexión de AWS Direct Connect . Envía una notificación cuando el estado de conexión esté inactivo durante cinco periodos consecutivos de un minuto. Para obtener más información sobre lo que debe saber para crear una alarma y obtener más información sobre cómo crear una alarma, consulte Uso de Amazon CloudWatch Alarms en la Guía del CloudWatch usuario de Amazon.

Para crear una CloudWatch alarma.

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Alarms (Alarmas) y, a continuación, elija All Alarms (Todas las alarmas).
3. Seleccione Crear alarma.
4. Elija Seleccionar métrica y, a continuación, elija DX.
5. Elija la métrica de Métricas de conexión.
6. Seleccione la AWS Direct Connect conexión y, a continuación, elija la métrica Seleccionar métrica.
7. En la página Especificar la métrica y las condiciones, configure los parámetros de la alarma. Para obtener información más específica sobre las métricas y las condiciones, consulte Uso de Amazon CloudWatch Alarms en la Guía del CloudWatch usuario de Amazon.
8. Seleccione Siguiente.
9. Configure las acciones de alarma en la página Configurar acciones. Para obtener más información sobre la configuración de las acciones de alarma, consulta Acciones de alarma en la Guía del CloudWatch usuario de Amazon.
10. Seleccione Siguiente.
11. En la página Agregar nombre y descripción, ingrese un Nombre y una Descripción de alarma opcional para describir esta alarma y, a continuación, elija Siguiente.
12. Verifique la alarma propuesta en la página Vista previa y creación.
13. Si es necesario, elija Editar para cambiar cualquier información y, a continuación, elija Crear alarma.

    En la página Alarmas se muestra una fila nueva con información sobre la alarma nueva. En el estado de Acciones se muestran las Acciones habilitadas, lo que indica que la alarma se encuentra activa.

AWS Direct Connect cuotas

En la siguiente tabla se enumeran las cuotas relacionadas con AWS Direct Connect.

Componente	Cuota	Comentarios
Interfaces virtuales públicas o privadas por conexión AWS Direct Connect dedicada	50	Este límite no se puede aumentar.
Interfaces virtuales de tránsito por conexión AWS Direct Connect dedicada	4	Este límite no se puede aumentar.
Interfaces virtuales privadas o públicas por conexión AWS Direct Connect dedicada e interfaces virtuales de tránsito por conexión AWS Direct Connect dedicada	51	Cuando se lanzó la AWS Direct Connect compatibilidad con Amazon VPC Transit Gateways, se añadió una cuota de una (1) interfaz virtual de tránsito a la cuota de 50 interfaces virtuales públicas o privadas por conexión dedicada. El número de interfaces virtuales de tránsito permitido ahora es de cuatro (4) y se tiene en cuenta para el máximo de 51 interface s virtuales por conexión dedicada. Este límite no se puede aumentar.
Interfaces virtuales privadas, públicas o de tránsito por AWS Direct Connect conexión alojada	1	Este límite no se puede aumentar.
AWS Direct Connect Conexiones activas por ubicación de Direct Connect por región y cuenta	10	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Número de interfaces virtuales por grupo de agregación de enlaces (LAG)	51	Cuando se lanzó la AWS Direct Connect compatibilidad con Amazon VPC Transit Gateways, se añadió una cuota de una (1) interfaz virtual de tránsito a la cuota

Componente	Cuota	Comentarios
		de 50 interfaces virtuales públicas o privadas por LAG. El número de interfaces virtuales de tránsito permitido ahora es de cuatro (4) y se tiene en cuenta para el máximo de 51 interfaces virtuales por LAG. Este límite no se puede aumentar.
Rutas por sesión de Border Gateway Protocol (BGP) en una interfaz virtual privada o en una interfaz virtual de tránsito desde una instalación local a otra. AWS Si anuncia más de 100 rutas cada una para IPv4 e IPv6 en la sesión de BGP, esta cambiará a un estado de inactividad con la sesión de BGP INACTIVA.	100 cada una para IPv4 e IPv6	Este límite no se puede aumentar.
Rutas por sesión de protocolo de gateway fronteriza (BGP) en una interfaz virtual pública	1 000	Este límite no se puede aumentar.

Componente	Cuota	Comentarios
Conexiones dedicadas por grupo de agregación de enlace (LAG)	4 cuando la velocidad del puerto es inferior a 100 G 2 cuando la velocidad del puerto es de 100 G	
Grupos de agregación de enlaces (LAG) por región	10	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
AWS Direct Connect puertas de enlace por cuenta	200	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Puertas de enlace privadas virtuales por puerta de enlace AWS Direct Connect	20	Este límite no se puede aumentar.
Pasarelas de tránsito por puerta de enlace AWS Direct Connect	6	Este límite no se puede aumentar.

Componente	Cuota	Comentarios
Interfaces virtuales (privadas o de tránsito) por AWS Direct Connect puerta de enlace	30	Este límite no se puede aumentar.
Número de prefijos por AWS Transit Gateway trayecto AWS y local en una interfaz virtual de tránsito	200 combinados en total para IPv4 e IPv6	Este límite no se puede aumentar.
Número de interfaces virtuales por puerta de enlace privada virtual	No hay límite.	
Número de puertas de enlace de Direct Connect asociadas a una puerta de enlace de tránsito	20	Este límite no se puede aumentar.
SiteLink límite de prefijos	100	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.

AWS Direct Connect admite estas velocidades de puerto a través de fibra monomodo: 1 Gbps: 1000BASE-LX (1310 nm), 10 Gbps: 10GBASE-LR (1310 nm) y 100 Gbps: 100GBASE-LR4.

Cuotas del BGP

Las siguientes son cuotas del BGP. Los temporizadores del BGP negocian hasta el valor más bajo entre los enrutadores. Los intervalos de la BFD los define el dispositivo más lento.

- Temporizador de retención predeterminado: 90 segundos
- Temporizador de retención mínimo: 3 segundos

  No se admite un valor de retención de 0.

- Temporizador de keepalive predeterminado: 30 segundos
- Temporizador de keepalive mínimo: 1 segundo
- Temporizador de reinicio fluido: 120 segundos

  Le recomendamos que no configure el reinicio fluido y la BFD de forma simultánea.
- Intervalo mínimo de detección de usuarios reales de la BFD: 300 ms
- Multiplicador mínimo de la BFD: 3

Consideraciones sobre el equilibrio de carga

Si desea utilizar el balanceo de carga con varias VIF públicas, todas las VIF deben estar en la misma región.

Solución de problemas AWS Direct Connect

La siguiente información de solución de problemas puede ayudarlo a diagnosticar y solucionar problemas con su conexión de AWS Direct Connect .

Contenido

Solución de problemas de capa 1 (físicos)

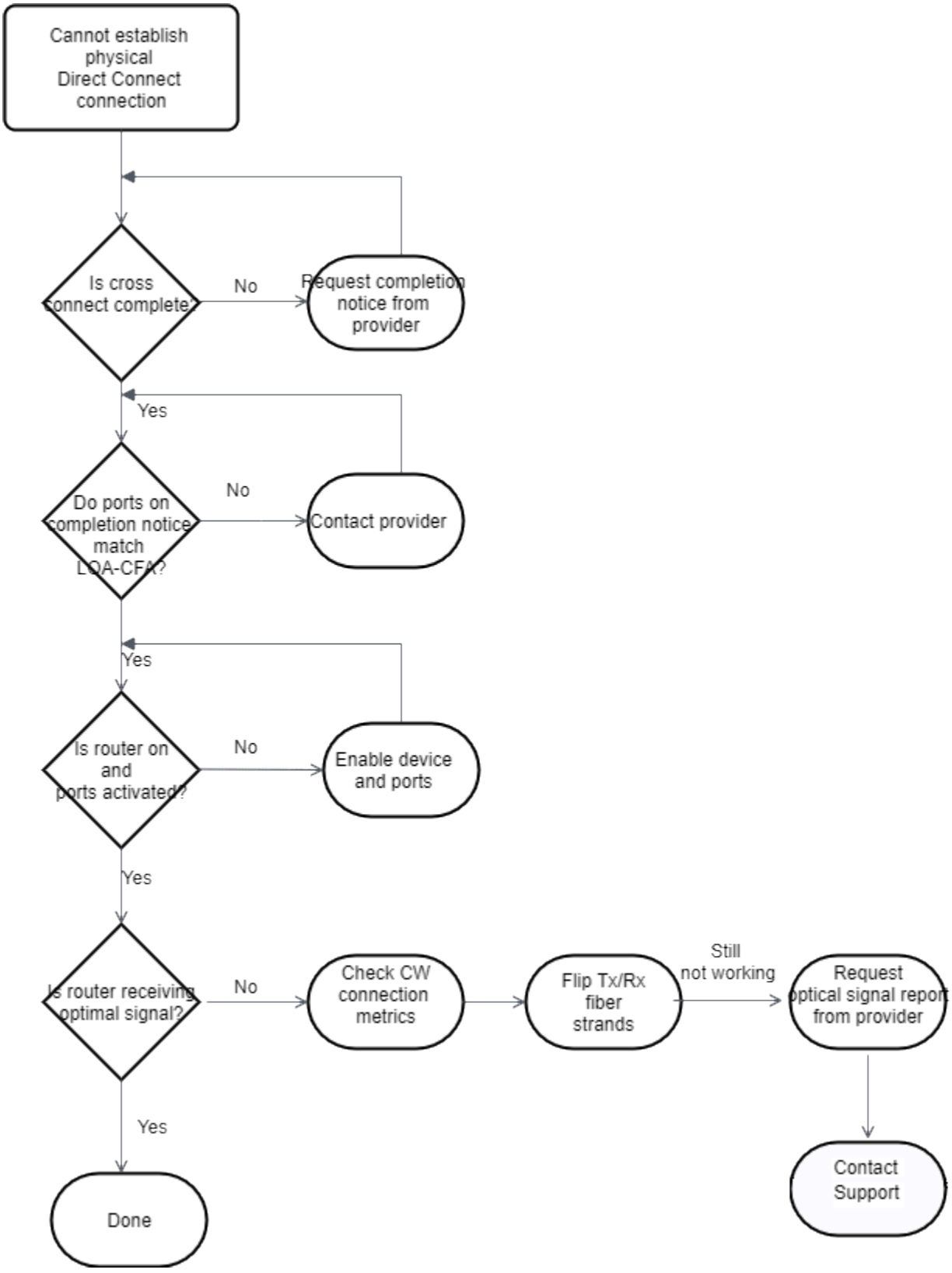
Si tú o tu proveedor de red tienen dificultades para establecer la conectividad física con un AWS Direct Connect dispositivo, sigue estos pasos para solucionar el problema.

1. Con la ayuda del proveedor de coubicación, compruebe que la conexión cruzada se ha completado. Pídale a él o a su proveedor de red que le faciliten una notificación de finalización de conexión cruzada y compare los puertos con los que aparecen en el documento LOA-CFA.
2. Compruebe que su router o el router del proveedor está encendido y que los puertos están activados.
3. Asegúrese de que los enrutadores utilicen el transceptor óptico correcto. La negociación automática del puerto debe estar deshabilitada si tiene una conexión con una velocidad de puerto superior a 1 Gbps. Sin embargo, según el punto final de AWS Direct Connect que dé servicio a su conexión, es posible que sea necesario activar o desactivar la negociación automática para las conexiones de 1 Gbps. Si es necesario deshabilitar la negociación automática para sus conexiones, la velocidad del puerto y el modo dúplex completo se deben configurar de forma manual. Si la interfaz virtual permanece inactiva, consulte Solución de problemas de capa 2 (enlace de datos).
4. Compruebe que el router está recibiendo una señal óptica aceptable a través de la conexión cruzada.
5. Intente voltear (o girar) las hebras de fibra de transmisión/recepción.
6. Consulta las CloudWatch estadísticas de Amazon para AWS Direct Connect. Puede verificar las lecturas ópticas de Tx/Rx del AWS Direct Connect dispositivo (tanto de 1 Gbps como de 10 Gbps),

el recuento de errores físicos y el estado operativo. Para obtener más información, consulta Monitoring with Amazon CloudWatch.

7. Póngase en contacto con el proveedor de coubicación y solicite un informe escrito para la señal óptica de transmisión/recepción a través de la conexión cruzada.
8. Si los pasos anteriores no resuelven los problemas de conectividad física, póngase en contacto con AWS Support y facilite la notificación de finalización de la conexión cruzada y el informe de la señal óptica que le ha proporcionado el proveedor de coubicación.

El siguiente diagrama contiene los pasos para diagnosticar problemas con la conexión física.

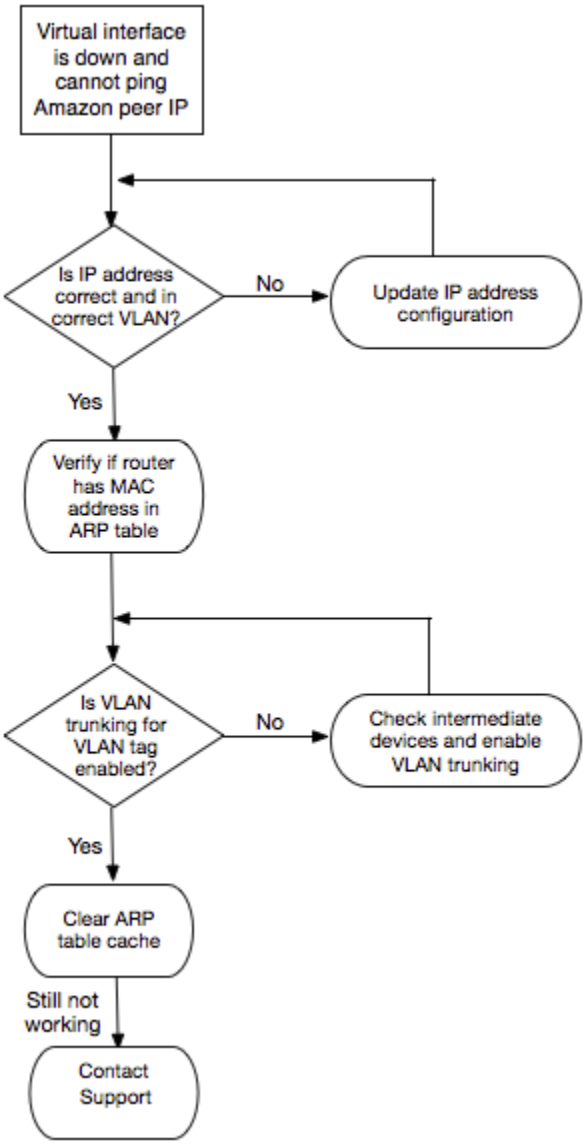

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check CW connection metrics
Flip Tx/Rx fiber strands
Still not working
Request optical signal report from provider
Contact Support
Yes
Done

Solución de problemas de capa 2 (enlace de datos)

Si la conexión AWS Direct Connect física está activa pero la interfaz virtual no funciona, siga los siguientes pasos para solucionar el problema.

1. Si no puede hacer ping a la dirección IP de mismo nivel de Amazon, compruebe que la dirección IP de mismo nivel está configurada correctamente y en la VLAN correcta. Asegúrese de que la dirección IP esté configurada en la subinterfaz de VLAN y no en la interfaz física (por ejemplo, GigabitEthernet 0/0.123 en lugar de 0/0). GigabitEthernet
2. Compruebe si el router tiene una entrada de dirección MAC desde el AWS punto final en la tabla de protocolos de resolución de direcciones (ARP).
3. Asegúrese de que los dispositivos intermedios entre los distintos puntos de enlace tienen habilitadas las redes troncales VLAN para la etiqueta de VLAN 802.1Q. El ARP no se puede establecer de forma AWS paralela hasta que AWS reciba el tráfico etiquetado.
4. Borre la caché de su tabla de ARP o de la del proveedor.
5. Si los pasos anteriores no establecen el ARP o sigues sin poder hacer ping a la IP del mismo nivel de Amazon, ponte en contacto con AWS Support.

El siguiente diagrama contiene los pasos para diagnosticar problemas con el enlace de datos.



Si la sesión de BGP sigue sin establecerse después de verificar estos pasos, consulte Solución de problemas de capa 3/4 (red/transporte). Si la sesión de BGP se ha establecido pero experimenta problemas de direccionamiento, consulte Solución de problemas de direccionamiento.

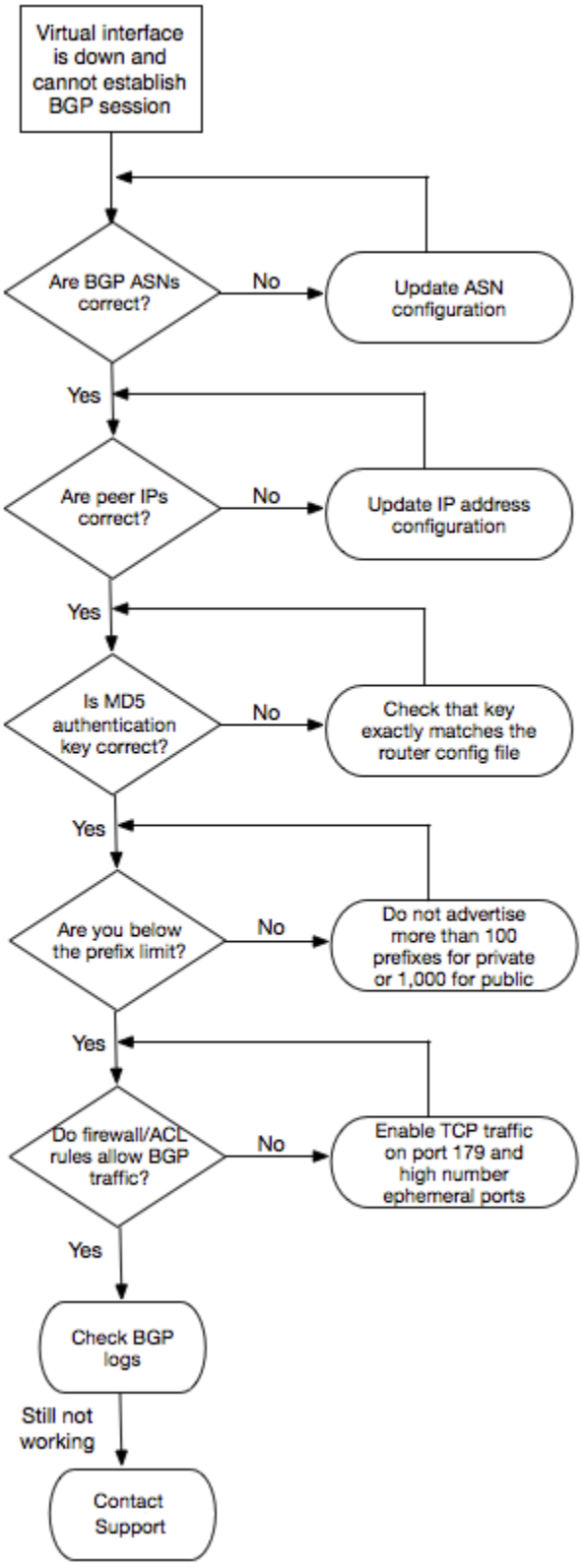
Solución de problemas de capa 3/4 (red/transporte)

Imagina una situación en la que tu conexión AWS Direct Connect física esté activa y puedas hacer ping a la dirección IP del mismo nivel de Amazon. Si la interfaz virtual no funciona y la sesión de intercambio de tráfico BGP no se puede establecer, siga estos pasos para solucionar el problema:

1. Asegúrese de que el número de sistema autónomo (ASN) local de BGP y el ASN de Amazon están configurados correctamente.

2. Asegúrese de que las direcciones IP de mismo nivel para ambos lados de la sesión de intercambio de tráfico BGP están configuradas correctamente.
3. Asegúrese de que la clave de autenticación MD5 está configurada y coincide exactamente con la clave del archivo de configuración del router que ha descargado. Compruebe que no haya espacios o caracteres adicionales.
4. Compruebe que tanto usted como su proveedor no estén comunicando más de 100 prefijos para interfaces virtuales privadas o 1 000 prefijos para interfaces virtuales públicas. Estos son los límites máximos y no deben superarse.
5. Asegúrese de que no hay reglas de ACL ni de firewall que estén bloqueando el puerto TCP 179 ni ningún otro puerto TCP efímero con numeración alta. BGP necesita estos puertos para establecer una conexión TCP entre las direcciones IP de mismo nivel.
6. Compruebe si hay errores o mensajes de advertencia en los logs de BGP.
7. Si los pasos anteriores no establecen la sesión de peering de BGP, póngase en contacto con Support AWS.

El siguiente diagrama contiene los pasos para diagnosticar problemas con la sesión de intercambio de tráfico BGP.



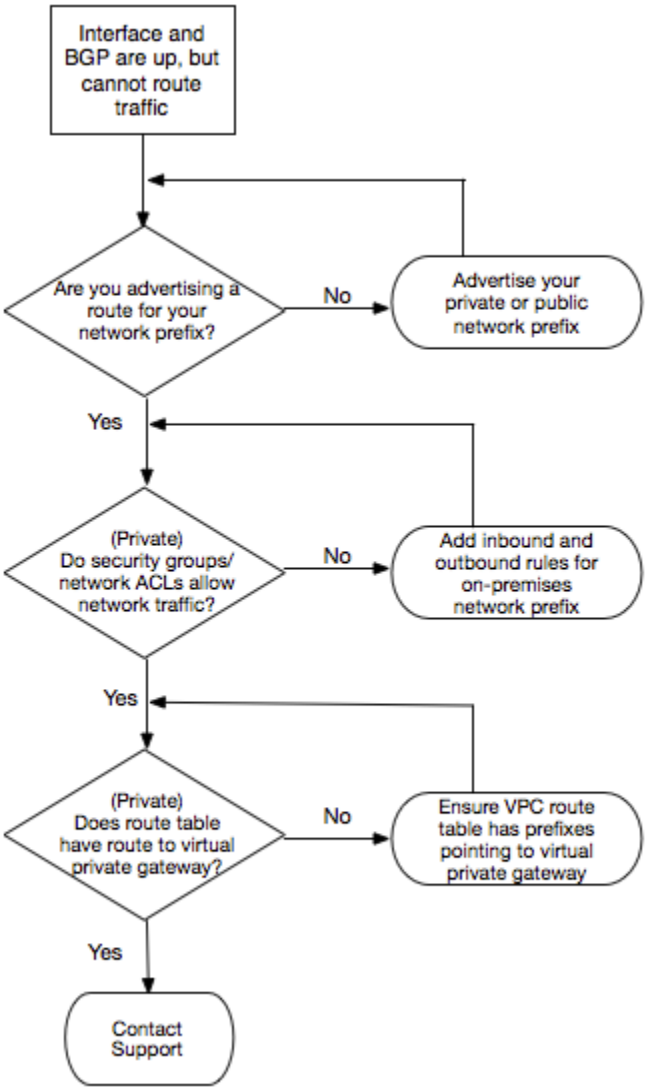
Si la sesión de intercambio de tráfico BGP se ha establecido, pero experimenta problemas de direccionamiento, consulte Solución de problemas de direccionamiento.

Solución de problemas de direccionamiento

Imagine una situación en la que la interfaz virtual está activa y ha establecido una sesión de intercambio de tráfico BGP. Si no puede dirigir el tráfico a través de la interfaz virtual, siga estos pasos para solucionar el problema:

1. Asegúrese de que comunica una ruta para el prefijo de red local en la sesión de BGP. En una interfaz virtual privada, este puede ser un prefijo de red público o privado. En una interfaz virtual pública, este debe ser el prefijo de red direccionable públicamente.
2. En una interfaz virtual privada, asegúrese de que los grupos de seguridad de VPC y las ACL de red permiten el tráfico entrante y saliente para el prefijo de red local. Para obtener más información, consulte Grupos de seguridad y ACL de red en la Guía del usuario de Amazon VPC.
3. En una interfaz virtual privada, asegúrese de que las tablas de ruteo de la VPC tienen prefijos que apuntan a la gateway privada virtual a la que está conectada su interfaz virtual privada. Por ejemplo, si quiere que todo el tráfico se dirija a su red local de forma predeterminada, puede agregar la ruta predeterminada (0.0.0.0/0 o ::/0) con la gateway privada virtual como destino en las tablas de ruteo de la VPC.
   - También puede habilitar la propagación de rutas para actualizar automáticamente sus tablas de ruteo en función de los anuncios de ruta dinámicos de BGP. Puede tener hasta 100 rutas propagadas por tabla de rutas. Este límite no se puede aumentar. Para obtener más información, consulte Habilitación y deshabilitación de la propagación de ruta en la Guía del usuario de Amazon VPC.
4. Si los pasos anteriores no resuelven sus problemas de enrutamiento, póngase en contacto con AWS Support.

El siguiente diagrama contiene los pasos para diagnosticar problemas de direccionamiento.


Interface and BGP are up, but cannot route traffic
Are you advertising a route for your network prefix?
No
Advertise your private or public network prefix
Yes
(Private) Do security groups/ network ACLs allow network traffic?
No
Add inbound and outbound rules for on-premises network prefix
Yes
(Private) Does route table have route to virtual private gateway?
No
Ensure VPC route table has prefixes pointing to virtual private gateway
Yes
Contact Support

Historial del documento

En la tabla siguiente se describen las versiones de las AWS Direct Connect.

Funcionalidad	Descripción	Fecha
Support para SiteLink	Puede crear una interfaz privada virtual que permita la conectividad entre dos puntos de presencia de Direct Connect (PoPs) en la misma AWS región. Para más información, consulte Interfaces virtuales alojadas.	01/12/2021
Compatibilidad con la seguridad de MAC	Puede utilizar conexiones de AWS Direct Connect compatibles con MACsec para cifrar los datos desde el centro de datos corporativo hasta la ubicación de AWS Direct Connect. Para más información, consulte Seguridad de MAC.	2021-03-31
Compatibilidad con 100 G	Temas actualizados para incluir la compatibilidad con conexiones dedicadas de 100 G.	2021-02-12
Ubicación nueva en Italia	Tema actualizado para incluir la ubicación nueva en Italia. Para más información, consulte the section called “Europa (Milán)”.	2021-01-22
Nueva ubicación en Israel	Tema actualizado para incluir la ubicación nueva en Israel. Para más información, consulte the section called “Israel (Tel Aviv)”.	2020-07-07
Compatibilidad de la prueba de conmutación por error del conjunto de herramientas de resiliencia	Utilice la característica de prueba de conmutación por error del conjunto de herramientas de resiliencia para probar la resiliencia de sus conexiones. Para más información, consulte the section called “Prueba de conmutación por error de AWS Direct Connect”.	03-06-2020

Funcionalidad	Descripción	Fecha
CloudWatch Soporte métrico VIF	Puede monitorear AWS Direct Connect las conexiones físicas y las interfaces virtuales mediante CloudWatch. Para más información, consulte the section called “Monitorización con Amazon CloudWatch”.	11-05-2020
AWS Direct Connect Resiliency Toolkit	AWS Direct Connect Resiliency Toolkit proporciona un asistente de conexión con varios modelos de resiliencia que lo ayuda a solicitar conexiones dedicadas para alcanzar su objetivo de SLA. Para más información, consulte ¿Cómo usar el kit de herramientas AWS Direct Connect de resiliencia para empezar.	07-10-2019
Compatibilidad con regiones adicionales para permitir el uso de AWS Transit Gateway entre cuentas	Para obtener más información, consulte the section called “Asociaciones de la puerta de enlace de tránsito”.	30-09-2019
AWS Direct Connect Compatibilidad con AWS Transit Gateway	Puede utilizar una gateway de AWS Direct Connect para establecer la conexión de AWS Direct Connect a través de una interfaz virtual de tránsito con las VPC o VPN conectadas a su gateway de tránsito. Primero debe asociar una gateway de Direct Connect a la gateway de tránsito y, a continuación, crear una interfaz virtual de tránsito para la conexión de AWS Direct Connect con la gateway de Direct Connect. Para obtener más información, consulte the section called “Asociaciones de la puerta de enlace de tránsito”.	27-03-2019

Funcionalidad	Descripción	Fecha
Compatibilidad con tramas gigantes	Puede enviar tramas gigantes (9001 MTU) sobre AWS Direct Connect. Para más información, consulte Establecer la MTU de red para interfaces virtuales privadas o de tránsito.	11/10/2018
Comunidades de BGP de preferencia local	Puede utilizar las etiquetas de comunidad de BGP de preferencia local para lograr el equilibrio entre el balanceo de carga y las preferencias de ruta del tráfico entrante a la red. Para más información, consulte Comunidades de BGP de preferencia local.	06/02/2018
Puerta de enlace de AWS Direct Connect	Puede usar una gateway de Direct Connect para establecer la conexión de AWS Direct Connect con las VPC de regiones remotas. Para más información, consulte Uso de puertas de enlace de Direct Connect.	01/11/2017
CloudWatch Métricas de Amazon	Puedes ver CloudWatch las métricas de tus AWS Direct Connect conexiones. Para más información, consulte Monitorización con Amazon CloudWatch.	2017-06-29
Grupos de agregación de enlaces (LAG)	Puede crear un grupo de agregación de enlaces (LAG) para agregar varias conexiones de AWS Direct Connect. Para más información, consulte Grupos de agregación de enlaces (LAG).	13/02/2017
Compatibilidad con IPv6	La interfaz virtual ahora es compatible una sesión de intercambio de tráfico BGP IPv6. Para más información, consulte Adición o eliminación de un BGP de mismo nivel.	01/12/2016
Compatibilidad del etiquetado	A partir de ahora, puede etiquetar los recursos de AWS Direct Connect. Para más información, consulte Etiquetado de recursos de AWS Direct Connect.	04/11/2016

Funcionalidad	Descripción	Fecha
Autoservicio de LOA-CFA	A partir de ahora, puede descargar la Carta de autorización y Asignación de instalaciones de conexión (LOA-CFA) mediante la consola o API de AWS Direct Connect.	22/06/2016
Nueva ubicación en Silicon Valley	Tema actualizado para incluir la ubicación nueva en Silicon Valley en la región Oeste de EE. UU. (Norte de California).	03/06/2016
Nueva ubicación en Ámsterdam	Tema actualizado para incluir la ubicación nueva en Ámsterdam en la región Europa (Fráncfort).	19/05/2016
Nuevas ubicaciones en Portland, Oregón y Singapur	Tema actualizado para incluir las ubicaciones nuevas en Portland, Oregón y Singapur en las regiones Oeste de EE. UU. (Oregón) y Asia-Pacífico (Singapur).	27/04/2016
Nueva ubicación en São Paulo, Brasil	Tema actualizado para incluir la ubicación nueva en São Paulo en la región América del Sur (São Paulo).	09/12/2015
Nuevas ubicaciones en Dallas, Londres, Silicon Valley y Mumbai	Se actualizaron los temas para incluir la incorporación de nuevas ubicaciones en Dallas (región EE.UU. Este (Norte de Virginia)), Londres (región Europa (Irlanda)), Silicon Valley AWS GovCloud (región EE.UU. Oeste) y Bombay (región Asia Pacífico (Singapur)).	27/11/2015
Ubicación nueva en la región China (Pekín)	Temas actualizados para incluir la ubicación nueva en Pekín en la región China (Pekín).	14/04/2015

Funcionalidad	Descripción	Fecha
Nueva ubicación en Las Vegas en la región EE. UU. Oeste (Oregón)	Temas actualizados para incluir la nueva ubicación de AWS Direct Connect en Las Vegas en la región EE. UU. Oeste (Oregón).	10/11/2014
Nueva región UE (Fráncfort)	Temas actualizados para incluir la nuevas ubicaciones de AWS Direct Connect que sirven a la región UE (Fráncfort).	23/10/2014
Nuevas ubicaciones en la región Asia Pacífico (Sídney)	Temas actualizados para incluir las nuevas ubicaciones de AWS Direct Connect que sirven a la región Asia Pacífico (Sídney).	14/07/2014
Soporte para AWS CloudTrail	Se ha añadido un tema nuevo para explicar cómo se puede utilizar CloudTrail para registrar la actividad. AWS Direct Connect Para más información, consulte Registro de llamadas a la API de AWS Direct Connect mediante AWS CloudTrail.	04/04/2014
Compatibilidad con el acceso a las regiones de AWS remotas	Nuevo tema añadido que explica cómo puede acceder a los recursos públicos de una región remota. Para más información, consulte Acceso a una región de AWS remota.	19/12/2013
Compatibilidad con conexiones alojadas	Temas actualizados para incluir la compatibilidad con conexiones alojadas.	22/10/2013

Funcionalidad	Descripción	Fecha
Nueva ubicación en la región UE (Irlanda)	Temas actualizados para incluir la nueva ubicación de AWS Direct Connect que sirve a la región UE (Irlanda).	24/06/2013
Nueva ubicación en Seattle en la región EE. UU. Oeste (Oregón)	Temas actualizados para incluir la nueva ubicación de AWS Direct Connect en Seattle en la región EE. UU. Oeste (Oregón).	08/05/2013
Compatibilidad para utilizar IAM con AWS Direct Connect	Tema añadido que explica cómo utilizar AWS Identity and Access Management con AWS Direct Connect. Para más información, consulte the section called “Identity and Access Management”.	21/12/2012
Nueva región Asia Pacífico (Sídney)	Temas actualizados para incluir la nueva ubicación de AWS Direct Connect que sirve a la región Asia Pacífico (Sídney).	14/12/2012

Funcionalidad	Descripción	Fecha
Consola de AWS Direct Connect nueva y regiones Este de EE. UU. (Norte de Virginia) y América del Sur (São Paulo)	La Guía de usuario de AWS Direct Connect ha reemplazado a la Guía de introducción a AWS Direct Connect. Nuevos temas añadidos sobre la nueva consola de AWS Direct Connect. Además, se ha añadido un tema sobre facturación, información sobre la configuración del router y se han actualizado temas para incluir las dos nuevas ubicaciones de AWS Direct Connect que sirven a las regiones EE. UU. Este (Norte de Virginia) y América del Sur (São Paulo).	13/08/2012
Compatibilidad con las regiones UE (Irlanda), Asia Pacífico (Singapur) y Asia Pacífico (Tokio)	Nueva sección de solución de problemas y temas actualizados para incluir las cuatro nuevas ubicaciones de AWS Direct Connect que sirven a las regiones EE. UU. Oeste (Norte de California), UE (Irlanda), Asia Pacífico (Singapur) y Asia Pacífico (Tokio).	10/01/2012
Compatibilidad con la región EE. UU. Oeste (Norte de California)	Temas actualizados para la región EE. UU. Oeste (Norte de California).	08/09/2011
Versión pública	La primera versión de AWS Direct Connect.	03/08/2011

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.