Guía del usuario de

AWS Direct Connect

AWS Direct Connect: Guía del usuario de

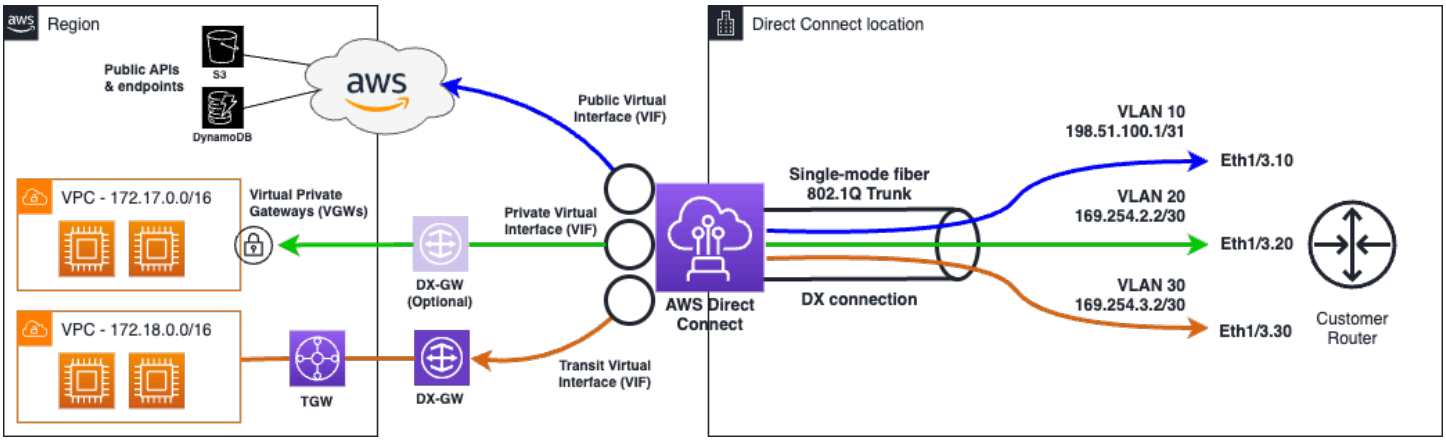
Table of Contents

¿Qué es () Direct Connect?

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

- Para obtener una lista de las ubicaciones de Direct Connect a las que se puede conectar, consulte Ubicaciones de AWS Direct Connect.
- Para obtener respuestas a preguntas sobre Direct Connect, consulte las Preguntas frecuentes sobre Direct Connect.

En el siguiente diagrama se muestra información general sobre cómo Direct Connect se conecta con su red.



Contenido

- Direct Connect políticas de enrutamiento y comunidades BGP

Direct ConnectComponentes de

Los siguientes son los componentes clave que se utilizan para Direct Connect:

Connections

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

Interfaces virtuales

Cree una interfaz virtual para permitir el acceso a los servicios de AWS. Una interfaz virtual pública lo habilita para acceder a servicios públicos, como Amazon S3. Una interfaz virtual privada permite el acceso a su VPC. Los tipos de interfaces admitidas se describen a continuación en the section called “Tipos de interfaz virtual de Direct Connect admitidos”. Para obtener más información sobre las interfaces admitidas, consulte Interfaces virtuales e interfaces virtuales alojadas de Direct Connect y Requisitos previos de las interfaces virtuales.

Requisitos de red

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

- La red está coubicada en una ubicación de Direct Connect existente. Para obtener más información sobre las ubicaciones de Direct Connect disponibles, consulte Detalles del producto de AWS Direct Connect.
- Está trabajando con un socio de Direct Connect que es miembro de la red de socios de AWS (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 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, un 100GBASE-LR4 para 100 gigabit Ethernet o un 400GBASE-LR4 para 400 gigabit Ethernet.

- Según el punto de conexión de AWS Direct Connect que proporcione su conexión, es posible que sea necesario habilitar o deshabilitar la negociación automática de dispositivos locales para cualquier conexión dedicada. Si una interfaz virtual permanece inactiva cuando hay una conexión Direct Connect activa, 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 de forma automática para cada interfaz virtual de 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.

Direct Connect es compatible con los protocolos de comunicación IPv4 e IPv6. Es posible acceder a las direcciones IPv6 proporcionadas por los servicios de AWS públicos a través de las interfaces virtuales públicas de Direct Connect.

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 MTU para interfaces virtuales privadas o interfaces virtuales de tránsito.

Tipos de interfaz virtual de Direct Connect admitidos

AWS Direct Connect admite los siguientes tres tipos de interfaz virtual (VIF):

- Interfaz virtual privada

  Este tipo de interfaz se utiliza para acceder a una Amazon Virtual Private Cloud (VPC) mediante direcciones IP privadas. Con una interfaz virtual privada puede

  - Conectarse directamente a una única VPC por interfaz virtual privada para acceder a esos recursos con IP privadas en la misma región.
  - Conecte una interfaz virtual privada a una puerta de enlace de Direct Connect para acceder a varias puertas de enlace privadas virtuales en cualquier cuenta y región de AWS (excepto las regiones de AWS China).

- Interfaz virtual privada

  Este tipo de interfaz virtual se utiliza para acceder a todos los servicios públicos de AWS con direcciones IP públicas. Con una interfaz virtual pública puede conectarse a todas las direcciones IP públicas y servicios de AWS a nivel global.

- Interfaz virtual de tránsito

  Este tipo de interfaz se utiliza para acceder a una o varias puertas de enlace de tránsito de Amazon VPC asociadas a puertas de enlace de Direct Connect. Con una interfaz virtual de tránsito se conectan múltiples puertas de enlace de tránsito de Amazon VPC a través de múltiples cuentas y regiones de Regiones de AWS (excepto las regiones de AWS China).

  > **Note**
  >
  > La cantidad de tipos diferentes de asociaciones entre una puerta de enlace de Direct Connect y una interfaz virtual está limitada. Para obtener más información acerca de los límites específicos, consulte la página Cuotas de Direct Connect.

Para obtener más información acerca de las interfaces virtuales, consulte Interfaces virtuales e interfaces virtuales alojadas.

Precios de Direct Connect

AWS Direct Connect tiene dos elementos de facturación: horas de puerto y 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 cargos de transferencia de salida de datos para las interfaces privadas y las interfaces virtuales de tránsito se asignan a la cuenta de AWS responsable de la transferencia de datos. No se realizan cargos adicionales por usar una puerta de enlace de AWS Direct Connect con varias cuentas.

En el caso de los recursos de AWS disponibles públicamente (por ejemplo, buckets de Amazon S3, instancias de EC2 clásicas o tráfico de EC2 que pasa a través de una puerta de enlace de Internet), si el tráfico saliente está destinado a prefijos públicos propiedad de la misma cuenta de pago de AWS y se anuncia de forma activa en AWS través de una interfaz virtual pública de Direct Connect, el uso de la transferencia de datos salientes (DTO) se mide respecto al propietario del recurso a la velocidad de transferencia de datos de Direct Connect.

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

Acceso a regiones remotas de Direct Connect

Las ubicaciones de 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 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 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 enrutamiento y sobre las comunidades de BGP admitidas para las conexiones de Direct Connect, consulte Routing policies and BGP communities.

Acceda 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 puerta de enlace fronteriza (BGP). Para obtener más información, consulte Interfaces virtuales e interfaces virtuales alojadas.

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.

Acceda a una VPC en una región remota

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

Si lo prefiere, puede crear una interfaz virtual pública para la conexión de 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

Direct Connect políticas de enrutamiento y comunidades BGP

Direct Connect aplica políticas de enrutamiento entrantes (desde su centro de datos local) y salientes (desde su AWS región) para una conexión pública. 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 enrutamiento de interfaces virtuales públicas

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

Se aplican las siguientes políticas de enrutamiento 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 enrutamiento transitivo entre las conexiones.
- 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 enrutamiento de salida:

- AS_PATH y Longest Prefix Match se utilizan para determinar la ruta de enrutamiento. AWS recomienda anunciar rutas más específicas Direct Connect si se anuncia el mismo prefijo tanto en Internet como en una interfaz virtual pública.

- 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 AWS China solo se anuncian en las regiones de 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.

- Direct Connect anuncia prefijos con una longitud de ruta mínima de 3.
- 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 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 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 enrutamiento de Internet pública.
- 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 interfaz virtual pública en ninguno de los siguientes sitios:
  - Otros clientes Direct Connect
  - Redes compatibles con la red AWS global
  - Proveedores de conexión de Amazon
- Puede utilizar un ASN público o privado con una interfaz pública. Sin embargo, existen algunas consideraciones importantes:

- Público ASNs: debes ser el propietario de la ASN y tener derecho a anunciarla. AWS verificará que eres el propietario de la ASN. Se admiten tanto ASNs (1-2147483647) como largas ASNs (1-4294967295).
- Privado: puedes usar el ASNs modo privado desde los siguientes rangos: ASNs
  - privado ASNs: 64512-65534
  - longitud privada: 4200000000-4294967294 ASNs

  Sin embargo, Direct Connect sustituirá el ASN privado por el AWS ASN (7224) cuando anuncie sus prefijos a otros clientes o a través de Internet. AWS
- Anteposición del ASN:
  - En el caso de un ASN público (tanto el ASN como el ASN largo), la anteposición funcionará según lo previsto y el ASN antepuesto estará visible en otras redes.
  - En el caso de un ASN privado (tanto el ASN como el ASN largo), se eliminarán todos los prefijos que utilices cuando sustituyas tu ASN privado por el 7224. AWS Esto significa que la suplantación de un ASN no es eficaz para influir en las decisiones de enrutamiento si no AWS se utiliza un ASN privado en una interfaz virtual pública.
- Al establecer una sesión de emparejamiento de BGP a AWS través de una interfaz virtual pública, utilice 7224 como números de sistema autónomo (ASN) para establecer la sesión de BGP de forma paralela. AWS El ASN de su router o dispositivo de puerta de enlace de cliente debe ser diferente al de ese ASN. El ASN de su cliente puede ser un ASN (1-2147483647, sin incluir los rangos reservados) o un ASN largo (1-4294967295, sin incluir los rangos reservados).

Comunidades BGP de interfaces virtuales públicas

Direct Connect admite las etiquetas de la 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 América del Norte
  - 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 Direct Connect.

Para las políticas de enrutamiento de salida, 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 Direct Connect punto de presencia.
- `7224:8200`—Rutas que se originan en el mismo continente al que está asociado el 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 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.

Direct Connect también proporciona etiquetas de comunidad BGP en las rutas de Amazon anunciadas. Si lo utilizas 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 Direct Connect se anuncian a los clientes se etiquetan con la etiqueta comunitaria NO_EXPORT.

Políticas de enrutamiento 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 IPv6 prefijos que desee anunciar a través de BGP. IPv4 Estos prefijos pueden ser públicos o privados.

Las siguientes reglas de enrutamiento de salida se aplican según 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 pensadas para active/passive conexiones. Consulte Influencing Traffic over Hybrid Networks using Longest Prefix Match para obtener más información.
- La preferencia local es el atributo BGP que se recomienda usar cuando las rutas de enrutamiento deseadas estén destinadas a active/passive conexiones 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 únicamente se aplica si no hay asignadas etiquetas de comunidad de preferencia local.
- La longitud AS_PATH se puede utilizar para determinar la ruta de enrutamiento si la longitud del prefijo y la preferencia local son iguales.
- El discriminador de salidas múltiples (MED) se puede utilizar para determinar la ruta de enrutamiento cuando la longitud del prefijo, la preferencia local y AS_PATH coinciden. AWS no recomienda utilizar valores MED debido a su menor prioridad en la evaluación.

- AWS utiliza el enrutamiento de rutas múltiples (ECMP) de igual costo a través de múltiples interfaces virtuales privadas o de tránsito cuando los prefijos tienen la misma longitud de AS_PATH y los mismos atributos de BGP. No es necesario que coincidan los ASNs prefijos en el AS_PATH.

Comunidades BGP de interfaces virtuales privadas e interfaces virtuales de tránsito

Cuando una Región de AWS ruta el tráfico a ubicaciones locales a través de interfaces virtuales privadas o de tránsito de Direct Connect, la ubicación Región de AWS de Direct Connect asociada influye en la capacidad de usar ECMP. Regiones de AWS prefieren las ubicaciones de Direct Connect en las mismas ubicaciones asociadas Región de AWS de forma predeterminada. Consulte Ubicaciones de AWS Direct Connect para identificar la Región de AWS asociada de cualquier ubicación de Direct Connect.

Cuando no se aplican etiquetas de comunidad de preferencia local, Direct Connect admite ECMP a través de interfaces virtuales privadas o de tránsito en el caso de prefijos con la misma longitud AS_PATH y el mismo valor MED en dos o más rutas en las siguientes situaciones:

- 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 Active/Active configuro una conexión de Active/Passive Direct Connect AWS desde una interfaz virtual privada o de tránsito?

> **Note**
>
> Esto no afecta al ECMP hacia y Región de AWS desde las ubicaciones locales.

Para controlar las preferencias de ruta, Direct Connect admite etiquetas de comunidad de BGP de preferencia local para interfaces virtuales privadas e 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 Direct Connect conexiones (activas/activas) alojadas en la misma región o en AWS regiones diferentes, aplique la misma etiqueta de comunidad `7224:7200` (por ejemplo, de preferencia media) a los prefijos de las conexiones. Si se produce un error en una de las conexiones, el tráfico se equilibrará mediante ECMP en el resto de las conexiones activas, independientemente de su asociación con la región principal. Para permitir la conmutación por error en varias conexiones de 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).

Soporte de ASN prolongado en Direct Connect

Support for long ASNs (4 bytes) le permite configurar números de sistema autónomos largos (ASNs) como parte de los parámetros de la sesión de BGP establecida entre el dispositivo de AWS red y su dispositivo de red. Esta característica se habilita o deshabilita por cuenta.

Puede configurar el rango de ASN o ASN largo en la consola o a través del. APIs

- Al utilizar la consola, el campo ASN admite tanto como ASNs long. ASNs Puede agregar cualquier rango, desde 1 hasta 4294967294.
- Al utilizar el APIs para crear una interfaz virtual, puede especificar un ASN (`asn`) o un ASN largo (`asnLong`), pero no ambos. Para obtener más información sobre el uso de ASN o ASN largo, consulta lo siguiente APIs en la referencia de la API:Direct Connect

- `BGPPeer`
- `DeleteBGPPeerRequest`
- `NewBGPPeer`
- `NewPrivateVirtualInterface`
- `NewPrivateVirtualInterfaceAllocation`
- `NewPublicVirtualInterface`
- `NewPublicVirtualInterfaceAllocation`
- `NewTransitVirtualInterface`
- `NewTransitVirtualInterfaceAllocation`
- `VirtualInterface`

Consideraciones

Cuando se decida por usar un ASN o un ASN largo, deberá tener en cuenta lo siguiente:

- Compatibilidad con versiones anteriores: Direct Connect gestiona automáticamente las sesiones de BGP con routers compatibles con ASN y ASN largo. Si su router no admite un modo prolongado ASNs, la sesión de BGP funcionará en modo ASN.
- Formato ASN: puede especificar 4 bytes ASNs en formato simple, por ejemplo, `4200000000` o en formato de puntos, por ejemplo. `64086.59904` Direct Connect acepta ambos formatos, pero se muestra ASNs en formato simple.
- Intervalos de ASN privados: cuando se usa private long ASNs (`4200000000-4294967294`), se aplica el mismo comportamiento de reemplazo que con private. ASNs Direct Connect sustituirá su ASN privado por `7224` cuando se publique en otras redes.
- Etiquetas de comunidad BGP: todas las etiquetas de comunidad BGP existentes (`7224:xxxx`) funcionan con long. ASNs El formato de las etiquetas de comunidad permanece inalterado.
- Supervisión y solución de problemas: CloudWatch las métricas, los registros de sesiones de BGP y las herramientas de solución de problemas se muestran extensamente ASNs en un formato simple para garantizar la coherencia.

Disponibilidad y precios

Tenga en cuenta lo siguiente para obtener una compatibilidad prolongada con ASN con: Direct Connect

- Disponibilidad: el ASN largo está disponible en todas AWS las regiones en las que Direct Connect se admite.
- Precios: el soporte de ASN de larga duración no conlleva cargos adicionales aparte del precio estándar Direct Connect .

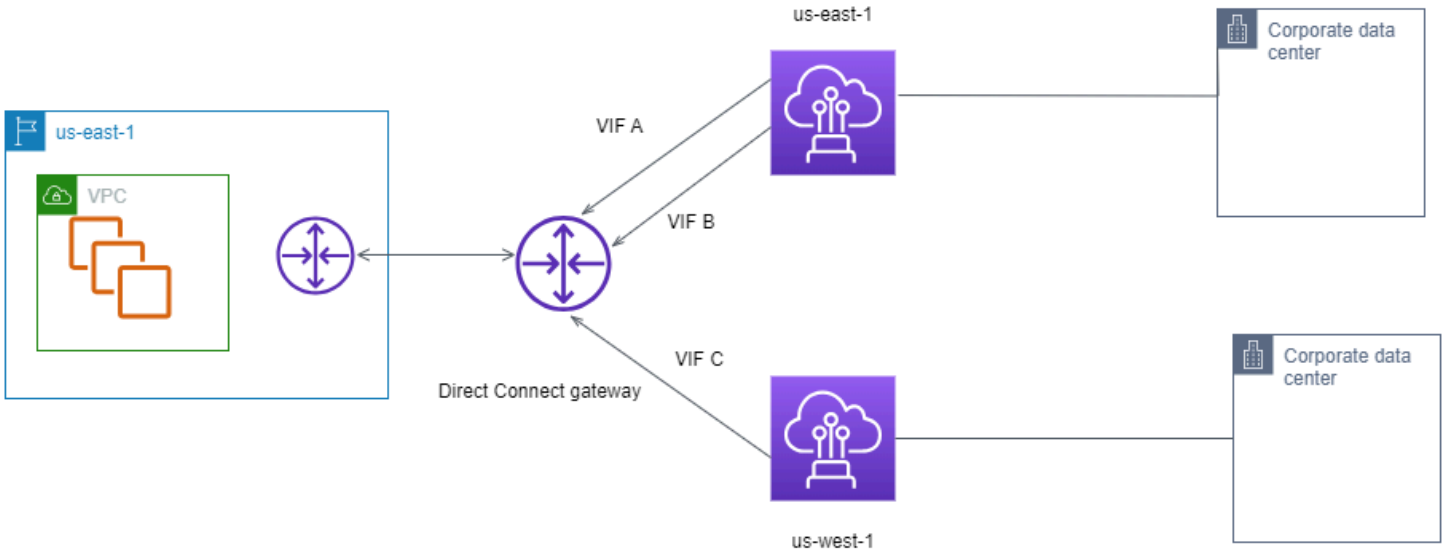
> **Note**
>
> La activación de una ASN larga se aplica a toda tu cuenta. AWS No puede habilitar la compatibilidad con el ASN largo para interfaces virtuales individuales o pares de BGP.

Direct Connect ejemplo de enrutamiento de interfaz virtual privada

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

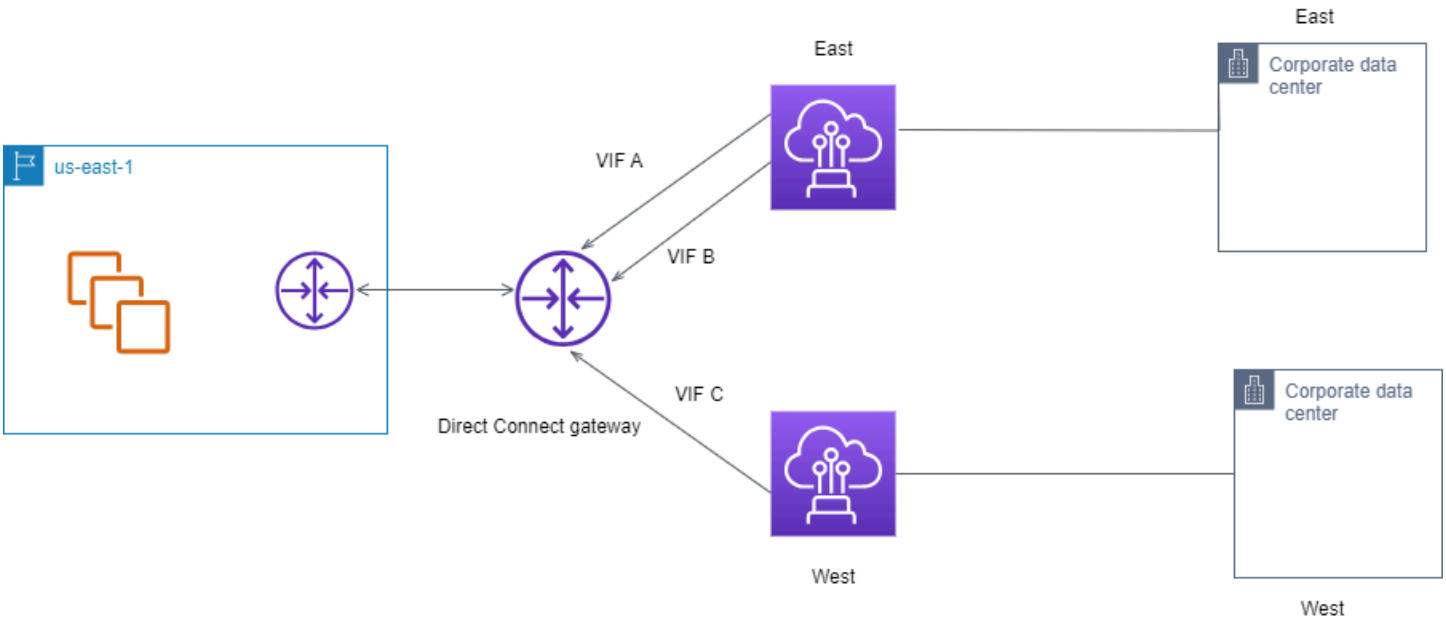
VIFs Tienen las siguientes configuraciones:

- La interfaz virtual A (en us-east-1) anuncia 172.16.0.0/16 y tiene un atributo AS_PATH de 65001, 65001, 65001
- La interfaz virtual B (en us-east-1) anuncia 172.16.0.0/16 y tiene un atributo AS_PATH de 65001, 65001
- La interfaz virtual 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 de CIDR de la interfaz virtual C, las rutas que se encuentren dentro del rango de CIDR de la interfaz virtual C utilizarán la interfaz virtual C porque tiene la longitud de prefijo más larga.

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



Direct Connect opciones de conexión

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.

Están disponibles las siguientes opciones de conexión para. Direct Connect

- Maximum Resiliency (Máxima resiliencia): este modelo está disponible para AWS Direct Connect Resiliency Toolkit y 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 Direct Connect. Para obtener más información, consulte la AWS Direct Connect Resiliency Toolkit.
- Alta resiliencia: este modelo está disponible en el kit de herramientas de AWS Direct Connect resiliencia y le permite solicitar conexiones dedicadas para lograr 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 Direct Connect. Para obtener más información, consulte la AWS Direct Connect Resiliency Toolkit.
- Development and Test (Desarrollo y pruebas): este modelo está disponible para AWS Direct Connect Resiliency Toolkit y 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. Para obtener más información, consulte la AWS Direct Connect Resiliency Toolkit.
- Clásico: una conexión clásica crea una conexión sin necesidad del kit de herramientas de resiliencia. AWS Direct Connect Está destinado a aquellos usuarios que tengan conexiones existentes y que deseen agregar otros sin usar el kit de herramientas. Este modelo tiene un SLA del 95 %, pero no proporciona resiliencia ni redundancia. Para obtener más información, consulte Conexión clásica.

Temas

- Requisitos previos para la conexión
- AWS Direct Connect Resiliency Toolkit
- Direct Connect Conexión clásica

Requisitos previos para la conexión

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, 100GBASE- para Ethernet de 100 gigabit o 400GBASE- para Ethernet de 400 Gbps. LR4 LR4

Puede configurar Direct Connect una conexión mediante el kit de herramientas de resiliencia o una conexión clásica de una de las siguientes maneras: AWS Direct Connect

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

Modelo	Ancho de banda	Método
Conexión alojada	50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps y 25 Gbps.	Trabaje con un socio del programa de socios para conectar un router desde su centro de datos, oficina o entorno de colocación a AWS Direct Connect una ubicación. Direct Connect Solo algunos socios proporcio nan las conexiones de mayor capacidad.

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

- La red debe utilizar fibra monomodo con un transceptor 1000BASE-LX (1310 nm) para Ethernet de 1 gigabit, un transceptor 10GBASE-LR (1310 nm) para 10 gigabits, un transceptor 100GBASE- para Ethernet de 100 gigabit o un transceptor 400GBASE- para Ethernet de 400 Gbps. LR4 LR4
- Según el punto de conexión de AWS Direct Connect que dé servicio a su conexión, es posible que sea necesario habilitar o deshabilitar la negociación automática de los dispositivos locales para cualquier conexión dedicada. Si una interfaz virtual permanece inactiva cuando hay una conexión Direct Connect activa, 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.
- El dispositivo debe ser compatible con el protocolo Border Gateway (BGP) y la autenticación BGP. MD5
- (Opcional) Puede configurar la detección de reenvío bidireccional (BFD) en la red. El BFD asíncrono se habilita automáticamente para cada interfaz virtual. 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 en caso de que no vaya a crear una conexión clásica. Para ver las opciones de AWS Direct Connect conexión del Resiliency Toolkit, consulte la. AWS Direct Connect Resiliency Toolkit
- La velocidad, la ubicación y el socio de todas las conexiones.

  Solo necesita la velocidad para una conexión.

AWS Direct Connect Resiliency Toolkit

AWS ofrece a los clientes la capacidad de establecer conexiones de red muy resiliente entre Amazon Virtual Private Cloud (Amazon VPC) y su infraestructura en las instalaciones. AWS Direct Connect Resiliency Toolkit 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 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.

AWS Direct Connect Resiliency Toolkit tiene los siguientes beneficios:

- Proporciona directrices para determinar y después solicitar las conexiones dedicadas de Direct Connect redundantes apropiadas.
- Garantiza que las conexiones dedicadas redundantes tengan la misma velocidad.
- Configura automáticamente los nombres de conexión dedicados.
- Aprueba de forma automática sus conexiones dedicadas cuando tiene una cuenta de AWS existente y selecciona un socio de AWS Direct Connect conocido. La Carta de autorización (LOA) está disponible para su descarga inmediata.
- Crea automáticamente una incidencia de soporte para la aprobación de conexiones dedicadas en el caso de clientes nuevos de AWS o cuando se selecciona un socio desconocido (Other (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, 100 Gbps o 400 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 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 Direct Connect".
- Proporciona métricas de Amazon CloudWatch para conexiones e interfaces virtuales. Para obtener más información, consulte Supervisar los recursos de Direct Connect.

Después de seleccionar el modelo de resiliencia, AWS Direct Connect Resiliency Toolkit lo 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

Modelos de resiliciencia disponibles

Los modelos de resiliencia disponibles en AWS Direct Connect Resiliency Toolkit son los siguientes:

- Maximum resiliency (Máxima resiliencia): este modelo 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 Direct Connect.
- High resiliency (Alta resiliencia): este modelo 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 Direct Connect.
- Development and test (Desarrollo y pruebas): este modelo 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.

La práctica recomendada consiste en utilizar el Asistente de conexión de AWS Direct Connect Resiliency Toolkit para alcanzar su objetivo de SLA.

> **Note**
>
> Si no desea crear un modelo de resiliencia con AWS Direct Connect Resiliency Toolkit, puede crear una conexión clásica. Para obtener más información sobre las conexiones clásicas, consulte Conexión clásica.

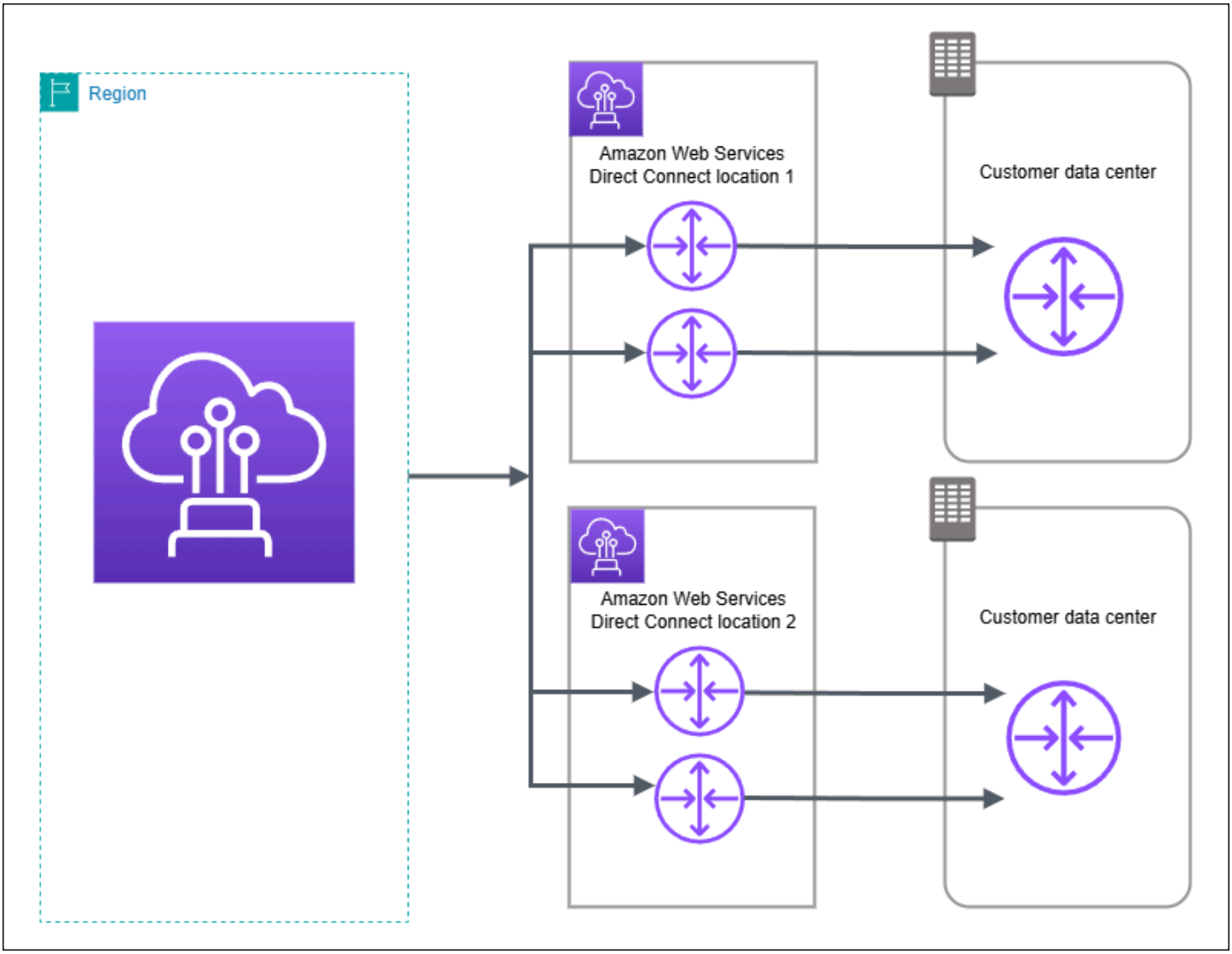
Requisitos previos de AWS Direct Connect Resiliency Toolkit

Tenga en cuenta la siguiente información antes de comenzar la configuración:

- Conozca los Requisitos previos para la conexión.
- El modelo de resiliencia disponible que desea utilizar.

Resiliencia máxima

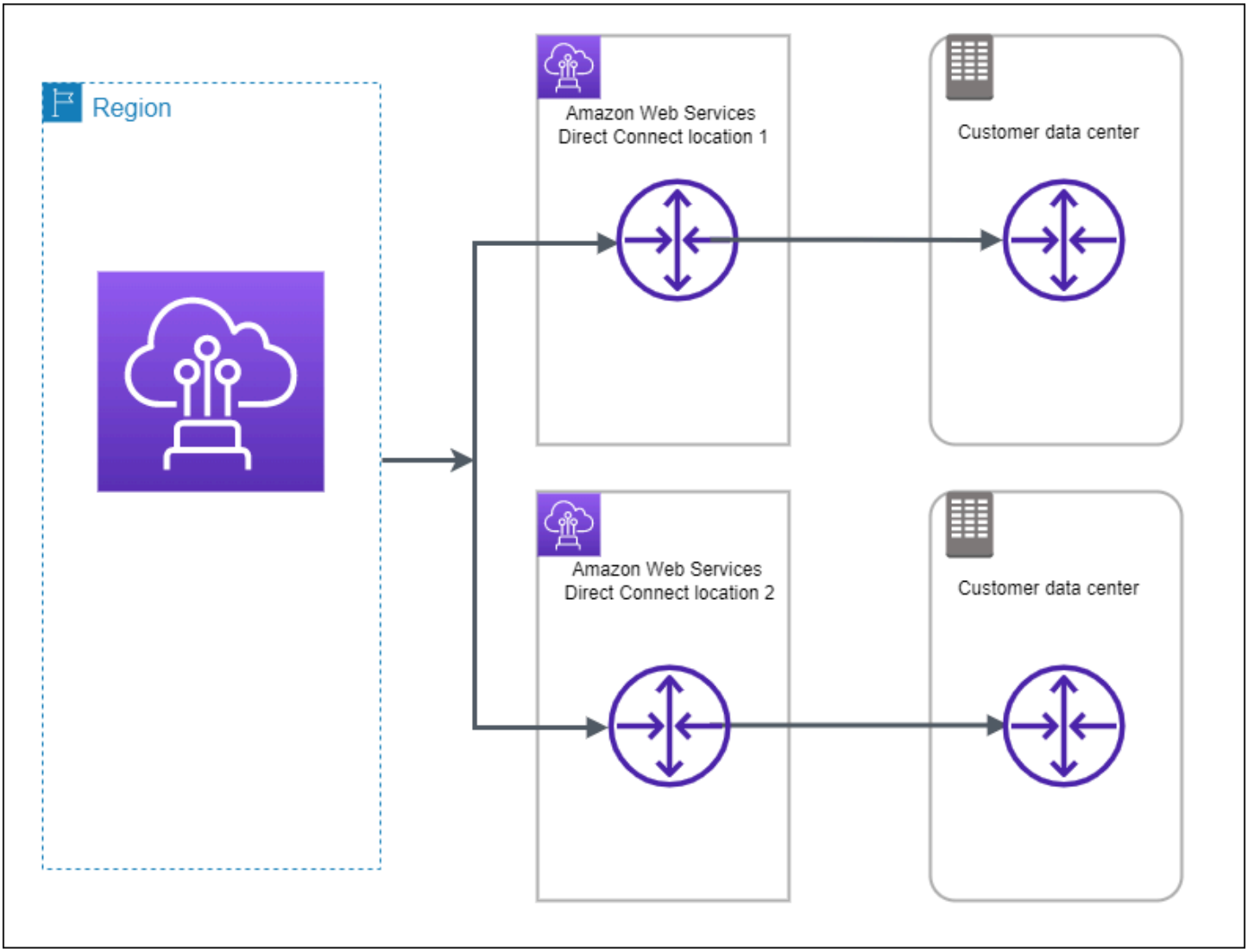
Puede conseguir la máxima resiliencia para cargas de trabajo críticas mediante el uso de conexiones independientes que terminan en dispositivos independientes en más de una ubicación (tal y como se muestra en la siguiente figura). Este modelo proporciona resistencia frente a errores de dispositivo, conectividad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



Para conocer el procedimiento para utilizar el kit de resiliencia de AWS Direct Connect para configurar un modelo de resiliencia máxima, consulte Configuración de la máxima resiliencia.

Alta resiliencia

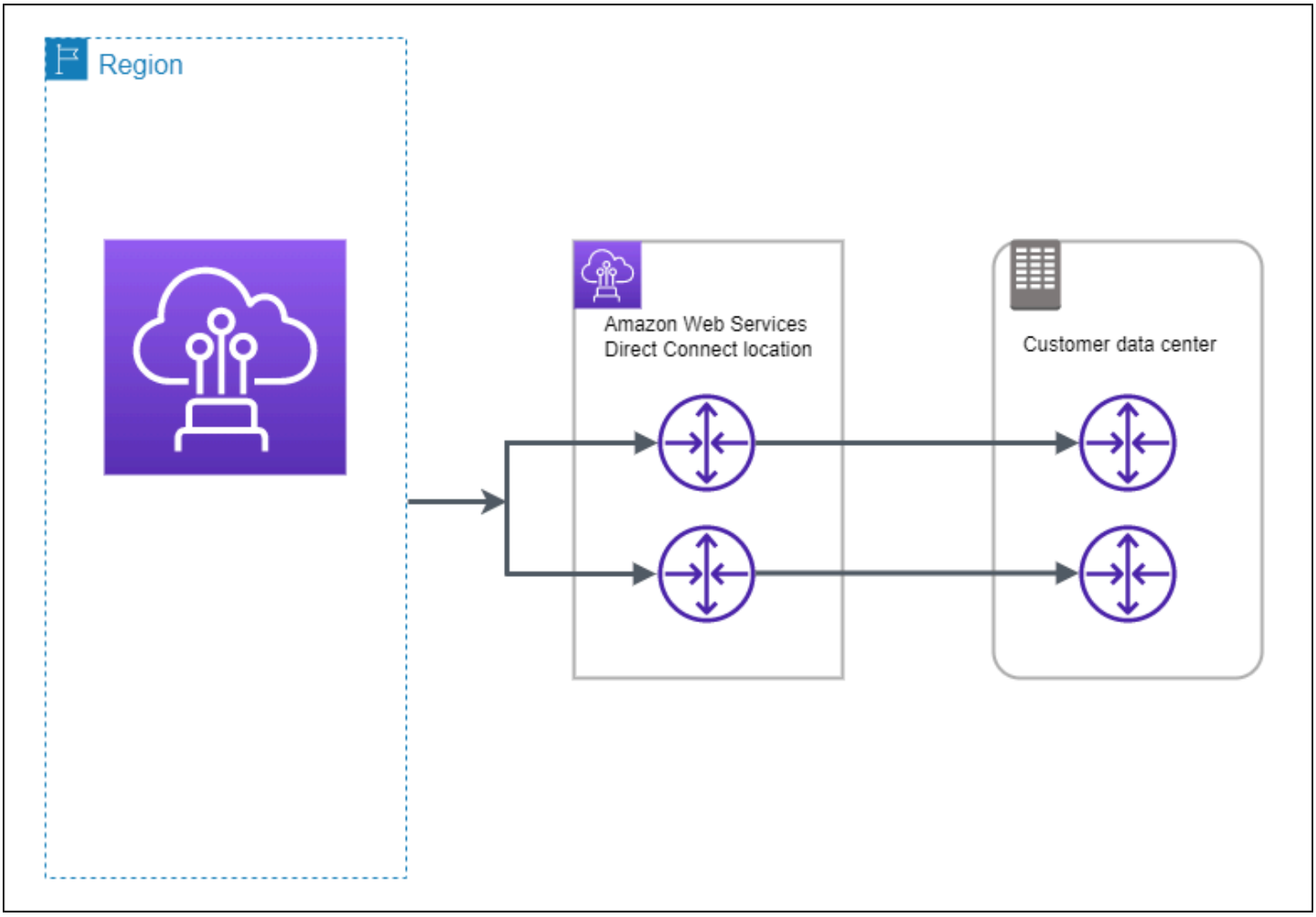
Puede conseguir una alta resiliencia para cargas de trabajo críticas mediante el uso de dos conexiones únicas a varias ubicaciones (tal y como se muestra en la siguiente figura). Este modelo proporciona resiliencia frente a errores de conectividad provocados por un corte de fibra o un error del dispositivo.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



Para conocer el procedimiento para utilizar el kit de resiliencia de AWS Direct Connect para configurar un modelo de alta resiliencia, consulte Configuración de alta resiliencia.

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.



Para conocer el procedimiento para utilizar el kit de resiliencia de AWS Direct Connect para configurar un modelo de resiliencia máxima, consulte Configuración de la resiliencia de las pruebas y el desarrollo.

Prueba de conmutación por error de AWS Direct Connect

Utilice el kit de herramientas de resiliencia de AWS Direct Connect para verificar las rutas de tráfico y comprobar que cumplen los requisitos de resiliencia.

Para conocer los procedimientos para utilizar el kit de herramientas de resiliencia de AWS Direct Connect para realizar pruebas de conmutación por error, consulte Prueba de conmutación por error de Direct Connect.

Configuración de Direct Connect para una máxima resiliciencia con AWS Direct Connect Resiliency Toolkit

En este ejemplo, el kit de herramientas de Direct Connect resiliencia se utiliza para configurar un modelo de máxima resiliencia

Tareas

- 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 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 suscribirse a una Cuenta de AWS

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

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto 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. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a 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 Consola de administración de AWScomo 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 Iniciar sesión como usuario raíz 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.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use 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 Direct Connectconsola en la versión 2/homehttps://console.aws.amazon.com/directconnect/.
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 First Location Service Provider, selecciona la 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 tiene salas de reuniones (MMRs) 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 Segundo proveedor de servicios de ubicación, seleccione la ubicación adecuada Direct Connect .

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 tiene salas de reuniones (MMRs) 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 LOAs está preparado, puede elegir Descargar LOA y, a continuación, hacer clic en Continuar.

   La revisión de tu solicitud y el aprovisionamiento de un puerto AWS para tu conexión pueden tardar hasta 72 horas laborables. 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 VPCs.

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

Recurso	Información necesaria
Conexión	El grupo de 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 Puertas de enlace 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 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 puede admitir una sesión de interconexión BGP para IPv4 cada sesión o una de ellas (doble pila). IPv6 No utilices Elastic IPs (EIPs) ni traigas tus 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 enrutamiento IP en la misma interfaz virtual. Los rangos de

Recurso	Información necesaria

	las direcciones IP que se asignan a cada extremo de la interfaz virtual para la sesión de intercambio de tráfico del BGP.
	
	• IPv4:
	  • (Solo interfaz virtual pública) Debe especificar IPv4 direcciones públicas únicas de su propiedad. El valor puede ser uno de los siguientes:
	  • Un CIDR propiedad del cliente IPv4
	
	Puede ser cualquier tipo de máscara pública IPs (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. Ponte en contacto con AWS Support para solicitar un IPv4 CIDR público (y proporciona un caso de uso en tu solicitud)
	
	Note
	No podemos garantizar que podamos tramitar todas las solicitudes AWS de direcciones públicas IPv4 proporcionadas.
	  • (Solo interfaz virtual privada) Amazon puede generar IPv4 direcciones privadas para usted. Si especifica la suya propia, asegúrese de especific ar privada únicamente CIDRs 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`

Recurso	Información necesaria
	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 te asigna automáticamente un CIDR de IPv6 /125. No puede especificar sus propias direcciones homólogas. IPv6
Familia de direcciones	Si la sesión de emparejamiento de BGP finalizará o. IPv4 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. Para un ASN de 32 bits, el valor debe estar comprendido entre 1 y 4294967294. El sistema autónomo (AS) que se antepone no funciona si utiliza un ASN privado para una interfaz virtual pública. • AWS habilita de forma predeterminada. MD5 Esta opción no se puede modificar. • Una clave de autenticación MD5 BGP. 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	IPv4 Rutas públicas o IPv6 rutas para anunciar a través de BGP. Debe comunicar al menos un prefijo a través del BGP, hasta un máximo de 1 000 prefijos.
	• IPv4: El IPv4 CIDR puede superponerse con otro IPv4 CIDR público que se haya anunciado que Direct Connect se utilice cuando se dé alguna de las siguientes condiciones:
	  • CIDRs Son de diferentes 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. active/passive
	  Para obtener más información, consulte Políticas de enrutamiento y comunidades de BGP.
	• A través de una interfaz virtual pública de Direct Connect, puede especificar cualquier longitud de prefijo de /1 a /32 IPv4 y de /1 a /64 para. IPv6
	• Puede agregar prefijos adicionales a una interfaz virtual 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 interfaz virtual pública y anunciar.

(Solo para interfaces virtuales privadas y de tránsito) Tramas gigantes	La unidad de transmisión máxima (MTU) de los paquetes superados. 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. Direct Connect Si agrega rutas estáticas a una tabla de enrutamiento que apuntan a una puerta de enlace 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 Direct Connect consola y busque Jumbo Frame Capable en la página de configuración general de la interfaz virtual.

Si sus prefijos son públicos o ASNs pertenecen a un ISP o a un operador de red, le solicitamos información adicional. Puede ser un documento con el membrete oficial de la empresa o un correo electrónico con el nombre de dominio de la empresa para comprobar que prefix/ASN puedes utilizar la red.

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

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

1. Abre la Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión 2/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 puerta de enlace fronteriza (BGP) de la puerta de enlace.

      Los valores válidos van desde 1 hasta 4294967294. Esto incluye soporte para ambos ASNs (1-2147483647) y largos (1-4294967294). ASNs Para obtener más información sobre la extensión y la extensión, consulte. ASNs ASNs Soporte de ASN prolongado en Direct Connect
6. En Additional settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un IPv4 BGP o un IPv6 peer, haga lo siguiente:

      [IPv4] Para configurar un par de IPv4 BGP, elija IPv4y realice una de las siguientes acciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip, introduzca la dirección IPv4 CIDR de destino a la que Amazon debe enviar el tráfico.

- En el caso de la IP homóloga del router Amazon, introduce la dirección IPv4 CIDR a la que se va a enviar el tráfico. AWS

  [IPv6] Para configurar un par IPv6 BGP, elija. IPv6 Las IPv6 direcciones homólogas se asignan automáticamente desde el conjunto de IPv6 direcciones de Amazon. No puedes especificar IPv6 direcciones personalizadas.

b. Para proporcionar su propia clave BGP, introduzca su clave BGP MD5 .

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

c. Para anunciar prefijos en Amazon, en el caso de los prefijos que desee anunciar, introduzca las direcciones de destino del IPv4 CIDR (separadas por comas) a las que se debe enrutar 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 consola en la v2/home. Direct Connecthttps://console.aws.amazon.com/directconnect/
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, selecciona Otra AWS cuenta y, a continuación, introduce 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 van desde 1 hasta 4294967294. Esto incluye soporte para ambos ASNs (1-2147483647) y largos (1-4294967294). ASNs Para obtener más información sobre la extensión y la extensión, consulte. ASNs ASNs Soporte de ASN prolongado en Direct Connect

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

   a. Para configurar un IPv4 BGP o un IPv6 peer, haga lo siguiente:

      [IPv4] Para configurar un par de IPv4 BGP, elija IPv4y realice una de las siguientes acciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip, introduzca la dirección IPv4 CIDR de destino a la que Amazon debe enviar el tráfico.
      - Para el router peer ip de Amazon, introduce la dirección IPv4 CIDR a la que se va a enviar el tráfico. AWS

      > **Important**
      >
      > Al configurar las interfaces virtuales de AWS Direct Connect, puede especificar sus propias direcciones IP mediante RFC 1918, utilizar otros esquemas de direccionamiento u optar por direcciones CIDR asignadas de IPv4 /29 direcciones CIDR AWS asignadas desde el rango Link-Local RFC 3927 IPv4 169.254.0.0/16 para la conectividad. point-to-point Estas point-to-point conexiones deben usarse exclusivamente para la interconexión eBGP entre el router de puerta de enlace del cliente y el punto final de Direct Connect. Para el tráfico de VPC o la creación de túneles, como AWS Site-to-Site Private IP VPN o Transit Gateway Connect, AWS recomienda utilizar una interfaz de bucle invertido o LAN en el router de puerta de enlace del cliente como dirección de origen o destino en lugar de las conexiones. point-to-point

- Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.
- Para obtener más información sobre el RFC 3927, consulte Configuración dinámica de direcciones locales de enlace. IPv4

[IPv6] Para configurar un par IPv6 BGP, elija. IPv6 Las IPv6 direcciones homólogas se asignan automáticamente desde el conjunto de IPv6 direcciones de Amazon. No puedes especificar IPv6 direcciones 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 los requisitos de resiliencia. Para obtener más información, consulte the section called "Prueba de conmutación por error de 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 Direct Connect identificador esté en el rastreo de la red.

Para verificar la conexión de la interfaz virtual a Amazon VPC

1. Con una AMI a la que se pueda hacer ping, como una AMI de Amazon Linux, lance una EC2 instancia en la VPC que está conectada a la puerta de enlace privada virtual. Los Amazon Linux AMIs están disponibles en la pestaña Inicio rápido cuando utilizas el asistente de lanzamiento de instancias en la EC2 consola de Amazon. Para obtener más información, consulte Lanzar una instancia en la Guía del EC2 usuario de Amazon. 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. Una vez ejecutada la instancia, obtén su IPv4 dirección privada (por ejemplo, 10.0.0.4). La EC2 consola de Amazon muestra la dirección como parte de los detalles de la instancia.
3. Haz ping a la IPv4 dirección privada y obtén una respuesta.

Configuración de Direct Connect para una alta resiliciencia con AWS Direct Connect Resiliency Toolkit

En este ejemplo, el kit de herramientas de Direct Connect resiliencia se utiliza para configurar un modelo de alta resiliencia

Tareas

- 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 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. Abrir https://portal.aws.amazon.com/billing/registro.

2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto 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. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a 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 Consola de administración de AWScomo 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 Iniciar sesión como usuario raíz 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.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use 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 Direct Connectconsola en la versión 2/homehttps://console.aws.amazon.com/directconnect/.
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 First Location Service Provider, seleccione la ubicación adecuada Direct Connect .

   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 tiene salas de reuniones (MMRs) 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 Segundo proveedor de servicios de ubicación, seleccione la ubicación adecuada Direct Connect .

   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 tiene salas de reuniones (MMRs) 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 LOAs está preparado, puede elegir Descargar LOA y, a continuación, hacer clic en Continuar.

La revisión de tu solicitud y el aprovisionamiento de un puerto AWS para tu conexión pueden tardar hasta 72 horas laborables. 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 al registrarte 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 VPCs.

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

Recurso	Información necesaria
Conexión	El grupo de 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 Puertas de enlace 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 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 puede admitir una sesión de interconexión BGP para IPv4 cada sesión o una de ellas (doble pila). IPv6 No utilices Elastic IPs (EIPs) ni traigas tus 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 enrutamiento 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 interfaz virtual pública) Debe especificar IPv4 direcciones públicas únicas de su propiedad. El valor puede ser uno de los siguientes: • Un CIDR propiedad del cliente IPv4 Puede ser cualquier tipo de máscara pública IPs (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. Ponte en contacto con AWS Support para solicitar un IPv4 CIDR público (y proporciona un caso de uso en tu solicitud) **Note** No podemos garantizar que podamos tramitar todas las solicitudes AWS de direcciones públicas IPv4 proporcionadas. • (Solo interfaz virtual privada) Amazon puede generar IPv4 direcciones privadas para usted. Si especifica la suya propia, asegúrese de especific ar privada únicamente CIDRs para la interfaz de su router y la interfaz

Recurso	Información necesaria
	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 te asigna automáticamente un CIDR de IPv6 /125. No puede especificar sus propias direcciones homólogas. IPv6
Familia de direcciones	Si la sesión de emparejamiento de BGP finalizará o. IPv4 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. Para un ASN de 32 bits, el valor debe estar comprendido entre 1 y 4294967294. El sistema autónomo (AS) que se antepone no funciona si utiliza un ASN privado para una interfaz virtual pública. • AWS habilita de forma predeterminada. MD5 Esta opción no se puede modificar. • Una clave de autenticación MD5 BGP. 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	IPv4 Rutas públicas o IPv6 rutas para anunciar a través de BGP. Debe comunicar al menos un prefijo a través del BGP, hasta un máximo de 1 000 prefijos.
	• IPv4: El IPv4 CIDR puede superponerse con otro IPv4 CIDR público que se haya anunciado que Direct Connect se utilice cuando se dé alguna de las siguientes condiciones:
	  • CIDRs Son de diferentes 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. active/passive
	  Para obtener más información, consulte Políticas de enrutamiento y comunidades de BGP.
	• A través de una interfaz virtual pública de Direct Connect, puede especificar cualquier longitud de prefijo de /1 a /32 IPv4 y de /1 a /64 para. IPv6
	• Puede agregar prefijos adicionales a una interfaz virtual 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 interfaz virtual pública y anunciar.

(Solo para interfaces virtuales privadas y de tránsito) Tramas gigantes	La unidad de transmisión máxima (MTU) de los paquetes superados. 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. Direct Connect Si agrega rutas estáticas a una tabla de enrutamiento que apuntan a una puerta de enlace 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 Direct Connect consola y busque Jumbo Frame Capable en la página de configuración general de la interfaz virtual.

Si sus prefijos son públicos o ASNs pertenecen a un ISP o a un operador de red, AWS le solicita información adicional. Puede ser un documento con el membrete oficial de la empresa o un correo electrónico con el nombre de dominio de la empresa para comprobar que prefix/ASN puedes utilizar la red.

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

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

1. Abre la Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión 2/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 puerta de enlace fronteriza (BGP) de la puerta de enlace.

      Los valores válidos van desde 1 hasta 4294967294. Esto incluye soporte para ambos ASNs (1-2147483647) y largos (1-4294967294). ASNs Para obtener más información sobre la extensión y la extensión, consulte. ASNs ASNs Soporte de ASN prolongado en Direct Connect
6. En Additional settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un IPv4 BGP o un IPv6 peer, haga lo siguiente:

      [IPv4] Para configurar un par de IPv4 BGP, elija IPv4y realice una de las siguientes acciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip, introduzca la dirección IPv4 CIDR de destino a la que Amazon debe enviar el tráfico.

- En el caso de la IP homóloga del router Amazon, introduce la dirección IPv4 CIDR a la que se va a enviar el tráfico. AWS

  [IPv6] Para configurar un par IPv6 BGP, elija. IPv6 Las IPv6 direcciones homólogas se asignan automáticamente desde el conjunto de IPv6 direcciones de Amazon. No puedes especificar IPv6 direcciones personalizadas.

b. Para proporcionar su propia clave BGP, introduzca su clave BGP MD5 .

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

c. Para anunciar prefijos en Amazon, en el caso de los prefijos que desee anunciar, introduzca las direcciones de destino del IPv4 CIDR (separadas por comas) a las que se debe enrutar 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 consola en la v2/home. Direct Connecthttps://console.aws.amazon.com/directconnect/
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, selecciona Otra AWS cuenta y, a continuación, introduce 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 van desde 1 hasta 4294967294. Esto incluye soporte para ambos ASNs (1-2147483647) y largos (1-4294967294). ASNs Para obtener más información sobre la extensión y la extensión, consulte. ASNs ASNs Soporte de ASN prolongado en Direct Connect

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

   a. Para configurar un IPv4 BGP o un IPv6 peer, haga lo siguiente:

      [IPv4] Para configurar un par de IPv4 BGP, elija IPv4y realice una de las siguientes acciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip, introduzca la dirección IPv4 CIDR de destino a la que Amazon debe enviar el tráfico.
      - Para el router peer ip de Amazon, introduce la dirección IPv4 CIDR a la que se va a enviar el tráfico. AWS

      > **Important**
      >
      > Al configurar las interfaces virtuales de AWS Direct Connect, puede especificar sus propias direcciones IP mediante RFC 1918, utilizar otros esquemas de direccionamiento u optar por direcciones CIDR asignadas de IPv4 /29 direcciones CIDR AWS asignadas desde el rango Link-Local RFC 3927 IPv4 169.254.0.0/16 para la conectividad. point-to-point Estas point-to-point conexiones deben usarse exclusivamente para la interconexión eBGP entre el router de puerta de enlace del cliente y el punto final de Direct Connect. Para el tráfico de VPC o la creación de túneles, como AWS Site-to-Site Private IP VPN o Transit Gateway Connect, AWS recomienda utilizar una interfaz de bucle invertido o LAN en el router de puerta de enlace del cliente como dirección de origen o destino en lugar de las conexiones. point-to-point

- Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.
- Para obtener más información sobre el RFC 3927, consulte Configuración dinámica de direcciones locales de enlace. IPv4

[IPv6] Para configurar un par IPv6 BGP, elija. IPv6 Las IPv6 direcciones homólogas se asignan automáticamente desde el conjunto de IPv6 direcciones de Amazon. No puedes especificar IPv6 direcciones 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 los requisitos de resiliencia. Para obtener más información, consulte the section called "Prueba de conmutación por error de 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 Direct Connect identificador esté en el rastreo de la red.

Para verificar la conexión de la interfaz virtual a Amazon VPC

1. Con una AMI a la que se pueda hacer ping, como una AMI de Amazon Linux, lance una EC2 instancia en la VPC que está conectada a la puerta de enlace privada virtual. Los Amazon Linux AMIs están disponibles en la pestaña Inicio rápido cuando utilizas el asistente de lanzamiento de instancias en la EC2 consola de Amazon. Para obtener más información, consulte Lanzar una instancia en la Guía del EC2 usuario de Amazon. 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. Una vez ejecutada la instancia, obtén su IPv4 dirección privada (por ejemplo, 10.0.0.4). La EC2 consola de Amazon muestra la dirección como parte de los detalles de la instancia.
3. Haz ping a la IPv4 dirección privada y obtén una respuesta.

Configure AWS Direct Connect para desarrollar y probar la resiliencia con el kit de herramientas de AWS Direct Connect resiliencia

En este ejemplo, el kit de herramientas de Direct Connect resiliencia se utiliza para configurar un modelo de resiliencia de desarrollo y prueba

Tareas

- 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 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 suscribirse a una Cuenta de AWS

1. Abrir https://portal.aws.amazon.com/billing/registro.

2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto 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. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a 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 Consola de administración de AWScomo 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 Iniciar sesión como usuario raíz 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.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use 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 Direct Connectconsola en la versión 2/homehttps://console.aws.amazon.com/directconnect/.
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 First Location Service Provider, seleccione la ubicación adecuada Direct Connect .

   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 tiene salas de reuniones (MMRs) 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 LOAs está preparado, puede elegir Descargar LOA y, a continuación, hacer clic en Continuar.

   La revisión de tu solicitud y el aprovisionamiento de un puerto AWS para tu conexión pueden tardar hasta 72 horas laborables. 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 al registrarte AWS. Si no responde en un plazo de 7 días, se eliminará la conexión.

Paso 3: Crear una interfaz virtual

Para empezar a utilizar 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 VPCs.

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

Recurso	Información necesaria
Conexión	El grupo de 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 Puertas de enlace 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 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 puede admitir una sesión de interconexión BGP para IPv4 cada sesión o una de ellas (doble pila). IPv6 No utilices Elastic IPs (EIPs)

Recurso	Información necesaria
	ni traigas tus 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 enrutamiento 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 interfaz virtual pública) Debe especificar IPv4 direcciones públicas únicas de su propiedad. El valor puede ser uno de los siguientes: • Un CIDR propiedad del cliente IPv4 Puede ser cualquier tipo de máscara pública IPs (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. Ponte en contacto con AWS Support para solicitar un IPv4 CIDR público (y proporciona un caso de uso en tu solicitud) **Note** No podemos garantizar que podamos tramitar todas las solicitudes AWS de direcciones públicas IPv4 proporcionadas. • (Solo interfaz virtual privada) Amazon puede generar IPv4 direcciones privadas para usted. Si especifica la suya propia, asegúrese de especific ar privada únicamente CIDRs 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

Recurso	Información necesaria
	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 te asigna automáticamente un CIDR de IPv6 /125. No puede especificar sus propias direcciones homólogas. IPv6
Familia de direcciones	Si la sesión de emparejamiento de BGP finalizará o. IPv4 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. Para un ASN de 32 bits, el valor debe estar comprendido entre 1 y 4294967294. El sistema autónomo (AS) que se antepone no funciona si utiliza un ASN privado para una interfaz virtual pública. • AWS habilita de forma predeterminada. MD5 Esta opción no se puede modificar. • Una clave de autenticación MD5 BGP. 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	IPv4 Rutas públicas o IPv6 rutas para anunciar a través de BGP. Debe comunicar al menos un prefijo a través del BGP, hasta un máximo de 1 000 prefijos.
	• IPv4: El IPv4 CIDR puede superponerse con otro IPv4 CIDR público que se haya anunciado que Direct Connect se utilice cuando se dé alguna de las siguientes condiciones:
	  • CIDRs Son de diferentes 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. active/passive
	  Para obtener más información, consulte Políticas de enrutamiento y comunidades de BGP.
	• A través de una interfaz virtual pública de Direct Connect, puede especificar cualquier longitud de prefijo de /1 a /32 IPv4 y de /1 a /64 para. IPv6
	• Puede agregar prefijos adicionales a una interfaz virtual 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 interfaz virtual pública y anunciar.

(Solo para interfaces virtuales privadas y de tránsito) Tramas gigantes	La unidad de transmisión máxima (MTU) de los paquetes superados. 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. Direct Connect Si agrega rutas estáticas a una tabla de enrutamiento que apuntan a una puerta de enlace 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 Direct Connect consola y busque Jumbo Frame Capable en la página de configuración general de la interfaz virtual.

Si sus prefijos son públicos o ASNs pertenecen a un ISP o a un operador de red, le solicitamos información adicional. Puede ser un documento con el membrete oficial de la empresa o un correo electrónico con el nombre de dominio de la empresa para comprobar que prefix/ASN puedes utilizar la red.

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

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

1. Abre la Direct Connectconsola en la versión 2/home. https://console.aws.amazon.com/directconnect/
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 puerta de enlace fronteriza (BGP) de la puerta de enlace.

      Los valores válidos van desde 1 hasta 4294967294. Esto incluye soporte para ambos ASNs (1-2147483647) y largos (1-4294967294). ASNs Para obtener más información sobre la extensión y la extensión, consulte. ASNs ASNs Soporte de ASN prolongado en Direct Connect
6. En Additional settings (Configuración adicional), haga lo siguiente:

   a. Para configurar un IPv4 BGP o un IPv6 peer, haga lo siguiente:

      [IPv4] Para configurar un par de IPv4 BGP, elija IPv4y realice una de las siguientes acciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip, introduzca la dirección IPv4 CIDR de destino a la que Amazon debe enviar el tráfico.

- En el caso de la IP homóloga del router Amazon, introduce la dirección IPv4 CIDR a la que se va a enviar el tráfico. AWS

  [IPv6] Para configurar un par IPv6 BGP, elija. IPv6 Las IPv6 direcciones homólogas se asignan automáticamente desde el conjunto de IPv6 direcciones de Amazon. No puedes especificar IPv6 direcciones personalizadas.

b. Para proporcionar su propia clave BGP, introduzca su clave BGP MD5 .

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

c. Para anunciar prefijos en Amazon, en el caso de los prefijos que desee anunciar, introduzca las direcciones de destino del IPv4 CIDR (separadas por comas) a las que se debe enrutar 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 consola en la v2/home. Direct Connecthttps://console.aws.amazon.com/directconnect/
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, selecciona Otra AWS cuenta y, a continuación, introduce 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 van desde 1 hasta 4294967294. Esto incluye soporte para ambos ASNs (1-2147483647) y largos (1-4294967294). ASNs Para obtener más información sobre la extensión y la extensión, consulte. ASNs ASNs Soporte de ASN prolongado en Direct Connect

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

   a. Para configurar un IPv4 BGP o un IPv6 peer, haga lo siguiente:

      [IPv4] Para configurar un par de IPv4 BGP, elija IPv4y realice una de las siguientes acciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip, introduzca la dirección IPv4 CIDR de destino a la que Amazon debe enviar el tráfico.
      - Para el router peer ip de Amazon, introduce la dirección IPv4 CIDR a la que se va a enviar el tráfico. AWS

      > **Important**
      >
      > Al configurar las interfaces virtuales de AWS Direct Connect, puede especificar sus propias direcciones IP mediante RFC 1918, utilizar otros esquemas de direccionamiento u optar por direcciones CIDR asignadas de IPv4 /29 direcciones CIDR AWS asignadas desde el rango Link-Local RFC 3927 IPv4 169.254.0.0/16 para la conectividad. point-to-point Estas point-to-point conexiones deben usarse exclusivamente para la interconexión eBGP entre el router de puerta de enlace del cliente y el punto final de Direct Connect. Para el tráfico de VPC o la creación de túneles, como AWS Site-to-Site Private IP VPN o Transit Gateway Connect, AWS recomienda utilizar una interfaz de bucle invertido o LAN en el router de puerta de enlace del cliente como dirección de origen o destino en lugar de las conexiones. point-to-point

- Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.
- Para obtener más información sobre el RFC 3927, consulte Configuración dinámica de direcciones locales de enlace. IPv4

[IPv6] Para configurar un par IPv6 BGP, elija. IPv6 Las IPv6 direcciones homólogas se asignan automáticamente desde el conjunto de IPv6 direcciones de Amazon. No puedes especificar IPv6 direcciones 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 los requisitos de resiliencia. Para obtener más información, consulte the section called "Prueba de conmutación por error de 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 Direct Connect identificador esté en el rastreo de la red.

Para verificar la conexión de la interfaz virtual a Amazon VPC

1. Con una AMI a la que se pueda hacer ping, como una AMI de Amazon Linux, lance una EC2 instancia en la VPC que está conectada a la puerta de enlace privada virtual. Los Amazon Linux AMIs están disponibles en la pestaña Inicio rápido cuando utilizas el asistente de lanzamiento de instancias en la EC2 consola de Amazon. Para obtener más información, consulte Lanzar una instancia en la Guía del EC2 usuario de Amazon. 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. Una vez ejecutada la instancia, obtén su IPv4 dirección privada (por ejemplo, 10.0.0.4). La EC2 consola de Amazon muestra la dirección como parte de los detalles de la instancia.
3. Haz ping a la IPv4 dirección privada y obtén una respuesta.

Direct ConnectPrueba de conmutación por error de

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 característica durante un periodo de mantenimiento de Direct Connect, ya que es posible que la sesión BGP se restablezca 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 “Consulte un historial de pruebas de conmutación por error de la 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.

Temas

- Iniciar una prueba de conmutación por error de interfaz virtual del kit de herramientas de resiliencia de AWS Direct Connect
- Consulte el historial de pruebas de conmutación por error de la interfaz virtual del kit de herramientas de resiliencia de AWS Direct Connect
- Detener una prueba de conmutación por error de interfaz virtual del kit de herramientas de resiliencia de AWS Direct Connect

Iniciar una prueba de conmutación por error de interfaz virtual del kit de herramientas de resiliencia de AWS Direct Connect

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

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

1. Abra la consola de Direct Connect 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 hábiles).

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

Utilice StartBgpFailoverTest.

Consulte el historial de pruebas de conmutación por error de la interfaz virtual del kit de herramientas de resiliencia de AWS Direct Connect

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

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

1. Abra la consola de Direct Connect 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

Utilice ListVirtualInterfaceTestHistory.

Detener una prueba de conmutación por error de interfaz virtual del kit de herramientas de resiliencia de AWS Direct Connect

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

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

1. Abra la consola de Direct Connect 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. Elija 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

Utilice StopBgpFailoverTest.

Direct Connect Conexión clásica

Una conexión clásica ofrece un enfoque sencillo para establecer una conectividad de red dedicada entre su local en las instalaciones y AWS. Este tipo de conexión es ideal para las organizaciones que prefieren administrar sus propias configuraciones de red y que ya cuentan con una infraestructura de Direct Connect. La conexión clásica no se basa en el kit de herramientas de resiliencia de AWS Direct Connect .

Seleccione la conexión clásica si tiene conexiones existentes y desea agregar otras más. Una conexión clásica tiene un SLA del 95 %. Sin embargo, no proporciona resiliencia ni redundancia, que solo se encuentran en el kit de herramientas de AWS Direct Connect resiliencia al crear una conexión.

> **Note**
>
> Antes de configurar una conexión clásica, conozca Requisitos previos para la conexión.

Tareas

- Configure una conexión clásica Direct Connect

Configure una conexión clásica Direct Connect

Configure una conexión clásica cuando tenga conexiones de Direct Connect existentes.

Paso 1: Inscríbase en AWS

Para usarla 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 suscribirse a una Cuenta de AWS

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

   Parte del procedimiento de registro consiste en recibir una llamada telefónica o mensaje de texto 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. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a 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 Consola de administración de AWScomo 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 Iniciar sesión como usuario raíz 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.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use 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 Direct Connect dedicada

En el caso de las conexiones dedicadas, puede enviar una solicitud de conexión mediante la 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 Direct Connect ubicación en la que se va a finalizar la conexión.

> **Note**
>
> No puede usar la 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 Direct Connect conexión nueva

1. Abre la Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión 2/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 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 tiene salas de reuniones (MMRs) 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 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 AWS para su conexión pueden tardar hasta 72 horas laborables. 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 Direct Connect conexiones dedicadas y alojadas.

Aceptación de la conexión alojada

Debe aceptar la conexión alojada en la 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 Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión 2/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 conectarse y el proveedor de AWS 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 la versión 2/home. Direct Connecthttps://console.aws.amazon.com/directconnect/
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 laborales, póngase en contacto con AWS Support.

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

   - Si trabajas con un AWS Direct Connect socio o un proveedor de red, envíales la LOA-CFA para que puedan solicitarte una conexión cruzada en esa ubicación. 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 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.

Direct Connect las ubicaciones que aparecen como sitios múltiples (por ejemplo, Equinix DC1 - DC6 y DC1 0-DC11) se configuran como un 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 Direct Connect ubicación. Para conseguir un alto nivel de disponibilidad, configure conexiones con diferentes ubicaciones de Direct Connect .

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

Paso 4: Crear una interfaz virtual

Para empezar a utilizar 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 VPCs.

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

Recurso	Información necesaria
Conexión	El grupo de 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 Puertas de enlace 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 Direct Connect .

Recurso	Información necesaria
	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 puede admitir una sesión de interconexión BGP para IPv4 cada sesión o una de ellas (doble pila). IPv6 No utilices Elastic IPs (EIPs) ni traigas tus 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 enrutamiento 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 interfaz virtual pública) Debe especificar IPv4 direcciones públicas únicas de su propiedad. El valor puede ser uno de los siguientes: • Un CIDR propiedad del cliente IPv4 Puede ser cualquier tipo de máscara pública IPs (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. Ponte en contacto con AWS Support para solicitar un IPv4 CIDR público (y proporciona un caso de uso en tu solicitud) **Note** No podemos garantizar que podamos tramitar todas las solicitudes AWS de direcciones públicas IPv4 proporcionadas. • (Solo interfaz virtual privada) Amazon puede generar IPv4 direcciones privadas para usted. Si especifica la suya propia, asegúrese de especific ar privada únicamente CIDRs para la interfaz de su router y la interfaz

Recurso	Información necesaria
	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 te asigna automáticamente un CIDR de IPv6 /125. No puede especificar sus propias direcciones homólogas. IPv6
Familia de direcciones	Si la sesión de emparejamiento de BGP finalizará o. IPv4 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. Para un ASN de 32 bits, el valor debe estar comprendido entre 1 y 4294967294. El sistema autónomo (AS) que se antepone no funciona si utiliza un ASN privado para una interfaz virtual pública. • AWS habilita de forma predeterminada. MD5 Esta opción no se puede modificar. • Una clave de autenticación MD5 BGP. 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	IPv4 Rutas públicas o IPv6 rutas para anunciar a través de BGP. Debe comunicar al menos un prefijo a través del BGP, hasta un máximo de 1 000 prefijos.
	• IPv4: El IPv4 CIDR puede superponerse con otro IPv4 CIDR público que se haya anunciado que Direct Connect se utilice cuando se dé alguna de las siguientes condiciones:
	  • CIDRs Son de diferentes 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. active/passive
	  Para obtener más información, consulte Políticas de enrutamiento y comunidades de BGP.
	• A través de una interfaz virtual pública de Direct Connect, puede especificar cualquier longitud de prefijo de /1 a /32 IPv4 y de /1 a /64 para. IPv6
	• Puede agregar prefijos adicionales a una interfaz virtual 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 interfaz virtual pública y anunciar.

(Solo para interfaces virtuales privadas y de tránsito) Tramas gigantes	La unidad de transmisión máxima (MTU) de los paquetes superados. 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. Direct Connect Si agrega rutas estáticas a una tabla de enrutamiento que apuntan a una puerta de enlace 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 Direct Connect consola y busque Jumbo Frame Capable en la página de configuración general de la interfaz virtual.

Le solicitamos información adicional si sus prefijos son públicos o si ASNs pertenecen a un ISP o a un operador de red. Puede ser un documento con el membrete oficial de la empresa o un correo electrónico con el nombre de dominio de la empresa para comprobar que usted prefix/ASN puede utilizar la red.

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 marcos gigantes, selecciónela en la 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 laborables.

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

1. Abre la Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión 2/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 de protocolo de puerta de enlace fronteriza del enrutador del mismo nivel de las instalaciones de la nueva interfaz virtual. Los valores válidos van desde 1 hasta 4294967294. Esto incluye soporte para ambos ASNs

(1-2147483647) y largos (1-4294967294). ASNs Para obtener más información sobre la extensión y la extensión, consulte. ASNs ASNs Soporte de ASN prolongado en Direct Connect

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

   a. Para configurar un IPv4 BGP o un IPv6 peer, haga lo siguiente:

      [IPv4] Para configurar un par de IPv4 BGP, elija IPv4y realice una de las siguientes acciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip, introduzca la dirección IPv4 CIDR de destino a la que Amazon debe enviar el tráfico.
      - En el caso de la IP homóloga del router Amazon, introduce la dirección IPv4 CIDR a la que se va a enviar el tráfico. AWS

      [IPv6] Para configurar un par IPv6 BGP, elija. IPv6 Las IPv6 direcciones homólogas se asignan automáticamente desde el conjunto de IPv6 direcciones de Amazon. No puedes especificar IPv6 direcciones personalizadas.

   b. Para proporcionar su propia clave BGP, introduzca su clave BGP MD5 .

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

   c. Para anunciar prefijos en Amazon, en el caso de los prefijos que desee anunciar, introduzca las direcciones de destino del IPv4 CIDR (separadas por comas) a las que se debe enrutar 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 consola en la v2/home. Direct Connecthttps://console.aws.amazon.com/directconnect/
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, selecciona Otra AWS cuenta y, a continuación, introduce 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 van desde 1 hasta 4294967294. Esto incluye soporte para ambos ASNs (1-2147483647) y largos (1-4294967294). ASNs Para obtener más información sobre la extensión y la extensión, consulte. ASNs ASNs Soporte de ASN prolongado en Direct Connect

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

   a. Para configurar un IPv4 BGP o un IPv6 peer, haga lo siguiente:

      [IPv4] Para configurar un par de IPv4 BGP, elija IPv4y realice una de las siguientes acciones:

      - Para especificar estas direcciones IP usted mismo, en Your router peer ip, introduzca la dirección IPv4 CIDR de destino a la que Amazon debe enviar el tráfico.
      - Para el router peer ip de Amazon, introduce la dirección IPv4 CIDR a la que se va a enviar el tráfico. AWS

      > **Important**
      >
      > Al configurar las interfaces virtuales de AWS Direct Connect, puede especificar sus propias direcciones IP mediante RFC 1918, utilizar otros esquemas de direccionamiento u optar por direcciones CIDR asignadas de IPv4 /29 direcciones

CIDR AWS asignadas desde el rango Link-Local RFC 3927 IPv4 169.254.0.0/16 para la conectividad. point-to-point Estas point-to-point conexiones deben usarse exclusivamente para la interconexión eBGP entre el router de puerta de enlace del cliente y el punto final de Direct Connect. Para el tráfico de VPC o la creación de túneles, como AWS Site-to-Site Private IP VPN o Transit Gateway Connect, AWS recomienda utilizar una interfaz de bucle invertido o LAN en el router de puerta de enlace del cliente como dirección de origen o destino en lugar de las conexiones. point-to-point

- Para obtener más información sobre la RFC 1918, consulte Address Allocation for Private Internets.
- Para obtener más información sobre la RFC 3927, consulte Configuración dinámica de direcciones locales de enlace. IPv4

[IPv6] Para configurar un par IPv6 BGP, elija. IPv6 Las IPv6 direcciones homólogas se asignan automáticamente desde el conjunto de IPv6 direcciones de Amazon. No puedes especificar IPv6 direcciones 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 interfaz virtual pública.

Paso 5: Descargar la configuración del enrutador

Una vez que haya creado una interfaz virtual para la 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 Direct Connectconsola en la 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 Direct Connect.

Para obtener más información sobre la configuración manual de su router, consulte Descargar el archivo de configuración del enrutador.

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 Direct Connect dispositivo, consulte. Solución 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 enrutamiento.

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

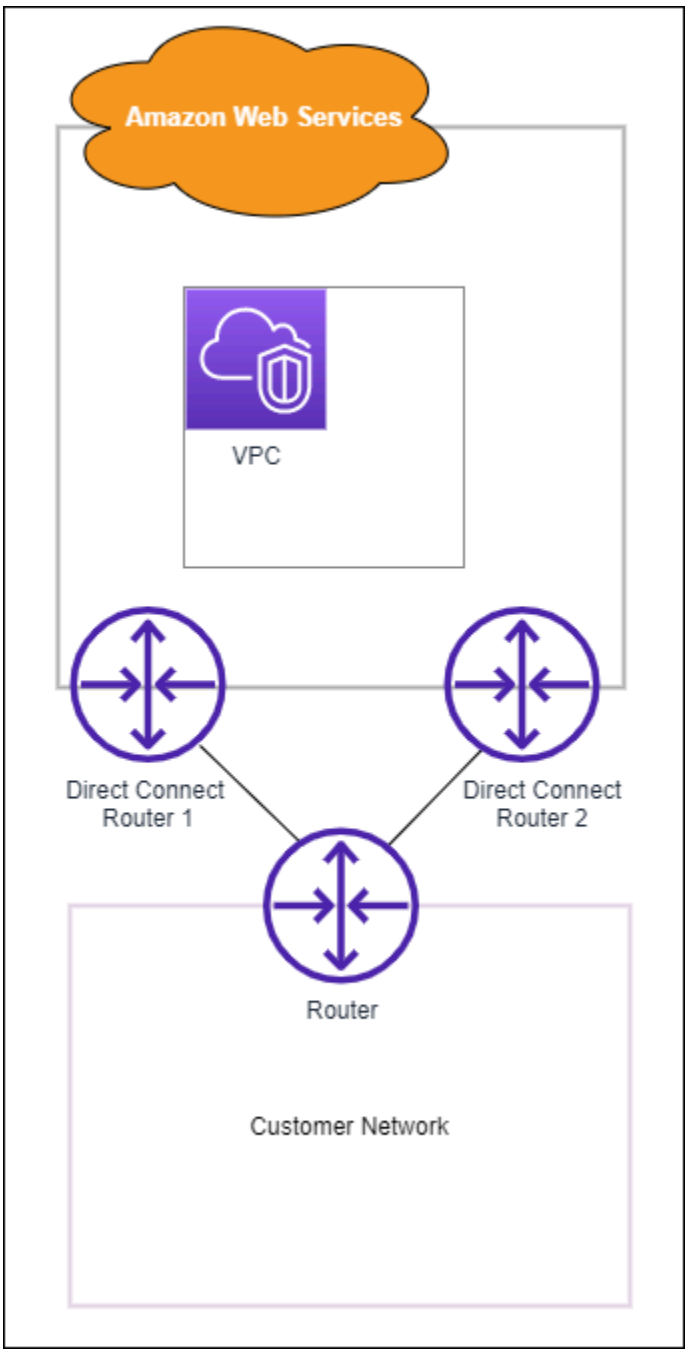
- Ejecute `traceroute` y verifique que el Direct Connect identificador esté en el rastreo de la red.

Para verificar la conexión de la interfaz virtual a Amazon VPC

1. Con una AMI a la que se pueda hacer ping, como una AMI de Amazon Linux, lance una EC2 instancia en la VPC que está conectada a la puerta de enlace privada virtual. Los Amazon Linux AMIs están disponibles en la pestaña Inicio rápido cuando utilizas el asistente de lanzamiento de instancias en la EC2 consola de Amazon. Para obtener más información, consulte Lanzar una instancia en la Guía del EC2 usuario de Amazon. 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. Una vez ejecutada la instancia, obtén su IPv4 dirección privada (por ejemplo, 10.0.0.4). La EC2 consola de Amazon muestra la dirección como parte de los detalles de la instancia.
3. Haz ping a la IPv4 dirección privada y obtén 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. 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 enrutamiento de la tabla de ruteo para direccionar a la nueva interfaz de red.

- Puede utilizar sus propias instancias para el enrutamiento; 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. Direct Connect

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

Direct Connect mantenimiento

Direct Connect se compromete a garantizar la seguridad, la disponibilidad y la escalabilidad del servicio. Es por ello que, para mantener estos estándares, es necesario un mantenimiento periódico de los dispositivos de red de hardware. El mantenimiento de Direct Connect se divide en dos tipos: planificado y de emergencia.

Estos eventos de mantenimiento incluyen abordar las vulnerabilidades de seguridad y los problemas de hardware, así como realizar migraciones de dispositivos para cumplir con las normas, solucionar los desperfectos y ofrecer nuevas características. Las prácticas descritas en Preparación de los eventos de mantenimiento preparan mejor su entorno de Direct Connect para evitar interrupciones durante los eventos de mantenimiento. Si tiene una configuración de red no resiliente o una conexión única, experimentará una interrupción en la conectividad entre la red local y los recursos. AWS

Direct Connect envía notificaciones por correo electrónico sobre los eventos de mantenimiento planificados y de emergencia a la dirección de correo electrónico asociada a la AWS cuenta propietaria de la conexión Direct Connect o del recurso de interfaz virtual. Si utiliza una conexión alojada de Direct Connect con uno de los socios de entrega de Direct Connect, se comunicará por correo electrónico sobre el evento de mantenimiento a usted y a la cuenta del socio. Además, podrá agregar direcciones de correo electrónico o listas de distribución adicionales para recibir notificaciones. Consulte Actualizar los contactos alternativos de su AWS cuenta para obtener más información.

Eventos de mantenimiento

- Mantenimiento planificado de Direct Connect
- Mantenimiento de emergencia de Direct Connect
- Mantenimiento de terceros
- Preparación de los eventos de mantenimiento
- Solicitudes de aplazamiento o cancelación de eventos de mantenimiento

Mantenimiento planificado de Direct Connect

Los eventos de mantenimiento planificados son actualizaciones de red, como, por ejemplo, la aplicación de parches al sistema operativo y las actualizaciones de configuración en los puntos de conexión del dispositivo de hardware, que son fundamentales para mejorar la disponibilidad y ofrecer nuevas características.

Estos eventos de mantenimiento se programan con 14 días de antelación y, por lo general, se producen durante un periodo de cuatro horas cuando hay poco tráfico en la ubicación de Direct Connect donde se encuentra el punto de conexión del dispositivo. Pero es normal que las actividades de mantenimiento se completen antes de las cuatro horas. Recibirá una notificación cuando se termine el trabajo. En casos poco comunes, cuando circunstancias imprevistas obliguen a aumentar el periodo de mantenimiento, se le enviará una notificación por separado con la estimación de finalización.

Siguiendo el siguiente programa, la notificación inicial y las notificaciones de recordatorio se envían a la AWS cuenta propietaria del recurso:

- 14 días calendario antes del evento de mantenimiento planificado,
- 7 días calendario antes del evento de mantenimiento planificado, y
- 1 día antes del evento de mantenimiento planificado.

> **Note**
>
> Los días de calendario incluyen los días no hábiles y los días festivos locales.

Además:

- Recibirá notificaciones en su sistema de monitoreo o de tickets mediante la integración con AWS Health. Para realizar la integración AWS Health, consulta Monitorizar eventos AWS Health con Amazon EventBridge en la Guía del AWS Health usuario.
- Verá los programas de mantenimiento planificados en su AWS Health Dashboard.

Es posible que, en circunstancias excepcionales, un evento de mantenimiento planificado no pueda ocurrir según lo programado. Si esto sucede, enviaremos una notificación de cancelación y reprogramaremos el evento más adelante siguiendo el mismo proceso que se describió anteriormente.

Mantenimiento de emergencia de Direct Connect

Los eventos de mantenimiento de emergencia se inician como base fundamental para evitar que eventos inminentes afecten al servicio o para resolver los problemas que ya hayan provocado una

interrupción de conectividad. En estos casos, será necesario tomar medidas inmediatas para que el punto de conexión afectado esté nuevamente en buen estado.

Si bien nos esforzamos por avisar con antelación, algunas situaciones harán que el mantenimiento comience de inmediato. Recibirá notificaciones cuando el mantenimiento de emergencia esté programado, en marcha y cuando se complete.

Estos eventos suelen producirse durante un periodo de dos horas en la ubicación de Direct Connect donde se encuentra el punto de conexión del dispositivo. Es normal que las actividades de mantenimiento se completen dentro de este periodo. En situaciones donde circunstancias imprevistas obliguen a aumentar el periodo de mantenimiento, como el reemplazo de hardware, se le enviará una notificación por separado con la estimación de finalización.

Mantenimiento de terceros

Además de los eventos de mantenimiento AWS iniciados, el socio de entrega de Direct Connect o el proveedor de servicios de red que proporciona conectividad de red desde sus instalaciones a la ubicación de Direct Connect podrían realizar actividades de mantenimiento. Los socios de Direct Connect Delivery reciben notificaciones de eventos de mantenimiento AWS para que puedan planificar sus propios programas de mantenimiento y evitar la superposición. AWS no puede ver las actividades de mantenimiento de un socio, por lo que tendrá que consultar con ellos su proceso de programación, sus métodos de notificación y sus prácticas recomendadas.

Preparación de los eventos de mantenimiento

Para garantizar que las cargas de trabajo de producción sigan funcionando durante un evento de mantenimiento, Direct Connect recomienda utilizar el kit de herramientas de resiliencia de AWS Direct Connect para configurar las conexiones de red para obtener la máxima resiliencia. Para ver un ejemplo de modelo de máxima resiliencia, consulte Resiliencia máxima.

Con la máxima resiliencia, las conexiones se distribuyen en al menos dos ubicaciones de Direct Connect, con la terminación en dos puntos de conexión de dispositivo únicos dentro de cada ubicación de Direct Connect. Esto ofrece varios niveles de redundancia, lo que reduce el riesgo de que falle un solo punto de conexión y ayuda a mantener la conectividad durante los eventos de mantenimiento. Direct Connect nunca programará un evento de mantenimiento planificado que desactive simultáneamente las conexiones redundantes. Para conocer los pasos para usar el kit de herramientas de AWS Direct Connect resiliencia a fin de configurar la máxima resiliencia, consulte. Configuración de la máxima resiliencia

Durante un evento de mantenimiento planificado, Direct Connect drena el tráfico hacia el punto de conexión que está realizando el mantenimiento y desde él, y obliga al tráfico a utilizar las conexiones redundantes. Esto permite que se realice un redireccionamiento del tráfico de red más fluido sin necesidad de intervención manual si no se ha configurado la máxima resiliencia. Puede optar, como alternativa, por controlar el redireccionamiento del tráfico entre conexiones redundantes durante los periodos de mantenimiento mediante el uso de las comunidades de protocolo de puerta de enlace fronteriza (BGP) preferidas a nivel local. Para obtener más información acerca de las comunidades de BGP, consulte Routing policies and BGP communities.

La configuración de su entorno Direct Connect con el modelo de máxima resiliencia permite garantizar que su empresa no se vea afectada durante los eventos de mantenimiento y las fallas de la infraestructura. Cuando se implementan y prueban correctamente, por lo general, no es necesario tomar ninguna medida en relación con estos eventos de mantenimiento.

Validación de resiliencia

Si ha configurado su entorno de Direct Connect para que sea resistente, compruebe periódicamente que el tráfico se dirija a través de otras conexiones redundantes cuando haya out-of-service una conexión. Las pruebas proactivas periódicas permiten identificar y resolver cualquier posible problema antes de que afecte a las cargas de trabajo de producción durante un evento de mantenimiento o en un escenario de fallo. Esto garantizará una mayor confianza en la fiabilidad de su red durante un evento de mantenimiento. Utilice la prueba de conmutación por error de Direct Connect para validar la resistencia de las conexiones redundantes. Para obtener más información sobre los pasos para utilizar la prueba de conmutación por error de Direct Connect , consulte Prueba de conmutación por error de Direct Connect.

También puede utilizar Amazon CloudWatch Network Monitor para supervisar activamente sus conexiones de Direct Connect. Para obtener más información, consulte Supervisar la conectividad híbrida con Amazon CloudWatch Network Synthetic Monitor.

Solicitudes de aplazamiento o cancelación de eventos de mantenimiento

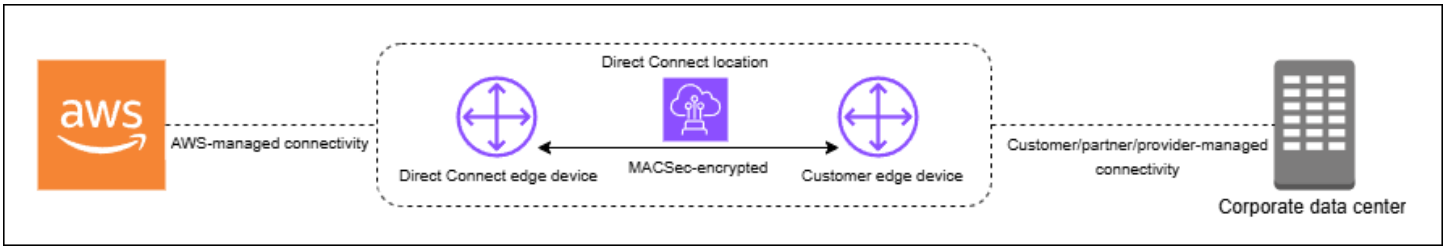
Los dispositivos Direct Connect se comparten entre varios clientes. Por lo tanto, no aceptamos solicitudes específicas de reprogramación o cancelación de mantenimientos. La reprogramación o cancelación de las solicitudes de un cliente puede afectar negativamente a otros clientes que utilicen ese punto de conexión. Esto también puede suponer un riesgo para mitigar los problemas de disponibilidad o seguridad a tiempo.

Seguridad MAC en Direct Connect

La seguridad de MAC (MACsec) es un estándar IEEE que proporciona confidencialidad, integridad y autenticidad del origen de los datos. MACsec proporciona cifrado punto a punto de capa 2 a través de la conexión cruzada con AWS, la cual funciona entre dos routers de capa 3. Si bien MACsec protege la conexión entre el router y la ubicación de Direct Connect en la capa 2, AWS ofrece seguridad adicional al cifrar todos los datos en la capa física a medida que fluyen por la red entre ubicaciones de Direct Connect y regiones de AWS. Esto crea un enfoque de seguridad por capas en el que el tráfico está protegido durante la entrada inicial a AWS y durante el tránsito por la red de AWS.

En el siguiente diagrama, la conexión cruzada de Direct Connect debe estar conectada a una interfaz compatible con MACsec en el dispositivo de periferia del cliente. MACsec en Direct Connect brinda cifrado de capa 2 para el tráfico punto a punto entre el dispositivo de periferia de Direct Connect y el dispositivo de periferia del cliente. Este cifrado se produce después de intercambiar y verificar las claves de seguridad entre las interfaces de ambos extremos de la conexión cruzada.

> **Note**
>
> MACsec otorga seguridad punto a punto en los enlaces Ethernet, por lo tanto, no proporciona cifrado de extremo a extremo en varios segmentos secuenciales de Ethernet u otros segmentos de red.



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 de asociación segura (SAK): una clave de sesión que establece la conectividad de MACsec entre el enrutador en las instalaciones del cliente y el puerto de conexión de la ubicación de Direct Connect. La SAK no se comparte previamente, sino que se deriva automáticamente del par CKN/CAK mediante un proceso de generación de claves criptográficas. Esta derivación se produce en ambos extremos de la conexión después de proporcionar y aprovisionar el par CKN/CAK. La SAK se regenera periódicamente por motivos de seguridad y siempre que se establezca una sesión de MACsec.
- Nombre de clave de asociación de conectividad (CKN) y clave de asociación de conectividad (CAK): los valores de este par se utilizan para generar la clave de MACsec. Genera los valores del par, los asocia a una conexión de Direct Connect y luego los aprovisiona en el dispositivo de periferia que se encuentra en el extremo de la conexión de Direct Connect. Direct Connect es compatible con el modo CAK estático, pero no con el modo CAK dinámico. Como solo es compatible con el modo CAK estático, se recomienda seguir sus propias políticas de administración de claves para la generación, distribución y rotación de claves.
- Formato de clave: el formato de clave debe utilizar caracteres hexadecimales, con una longitud exacta de 64 caracteres. Direct Connect solo es compatible con claves de 256 bits del Estándar de cifrado avanzado (AES) para conexiones dedicadas, lo que corresponde a una cadena hexadecimal de 64 caracteres.
- Modos de cifrado: Direct Connect es compatible con dos modos de cifrado de MACsec:
  - must_encrypt: la conexión requiere el cifrado de MACsec para todo el tráfico. Si la negociación de MACsec falla o no se puede establecer el cifrado, la conexión no transmitirá ningún tráfico. Este modo ofrece la máxima garantía de seguridad, pero puede afectar a la disponibilidad si hay algún problema relacionado con MACsec.
  - should_encrypt: la conexión intenta establecer el cifrado de MACsec, pero recurrirá a una comunicación no cifrada si la negociación MACsec falla. Este modo proporciona más flexibilidad y mayor disponibilidad, pero puede permitir el tráfico sin cifrar en determinadas situaciones de error.

  El modo de cifrado se puede configurar durante la configuración de la conexión y se puede modificar más adelante. Por defecto, las nuevas conexiones habilitadas para MACsec están configuradas en el modo “should_encrypt” para evitar futuros problemas de conectividad durante la configuración inicial.

Rotación de claves MACSec

- Rotación CNN/CAK (manual)

  Direct Connect MACsec admite secuencias de claves MACsec con capacidad para almacenar hasta tres pares CKN/CAK. Permite girar manualmente estas claves de larga duración sin interrumpir la conexión. Al asociar un nuevo par CKN/CAK mediante el comando `associate-mac-sec-key`, debe configurar el mismo par en el dispositivo. El dispositivo de Direct Connect intenta usar la más reciente clave agregada. Si esa clave no coincide con la del dispositivo, vuelve a la clave de trabajo anterior, lo que garantiza la estabilidad de la conexión durante la rotación.

  Para obtener información sobre el uso de `associate-mac-sec-key`, consulte asociar-clave-de-mac-sec.
- Rotación automática de la clave de asociación segura (SAK)

  La SAK, que se deriva del par CKN/CAK activo, se somete a una rotación automática según lo siguiente:

  - intervalos de tiempo
  - volumen de tráfico cifrado
  - Establecimiento de una sesión de MACsec

  El protocolo gestiona automáticamente esta rotación. Se produce de forma transparente sin interrumpir la conexión y no requiere ninguna intervención manual. La SAK nunca se almacena de forma persistente y se regenera mediante un proceso seguro de derivación de claves que sigue el estándar IEEE 802.1X.

Conexiones compatibles

MACsec está disponible en una conexión dedicada de Direct Connect y en grupos de agregación de enlaces:

Conexiones MACsec compatibles

- Conexiones dedicadas
- LAG
- Interconexiones de socios

> **Note**
>
> Los socios que utilizan dispositivos compatibles pueden usar MACsec para cifrar la conexión de capa 2 entre su dispositivo de red de periferia y el dispositivo Direct Connect. Los socios que habiliten la característica pueden cifrar todo el tráfico que atraviesa el enlace seguro. El cifrado MACsec funciona entre los dos dispositivos específicos de la capa 2, pero no es compatible con las conexiones alojadas.

Para obtener información sobre cómo solicitar conexiones compatibles con MACsec, consulte AWS Direct Connect.

Conexiones dedicadas

A continuación encontrará información para familiarizarse con MACsec en las conexiones dedicadas de Direct Connect. No existen cargos adicionales por utilizar MACsec. Los pasos a seguir para configurar MACsec en una conexión dedicada se indican en Comience a utilizar MACsec en una conexión dedicada.

Las operaciones de interconexión de los socios siguen los mismos procedimientos que las conexiones dedicadas. Si procede, cuando se ejecuten comandos de CLI o SDK para las interconexiones de los socios, las respuestas incluirán información relacionada con MACsec.

Requisitos previos de MACsec para conexiones dedicadas

Tenga en cuenta los siguientes requisitos para MACsec en una conexión dedicada:

- MACsec es compatible con conexiones de Direct Connect dedicadas de 10 Gbps, 100 Gbps y 400 Gbps en puntos de presencia seleccionados. Los siguientes conjuntos de cifrado MACsec son compatibles con estas conexiones:
  - Para las conexiones de 10 Gbps, GCM-AES-256 y GCM-AES-XPN-256.
  - Para las conexiones de 100 Gbps y 400 Gbps, GCM-AES-XPN-256.
- Solo se admiten claves MACsec de 256 bits.
- Se requiere la numeración extendida de paquetes (XPN) para las conexiones de 100 Gbps y 400 Gbps. Para las conexiones de 10 Gbps, Direct Connect admite tanto GCM-AES-256 como GCM-AES-XPN-256. Las conexiones de alta velocidad, como las dedicadas de 100 Gbps y 400 Gbps, pueden agotar rápidamente el espacio original de numeración de paquetes de 32 bits

de MACsec, lo que obligaría a rotar las claves de cifrado cada pocos minutos para establecer una nueva asociación de conexión. Para evitar esta situación, la modificación de la norma IEEE 802.1AEbw-2013 introdujo la numeración extendida de paquetes, con lo que se aumentó el espacio de numeración a 64 bits y se alivió el requisito de puntualidad para la rotación de claves.

- El identificador de canal seguro (SCI) es necesario y debe estar activado. No se puede ajustar esta configuración.
- IEEE 802.1Q (Dot1q/VLAN) tag offset/dot1q-in-clear no es compatible para trasladar una etiqueta VLAN fuera de una carga útil cifrada.

Asimismo, debe completar las siguientes tareas antes de configurar MACsec en una conexión dedicada.

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

  Puede crear el par con una herramienta estándar abierta. El par debe cumplir los requisitos especificados de the section called “Configure el 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 más avanzada.

LAG

Los siguientes requisitos permitirán conocer MACsec para los grupos de agregación de enlaces (LAG) de Direct Connect.

- Los LAG deben estar compuestos por conexiones dedicadas compatibles con MACsec que admitan el cifrado MACsec
- Todas las conexiones de un LAG deben tener el mismo ancho de banda y ser compatibles con MACsec
- La configuración MACsec se aplica de manera uniforme en todas las conexiones del LAG
- La habilitación de la creación de LAG y la MACsec se pueden realizar simultáneamente
- Solo se puede utilizar una clave de MACsec en todos los enlaces del LAG en cualquier momento. La capacidad de admitir varias claves de MACsec es únicamente para fines de rotación de claves.

Interconexiones de socios

La cuenta de socio propietaria de la interconexión puede usar MACsec en esa conexión física o ese LAG. Las operaciones son las mismas que las de las conexiones dedicadas, pero se realizan mediante llamadas a la API/SDK específicas del socio.

Roles vinculados a servicios

Direct Connect utiliza roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM que está vinculado directamente a Direct Connect. Los roles vinculados a servicios están predefinidos por Direct Connect e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre. Con un rol vinculado a servicios, resulta más sencillo configurar Direct Connect, porque no es preciso agregar los permisos necesarios manualmente. Direct Connect define los permisos de los roles vinculados con su propio servicio y, a menos que esté definido de otra manera, solo Direct Connect puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM. Para obtener más información, consulte the section called “Roles vinculados a servicios”.

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

AWS Direct Connect utiliza CMK administradas por AWS 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.

Comience a utilizar MACsec en una conexión de Direct Connect dedicada

La siguiente tarea permite comenzar a configurar MACsec para utilizarlo en una conexión dedicada de Direct Connect

Paso 1: Cree una conexión

Para comenzar a utilizar MACsec, debe activar la característica al crear una conexión dedicada.

(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 Consideraciones de MACsec y Crear un grupo de agregación de enlaces (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:

- Asocie un MACsec CKN/CAK a una conexión
- 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 de MACsec del enrutador en las instalaciones y en la ubicación de Direct Connect deben coincidir. Para obtener más información, consulte Descargar el archivo de configuración del enrutador.

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

Opcionalmente, puede eliminar la asociación entre el CKN/CAK y la conexión o el LAG. Si necesita eliminar la asociación, consulte una de las siguientes opciones:

- Elimine la asociación entre una clave MACsec secreta y una conexión
- Eliminar la asociación entre una clave secreta de MACsec y un LAG

Direct Connect conexiones dedicadas y alojadas

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

Existen dos tipos de conexiones:

- Conexión dedicada: una conexión Ethernet física asociada a un único cliente. Los clientes pueden solicitar una conexión dedicada a través de la Direct Connect consola, la CLI o la API. Para obtener más información, consulte Conexiones dedicadas de .
- Conexión alojada: una 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 Conexiones alojadas.

Temas

Direct Connect Conexiones dedicadas

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

Direct Connect location

Trabaje con un AWS Direct Connect socio del Programa de Socios para que lo ayude a establecer circuitos de red entre una 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 Direct Connect.

Velocidad del puerto

Los valores posibles son 1 Gbps, 10 Gbps, 100 Gbps y 400 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.

Después de solicitar la conexión, podrá descargar una Carta de autorización y asignación de instalación de conexión (LOA-CFA) o recibirá un correo electrónico en el que se le solicitará 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 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:

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

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 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 Interfaces virtuales e interfaces virtuales alojadas.

Si no tiene equipo en una 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 Direct Connect.

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

Carta de autorización y asignación de instalación de conexión (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 carta de autorización descargada está firmada digitalmente y tiene una marca de agua para validar la autenticidad de la carta de autorización emitida por AWS. La firma digital y la marca de agua en la carta de autorización. El documento PDF impide que una carta de autorización modificada o potencialmente fraudulenta pueda ser utilizada por el proveedor de la instalación en los sitios de Direct Connect. Para autenticar la firma digital, abra el PDF y revise el panel de firma. En un documento válido aparecerá “La firma es válida” y “El documento no ha sido modificado desde que se firmó”. La marca de agua repite el panel de conexiones y los hilos asignados a lo largo del contenido de la carta de autorización como indicador visual, pero no seguro, de autenticidad.

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.

Para conocer los pasos que se deben seguir para descargar la carta de autorización y asignación de instalación de conexión (LoA-CFA), consulte Descargar la LOA-CFA .

> **Note**
>
> Para obtener más información sobre los precios, consulte Precios de 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 una Direct Connect conexión.

Temas

- Cree una conexión Direct Connect dedicada mediante el asistente de conexión
- Crea una conexión Direct Connect clásica
- Descarga el Direct Connect LOA-CFA
- Asocie un MACsec CKN/CAK a una conexión Direct Connect
- Elimine la asociación entre una clave MACsec secreta y una Direct Connect conexión

Cree una conexión Direct Connect dedicada 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 Direct Connect dedicada”.

Para crear una conexión mediante el asistente de conexión

1. Abre la Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión 2/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 the section called “AWS Direct Connect Resiliency Toolkit”.
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. Este valor puede oscilar entre 1 Gbps y 400 Gbps.

   b. En Ubicación, elija la 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 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 MAC (MACsec) para la conexión. En Configuración adicional, selecciona Solicitar un puerto MACsec compatible.

      MACsec solo está disponible en conexiones dedicadas.

   e. (Opcional) Seleccione Añadir etiqueta para añadir key/value pares y así poder identificar mejor 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 “Carta de autorización y asignación de instalación de conexión (LOA-CFA)”.

Utilice uno de los siguientes comandos.

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

Crea una conexión Direct Connect clásica

En el caso de las conexiones dedicadas, puede enviar una solicitud de conexión mediante la 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 Direct Connect ubicación en la que se va a finalizar la conexión.

> **Note**
>
> No puede usar la 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 Direct Connect conexión nueva

1. Abra la Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión 2/home.
2. En la pantalla 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 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 tiene salas de reuniones (MMRs) 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 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 Añadir etiqueta para añadir key/value pares 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 la solicitud y el aprovisionamiento de un puerto AWS para la conexión pueden tardar hasta 72 horas laborables. 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 Conexiones dedicadas y alojadas.

Descarga el Direct Connect LOA-CFA

Puede descargar la LOA-CFA desde la consola o desde la línea de comandos. Direct Connect En cuanto haya descargado la LOA-CFA y se la haya entregado al proveedor de red o de coubicación, este podrá pedir la conexión cruzada en su nombre.

Para descargar el documento LOA-CFA

1. Abra la Direct Connectconsola en la versión 2/home. https://console.aws.amazon.com/directconnect/
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 a ubicaciones de Direct Connect.

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

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

Asocie un MACsec CKN/CAK a una conexión Direct Connect

Después de crear la conexión que admite MACsec, puede CKN/CAK asociar a a la conexión. Puede crear la asociación mediante la Direct Connect consola, la línea de comandos o la API.

> **Note**
>
> No puede modificar una clave MACsec secreta 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 Elimine la asociación entre una clave MACsec secreta y una conexión.

Para asociar una MACsec clave a una conexión

1. Abre la Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión 2/home.
2. En el panel izquierdo, elija Connections (Conexiones).

3. Seleccione una conexión y, a continuación, elija Ver detalles.
4. Elija Asociar clave.
5. Introduzca la clave. MACsec

   [Utilice el CAK/CKN par] Elija el par de claves y, a continuación, haga lo siguiente:

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

   [Usa el secreto] Elige el secreto del administrador secreto existente y, a continuación, en Secreto, selecciona la clave MACsec secreta.
6. Elija Asociar clave.

Para asociar una MACsec clave a una conexión mediante la línea de comandos o la API

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

Elimine la asociación entre una clave MACsec secreta y una Direct Connect conexión

Puede eliminar la asociación entre la conexión y la MACsec clave mediante la Direct Connect consola, la línea de comandos o la API.

Para eliminar una asociación entre una conexión y una clave MACsec

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

Para eliminar una asociación entre una conexión y una MACsec clave mediante la línea de comandos o la API

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

Direct Connect Conexiones alojadas

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

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 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 Direct Connect.

> **Note**
>
> No puede solicitar una conexión alojada a través de la 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 Aceptar una conexión alojada.

Velocidad del puerto

En el caso de 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 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 únicamente se encuentran disponibles en ubicaciones de Direct Connect con velocidades de puerto disponibles de 100 Gbps.

Tenga en cuenta lo siguiente:

- Las velocidades de los puertos de conexión solo las puede cambiar su socio de AWS Direct Connect. Consulte con su socio de AWS Direct Connect para ver si admiten la actualización o la degradación de una conexión existente. Si su socio admite la ampliación o reducción de su conexión, entonces ya no será necesario eliminarla y volver a crearla para ampliar o reducir el ancho de banda de una conexión alojada existente.
- AWS utiliza el control de 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 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:

- Eliminar una conexión
- Actualizar una conexión
- Ver los detalles de la conexión de

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 Interfaces virtuales e interfaces virtuales alojadas.

Acepte una conexión Direct Connect 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 Direct Connect .

Antes de empezar a utilizar una conexión alojada, debe aceptar la conexión. Puede aceptar una conexión alojada mediante la Direct Connect consola, la línea de comandos o la API.

1. Abre la Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión 2/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.

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

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

Eliminar una Direct Connect conexión

Puede eliminar una conexión siempre y cuando no tenga interfaces virtuales adjuntas. Si eliminas la conexión, se detendrán todos los cargos por hora de puerto de esta conexión, pero es posible que continúes incurriendo en cargos por conexiones cruzadas o por circuitos de red (ver más abajo). 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 una interfaz virtual.

Antes de eliminar una conexión, descargue la LOA de la conexión que contiene la información de las diferentes cuentas para disponer de la información relevante sobre los circuitos que se desconectan. Para conocer los pasos a fin de descargar la LOA de conexión, consulte Carta de autorización y asignación de instalación de conexión (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 el proveedor de servicios de coubicación o de circuitos aún cobre cargos por conexión cruzada o por circuito de red, ya que es posible que el cable de conexión cruzada permanezca conectado al dispositivo de red. Estos cargos por la conexión cruzada son ajenos a Direct Connect, y se deben anular con el proveedor de servicios de coubicación o de circuitos a partir de la información que figura en 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.

Puede eliminar una conexión mediante la Direct Connect consola, la línea de comandos o la API.

Para eliminar una conexión

1. Abre la Direct Connectconsola en la 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).

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

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

Actualizar una Direct Connect conexión

Puede actualizar el siguiente atributo de conexión mediante la Direct Connect consola, la línea de comandos o la API.

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

> **Note**
>
> Si bien no se pueden modificar directamente MACSec las propiedades de las conexiones alojadas, los socios pueden MACSec habilitarlas por sí mismos para proporcionar conexiones alojadas seguras a sus clientes.

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`

Para actualizar una conexión

1. Abre la Direct Connectconsola en la versión 2/homehttps://console.aws.amazon.com/directconnect/.
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.

   [Agregar una etiqueta] Elija Agregar 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).

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

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

Ver los detalles Direct Connect de la conexión

Puede ver el estado actual de la conexión mediante la Direct Connect consola, la línea de comandos o la API. 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 Supervisar los recursos de Direct Connect.

Para ver los detalles de una conexión

1. Abre la Direct Connectconsola en la 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.

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

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

Solicitud de conexiones cruzadas a ubicaciones de Direct Connect

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 equipos en una ubicación de Direct Connect, póngase en contacto con el proveedor adecuado para completar la conexión. Para obtener instrucciones específicas sobre cada proveedor, consulte las tablas que aparecen a continuación. Los socios y la información de contacto aparecen organizados por regiones. Para conocer los precios específicos de las conexiones cruzadas, contacte directamente al socio de Direct Connect. Una vez que se haya establecido la conexión puede crear las interfaces virtuales mediante la consola de Direct Connect.

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

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

Una conexión de Direct Connect puede dar acceso a recursos de otras regiones. Para obtener más información, consulte Acceso a regiones remotas de Direct Connect.

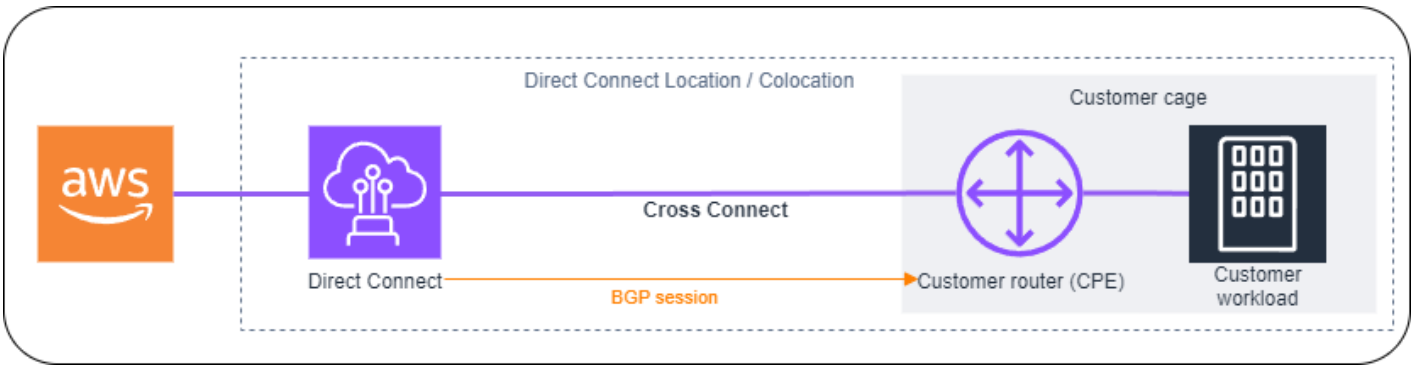
> **Note**
>
> Si pasados 90 días la conexión no se ha completado la autoridad que concede el documento LOA-CFA caduca. Para renovar un documento LOA-CFA caducado, puede volver a descargarlo desde la consola de Direct Connect. Para obtener más información, consulte Carta de autorización y asignación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

Opciones de conectividad

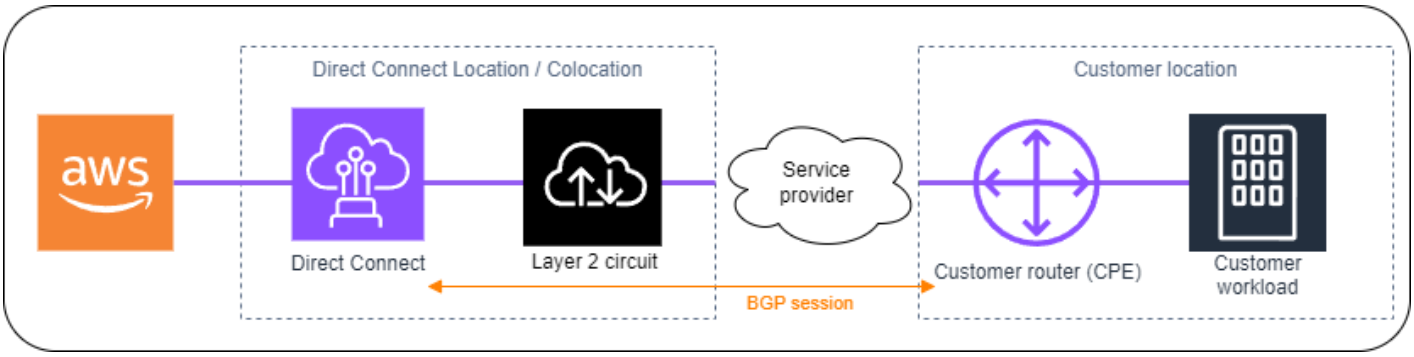
Es posible que las opciones disponibles para establecer conexión con una ubicación de Direct Connect varíen según el socio y la región de AWS. Puede trabajar con uno de los socios de la

Red de socios de AWS (APN), quien podrá proporcionar una o más de las siguientes opciones de conectividad:

- Si tiene recursos implementados en el mismo centro de datos/instalación de coubicación que la ubicación de Direct Connect, la instalación es capaz de proporcionar una conexión cruzada entre el equipo de Direct Connect y los recursos. Para ello, primero debe proporcionar la LOA-CFA a la instalación. Para obtener más información, consulte Carta de autorización y asignación de instalación de conexión (LOA-CFA). A continuación aparece un ejemplo de esta opción de conectividad de Direct Connect:

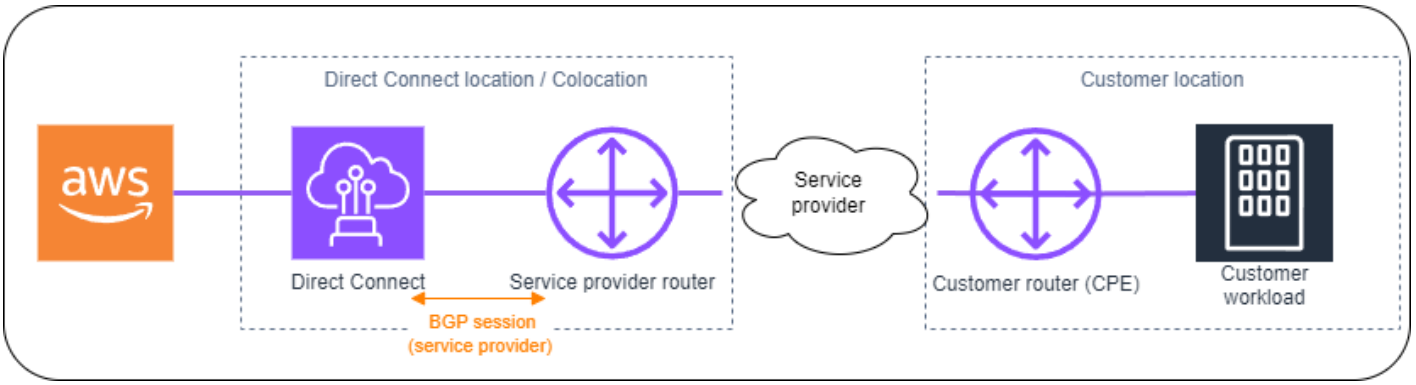


- Amplíe la conexión de Direct Connect a nivel 2 (nivel de enlace de datos) mediante un "circuito" desde la ubicación de Direct Connect hasta la ubicación del cliente. Para ello, trabaje con los socios de Direct Connect. El enrutador instalado en la ubicación del cliente formará directamente una sesión BGP con el equipo de AWS. Por ejemplo, se pueden utilizar tecnologías como Metro Ethernet, fibra oscura o longitud de onda. A continuación aparece un ejemplo de esta opción de conectividad Direct Connect.



- Amplíe la conexión de Direct Connect a nivel 3 (nivel de red) desde la ubicación de Direct Connect hasta la suya. Para ello, trabaje con los socios de Direct Connect. Para esta opción de conectividad, el socio de Direct Connect proporciona un enrutador dentro de la ubicación de Direct Connect que forma una sesión de protocolo de puerta de enlace fronteriza (BGP) con el equipo de AWS. A continuación, el socio de Direct Connect establece otro BGP con usted, el cual, por

ejemplo, podría ser a través de la conmutación de etiquetas multiprotocolo (MPLS). A continuación aparece un ejemplo de esta opción de conectividad Direct Connect.



Este de EE. UU. (Ohio)

Ubicación	Cómo solicitar una conexión
Cologix COL2, Columbus	Póngase en contacto con Cologix en sales@cologix.com.
Cologix MIN3, Minneapolis	Póngase en contacto con Cologix en sales@cologix.com.
CyrusOne West III, Houston	Envíe una solicitud mediante el formulario de contacto 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.

Ubicación	Cómo solicitar una conexión
CoreSite 32k, Nueva York	Haga un pedido con el Portal del cliente de CoreSite. Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web.
CoreSite VA1-VA2, Reston	Haga un pedido en el Portal del cliente de CoreSite. Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web.
Digital Realty ATL1 &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 & DC10-D12, Ashburn	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix DAA1-DC3 & 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	Contacte a KIO Networks".
Markley, One Summer Street, Boston	Para los clientes actuales, cree una solicitud a través del portal de clientes. Para nuevas consultas, póngase en contacto con sales@markleygroup.com.
Centros de datos de Netrality, 2ª planta 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	Haga un pedido con el Portal del cliente de CoreSite. Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web.
CoreSite SV2, Milpitas	Haga un pedido con el Portal del cliente de CoreSite. Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web.
CoreSite SV4, Santa Clara	Haga un pedido con el Portal del cliente de CoreSite. Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web MyCoreSite.
EdgeConneX, Phoenix	Haga un pedido con el Portal del cliente de EdgeOS. Una vez enviado el formulario, EdgeConneX enviará un formulario de pedido 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	Haga un pedido con el Portal del cliente de CoreSite. Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web.

Ubicación	Cómo solicitar una conexión
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 enviado el formulario, EdgeConneX enviará un formulario de pedido 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.
TierPoint Seattle	Póngase en contacto con TierPoint 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 awsdx@dci-indonesia.com.
Centro de datos NTT 2, Yakarta	Póngase en contacto con NTT en tps.cms.presales@global.ntt.

Asia-Pacífico (Mumbai)

Ubicación	Cómo solicitar una conexión
Equinix, Bombay	Póngase en contacto con Equinix en awsdealreg@equinix.com.
NetMagic DC2, Bangalore	Póngase en contacto con el equipo de ventas y marketing de NetMagic llamando al número gratuito 18001033130 o escribien do a la dirección 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 en enquiry.AWSDX@sttelemediagdc.in.
STT GDC Pvt. Ltd. VSB, Chennai	Póngase en contacto con STT en enquiry.AWSDX@sttelemediagdc.in.
STT Hyderabad DC1, Hyderabad	Póngase en contacto con STT en enquiry.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.

Ubicación	Cómo solicitar una conexión
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 de CDC.
Datacom DH6, Auckland	Contacte a Datacom a través de Datacom Orbit –Auckland.
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.

Ubicación	Cómo solicitar una conexión
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
Telehouse, 250 Front St W, Toronto	Póngase en contacto con product@ca.telehouse.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.

Ubicación	Cómo solicitar una conexión
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 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.

Ubicación	Cómo solicitar una conexión
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.
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	Contacte a Eircom a través de datacentre@eirevo.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.

Ubicación	Cómo solicitar una conexión
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.

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

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 MedOne en support@Medone.co.il
EdgeConnex, Herzliya	Contacte a EdgeConnect a través de info@edgeconnecx.com

Medio Oriente (Baréin)

Ubicación	Cómo solicitar una conexión
AWS Baréin DC53, Manama	Para realizar la conexión, puede colaborar con uno de nuestros socios proveedores de red de la ubicación para establecer la conectividad. Luego, proporcionará una carta de autorización (LOA) por parte del proveedor de red a AWS a través del Centro de soporte de AWS. AWS completa la conexión cruzada en esta ubicación.
AWS Baréin DC52, Manama	Para realizar la conexión, puede colaborar con uno de nuestros socios proveedores de red de la ubicación para establecer la conectividad. Luego, proporcionará una carta de autorización (LOA) por parte del proveedor de red a AWS a través del Centro de soporte de AWS. 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 datos Etisalat SmartHub, Fuyaira, EAU	Póngase en contacto con el Centro de datos Etisalat SmartHub en IntlSales-C&WS@etisalat.ae.

América del Sur (São Paulo)

Ubicación	Cómo solicitar una conexión
Cirion BNARAGMS, Buenos Aires	Contacte Cirion a través de cloud.connect@ciriontechnologies.com.
Equinix RJ2, Río de Janeiro	Póngase en contacto con Equinix en awsdealreg@equinix.com.

Ubicación	Cómo solicitar una conexión
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 (Oeste de EE. UU.)

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

Interfaces virtuales e interfaces virtuales alojadas de Direct Connect

Debe crear una de las siguientes interfaces virtuales (VIF) para comenzar a utilizar la conexión de 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 públicos de AWS 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 dedicada o alojada de Direct Connect de cualquier velocidad. Para obtener información acerca de las configuraciones de puerta de enlace Direct Connect, consulte Puertas de enlace de Direct Connect.

Para conectarse a otros servicios de AWS a través de direcciones IPv6, consulte la documentación del servicio correspondiente a fin de comprobar si existe compatibilidad con el enrutamiento IPv6.

Reglas de anuncio de prefijo de interfaz virtual pública

Anunciamos los prefijos de Amazon adecuados para que pueda acceder a las direcciones IP públicas de las cargas de trabajo en las VPC y otros servicios de AWS. Puede acceder a todos los prefijos de AWS a través de esta conexión; por ejemplo, direcciones IP públicas utilizadas por instancias de Amazon EC2, Amazon S3, puntos de conexión de API para servicios de AWS y Amazon.com. No tiene acceso a los prefijos que no son de Amazon. Para consultar la lista actualizada de prefijos utilizados por AWS, consulte Rangos de direcciones IP de AWS en la Guía del usuario de Amazon VPC. En esta página puede descargar un archivo `.json` de los rangos de IP de AWS publicados actualmente. Tenga en cuenta lo siguiente en el caso de los rangos de direcciones IP publicados:

- Los prefijos anunciados mediante BGP a través de una interfaz virtual pública se pueden agregar o quitar en comparación con lo que aparece en la lista de rangos de direcciones IP de AWS.

- Cualquier rango de direcciones IP que utilice en AWS a través de direcciones IP propias (BYOIP) no se incluye en el archivo `.json`, pero AWS aún anuncia estas direcciones BYOIP a través de una interfaz virtual pública.
- AWS no vuelve a anunciar los prefijos de cliente recibidos a través de las interfaces virtuales públicas de Direct Connect para las redes fuera de AWS. Los prefijos anunciados en una interfaz virtual pública estarán visibles para todos los clientes en AWS.

> **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.

Para obtener más información sobre las interfaces virtuales públicas y las políticas de enrutamiento, consulte the section called “Políticas de enrutamiento de interfaces virtuales públicas”.

SiteLink

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

SiteLink es una característica de Direct Connect opcional para interfaces privadas virtuales que habilita la conectividad entre dos puntos de presencia (PoP) de Direct Connect en la misma partición de AWS mediante la ruta más corta disponible a través de la red de AWS. 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 sobre SiteLink, consulte Introducción a Direct Connect SiteLink.

> **Note**
>
> - SiteLink no se encuentra disponible en las regiones de China ni AWS GovCloud (US).
> - SiteLink no funciona si un enrutador en las instalaciones anuncia la misma ruta a AWS en varias interfaces virtuales.

El uso de SiteLink conlleva una tarifa aparte. Para obtener más información, consulte Precios de AWS Direct Connect.

SiteLink no admite 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 admitido
Interfaz virtual privada	No admitido

El comportamiento del enrutamiento de tráfico desde Regiones de AWS (puertas de enlace virtuales o de tránsito) a ubicaciones en las instalaciones a través de una interfaz virtual habilitada para SiteLink varía ligeramente del comportamiento predeterminado de la interfaz virtual de Direct Connect con un prefijo de ruta de AWS. Cuando SiteLink se encuentra habilitado, las interfaces virtuales de una Región de AWS prefieren una ruta de BGP con una longitud de ruta AS más corta 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 se encuentra 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 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, en función del tipo de interfaz virtual. Para obtener más información, consulte MTU para interfaces virtuales privadas o interfaces virtuales 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 Cree 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
Connection	La conexión de Direct Connect o 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 cuenta de AWS de esa otra cuenta.
(Solo para la interfaz virtual privada) Conexión	Para conectarse a una VPC de la misma región de AWS, necesita la puerta de enlace privada virtual de la 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 Puertas de enlace de Direct Connect.

Recurso	Información necesaria
	Note • No se puede utilizar el mismo ASN para la puerta de enlace de cliente y la puerta de enlace virtual/puerta de enlace de Direct Connect en la interfaz virtual. • Sí se puede utilizar el mismo ASN de puerta de enlace de cliente para varias interfaces virtuales. • Varias interfaces virtuales pueden tener el mismo ASN de puerta de enlace virtual/puerta de enlace de Direct Connect y puerta de enlace de cliente de ASN, siempre que formen parte de conexiones de Direct Connect diferentes. Por ejemplo: Puerta de enlace virtual (ASN 64 496) <---Interfaz virtual 1 (conexión 1 de Direct Connect) ---> Puerta de enlace de cliente (ASN 64 511) Puerta de enlace virtual (ASN 64 496) <---Interfaz virtual 2 (conexión 2 de Direct Connect) ---> Puerta de enlace de cliente (ASN 64 511)
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 Direct Connect. Si cuenta con una conexión alojada, su socio de AWS Direct Connect 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 direcciones IP elásticas (EIP) ni direcciones IP propias (BYOIP) del grupo de Amazon para crear una interfaz virtual pública. No puede crear varias sesiones de BGP para la misma familia de enrutamiento 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. Note • Las IP de emparejamiento para las interfaces virtuales privadas y de tránsito pueden provenir de cualquier rango de IP válido. Esto también puede incluir direcciones IP públicas del cliente, siempre que solo se utilicen para crear la sesión de emparejamiento del BGP y no se anuncien en la interfaz virtual, o se utilicen para la NAT. • No podemos garantizar que podamos cumplir con todas las solicitudes de direcciones IPv4 públicas proporcionadas por AWS. 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 AWS), pero se debe utilizar la misma máscara de subred tanto para la IP de mismo nivel como para la IP de mismo nivel del enrutador

Recurso	Información necesaria
	de AWS. Por ejemplo, si asigna un rango `/31`, como `203.0.113.0/31`, podría utilizar `203.0.113.0` para su IP de mismo nivel y `203.0.113.1` para la IP de mismo nivel de AWS. O bien, si asigna un rango `/24`, como `198.51.100.0/24`, podría utilizar `198.51.100.10` para su IP de mismo nivel y `198.51.100.20` para la IP de mismo nivel de AWS. • Un rango de IP propiedad del socio de AWS Direct Connect o del proveedor de servicios de Internet, junto con una autorización LOA-CFA. • Un /31 CIDR proporcionado por AWS. Póngase en contacto con AWS Asistencia para solicitar un CIDR IPv4 público (e indique un caso de uso en su solicitud) • (Solo para la interfaz virtual privada) Amazon puede generar direcciones IPv4 privadas en su nombre. Si especifica la suya, asegúrese de especificar solo los CIDR privados para la interfaz de su enrutador y la interfaz de 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 de mismo nivel como para la IP de mismo nivel del enrutador de AWS. Por ejemplo, si asigna un rango `/30`, como `192.168.0.0/30`, podría utilizar `192.168.0.1` para su IP de mismo nivel y `192.168.0.2` para la IP de mismo nivel de AWS. • 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.

Recurso	Información necesaria
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 IPv4 puede superponerse con otro CIDR IPv4 público que se haya anunciado mediante Direct Connect cuando se cumple alguna de las siguientes condiciones:
	  • Los CIDR provienen de distintas regiones de 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 de BGP.
	• A través de una interfaz virtual pública de Direct Connect, puede especificar cualquier longitud de prefijo de /1 a /32 para IPv4 y de /1 a /64 para IPv6.
	• Puede agregar prefijos adicionales a una interfaz virtual 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 interfaz virtual pública y anunciar.

Recurso	Información necesaria
(Solo para interfaces virtuales privadas y de tránsito) Tramas gigantes	La unidad de transmisión máxima (MTU) de paquetes que se puede pasar a través de 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 consola de Direct Connect y busque Con capacidad de tramas gigantes en la página Configuración general de la interfaz virtual.

Al crear una interfaz virtual, puede especificar la cuenta a la que pertenece. Si elige una cuenta de AWS que no es la suya, 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 puerta de enlace privada virtual o de Direct Connect.
- En interfaces virtuales públicas, la cuenta se usa para la facturación de las interfaces virtuales. El uso de la transferencia de datos (DTO) del propietario del recurso se mide a la velocidad de transferencia de datos de Direct Connect.

> **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.

MTU para interfaces virtuales privadas o interfaces virtuales de tránsito

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.

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 Direct Connect y busque Jumbo Frame Capable (Con capacidad de tramas gigantes) en la pestaña Summary (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

Las tramas gigantes solo se aplicarán a las rutas propagadas a través de Direct Connect y a las rutas estáticas a través de puertas de enlace 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 Unidad de transmisión máxima (MTU) de red de la instancia de 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 conocer los pasos que se deben seguir para configurar la MTU de una interfaz virtual privada, consulte Establecer las MTU de una interfaz virtual privada.

Direct ConnectInterfaces virtuales de

Puede crear una interfaz virtual de tránsito para conectarse a una puerta de enlace 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 cuentas en sus AWS Organizations, o AWS Organizations que son distintas de las suyas, cree una interfaz virtual alojada.

Consulte la siguiente información para crear una interfaz virtual:

- Cree una interfaz virtual pública
- Crear una interfaz virtual privada
- Cree una interfaz virtual de tránsito en la puerta de enlace de Direct Connect

Requisitos previos

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

Requisitos previos para interfaces virtuales de tránsito a una puerta de enlace de Direct Connect

Para establecer la conexión de Direct Connect con la puerta de enlace de tránsito, debe crear una interfaz de tránsito para la conexión. Especifique la puerta de enlace 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 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.

Cree una interfaz virtual pública de Direct Connect

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

Para aprovisionar una interfaz virtual pública

1. Abra la consola de Direct Connect 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 (ASN) para el 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 4294967294. Esto incluye la compatibilidad tanto con un ASN (1-2147483647) como con un ASN largo (1-4294967294). Para obtener más información sobre los ASN y los ASN largos, consulte Soporte de ASN prolongado en Direct Connect.

   > **Note**
   >
   > Al establecer una sesión de emparejamiento de BGP con AWS mediante una interfaz virtual pública, deberá utilizar 7224 como ASN para establecer la sesión de BGP del lado de AWS. El ASN de su router o dispositivo de puerta de enlace de cliente debe ser diferente al de ese ASN.

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 interfaz virtual 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 interfaz virtual 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 (API de Direct Connect)

Crear una interfaz virtual privada de Direct Connect

Puede aprovisionar una interfaz virtual privada en una puerta de enlace privada virtual en la misma región que la conexión de Direct Connect. Para obtener más información sobre el aprovisionamiento de una interfaz virtual privada en una puerta de enlace de Direct Connect, consulte 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 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 consola de Direct Connect 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. En Propietario de la interfaz virtual, elija Mi cuenta de AWS si la interfaz virtual es para su cuenta de AWS.

   d. En Puerta de enlace de Direct Connect, seleccione la puerta de enlace 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 4294967294. Esto incluye la compatibilidad tanto con un ASN (1-2147483647) como con un ASN largo (1-4294967294). Para obtener más información sobre los ASN y los ASN largos, consulte Soporte de ASN prolongado en Direct Connect.
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**
   >
   > Al configurar las interfaces virtuales de AWS Direct Connect, puede especificar sus propias direcciones IP mediante la RFC 1918, así como utilizar otros esquemas de direccionamiento u optar por direcciones IPv4 /29 CIDR asignadas por AWS y desde el rango de enlace local RFC 3927 169.254.0.0/16 IPv4 a fin de obtener una conectividad de punto a punto. Estas conexiones de punto a punto deben usarse exclusivamente para la interconexión eBGP entre el router de puerta de enlace de cliente y el punto de conexión de Direct Connect. Para el tráfico de VPC o la creación de túneles, como la IP privada AWS Site-to-Site VPN o Transit Gateway Connect, AWS recomienda utilizar una interfaz LAN o de bucle invertido en el router de la puerta de enlace de cliente como dirección de origen o destino, en lugar de utilizar conexiones de punto a punto.
   >
   > - 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).
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 (API de Direct Connect)

Cree una interfaz virtual de tránsito a la puerta de enlace de Direct Connect

Antes de conectar una interfaz virtual de tránsito a la puerta de enlace de Direct Connect, hay que familiarizarse con el texto.

Para aprovisionar una interfaz virtual de tránsito en una puerta de enlace de Direct Connect

1. Abra la consola de Direct Connect 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 Mi cuenta de AWS si la interfaz virtual es para su cuenta de AWS.

d. En Puerta de enlace de Direct Connect, seleccione la puerta de enlace 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 4294967294. Esto incluye la compatibilidad tanto con un ASN (1-2147483647) como con un ASN largo (1-4294967294). Para obtener más información sobre los ASN y los ASN largos, consulte Soporte de ASN prolongado en Direct Connect.

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**
>
> Al configurar las interfaces virtuales de AWS Direct Connect, puede especificar sus propias direcciones IP mediante la RFC 1918, así como utilizar otros esquemas de direccionamiento u optar por direcciones IPv4 /29 CIDR asignadas por AWS y desde el rango de enlace local RFC 3927 169.254.0.0/16 IPv4 a fin de obtener una conectividad de punto a punto. Estas conexiones de punto a punto deben usarse exclusivamente para la interconexión eBGP entre el router de puerta de enlace de cliente y el punto de conexión de Direct Connect. Para el tráfico de VPC o la creación de túneles, como la IP privada AWS Site-to-Site VPN o Transit Gateway Connect, AWS recomienda utilizar una interfaz LAN o de bucle invertido en el router de la puerta de enlace de cliente como dirección de origen o destino, en lugar de utilizar conexiones de punto a punto.

- 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 (API de Direct Connect)

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

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

Descargar el archivo de configuración del enrutador de Direct Connect

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

Cómo descargar el archivo de configuración del router

1. Abra la consola de Direct Connect 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 Direct Connect.
7. 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 multiplat aforma.
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 multiplat aforma.

Parámetro	Descripción
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>

Interfaces virtuales alojadas de Direct Connect

Para utilizar su conexión de Direct Connect con otra cuenta, puede crear una interfaz virtual alojada en 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 utilizar interfaces virtuales de tránsito con conexiones de Direct Connect dedicadas o alojadas 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
Connection	La conexión de Direct Connect o 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 cuenta de AWS de esa otra cuenta.
(Solo para la interfaz virtual privada) Conexión	Para conectarse a una VPC de la misma región de AWS, necesita la puerta de enlace privada virtual de la 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 Puertas de enlace 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 Direct Connect. Si cuenta con una conexión alojada, su socio de AWS Direct Connect 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 direcciones IP propias (BYOIP) del grupo de Amazon para crear una interfaz virtual pública. No puede crear varias sesiones de BGP para la misma familia de enrutamiento 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 AWS), pero se debe utilizar la misma máscara de subred tanto para la IP de mismo nivel como para la IP de mismo nivel del enrutador de AWS. Por ejemplo, si asigna un rango `/31`, como `203.0.113.0/31`, podría utilizar `203.0.113.0` para su IP de mismo nivel y `203.0.113.1` para la IP de mismo nivel de AWS. O bien, si asigna un rango `/24`, como `198.51.100.0/24`, podría utilizar `198.51.100.10` para su IP de mismo nivel y `198.51.100.20` para la IP de mismo nivel de AWS. • Un rango de IP propiedad de su socio de AWS Direct Connect o ISP, junto con una autorización LOA-CFA • Un CIDR /31 proporcionado por AWS. 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 proporcionadas por AWS. • (Solo para la interfaz virtual privada) Amazon puede generar direcciones IPv4 privadas en su nombre. Si especifica la suya, asegúrese de especificar solo los CIDR privados para la interfaz de su enrutador y la interfaz de 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 de mismo nivel como para la IP de mismo nivel del enrutador de AWS. Por ejemplo, si asigna un rango `/30`, como `192.168.0.0/30`, podría utilizar

Recurso	Información necesaria
	`192.168.0.1` para su IP de mismo nivel y `192.168.0.2` para la IP de mismo nivel de AWS. • 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 4294967294. 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 IPv4 puede superponerse con otro CIDR IPv4 público que se haya anunciado mediante Direct Connect cuando se cumple alguna de las siguientes condiciones:
	  • Los CIDR provienen de distintas regiones de 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 de BGP.
	• A través de una interfaz virtual pública de Direct Connect, puede especificar cualquier longitud de prefijo de /1 a /32 para IPv4 y de /1 a /64 para IPv6.
	• Puede agregar prefijos adicionales a una interfaz virtual 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 interfaz virtual pública y anunciar.

(Solo para interfaces virtuales privadas y de tránsito) Tramas gigantes	La unidad de transmisión máxima (MTU) de paquetes que se puede pasar a través de 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 rutas propagadas de Direct Connect. Si agrega rutas estáticas a una tabla de enrutamiento que apuntan a una puerta de enlace 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 consola de Direct Connect y busque Con capacidad de tramas gigantes en la página Configuración general de la interfaz virtual.

Crear una interfaz virtual privada alojada en Direct Connect

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

Para crear una interfaz virtual privada alojada

1. Abra la consola de Direct Connect 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 Virtual interface owner (Propietario de la interfaz virtual), elija Another AWS account (Otra cuenta) y, a continuación, en Virtual interface owner (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 a 4294967294. Esto incluye la compatibilidad tanto con un ASN (1-2147483647) como con un ASN largo (1-4294967294). Para obtener más información sobre los ASN y los ASN largos, consulte Soporte de ASN prolongado en Direct Connect.
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**
>
> Al configurar las interfaces virtuales de AWS Direct Connect, puede especificar sus propias direcciones IP mediante la RFC 1918, así como utilizar otros esquemas de direccionamiento u optar por direcciones IPv4 /29 CIDR asignadas por AWS y desde el rango de enlace local RFC 3927 169.254.0.0/16 IPv4 a fin de obtener una conectividad de punto a punto. Estas conexiones de punto a punto deben usarse exclusivamente para la interconexión eBGP entre el router de puerta de enlace de cliente y el punto de conexión de Direct Connect. Para el tráfico de VPC o la creación de túneles, como la IP privada AWS Site-to-Site VPN o Transit Gateway Connect, AWS recomienda utilizar una interfaz LAN o de bucle invertido en el router de la puerta de enlace de cliente como dirección de origen o destino, en lugar de utilizar conexiones de punto a punto.
>
> - 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) 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, podrá descargar el archivo de configuración. Para obtener más información, consulte 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 de Direct Connect)

Crear una interfaz virtual pública alojada en Direct Connect

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

Para crear una interfaz virtual privada pública

1. Abra la consola de Direct Connect 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 Virtual interface owner (Propietario de la interfaz virtual), elija Another AWS account (Otra cuenta) y, a continuación, en Virtual interface owner (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 a 4294967294. Esto incluye la compatibilidad tanto con un ASN (1-2147483647) como con un ASN largo (1-4294967294). Para obtener más información sobre los ASN y los ASN largos, consulte Soporte de ASN prolongado en Direct Connect.

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.

   [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, podrá descargar el archivo de configuración. Para obtener más información, consulte 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 (API de Direct Connect)

Cree una interfaz virtual de tránsito alojada en Direct Connect

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 consola de Direct Connect 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 Virtual interface owner (Propietario de la interfaz virtual), elija Another AWS account (Otra cuenta) y, a continuación, en Virtual interface owner (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 a 4294967294. Esto incluye la compatibilidad tanto con un ASN (1-2147483647) como con un ASN largo (1-4294967294). Para obtener más información sobre los ASN y los ASN largos, consulte Soporte de ASN prolongado en Direct Connect.

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**
      >
      > Al configurar las interfaces virtuales de AWS Direct Connect, puede especificar sus propias direcciones IP mediante la RFC 1918, así como utilizar otros esquemas de direccionamiento u optar por direcciones IPv4 /29 CIDR asignadas por AWS y desde el rango de enlace local RFC 3927 169.254.0.0/16 IPv4 a fin de obtener una conectividad de punto a punto. Estas conexiones de punto a punto deben usarse exclusivamente para la interconexión eBGP entre el router de puerta de enlace de cliente y el punto de conexión de Direct Connect. Para el tráfico de VPC o la creación de túneles, como la IP privada AWS Site-to-Site VPN o Transit Gateway Connect, AWS recomienda utilizar una interfaz LAN o de bucle invertido en el router de la puerta de enlace de cliente como dirección de origen o destino, en lugar de utilizar conexiones de punto a punto.
      >
      > - 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] 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. Después de que la interfaz virtual alojada sea aceptada por el propietario de la otra cuenta de AWS, podrá descargar el archivo de configuración del enrutador para el dispositivo. Para obtener más información, consulte 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 (API de Direct Connect)

Consultar los detalles de la interfaz virtual de Direct Connect

Puede ver el estado actual de la interfaz virtual mediante la consola de Direct Connect, la línea de comandos o la API. Los detalles incluyen:

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

Para ver los detalles de una interfaz virtual

1. Abra la consola de Direct Connect 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 (API de Direct Connect)

Agregar un intercambiador de tráfico BGP a una interfaz virtual de Direct Connect

Agregue o elimine una sesión de intercambio de tráfico BGP IPv4 o IPv6 a la interfaz virtual mediante la consola de Direct Connect, la línea de comandos o la API.

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.

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

Para añadir un BGP de mismo nivel

1. Abra la consola de Direct Connect 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**
>
> Al configurar las interfaces virtuales de AWS Direct Connect, puede especificar sus propias direcciones IP mediante la RFC 1918, así como utilizar otros esquemas de direccionamiento u optar por direcciones IPv4 /29 CIDR asignadas por AWS y desde el rango de enlace local RFC 3927 169.254.0.0/16 IPv4 a fin de obtener una conectividad de punto a punto. Estas conexiones de punto a punto deben usarse exclusivamente para la interconexión eBGP entre el router de puerta de enlace de cliente y el punto de conexión de Direct Connect. Para el tráfico de VPC o la creación de túneles, como la IP privada AWS Site-to-Site VPN o Transit Gateway Connect, AWS recomienda utilizar una interfaz LAN o de bucle invertido en el router de la puerta de enlace de cliente como dirección de origen o destino, en lugar de utilizar conexiones de punto a punto.
>
> - 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.

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 a 4294967294. Esto incluye la compatibilidad tanto con un ASN (1-2147483646) como con un ASN largo (1-4294967294). Para obtener más información sobre los ASN y los ASN largos, consulte Soporte de ASN prolongado en Direct Connect.

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 de Direct Connect)

Eliminar un intercambiador de tráfico BGP de interfaz virtual de Direct Connect

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). Puede eliminar un intercambiador de tráfico BGP de interfaz virtual mediante la consola de Direct Connect o a través de la línea de comandos o la API.

Para eliminar un BGP de mismo nivel

1. Abra la consola de Direct Connect 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. 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 de Direct Connect)

Establecer las MTU de una interfaz virtual privada de Direct Connect

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 obtener más información sobre las MTU y las interfaces virtuales privadas, consulte MTU para interfaces virtuales privadas o interfaces virtuales de tránsito.

Puede establecer las MTU de una interfaz virtual privada mediante la consola de Direct Connect o a través de la línea de comandos o la API.

Para establecer la MTU de una interfaz virtual privada

1. Abra la consola de Direct Connect 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 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 (API de Direct Connect)

Agregar o eliminar etiquetas de interfaz virtual de Direct Connect

Las etiquetas proporcionan un método para identificar la interfaz virtual. Puede agregar o eliminar una etiqueta mediante la consola de Direct Connect, la línea de comandos o la API si es el propietario de la cuenta de la interfaz virtual.

Para añadir o eliminar una etiqueta de interfaz virtual

1. Abra la consola de Direct Connect 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 una interfaz virtual de Direct Connect

Puede eliminar una o varias interfaces virtuales. Antes de poder eliminar una conexión, debe eliminar la interfaz virtual. Eliminar una interfaz virtual detiene los cargos por transferencia de datos de Direct Connect asociados a la interfaz virtual.

Puede eliminar una interfaz virtual mediante la consola de Direct Connect, la línea de comandos o la API.

Para eliminar una interfaz virtual

1. Abra la consola de Direct Connect 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)
- DeleteVirtualInterface (API de Direct Connect)

Aceptar una interfaz virtual de Direct Connect alojada

Para poder empezar a usar una interfaz virtual alojada, debe aceptar la interfaz virtual. En una interfaz virtual privada, también debe tener una puerta de enlace privada virtual o de Direct Connect. En una interfaz virtual de tránsito, debe tener una puerta de enlace de Direct Connect o una puerta de enlace de tránsito existente.

Puede aceptar una interfaz virtual alojada mediante la consola de Direct Connect, la línea de comandos o la API.

Para aceptar una interfaz virtual alojada

1. Abra la consola de Direct Connect 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 Aceptar interfaz virtual, seleccione una puerta de enlace de Direct Connect y, a continuación, elija Aceptar interfaz virtual.

   (Interfaz virtual privada) En el cuadro de diálogo Aceptar interfaz virtual, seleccione una puerta de enlace privada virtual o de Direct Connect y, a continuación, elija Aceptar.
6. Una vez que acepte la interfaz virtual alojada, el propietario de la conexión de 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 (API de Direct Connect)

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

- confirm-public-virtual-interface (AWS CLI)
- ConfirmPublicVirtualInterface (API de Direct Connect)

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

- confirm-transit-virtual-interface (AWS CLI)
- ConfirmTransitVirtualInterface (API de Direct Connect)

Migrar una interfaz virtual de Direct Connect

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 consola de Direct Connect 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

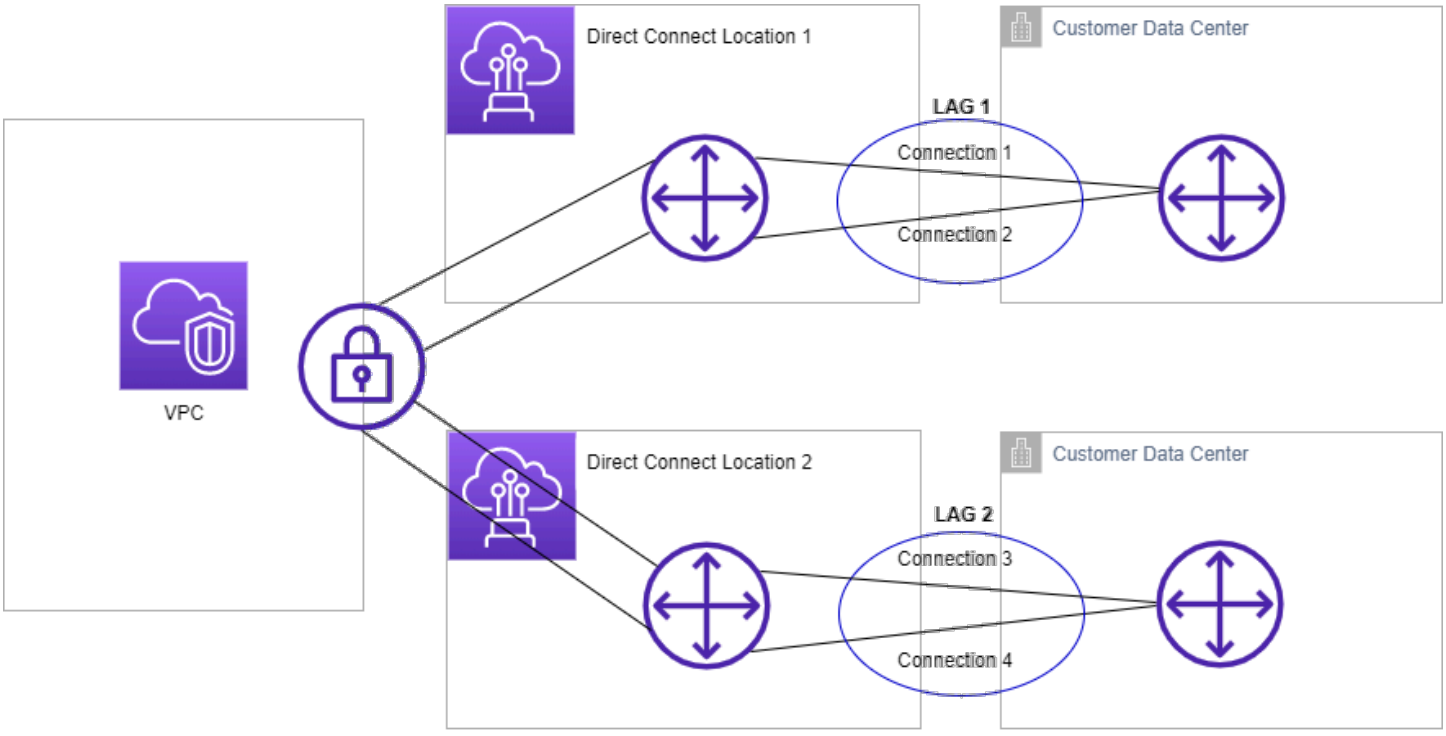
- associate-virtual-interface (AWS CLI)
- AssociateVirtualInterface (API de Direct Connect)

Grupos de agregación de enlaces (LAG) de Direct Connect

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 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 terminan en el mismo dispositivo de AWS y en la misma ubicación y, a continuación, utilizar 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, 100 Gbps o 400 Gbps.
- Todas las conexiones del LAG deben utilizar el mismo ancho de banda.
- Puede tener un máximo de dos conexiones de 100 Gbps o 400 Gbps, 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 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 una nueva conexión física de Direct Connect. Para obtener más información, consulte Carta de autorización y asignación de instalación de conexión (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 Direct Connect.

Temas

- Consideraciones de MACsec para Direct Connect
- Cree un LAG en un punto de conexión de Direct Connect
- Ver los detalles del LAG en un punto de conexión de Direct Connect
- Actualizar un LAG en un punto de conexión de Direct Connect

- Asociar una conexión a un LAG en un punto de conexión de Direct Connect
- Desasociar una conexión de un LAG en un punto de conexión de Direct Connect
- Asociar un CKN/CAK de MACsec a un LAG de punto de conexión de Direct Connect
- Eliminar la asociación entre una clave secreta de MACsec y un LAG de punto de conexión de Direct Connect
- Eliminar un LAG de punto de conexión de Direct Connect

Consideraciones de MACsec para Direct Connect

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.
- Solo se puede utilizar una clave de MACsec en todos los enlaces del LAG en cualquier momento. La capacidad de admitir varias claves de MACSec es únicamente para fines de rotación de claves.

Cree un LAG en un punto de conexión de Direct Connect

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 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.

Para crear un LAG con nuevas conexiones

1. Abra la consola de Direct Connect 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 1G o 10G; o dos cuando la velocidad del puerto es de 100 Gbps o 400 Gbps.
   - (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).

Para crear un LAG desde conexiones existentes

1. Abra la consola de Direct Connect 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 1G o 10G; o de dos cuando la velocidad del puerto es de 100 Gbps o 400 Gbps.
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).

Para crear un LAG mediante la línea de comandos o la API

- create-lag (AWS CLI)
- CreateLag (API de Direct Connect)

Para describir los LAG mediante la línea de comandos o la API

- describe-lags (AWS CLI)
- DescribeLags (API de Direct Connect)

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

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

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 en un punto de conexión de Direct Connect

Después de crear un LAG, podrá ver sus detalles a través de la consola de Direct Connect o mediante la línea de comandos o la API.

Para ver la información de los LAG

1. Abra la consola de Direct Connect 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 Direct Connect en el que terminan las conexiones.

Para ver información sobre su LAG con la línea de comandos o la API

- describe-lags (AWS CLI)
- DescribeLags (API de Direct Connect)

Actualizar un LAG en un punto de conexión de Direct Connect

Puede actualizar los siguientes atributos del grupo de agregación de enlaces (LAG) mediante la consola de Direct Connect, la línea de comandos o la API:

- 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.

Para actualizar un LAG

1. Abra la consola de Direct Connect 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).

Para actualizar un LAG mediante la línea de comandos o la API

- update-lag (AWS CLI)

- UpdateLag (API de Direct Connect)

Asociar una conexión a un LAG en un punto de conexión de Direct Connect

Puede asociar una conexión existente a un LAG a través de la consola de Direct Connect o mediante la línea de comandos o la API. 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.

Para asociar una conexión a un LAG

1. Abra la consola de Direct Connect 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).

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

- associate-connection-with-lag (AWS CLI)
- AssociateConnectionWithLag (API de Direct Connect)

Desasociar una conexión de un LAG en un punto de conexión de Direct Connect

Convierta una conexión en autónoma al desasociarla de un LAG ya sea mediante la consola de Direct Connect o a través de la línea de comandos o la API. 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.

Para desasociar una conexión de un LAG

1. Abra la consola de Direct Connect 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.

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

- disassociate-connection-from-lag (AWS CLI)
- DisassociateConnectionFromLag (API de Direct Connect)

Asociar un CKN/CAK de MACsec a un LAG de punto de conexión de Direct Connect

Después de crear el LAG compatible con MACsec, podrá asociar un CKN/CAK a la conexión a través de la consola de Direct Connect o mediante la línea de comandos o la API.

> **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”.

Para asociar una clave de MACsec a un LAG

1. Abra la consola de Direct Connect 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.

Para asociar una clave de MACsec a un LAG mediante la línea de comandos o la API

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

Eliminar la asociación entre una clave secreta de MACsec y un LAG de punto de conexión de Direct Connect

Puede eliminar la asociación entre el LAG y la clave de MACsec a través de la consola de Direct Connect o mediante la línea de comandos o la API.

Para eliminar una asociación entre un LAG y una clave de MACsec

1. Abra la consola de Direct Connect 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.

Para eliminar una asociación entre un LAG y una clave de MACsec a través de la línea de comandos o la API

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

Eliminar un LAG de punto de conexión de Direct Connect

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 una conexión.

Puede eliminar un LAG a través de la consola de Direct Connect o mediante la línea de comandos o la API.

Para eliminar un LAG

1. Abra la consola de Direct Connect 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.

Para eliminar un LAG mediante la línea de comandos o la API

- delete-lag (AWS CLI)
- DeleteLag (API de Direct Connect)

Puertas de enlace de Direct Connect

Puede utilizar puertas de enlace de Direct Connect mediante la consola de Amazon VPC o la AWS CLI.

- Puertas de enlace de Direct Connect

  Con una puerta de enlace de Direct Connect, se puede asociar la puerta de enlace de Direct Connect con una puerta de enlace de tránsito con varias VPC, con una puerta de enlace privada virtual o con WAN en la nube de AWS, a una red central de WAN en la nube.

- Asociaciones de la puerta de enlace privada virtual

  Con una puerta de enlace virtual privada, es posible asociar la puerta de enlace de Direct Connect a través de una interfaz virtual privada a una o varias VPC de cualquier cuenta ubicada en la misma región o en regiones diferentes.

- Asociaciones de la gateway de tránsito

  Utilice una puerta de enlace de Direct Connect para conectar la conexión de Direct Connect a través de una interfaz virtual de tránsito a las VPC o VPN que están vinculadas a la puerta de enlace de tránsito.

- Asociaciones de la red central de WAN en la nube

  Utilice una puerta de enlace de Direct Connect para asociarla con una red central de AWS Network Manager.

- Interacciones de prefijos permitidos

  Utilice prefijos permitidos para interactuar con puertas de enlace de tránsito y puertas de enlace privadas virtuales.

Temas

- Interacciones de prefijos permitidas para las puertas de enlace de Direct Connect

Puertas de enlace de Direct Connect

Utilice la puerta de enlace de Direct Connect para conectar las VPC. Puede asociar una puerta de enlace de Direct Connect con cualquiera de las siguientes opciones:

- Una puerta de enlace de tránsito cuando tiene varias VPC en la misma región
- Una puerta de enlace privada virtual
- Una red central WAN en la nube de AWS

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 puerta de enlace 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 China de AWS. Una puerta de enlace de Direct Connect es un componente virtual de Direct Connect diseñado para actuar como un conjunto distribuido de reflectores de rutas BGP. Puesto que funciona fuera de la ruta del tráfico de datos, esta evita la creación de un único punto de falla o evita la introducción de dependencias en Regiones de AWS específicas. La alta disponibilidad está intrínsecamente integrada en su diseño, lo que elimina la necesidad de tener múltiples puertas de enlace de Direct Connect.

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 puerta de enlace de Direct Connect no permite que las asociaciones de puerta de enlace que se encuentran en la misma puerta de enlace de Direct Connect se envíen tráfico entre sí (por ejemplo, una puerta de enlace privada virtual a otra puerta de enlace 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 con las asociaciones de VPC que tengan configurada la opción de agujero negro.

Temas

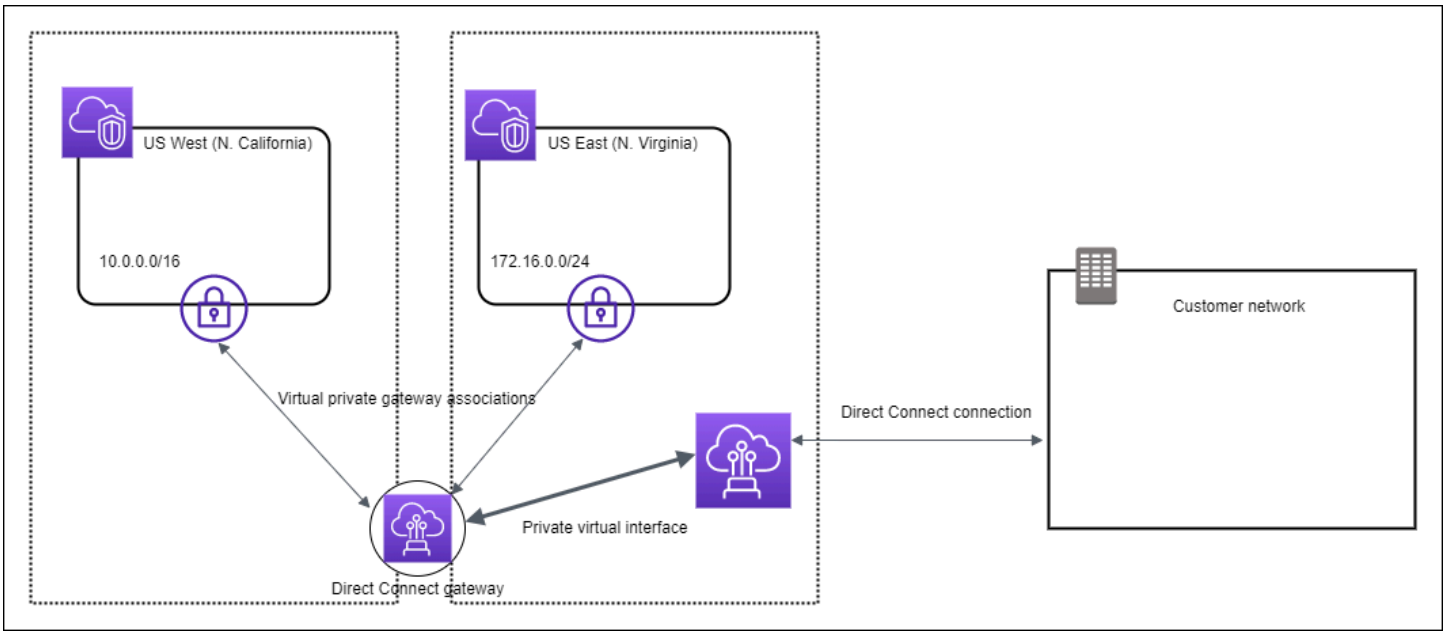
Escenarios

A continuación, se describen solo algunos casos en los que se pueden utilizar las puertas de enlace de Direct Connect.

Caso: asociaciones de puerta de enlace privada virtual

En el siguiente diagrama, la puerta de enlace de Direct Connect lo habilita para utilizar su conexión de 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).

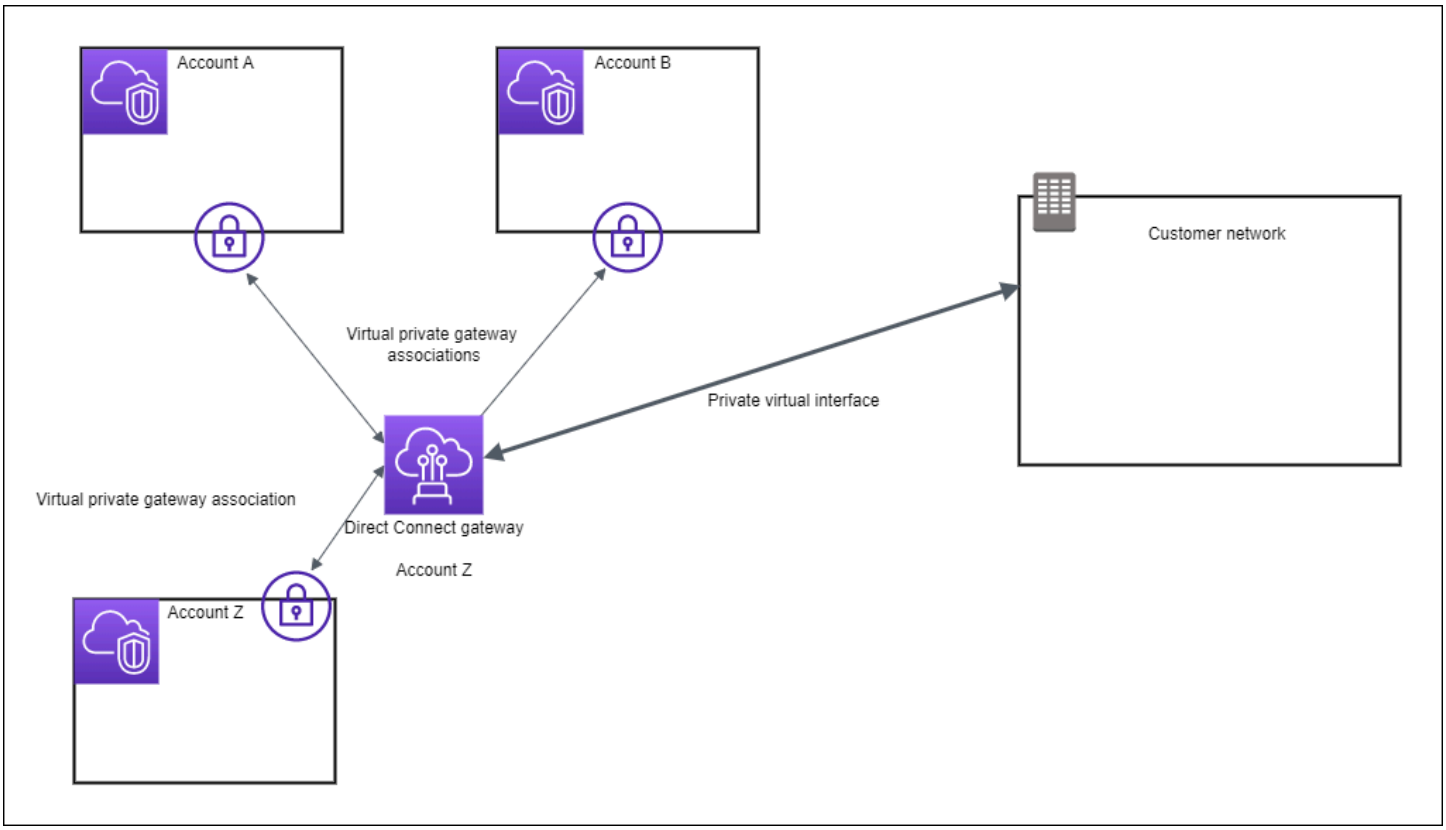
Cada VPC tiene una puerta de enlace privada virtual que se conecta a la puerta de enlace de Direct Connect mediante una asociación de puerta de enlace privada virtual. La puerta de enlace de Direct Connect utiliza una interfaz virtual privada para la conexión a la ubicación de Direct Connect. Hay una conexión de Direct Connect desde la ubicación hasta el centro de datos del cliente.



Caso: asociaciones de puerta de enlace privada virtual entre cuentas

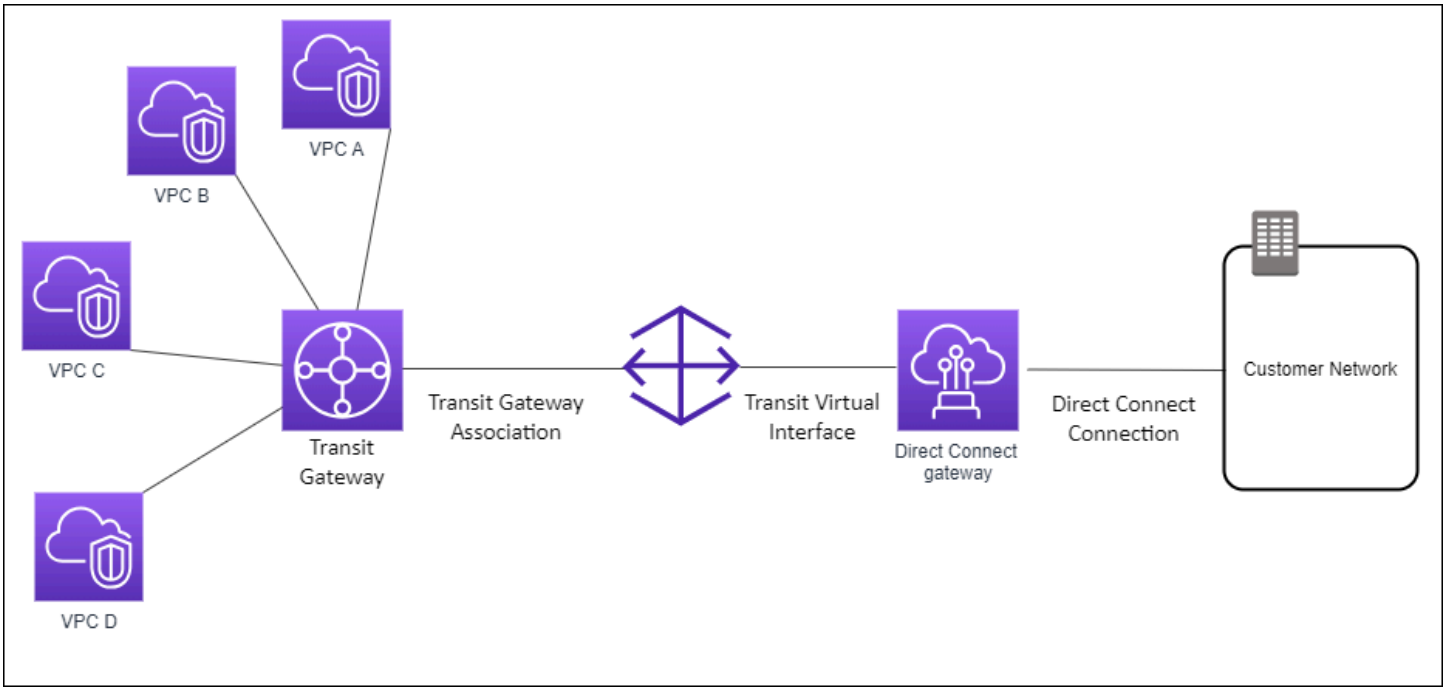
Considere este escenario en el que el propietario de una puerta de enlace de Direct Connect es la cuenta Z. Las cuentas A y B desean utilizar la puerta de enlace de Direct Connect. Las cuentas A y B envían sus respectivas propuestas de asociación a la cuenta Z. La cuenta Z acepta las propuestas de asociación y, si lo desea, puede actualizar los prefijos permitidos desde la puerta de enlace privada virtual de la cuenta A o desde la puerta de enlace 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 puerta de

enlace privada virtual a la puerta de enlace de Direct Connect. La cuenta Z también es propietaria del enrutamiento a los clientes, ya que la cuenta Z es la propietaria de la puerta de enlace.



Caso: asociaciones de puerta de enlace de tránsito

El siguiente diagrama muestra cómo le permite la puerta de enlace 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 puerta de enlace de Direct Connect.
- Una asociación entre la puerta de enlace de Direct Connect y la puerta de enlace de tránsito.
- Una interfaz virtual de tránsito vinculada a la puerta de enlace de Direct Connect.

Esta configuración ofrece los siguientes beneficios. Puede hacer lo siguiente:

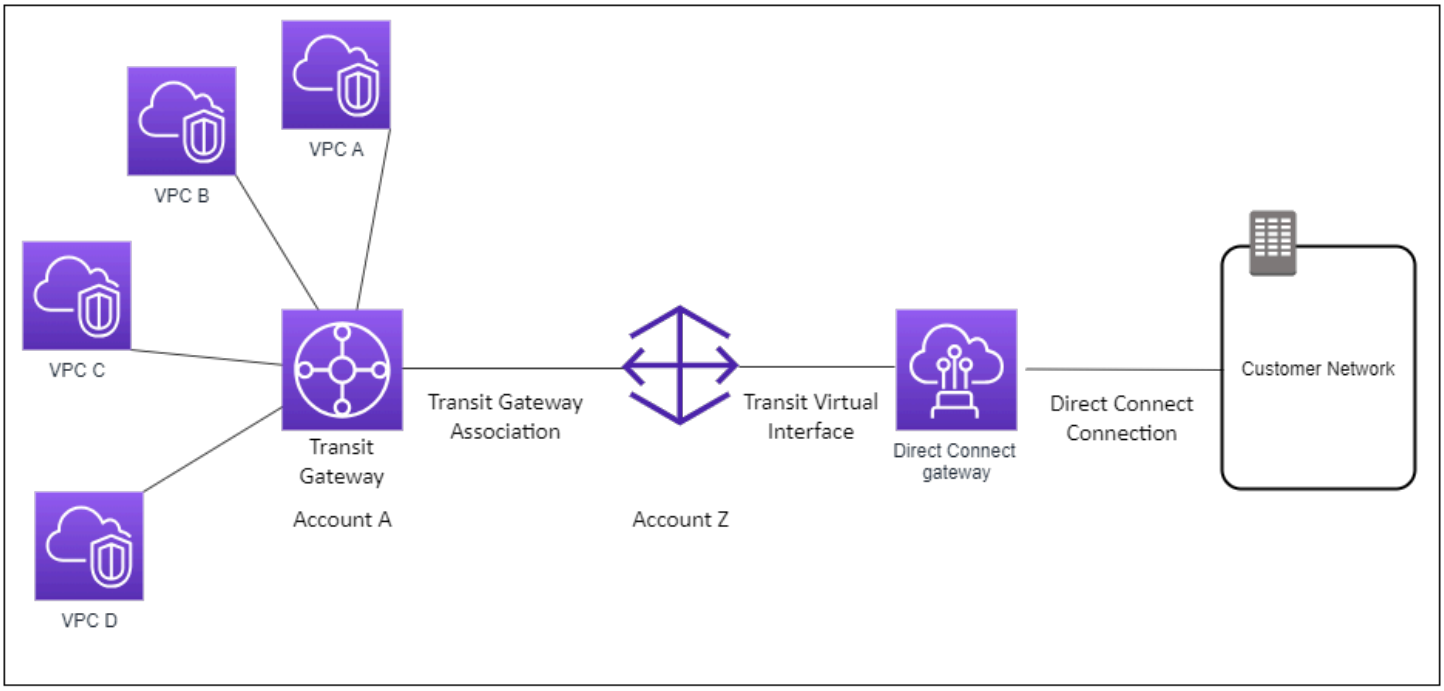
- Administrar una única conexión para las distintas VPC o VPN que haya en la misma región.
- Publicar los prefijos desde las instalaciones hasta AWS y desde AWS hasta las instalaciones.

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.

Caso: asociaciones de puerta de enlace de tránsito entre cuentas

Considere este escenario en el que el propietario de una puerta de enlace de Direct Connect es la cuenta 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 enrutamiento a los clientes, ya que la cuenta Z es la propietaria de la puerta de enlace.



Cree una puerta de enlace de Direct Connect

Puede crear una puerta de enlace de Direct Connect en cualquier región admitida mediante la consola de Direct Connect, la línea de comandos o la API.

Para crear una puerta de enlace de Direct Connect

1. Abra la consola de Direct Connect en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Puertas de enlace de Direct Connect.
3. Elija Crear puerta de enlace de Direct Connect.
4. Especifique la información siguiente y elija Crear puerta de enlace de Direct Connect.
   - Nombre: escriba un nombre que ayude a identificar la puerta de enlace 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.

> **Note**
>
> Si desea crear una puerta de enlace de Direct Connect para usarla con una red central de WAN en la nube de AWS. El ASN no debe estar en el mismo rango que el ASN de la red central.

Para crear una puerta de enlace de Direct Connect mediante la línea de comando o API

- create-direct-connect-gateway (AWS CLI)
- CreateDirectConnectGateway (API de Direct Connect)

Migrar de una puerta de enlace privada virtual a una puerta de enlace de Direct Connect

Puede migrar una puerta de enlace privada virtual que se encuentre vinculada a una interfaz virtual a una puerta de enlace de Direct Connect.

Si utiliza Direct Connect con VPC que actualmente omiten una zona de disponibilidad principal, no podrá migrar las conexiones o interfaces virtuales de Direct Connect.

A continuación, se describen los pasos que se deben seguir para migrar una puerta de enlace privada virtual a una puerta de enlace de Direct Connect.

Para migrar a una puerta de enlace de Direct Connect

1. Cree una puerta de enlace de Direct Connect.

   Si la puerta de enlace de Direct Connect aún no existe, deberá crearla. Para conocer los pasos que se deben seguir para crear una puerta de enlace de Direct Connect, consulte Cree una puerta de enlace de Direct Connect.
2. Cree una interfaz virtual para la puerta de enlace de Direct Connect.

   Se necesita una interfaz virtual para la migración. Si la interfaz no existe, deberá crearla. Para conocer los pasos que se deben seguir para crear la interfaz virtual, consulte Interfaces virtuales.
3. Asocie cada puerta de enlace privada virtual con la puerta de enlace de Direct Connect.

Es necesario asociar tanto la puerta de enlace de Direct Connect como una puerta de enlace privada virtual. Para conocer los pasos que se deben seguir para crear la asociación, consulte Asociar o desasociar puertas de enlace privadas virtuales.

4. Elimine la interfaz virtual que estaba asociada a la puerta de enlace privada virtual. Para obtener más información, consulte Eliminar una interfaz virtual.

Eliminar una puerta de enlace de Direct Connect

Si ya no necesita una puerta de enlace de Direct Connect, puede eliminarla. En primer lugar, debe desasociar todas las puertas de enlace privadas virtuales asociadas y eliminar la interfaz virtual privada adjunta. Una vez que haya desasociado las puertas de enlace privadas virtuales asociadas y eliminado las interfaces privadas virtuales vinculadas, podrá eliminar la puerta de enlace de Direct Connect mediante la consola de Direct Connect, la línea de comandos o la API.

- Para conocer los pasos que se deben seguir para desasociar una puerta de enlace privada virtual, consulte Asociar o desasociar puertas de enlace privadas virtuales.
- Para conocer los pasos que se deben seguir para eliminar una interfaz virtual, consulte Eliminar una interfaz virtual.

Para eliminar una puerta de enlace de Direct Connect

1. Abra la consola de Direct Connect en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Puertas de enlace de Direct Connect.
3. Seleccione las puertas de enlace y elija Eliminar.

Para eliminar una puerta de enlace de Direct Connect mediante la línea de comandos o la API

- delete-direct-connect-gateway (AWS CLI)
- DeleteDirectConnectGateway (API de Direct Connect)

Asociaciones de puerta de enlace privada virtual de Direct Connect

Puede asociar una puerta de enlace privada virtual a una puerta de enlace de Direct Connect para habilitar la conectividad entre su conexión de Direct Connect y las VPC en diferentes cuentas y

regiones. Cada VPC requiere una puerta de enlace privada virtual que pueda asociar una puerta de enlace de Direct Connect. Tras establecidas estas asociaciones, se crean interfaces virtuales privadas en la conexión de Direct Connect a la puerta de enlace de Direct Connect, lo que permite que varias VPC compartan la misma conexión de Direct Connect en sus respectivas asociaciones de la puerta de enlace privada virtual.

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 de forma incorrecta.
- Existen límites para la creación y el uso de puertas de enlace de Direct Connect. Para obtener más información, consulte Cuotas de Direct Connect.
- 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 puerta de enlace 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 puerta de enlace 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 puerta de enlace 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 puerta de enlace 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 puerta de enlace única de Direct Connect.
  - Comunicación directa entre las interfaces virtuales asociadas a una puerta de enlace única de Direct Connect y una conexión de VPN en una puerta de enlace privada virtual que está asociada con la misma puerta de enlace de Direct Connect.

- No se puede asociar una puerta de enlace privada virtual con más de una puerta de enlace de Direct Connect ni tampoco se puede adjuntar una interfaz virtual privada a más de una puerta de enlace de Direct Connect.
- Una puerta de enlace privada virtual que se asocia con una puerta de enlace de Direct Connect se debe adjuntar a una VPC.
- Una propuesta de asociación de puerta de enlace privada virtual caduca 7 días después de crearla.
- Una propuesta de puerta de enlace privada virtual aceptada o eliminada permanece visible durante 3 días.
- Una puerta de enlace privada virtual se puede asociar a una puerta de enlace 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.
- Si tiene previsto utilizar la puerta de enlace privada virtual para una puerta de enlace de Direct Connect y una conexión de VPN dinámica, defina el ASN de la puerta de enlace privada virtual en el valor que necesite para la conexión de VPN. De lo contrario, el ASN de la puerta de enlace privada virtual se puede configurar en cualquier valor admitido. La puerta de enlace de Direct Connect anuncia todas las VPC conectadas a través del ASN que tiene asignado.

Para establecer su conexión con Direct Connect a una VPC en la misma región solo, puede crear una puerta de enlace de Direct Connect. O bien, puede crear una interfaz virtual privada y asociarla a la puerta de enlace privada virtual para la VPC. Para obtener más información, consulte Crear una interfaz virtual privada y VPN CloudHub.

Para utilizar la conexión de Direct Connect con una VPC de otra cuenta, puede crear una interfaz virtual privada alojada en esa cuenta. Cuando el propietario de la otra cuenta acepte la interfaz virtual alojada, puede optar por asociarla a una puerta de enlace privada virtual o a una puerta de enlace de Direct Connect de la cuenta. Para obtener más información, consulte Interfaces virtuales e interfaces virtuales alojadas.

Temas

Creación de una puerta de enlace privada virtual de Direct Connect

La puerta de enlace privada virtual se debe adjuntar a la VPC a la que desea conectarse. Puede crear una puerta de enlace privada virtual y asociarla a una VPC mediante la consola de Direct Connect, la línea de comandos o la API.

> **Note**
>
> Si tiene previsto utilizar la puerta de enlace privada virtual para una puerta de enlace de Direct Connect y una conexión de VPN dinámica, defina el ASN de la puerta de enlace privada virtual en el valor que necesite para la conexión de VPN. De lo contrario, el ASN de la puerta de enlace privada virtual se puede configurar en cualquier valor admitido. La puerta de enlace de Direct Connect anuncia todas las VPC conectadas a través del ASN que tiene asignado.

Después de crear una puerta de enlace privada virtual, debe asociarla a la VPC.

Para crear una puerta de enlace privada virtual y adjuntarla a la VPC.

1. Abra la consola de Direct Connect 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 puerta de enlace 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 Crear puerta de enlace privada virtual.
6. Seleccione la puerta de enlace privada virtual que ha creado y, a continuación, elija Acciones, Asociar a la VPC.
7. Seleccione la VPC en la lista y elija Yes, Attach.

Para crear una puerta de enlace privada virtual mediante la línea de comando o API

- CreateVpnGateway (API de consulta de Amazon EC2)

- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

Para asociar una puerta de enlace privada virtual a una VPC mediante la línea de comando o API

- AttachVpnGateway (API de consulta de Amazon EC2)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Asociar o desasociar puertas de enlace privadas virtuales de Direct Connect

Puede asociar o desasociar una puerta de enlace privada virtual y una puerta de enlace de Direct Connect mediante la consola de Direct Connect o a través de la línea de comandos o la API. El propietario de la cuenta de la puerta de enlace privada virtual realiza estas operaciones.

Para asociar una puerta de enlace privada virtual

1. Abra la consola de Direct Connect 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 Puertas de enlace, elija las puertas de enlace privadas virtuales que desea asociar y, a continuación, elija Asociar puerta de enlace.

Puede ver todas las puertas de enlace privadas virtuales que están asociados con la puerta de enlace de Direct Connect. Para ello, elija Asociaciones de puerta de enlace.

Para desasociar una puerta de enlace privada virtual

1. Abra la consola de Direct Connect 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, seleccione la puerta de enlace de Direct Connect.
3. Elija Ver detalles.

4. Elija Asociaciones de puerta de enlace y, a continuación, seleccione la puerta de enlace privada virtual.
5. Elija Desasociar.

Para asociar una puerta de enlace privada virtual mediante la línea de comandos o la API

- create-direct-connect-gateway-association (AWS CLI)
- CreateDirectConnectGatewayAssociation (API de Direct Connect)

Para ver las puertas de enlace privadas virtuales asociadas con una puerta de enlace de Direct Connect mediante la línea de comandos o la API

- describe-direct-connect-gateway-associations (AWS CLI)
- DescribeDirectConnectGatewayAssociations (API de Direct Connect)

Para desasociar una puerta de enlace privada virtual mediante la línea de comandos o la API

- delete-direct-connect-gateway-association (AWS CLI)
- DeleteDirectConnectGatewayAssociation (API de Direct Connect)

Crear una interfaz virtual privada a la puerta de enlace de Direct Connect

Para conectar su conexión de Direct Connect a la VPC remota, debe crear una interfaz virtual privada para la conexión. Especifique la puerta de enlace de Direct Connect a la que se va a conectar. Puede crear una interfaz virtual privada mediante la consola de Direct Connect, la línea de comandos o la API.

> **Note**
>
> Si acepta una interfaz virtual privada alojada, puede asociarla a una puerta de enlace de Direct Connect de la cuenta. Para obtener más información, consulte Aceptar una interfaz virtual alojada.

Para aprovisionar una interfaz virtual privada en una puerta de enlace de Direct Connect

1. Abra la consola de Direct Connect 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. En Propietario de la interfaz virtual, elija Mi cuenta de AWS si la interfaz virtual es para su cuenta de AWS.

   d. En Puerta de enlace de Direct Connect, seleccione la puerta de enlace 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 4294967294. Esto incluye la compatibilidad tanto con un ASN (1-2147483647) como con un ASN largo (1-4294967294). Para obtener más información sobre los ASN y los ASN largos, consulte Soporte de ASN prolongado en Direct Connect.
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**
>
> Al configurar las interfaces virtuales de AWS Direct Connect, puede especificar sus propias direcciones IP mediante la RFC 1918, así como utilizar otros esquemas de direccionamiento u optar por direcciones IPv4 /29 CIDR asignadas por AWS y desde el rango de enlace local RFC 3927 169.254.0.0/16 IPv4 a fin de obtener una conectividad de punto a punto. Estas conexiones de punto a punto deben usarse exclusivamente para la interconexión eBGP entre el router de puerta de enlace de cliente y el punto de conexión de Direct Connect. Para el tráfico de VPC o la creación de túneles, como la IP privada AWS Site-to-Site VPN o Transit Gateway Connect, AWS recomienda utilizar una interfaz LAN o de bucle invertido en el router de la puerta de enlace de cliente como dirección de origen o destino, en lugar de utilizar conexiones de punto a punto.
>
> - 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 (API de Direct Connect)

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

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

Asociar una puerta de enlace privada virtual de Direct Connect entre cuentas

Puede asociar una puerta de enlace de Direct Connect a una puerta de enlace privada virtual que pertenezca a cualquier cuenta de AWS. La puerta de enlace de Direct Connect puede ser una puerta de enlace existente o puede crear una nueva puerta de enlace. El propietario de la puerta de enlace privada virtual crea una propuesta de asociación y el propietario de la puerta de enlace de Direct Connect debe aceptar la propuesta.

Una propuesta de asociación puede contener los prefijos que se permitirán desde la puerta de enlace privada virtual. El propietario de la puerta de enlace de Direct Connect puede anular cualquiera de los prefijos solicitados en la propuesta de asociación.

Prefijos permitidos

Al asociar una puerta de enlace privada virtual a una puerta de enlace de Direct Connect, debe especificar una lista de prefijos de Amazon VPC que se deben anunciar a la puerta de enlace de Direct Connect. La lista de prefijos actúa como un filtro que permite anunciar los mismos CIDR o unos CIDR más pequeños a la puerta de enlace de Direct Connect. En 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 puerta de enlace 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).

Los prefijos de red interior de interfaz virtual anunciados a través de Direct Connect se propagan únicamente a las puertas de enlace de tránsito entre 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 Interacciones de prefijos permitidos.

Asociaciones de puertas de enlace y puertas de enlace de tránsito de Direct Connect

Puede utilizar una puerta de enlace de Direct Connect para conectar la conexión de Direct Connect a través de una interfaz virtual de tránsito a las VPC o VPN asociadas 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 la conexión de Direct Connect con la puerta de enlace de 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 puertas de enlace de Direct Connect. Para obtener más información, consulte Cuotas de Direct Connect.
- Una puerta de enlace de Direct Connect admite la comunicación entre las interfaces virtuales de tránsito vinculadas 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 dirección de conectividad punto a punto que utilice un rango de `/30` (por ejemplo, `192.168.0.0/30`) no se propaga a una puerta de enlace de tránsito.

Asociación de una puerta de enlace de tránsito entre cuentas

Puede asociar una puerta de enlace de Direct Connect existente o una nueva con una puerta de enlace de tránsito que pertenezca a cualquier cuenta de AWS. 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 puerta de enlace 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 utiliza para dirigir el tráfico desde las instalaciones hasta AWS en la puerta de enlace de tránsito, aunque las VPC adjuntas a la puerta de enlace de tránsito no tengan CIDR asignados. Los prefijos de la lista de prefijos permitidos de la puerta de enlace de Direct Connect se originan en la puerta de enlace de Direct Connect y se publican en la red local. Para obtener más información sobre cómo los prefijos permitidos interactúan con las puertas de enlace de tránsito y las puertas de enlace privadas virtuales, consulte Interacciones de prefijos permitidos.

Temas

- Asociar Direct Connect a una puerta de enlace de tránsito o desasociarlo de esta
- Cree una interfaz virtual de tránsito a la puerta de enlace de Direct Connect
- Crear una puerta de enlace de tránsito y una propuesta de asociación de Direct Connect
- Aceptar o rechazar una puerta de enlace de tránsito y propuesta de asociación de Direct Connect
- Actualizar los prefijos permitidos para una puerta de enlace de tránsito y asociación de Direct Connect
- Eliminar una puerta de enlace de tránsito y propuesta de asociación de Direct Connect

Asociar Direct Connect a una puerta de enlace de tránsito o desasociarlo de esta

Asocie o desasocie una puerta de enlace de tránsito con la consola de Direct Connect o mediante la línea de comandos o la API.

Para asociar una puerta de enlace de tránsito

1. Abra la consola de Direct Connect 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, seleccione 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 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 Interacciones de prefijos permitidos.
7. Elija Asociar puerta de enlace

Puede ver todas las puertas de enlace que están asociadas a la puerta de enlace de Direct Connect. Para ello, elija Asociaciones de puerta de enlace.

Desasociación de una puerta de enlace de tránsito

1. Abra la consola de Direct Connect 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, seleccione la puerta de enlace de Direct Connect.
3. Elija Ver detalles.
4. Elija Asociaciones de puerta de enlace y, a continuación, seleccione la puerta de enlace 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 consola de Direct Connect 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 para la que desee modificar los prefijos permitidos 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 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. 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-association (AWS CLI)
- CreateDirectConnectGatewayAssociation (API de Direct Connect)

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-associations (AWS CLI)
- DescribeDirectConnectGatewayAssociations (API de Direct Connect)

Para desasociar una puerta de enlace de tránsito mediante la línea de comandos o la API

- delete-direct-connect-gateway-association (AWS CLI)
- DeleteDirectConnectGatewayAssociation (API de Direct Connect)

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-association (AWS CLI)
- UpdateDirectConnectGatewayAssociation (API de Direct Connect)

Cree una interfaz virtual de tránsito a la puerta de enlace de Direct Connect

Para establecer la conexión de Direct Connect con la puerta de enlace de tránsito, debe crear una interfaz de tránsito para la conexión. Especifique la puerta de enlace de Direct Connect a la que se va a conectar. Puede utilizar tanto la consola de Direct Connect como la línea de comandos o la API.

> **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 puerta de enlace de Direct Connect

1. Abra la consola de Direct Connect 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 Mi cuenta de AWS si la interfaz virtual es para su cuenta de AWS.
   d. En Puerta de enlace de Direct Connect, seleccione la puerta de enlace 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 4294967294. Esto incluye la compatibilidad tanto con un ASN (1-2147483647) como con un ASN largo (1-4294967294). Para obtener más información sobre los ASN y los ASN largos, consulte Soporte de ASN prolongado en Direct Connect.

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**
   >
   > Al configurar las interfaces virtuales de AWS Direct Connect, puede especificar sus propias direcciones IP mediante la RFC 1918, así como utilizar otros esquemas de direccionamiento u optar por direcciones IPv4 /29 CIDR asignadas por AWS y desde el rango de enlace local RFC 3927 169.254.0.0/16 IPv4 a fin de obtener una conectividad de punto a punto. Estas conexiones de punto a punto deben usarse exclusivamente para la interconexión eBGP entre el router de puerta de enlace de cliente y el punto de conexión de Direct Connect. Para el tráfico de VPC o la creación de túneles, como la IP privada AWS Site-to-Site VPN o Transit Gateway Connect, AWS recomienda utilizar una interfaz LAN o de bucle invertido en el router de la puerta de enlace de cliente como dirección de origen o destino, en lugar de utilizar conexiones de punto a punto.
   >
   > - 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 (API de Direct Connect)

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

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

Crear una puerta de enlace de tránsito y una propuesta de asociación de Direct Connect

Si es el propietario de la puerta de enlace de tránsito, debe crear la propuesta de asociación. La puerta de enlace de tránsito se debe adjuntar a una VPC o VPN de su cuenta de AWS. 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 puerta de enlace de Direct Connect debe aceptarla, para que usted pueda tener acceso a la red local a través de Direct Connect. Puede crear una propuesta de asociación mediante la consola de Direct Connect, la línea de comandos o la API.

Para crear una propuesta de asociación

1. Abra la consola de Direct Connect 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 Asociaciones de puerta de enlace de Direct Connect y, a continuación, elija Asociar puerta de enlace 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 ID de la puerta de enlace de Direct Connect), escriba el ID de la puerta de enlace 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 Asociar puerta de enlace de Direct Connect.

Para crear una propuesta de asociación mediante la línea de comandos o la API

- create-direct-connect-gateway-association-proposal (AWS CLI)
- CreateDirectConnectGatewayAssociationProposal (API de Direct Connect)

Aceptar o rechazar una puerta de enlace de tránsito y propuesta de asociación de Direct Connect

Si es el propietario de la puerta de enlace de Direct Connect, debe aceptar la propuesta de asociación para crear la asociación. También tiene la opción de rechazar la propuesta de asociación. Puede aceptar o rechazar la propuesta de asociación mediante la consola de Direct Connect, la línea de comandos o la API.

Para aceptar una propuesta de asociación

1. Abra la consola de Direct Connect en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Puertas de enlace de Direct Connect.
3. Seleccione la puerta de enlace de Direct Connect que tiene propuestas pendientes y, a continuación, elija 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 consola de Direct Connect en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Puertas de enlace de Direct Connect.
3. Seleccione la puerta de enlace de Direct Connect que tiene propuestas pendientes y, a continuación, elija Ver detalles.
4. En la pestaña Propuestas pendientes, seleccione la puerta de enlace de tránsito y, a continuación, elija 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-association-proposals (AWS CLI)
- DescribeDirectConnectGatewayAssociationProposals (API de Direct Connect)

Para aceptar una propuesta de asociación mediante la línea de comandos o la API

- accept-direct-connect-gateway-association-proposal (AWS CLI)
- AcceptDirectConnectGatewayAssociationProposal (API de Direct Connect)

Para rechazar una propuesta de asociación mediante la línea de comandos o la API

- delete-direct-connect-gateway-association-proposal (AWS CLI)
- DeleteDirectConnectGatewayAssociationProposal (API de Direct Connect)

Actualizar los prefijos permitidos para una puerta de enlace de tránsito y asociación de Direct Connect

Puede utilizar la consola de Direct Connect, la línea de comandos o la API para actualizar los prefijos permitidos desde la puerta de enlace de tránsito a través de la puerta de enlace de Direct Connect. Para actualizar los prefijos permitidos de una puerta de enlace de tránsito y asociación de Direct Connect mediante la consola de Direct Connect,

- Si es el propietario de la puerta de enlace de tránsito, tendrá que crear una nueva propuesta de asociación para esa puerta de enlace de Direct Connect, en la que se especifiquen los prefijos que se van a permitir. Para conocer los pasos que se deben seguir para crear una nueva propuesta de asociación, consulte Crear una propuesta de asociación de puerta de enlace de tránsito.
- Si es el propietario de la puerta de enlace de Direct Connect, puede actualizar los prefijos permitidos al aceptar la propuesta de asociación, o si actualiza los prefijos permitidos de una asociación existente. Para conocer los pasos que se deben seguir para actualizar los prefijos permitidos al aceptar la asociación, consulte Aceptar o rechazar una propuesta de asociación de puerta de enlace de tránsito.

Para actualizar los prefijos permitidos para una asociación existente mediante la línea de comandos o la API

- update-direct-connect-gateway-association (AWS CLI)
- UpdateDirectConnectGatewayAssociation (API de Direct Connect)

Eliminar una puerta de enlace de tránsito y propuesta de asociación de Direct Connect

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 puerta de enlace tránsito de la puerta de enlace de Direct Connect. Para obtener más información, consulte Crear una propuesta de asociación de puerta de enlace de tránsito.

Puede eliminar una puerta de enlace de tránsito y propuesta de asociación de Direct Connect mediante la consola de Direct Connect, la línea de comandos o la API.

Para eliminar una propuesta de asociación

1. Abra la consola de Direct Connect 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 Asociaciones pendientes de la puerta de enlace, seleccione la asociación y, a continuación, elija 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-association-proposal (AWS CLI)
- DeleteDirectConnectGatewayAssociationProposal (API de Direct Connect)

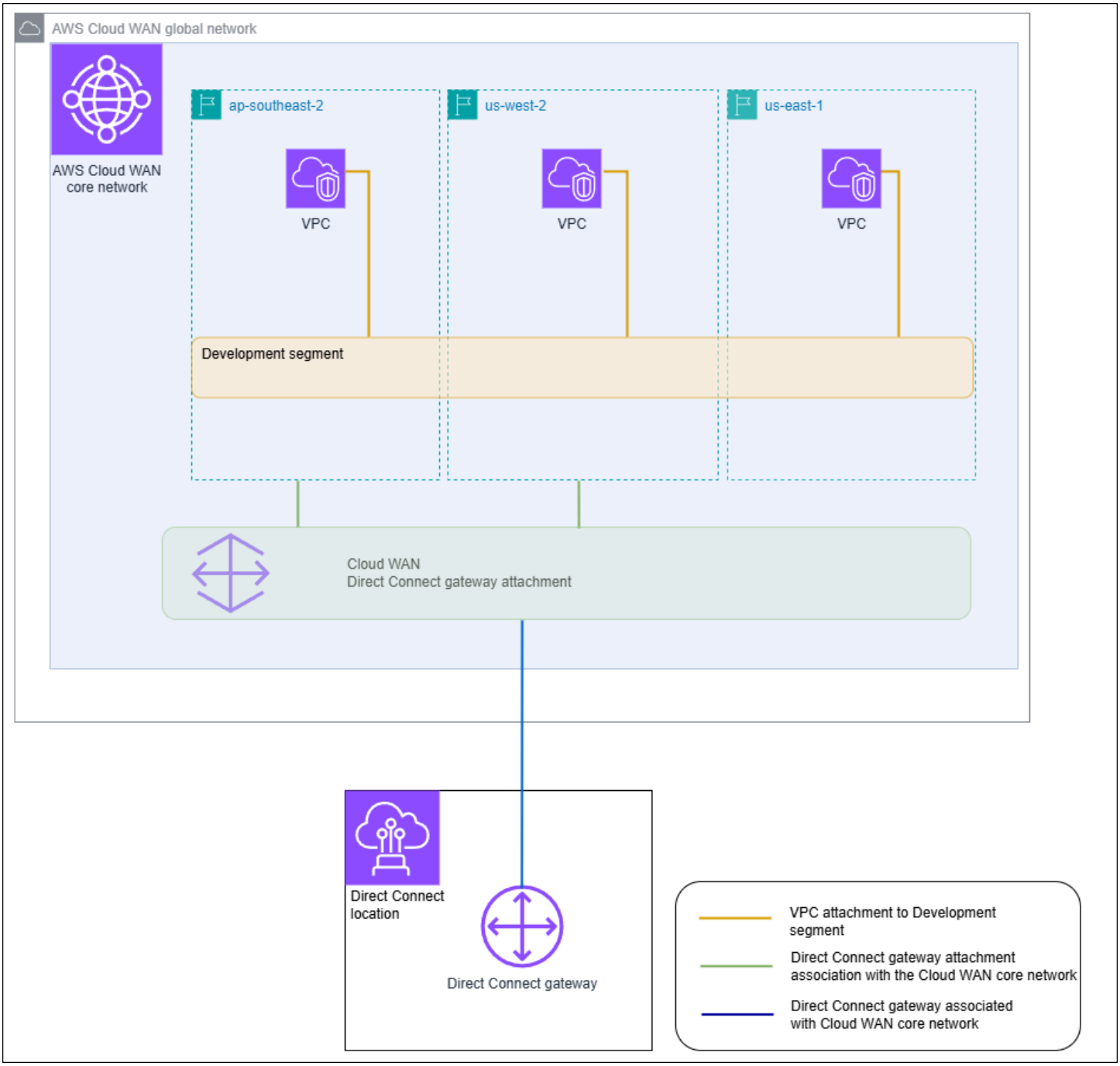
Asociaciones entre la puerta de enlace de Direct Connect y la red central de WAN en la nube de AWS

Asocie una puerta de enlace de Direct Connect a una red central de WAN en la nube de AWS mediante un tipo de conexión de Direct Connect en WAN en la nube. Esta asociación directa enruta el tráfico entre las ubicaciones periféricas seleccionadas de la red central y las conexiones de Direct Connect mediante la ruta más corta disponible.

El tipo de conexión de la puerta de enlace de Direct Connect admite el BGP (protocolo de puerta de enlace fronteriza) para la propagación automática de la información de enrutamiento entre la red central y las ubicaciones locales. La asociación de Direct Connect también es compatible con las características estándar de WAN en la nube, como la administración central basada en políticas, la automatización de las asociaciones basada en etiquetas y la segmentación para configuraciones de seguridad avanzadas.

> **Note**
>
> La asociación entre una red principal y una puerta de enlace de Direct Connect se crea, elimina y administra desde la consola de la WAN en la nube de la monitorización de la red. Al usar una puerta de enlace de Direct Connect con WAN en la nube, la consola de Direct Connect, las API y la CLI reflejarán la asociación, pero no se podrá usar para modificarla. Sin embargo, para comprobar si se creó una asociación, puede utilizar la API de Direct Connect o la línea de comandos.

El siguiente ejemplo muestra una red global de la WAN en la nube con tres regiones dentro de la red central. Cada región tiene su propia VPC conectada a un segmento de desarrollo de la red central compartido entre esas tres regiones. Con la WAN en la nube, se crea una asociación de puerta de enlace de Direct Connect dentro de la WAN en la nube mediante una puerta de enlace de Direct Connect, que se creó con Direct Connect. La asociación está vinculada a dos de las tres regiones, ap-southeast-2 y us-west-2, y se le permite el acceso al segmento de desarrollo. Aunque us-east-1 comparte el mismo segmento de desarrollo, la asociación a la puerta de enlace de Direct Connect no se comparte con esa región y, por lo tanto, no está disponible.



Temas

- Requisitos previos
- Consideraciones
- Asociaciones entre puertas de enlace de Direct Connect y una red central de WAN en la nube
- Verificación de la asociación de una puerta de enlace de Direct Connect con una red central de WAN en la nube de AWS

Requisitos previos

La asociación de una puerta de enlace de Direct Connect con una red central de WAN en la nube requiere lo siguiente:

- Una puerta de enlace de Direct Connect existente. Para conocer los pasos que se deben seguir para crear una puerta de enlace de Direct Connect, consulte Cree una puerta de enlace de Direct Connect.
- Una red central de WAN en la nube de AWS Para obtener más información sobre WAN en la nube, consulte la Guía del usuario de WAN en la nube de AWS.

Consideraciones

Los siguientes límites se aplican a las asociaciones de puertas de enlace de Direct Connect con una red central de WAN en la nube:

- Una puerta de enlace de Direct Connect se puede asociar a una sola red central de WAN en la nube y a un solo segmento de esa red central. Tras la creación de una asociación, esa puerta de enlace no se podrá asociar a otros recursos en las regiones de AWS. Si desasocia la puerta de enlace de la red central, podrá utilizarla para otros tipos de asociación.
- La asociación de la puerta de enlace de WAN en la nube en Direct Connect utiliza el tipo de interfaz virtual de tránsito para la conectividad.
- La asociación de WAN en la nube no admite listas de prefijos permitidos. Todos los prefijos de un segmento de red central se anunciarán en la puerta de enlace de Direct Connect asociada a ese segmento.
- La cuota máxima de prefijos que se pueden anunciar desde una red local a AWS mediante una interfaz virtual de tránsito es diferente de la cuota de prefijos anunciados desde una red central de WAN en la nube a una red local. Además, se aplican las cuotas para otros recursos de Direct Connect utilizados con una asociación de WAN en la nube. Consulte Cuotas de Direct Connect.
- El atributo AS-PATH del BGP se conservará en la red central, en la puerta de enlace de Direct Connect y en la interfaz virtual.
- El ASN de una puerta de enlace de Direct Connect debe estar fuera del rango del ASN configurado para la red central de WAN en la nube. Por ejemplo, si tiene un rango de ASN de 64512 a 65534 para la red central, el ASN de la puerta de enlace de Direct Connect debe usar un ASN fuera de ese rango.

- Es posible que WAN en la nube no sea compatible con los tipos de conexiones específicos si se utiliza el tipo de conexión de Direct Connect para la transferencia. Para obtener más información sobre las asociaciones de la puerta de enlace de Direct Connect a una red central de WAN en la nube, consulte los Asociaciones de la puerta de enlace de Direct Connect en WAN en la nube de AWS en la Guía del usuario de WAN en la nube de AWS.
- La monitorización de la red de CloudWatch es compatible con las métricas de latencia y la pérdida de paquetes cuando se utiliza con un tipo de conexión de puerta de enlace de Direct Connect con WAN en la nube. No es compatible con la característica Network Health Indicator. Para obtener más información, consulte Uso de Network Monitor de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

Asociaciones entre puertas de enlace de Direct Connect y una red central de WAN en la nube

La asociación de una puerta de enlace de Direct Connect a una red central de WAN en la nube de AWS se realiza mediante la consola de WAN en la nube de AWS, las API de WAN en la nube o la línea de comandos.

Para asociar una puerta de enlace de Direct Connect existente a una red central de WAN en la nube, debe crear una nueva asociación de Direct Connect en la consola de WAN en la nube. Tras la creación de la asociación de Direct Connect, esta queda establecida. Por defecto, al crear la asociación, puede elegir la opción predeterminada para incluir todas las ubicaciones periféricas de la red central en el segmento de red central elegida. Si lo desea, también puede indicar ubicaciones periféricas individuales.

Para obtener más información sobre las asociaciones de la puerta de enlace de Direct Connect a una red central de WAN en la nube, consulte los Asociaciones de la puerta de enlace de Direct Connect en WAN en la nube de AWS en la Guía del usuario de WAN en la nube de AWS.

Verificación de la asociación de una puerta de enlace de Direct Connect con una red central de WAN en la nube de AWS

Compruebe la asociación de una puerta de enlace de Direct Connect con una red central de WAN en la nube en la consola de Direct Connect, en la API de Direct Connect o en la línea de comandos.

Cómo comprobar la asociación de una puerta de enlace de Direct Connect con una red central de WAN en la nube mediante la consola

1. Abra la consola de Direct Connect en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, seleccione Direct Connect gateways (Puertas de enlace de Direct Connect).
3. Seleccione la asociación de la puerta de enlace de Direct Connect que desee ver.
4. Seleccione la pestaña de Asociaciones de puerta de enlace.
   - La columna ID muestra el ID de la red central a la que está asociada la puerta de enlace de Direct Connect.
   - La columna State (Estado) aparece asociada.
   - La columna Association type (Tipo de asociación) muestra Cloud WAN Core Network (Red central de WAN en la nube).

Cómo comprobar la asociación de una puerta de enlace de Direct Connect con una red central de WAN en la nube mediante la línea de comando o API

- DescribeDirectConnectGatewayAssociations (API de Direct Connect)
- describe-direct-connect-gateway-association (AWS CLI)

Interacciones de prefijos permitidas para las puertas de enlace de Direct Connect

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 Routing policies and BGP communities.

Asociaciones de la puerta de enlace 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 puerta de enlace 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 o eliminar el tráfico que utiliza ese prefijo.

Asociaciones de la gateway 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.

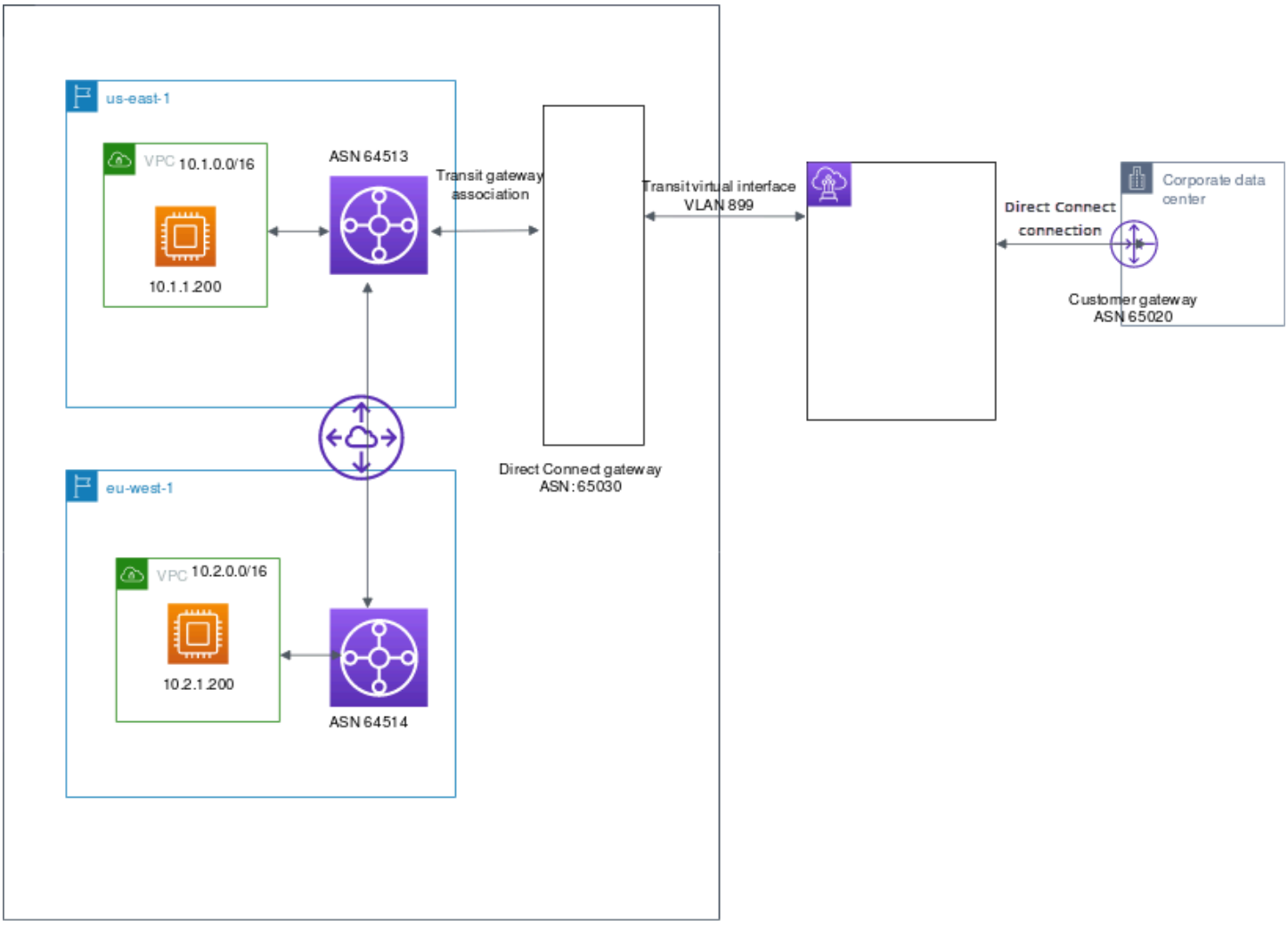
Cuando elimina o agrega un prefijo permitido, el tráfico que no lo utiliza no se ve afectado. Durante las actualizaciones, el estado cambia de `associated` a `updating`. La modificación de un prefijo existente solo puede retrasar o eliminar el tráfico que utiliza ese prefijo.

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 Direct Connect.



Configure las siguientes opciones para los recursos:

- Puerta de enlace de Direct Connect: establezca el ASN en 65 030. Para obtener más información, consulte Cree una puerta de enlace de Direct Connect.
- Interfaz virtual de tránsito: establezca la VLAN en 899 y el ASN del router del cliente en 65 020. Para obtener más información, consulte Cree 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 abarca ambos bloques de CIDR de la VPC (10.0.0.0/16 y 10.2.0.0/16). Para obtener más información, consulte Asociar una puerta de enlace de tránsito a Direct Connect o desasociarla de este..

- Ruta de la VPC: para enrutar el tráfico desde la VPC 10.2.0.0/16, cree una ruta en la tabla de enrutamiento de la VPC con un destino de 0.0.0.0/0 y el ID de la puerta de enlace de tránsito como destino. Esto permite que el tráfico de la VPC alcance la puerta de enlace de Direct Connect. 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.

Etiquetar recursos de AWS Direct Connect

Una etiqueta es un elemento que el propietario de un recurso asigna a sus recursos de 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 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 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 recursos	Clave de etiqueta	Valor de etiqueta
`dxcon-11aa22bb`	Finalidad	Producción
	Ubicación	Ámsterdam
`dxvif-33cc44dd`	Finalidad	Producción
`dxcon-abcabcab`	Finalidad	Copia de seguridad
	Ubicación	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 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 Direct Connect mediante la consola de Direct Connect, la API de 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
Connections	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
Puertas de enlace de Direct Connect	Sí	Sí	Sí	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 Administración de facturación y costos de AWS.

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 AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted 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 AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes 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 aplicables AWS Direct Connect, consulte los AWS servicios incluidos en el ámbito de aplicación por programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Direct Connect. Los siguientes temas muestran cómo configurarlo Direct Connect para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus Direct Connect recursos.

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 Direct Connect. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres 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, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la 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:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utiliza SSL/TLS para comunicarse con los recursos de AWS. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure los registros de API y de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre cómo utilizar registros de seguimiento de CloudTrail para capturar actividades de AWS, consulta Working with CloudTrail trails en la Guía del usuario de AWS CloudTrail.
- Utiliza las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de Servicios de AWS.
- Utiliza 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 140-3 al acceder a AWS a través de una interfaz de línea de comandos o una API, utiliza un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir 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 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 ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede 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 Seguridad de la infraestructura.
- Una asociación a VPC. Para obtener más información, consulte Asociaciones de la puerta de enlace privada virtual y Asociaciones de la gateway 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 Seguridad de la infraestructura.
- Una asociación a VPC. Para obtener más información, consulte Asociaciones de la puerta de enlace privada virtual y Asociaciones de la gateway 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 atraviesan AWS Direct Connect, debe utilizar las opciones de cifrado en

tránsito de ese servicio. Para obtener más información sobre el cifrado del tráfico de instancias de EC2, consulte Cifrado en tránsito 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 dedicadas de AWS Direct Connect 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 conexiones de Direct Connect compatibles con MACsec para cifrar los datos desde el centro de datos corporativo hasta la ubicación de Direct Connect. Para obtener más información, consulte Seguridad MAC (MACSec).

Identity and Access Management para Direct Connect

AWS Identity and Access Management (IAM) es un sistema Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Direct Connect. La IAM es una Servicio de AWS herramienta que puede utilizar sin coste adicional.

Temas

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicita permisos al administrador si no se puede acceder a las características (consulte Solución de problemas de identidad y acceso de Direct Connect).
- Administrador del servicio: determina el acceso de los usuarios y envía las solicitudes de permiso (consulte Funcionamiento de Direct Connect con IAM).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte Ejemplos de políticas basadas en identidades de Direct Connect).

Autenticación con identidades

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

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

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

Cuenta de AWS usuario root

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

Identidad federada

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

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

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

Usuarios y grupos de IAM

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

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

Roles de IAM

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

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

Administración del acceso con políticas

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

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

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

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de política de permisos JSON que asocia a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

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

Políticas basadas en recursos

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

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

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.

- Políticas de control de servicios (SCPs): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations .
- Políticas de control de recursos (RCPs): establece los permisos máximos disponibles para los recursos de tus cuentas. Para obtener más información, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del usuario de IAM.

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

Característica de IAM	Compatibilidad de Direct Connect
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACLs	No

Característica de IAM	Compatibilidad de Direct Connect
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 visión general de cómo funcionan Direct Connect y otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios 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 la identidad, consulte Definición de permisos de IAM personalizados con políticas administradas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de la política de 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

Admite 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 basada en recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones de políticas de Direct Connect

Compatibilidad con las acciones de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para obtener una lista de las acciones de Direct Connect, consulte Acciones definidas por Direct Connect en la Referencia de autorización de servicios.

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": [
      "directconnect:action1",
      "directconnectaction2"
         ]
```

Recursos de políticas de Direct Connect

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, 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 respectivos tipos ARNs, consulte Recursos definidos por Direct Connect en la referencia de la AWS Direct Connect API. 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

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

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 se puede utilizar una clave de condición, consulte Acciones, recursos y claves de condición para 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.

ACLs en Direct Connect

Soportes ACLs: No

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

ABAC con Direct Connect

Compatibilidad con 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 denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del director coincida con la etiqueta del recurso.

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

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

Para obtener más información sobre ABAC, consulte Definición de permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con Direct Connect

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a AWS los recursos a corto plazo y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Permisos de entidad principal entre servicios de Direct Connect

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos del principal que llama y los que solicitan Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Sesiones de acceso directo.

Roles de servicio de Direct Connect

Compatible con roles de servicio: sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear 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

Compatibilidad con roles vinculados al servicio: no

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta 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. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Direct Connect, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Direct Connect en la Referencia de autorización del 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 costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Acciones, recursos y condiciones de Direct Connect

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. 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 usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones de políticas de Direct Connect utilizan el siguiente prefijo antes de la acción: `directconnect:`. Por ejemplo, para conceder permiso a alguien para ejecutar una EC2 instancia de Amazon con la operación de la EC2 `DescribeVpnGateways` API de Amazon, debes incluir la `ec2:DescribeVpnGateways` acción en su 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 otorga acceso de lectura a Direct Connect.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

El siguiente ejemplo de política otorga acceso total a Direct Connect.

JSON

```
{
    "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 usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). En el caso de las acciones que no admiten permisos por recurso, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Direct Connect utiliza lo siguiente ARNs:

Recurso de conexión directa ARNs

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 sobre el formato de ARNs, consulte Amazon Resource Names (ARNs) y AWS Service Namespaces.

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 tipos ARNs, consulte los tipos de recursos definidos por 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 Acciones definidas por Direct Connect.

Si un ARN de recurso o un patrón de ARN de recurso distinto `*` del especificado en el `Resource` campo de la declaración de política de IAM para DescribeConnections,,, o,,,,,,,,,,,,,,,,,,, DescribeVirtualInterfaces,, DescribeDirectConnectGateways,, DescribeInterconnects,, DescribeLags,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,, `Effect` Sin embargo, si proporciona `*` como recurso en lugar de un ID de recurso específico para la declaración de la política de IAM, el `Effect` especificado funcionará.

En el siguiente ejemplo, ningún `Effect` se realizará correctamente si se invoca la acción `DescribeConnections` sin que se apruebe la solicitud `connectionId`.

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "directconnect:DescribeConnections"
```

```
        ],
        "Resource": [
            "arn:aws:directconnect:*:123456789012:dxcon/*"
        ]
    },
{
        "Effect": "Deny",
        "Action": [
            "directconnect:DescribeConnections"
        ],
        "Resource": [
            "arn:aws:directconnect:*:123456789012:dxcon/example1"
        ]
    }
]
```

Sin embargo, en el siguiente ejemplo, `"Effect": "Allow"` se realizará correctamente en la acción `DescribeConnections`, ya que `*` se proporcionó para el campo `Resource` de la declaración de política de IAM, independiente si `connectionId` se especificó en la solicitud.

```
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "directconnect:DescribeConnections
        ],
        "Resource": [
            "*"
        ]
    }
]
```

Claves de condición

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

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 AWS globales, consulte las claves de contexto de condición AWS globales 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 Acciones definidas por Direct Connect.

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 enumerar y ver detalles sobre los recursos de Direct Connect de su AWS cuenta. 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 garantizar que esas entidades puedan seguir utilizando la consola de Direct Connect, adjunte también la siguiente política AWS administrada 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 conceder permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. 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 completar esta acción en la consola o mediante programación mediante la API AWS CLI o 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 Direct Connect

El siguiente ejemplo de política otorga acceso de lectura a. Direct Connect

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Acceso completo a Direct Connect

El siguiente ejemplo de política otorga acceso total a Direct Connect.

JSON

```
{
    "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.

JSON

```
 {
"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

Puedes usar condiciones en tus políticas de IAM para controlar qué pares de etiquetas y valores se pueden transferir en una solicitud que etiqueta un recurso. AWS En el siguiente ejemplo, se muestra cómo se puede crear una política que permita utilizar la 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.

JSON

```
{
    "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.

JSON

```
 {
  "Version":"2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "directconnect:TagResource",
    "Resource": "*",
    "Condition": {
      "ForAllValues:StringEquals": {
        "aws:TagKeys": [
          "environment"
```

```
            ]
          }
        }
      }
    }
```

Funciones vinculadas al servicio para Direct Connect

AWS Direct Connect usa roles vinculados 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. Direct Connect Los roles vinculados al servicio están predefinidos 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 Direct Connect , ya que no es necesario añadir manualmente los permisos necesarios. Direct Connect define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo 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 es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege sus Direct Connect recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que son compatibles con los 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). Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de rol vinculados al servicio para Direct Connect

Direct Connect usa un rol vinculado a un servicio denominado. `AWSServiceRoleForDirectConnect` Esto permite Direct Connect recuperar el MACSec secreto almacenado AWS Secrets Manager en su nombre.

El rol vinculado al servicio `AWSServiceRoleForDirectConnect` depende de 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 Direct Connect debe tener los permisos necesarios. Para conceder los permisos necesarios, asocie la siguiente política a la identidad de IAM.

JSON

```
{
    "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.

Crear un rol vinculado a un servicio para Direct Connect

No es necesario crear manualmente un rol vinculado a un servicio. AWS Direct Connect crea el rol vinculado al servicio automáticamente. Al ejecutar el `associate-mac-sec-key` comando, AWS crea un rol vinculado al servicio que permite Direct Connect recuperar los MACsec secretos que

se almacenan en tu nombre AWS Secrets Manager en la API o en la Consola de administración de AWS API AWS CLI. AWS

> **Important**
>
> Este rol vinculado a servicios 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 eliminas este rol vinculado al servicio y, después, necesitas volver a crearlo, puedes usar el mismo proceso para volver a crear el rol en tu cuenta. Direct Connect vuelve a crear el rol vinculado al servicio para ti.

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 API AWS CLI o en la AWS API, cree un rol vinculado al servicio con el nombre del servicio. `directconnect.amazonaws.com` Para obtener más información, consulte Crear 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.

Edición de un rol vinculado a un servicio para Direct Connect

Direct Connect no permite editar el rol vinculado al `AWSServiceRoleForDirectConnect` servicio. 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 mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar un rol vinculado a un servicio para 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 están almacenados en el servicio AWS Secrets Manager web. La Consola de administración de AWS AWS CLI, la API o la AWS API Direct Connect limpian los recursos y eliminan automáticamente la función vinculada al servicio.

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 Direct Connect servicio utiliza el rol cuando intentas eliminar los recursos, es posible que no se pueda eliminar. En ese caso, espere unos minutos e intente de nuevo la operación.

Para eliminar Direct Connect los recursos utilizados por el **`AWSServiceRoleForDirectConnect`**

1. Elimine la asociación entre todas MACsec las claves y conexiones. Para obtener más información, consulte the section called “Elimine la asociación entre una clave MACsec secreta y una conexión”
2. Elimine la asociación entre todas MACsec las teclas y LAGs. Para obtener más información, consulte the section called “Eliminar la asociación entre una clave secreta de MACsec y un LAG”

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al `AWSServiceRoleForDirectConnect` servicio. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles para los roles vinculados al servicio Direct Connect

Direct Connect admite el uso de funciones vinculadas a servicios en todos los Regiones de AWS lugares donde esté disponible la función de seguridad MAC. Para obtener más información, consulte Ubicaciones de AWS Direct Connect.

AWS políticas gestionadas para AWS Direct Connect

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AWS política gestionada: AWSDirect ConnectFullAccess

Puede asociar la política `AWSDirectConnectFullAccess` a las identidades de IAM. Esta política otorga permisos que permiten el acceso total a Direct Connect.

Para ver los permisos de esta política, consulte AWSDirectConnectFullAccess en la Consola de administración de AWS.

AWS política gestionada: AWSDirect ConnectReadOnlyAccess

Puede asociar la política `AWSDirectConnectReadOnlyAccess` a las identidades de IAM. Esta política otorga permisos que permiten el acceso de solo lectura a. Direct Connect

Para ver los permisos de esta política, consulte AWSDirectConnectReadOnlyAccess en la Consola de administración de AWS.

AWS política gestionada: AWSDirect ConnectServiceRolePolicy

Esta política se adjunta a la función vinculada al servicio denominada AWSServiceRoleForDirectConnect Direct Connect para permitir recuperar los secretos de seguridad de MAC en su nombre. Para obtener más información, consulte the section called “Roles vinculados a servicios”.

Para ver los permisos de esta política, consulte AWSDirectConnectServiceRolePolicy en la Consola de administración de AWS.

Direct Connect actualizaciones de las políticas gestionadas AWS

Consulte los detalles sobre las actualizaciones de las políticas AWS administradas Direct Connect desde que este servicio comenzó a rastrear estos cambios. Para recibir alertas automáticas sobre los cambios en esta página, suscríbase a la fuente RSS de la página del historial del Direct Connect documento.

Cambio	Descripción	Fecha
AWSDirectConnectServiceRolePolicy: política nueva	Para respaldar la seguridad de MAC, se AWSServiceRoleForDirectConnectagregó la función vinculada al servicio.	31 de marzo de 2021
Direct Connect comenzó a rastrear los cambios	Direct Connect comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	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
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Direct Connect

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 AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: 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.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir la función 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 otorguen 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 AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Direct Connect

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admiten políticas basadas en recursos o listas de control de acceso (ACLs), puede usar esas políticas para permitir que las personas accedan a sus recursos.

Para obtener 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 sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte Proporcionar acceso a un usuario de IAM en otro de su propiedad en la Cuenta de AWS Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Registro y monitorización en AWS Direct Connect

Puede utilizar las siguientes herramientas de monitorización automatizado para vigilar 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 Supervisión de 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 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 Supervisar los recursos de Direct Connect.

Validación de conformidad en AWS Direct Connect

Para saber si un Servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte Servicios de AWS incluidos por programa de conformidad y escoja el programa de conformidad que le interese. Para obtener información general, consulte Programas de conformidad de AWS.

Puedes descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact.

Su responsabilidad de conformidad al utilizar Servicios de AWS se determina en función de la confidencialidad de los datos, los objetivos de conformidad de su empresa, así como de la legislación y los reglamentos aplicables. Para obtener más información sobre la responsabilidad de conformidad al usar Servicios de AWS, consulte la Documentación de seguridad de AWS.

Resiliencia en AWS Direct Connect

La infraestructura global de AWS se compone de regiones y zonas de disponibilidad de AWS. 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, 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 the section called “AWS Direct Connect Resiliency Toolkit”.

Seguridad de la infraestructura en () 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 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 principal de IAM. También puedes 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 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 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 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 de Direct Connect”.

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 How AWS is helping to secure internet routing.

Utilizar la CLI de Direct Connect

Puede utilizar la AWS CLI para crear y trabajar con los recursos de Direct Connect.

El ejemplo siguiente utiliza los comandos de la AWS CLI para crear una conexión de 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: Cree 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 Direct Connect. Para obtener más información, consulte Conexiones dedicadas y alojadas.

Para crear una solicitud de conexión

1. Describa las ubicaciones de 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 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 the section called “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 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 puerta de enlace 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 Direct Connect mediante AWS CloudTrail

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 Direct Connect. CloudTrail captura todas las llamadas a la API de Direct Connect como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Direct Connect y las llamadas desde el código a las operaciones de la API de 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 Direct Connect. Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Event history (Historial de eventos). Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a 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.

Direct ConnectInformación de en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad en Direct Connect, esa actividad se registra en un evento de CloudTrail junto con otros eventos de servicio de AWS en Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de eventos en la cuenta de AWS, incluidos los eventos de 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 más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Consulte Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail

- Recepción de archivos de registro de CloudTrail de varias regiones y Recepción de archivos de registro de CloudTrail de varias cuentas

Todas las acciones de Direct Connect las registra CloudTrail y se documentan en la Referencia de la API de 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.

Comprenda las entradas del archivo de registro de 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 de registro de CloudTrail pueden contener una o varias entradas de registro. Un evento representa una solicitud específica realizada desde un origen cualquiera 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 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
    },
    ...
  ]
}
```

Supervisión de recursos de Direct Connect

La supervisión es fundamental a la hora de mantener la fiabilidad, la disponibilidad y el rendimiento de los recursos de Direct Connect. Debe recopilar datos de monitorización de todas las partes de su solución de AWS para que le resulte más sencillo depurar un error que se produce en distintas partes del código, en caso de que ocurra. Sin embargo, antes de comenzar a supervisar Direct Connect, conviene crear un plan de supervisión 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 consiste en establecer un punto de referencia del rendimiento de Direct Connect normal en el entorno. Para ello se mide el rendimiento en distintos momentos y bajo distintas condiciones de carga. A medida que supervise Direct Connect, almacene datos de supervisión históricos. 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 un punto de referencia, conviene supervisar el uso, el estado y la condición de las conexiones físicas de Direct Connect.

Contenido

Herramientas de supervisión

AWS proporciona varias herramientas que puede utilizar para monitorear una conexión de Direct Connect. 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 supervisión automatizadas

Puede utilizar las siguientes herramientas de supervisión automatizada para vigilar Direct Connect e informar cuando algo no funcione correctamente:

- 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 información sobre las métricas y dimensiones disponibles, consulte Supervisión de 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 y Trabajo con archivos de registro de CloudTrail en la Guía del usuario de AWS CloudTrail.

Herramientas de supervisión manuales

Otra parte importante del monitoreo de una conexión de Direct Connect implica el monitoreo manual de los elementos que no cubren las alarmas de CloudWatch. Los paneles de consola de Direct Connect y CloudWatch ofrecen una visión general del estado del entorno de AWS.

- La consola de Direct Connect muestra:
  - Estado de la conexión (consulte la columna State)
  - Estado de la interfaz virtual (consulte la columna State)
- La página principal de CloudWatch muestra:
  - Alarmas y estado actual
  - Gráficos de alarmas y recursos
  - Estado de los servicios

  Además, puede utilizar CloudWatch para hacer lo siguiente:

  - Crear paneles personalizados para monitorear los servicios que le interesan.

- Realizar un gráfico con los datos de las métricas para resolver problemas y descubrir tendencias.
- Buscar y examinar todas sus métricas de recursos de AWS.
- Crear y editar las alarmas de notificación de problemas.

Supervisión de con Amazon CloudWatch

Puede monitorear las conexiones de Direct Connect físicas y las interfaces virtuales mediante CloudWatch. CloudWatch recopila datos sin procesar de Direct Connect y los convierte en métricas de fácil interpretación. De forma predeterminada, CloudWatch ofrece datos métricos de Direct Connect en intervalos de 5 minutos. Los datos métricos de cada intervalo son una agregación de al menos dos muestras recogidas durante ese intervalo.

Para obtener información detallada sobre CloudWatch, consulte la Guía del usuario de Amazon CloudWatch. También puede monitorear sus servicios de CloudWatch para ver cuáles utilizan los recursos. Para obtener más información, consulte Servicios de AWS que publican métricas de CloudWatch.

Contenido

Direct ConnectMétricas y dimensiones de

Las métricas están disponibles para las conexiones físicas de Direct Connect, así como para las interfaces virtuales.

Direct ConnectMétricas de conexión de

Las siguientes métricas están disponibles desde conexiones dedicadas de Diect 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: no se devuelven unidades para esta métrica.
`ConnectionBpsEgress`	La velocidad de bits de los datos de salida del extremo de AWS 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 de entrada del extremo de AWS 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 paquete de los datos de salida del extremo de AWS 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 paquete de los datos de entrada del extremo de AWS 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 redundanc ia 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 “suma”. 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
`ConnectionLightLevelTx`	Indica el estado de la conexión de fibra para el tráfico de salida del extremo de AWS de la conexión. Hay dos dimensiones para esta métrica. Para obtener más información, consulte Dimensiones disponibles de Direct Connect. Unidades: dBm

Métrica	Descripción
`ConnectionLightLevelRx`	Indica el estado de la conexión de fibra para el tráfico de entrada del extremo de AWS de la conexión. Hay dos dimensiones para esta métrica. Para obtener más información, consulte Dimensiones disponibles de Direct Connect. 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.

Direct ConnectMétricas de interfaz virtual de

Las siguientes métricas están disponibles desde interfaces virtuales de Direct Connect.

Métrica	Descripción
`VirtualInterfaceBpsEgress`	La velocidad de bits de los datos de salida del extremo de AWS 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
`VirtualInterfaceBpsIngress`	La velocidad de bits de los datos de entrada al extremo de AWS 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
`VirtualInterfacePpsEgress`	La velocidad de paquete de los datos de salida del extremo de AWS 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 paquete de los datos de entrada al extremo de AWS 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

Direct ConnectDimensiones de disponibles

Puede filtrar los datos de Direct Connect utilizando las siguientes dimensiones.

Dimensión	Descripción
`ConnectionId`	Esta dimensión está disponible en las métricas para la conexión de Direct Connect y la interfaz virtual. Esta dimensión filtra los datos por conexión.
`OpticalLaneNumber`	Esta dimensión filtra los datos de `ConnectionLightLevelTx` y `ConnectionLightLevelRx`, y los filtra por el número de carril óptico de la conexión de Direct Connect.

Dimensión	Descripción
`VirtualInterfaceId`	Esta dimensión está disponible en las métricas de la interfaz virtual de Direct Connect y filtra los datos por interfaz virtual.

Temas

- Ver métricas de CloudWatch de Direct Connect
- Cree alarmas de Amazon CloudWatch para supervisar las conexiones de Direct Connect

Ver métricas de CloudWatch de Direct Connect

Direct Connect envía las siguientes métricas sobre las conexiones de Direct Connect. Luego, Amazon CloudWatch agrega estos puntos de datos a intervalos de 1 o 5 minutos. De forma predeterminada, los datos de métricas de Direct Connect se escriben en CloudWatch cada 5 minutos.

> **Note**
>
> Cuando monitoree Direct Connect mediante CloudWatch, puede solicitar métricas en intervalos de un minuto. Sin embargo, CloudWatch controla la frecuencia de actualización. Puesto que CloudWatch controla el intervalo, Direct Connect no siempre puede garantizar intervalos inferiores a cinco minutos.

Puede utilizar los siguientes procedimientos para ver las métricas de las conexiones de Direct Connect.

Para ver las métricas a través de la consola de CloudWatch

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 utilizar Amazon CloudWatch a fin de ver las métricas de Direct Connect, incluida la adición de funciones matemáticas o consultas prediseñadas, consulte Uso de métricas de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

1. Abra la consola de CloudWatch 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 ConnectionId o el Nombre de la métrica y, a continuación, elija una de las siguientes opciones para definir aún más 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 Información de métricas, consulte Consultar las métricas con Información de métricas de CloudWatch en la Guía del usuario de Amazon CloudWatch.

Para consultar las métricas desde la consola de Direct Connect

1. Abra la consola de Direct Connect 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 métricas mediante la AWS CLI

En el símbolo del sistema, ejecute el siguiente comando.

```
aws cloudwatch list-metrics --namespace "AWS/DX"
```

Cree alarmas de Amazon CloudWatch para supervisar las conexiones de Direct Connect

Puede crear una alarma de CloudWatch 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 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 a fin de crear una alarma y sobre cómo crear una alarma, consulte Uso de alarmas de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

Para crear una alarma de CloudWatch.

1. Abra la consola de CloudWatch 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. Elija Crear alarma.
4. Elija Seleccionar métrica y, a continuación, elija DX.
5. Elija la métrica de Métricas de conexión.
6. Seleccione la conexión Direct Connect y, a continuación, seleccione la métrica Seleccionar métrica.
7. En la página Especificar la métrica y las condiciones, configure los parámetros de la alarma. Para obtener más información sobre la especificación de métricas y condiciones, consulte Uso de alarmas de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.
8. Elija Siguiente.
9. Configure las acciones de alarma en la página Configurar acciones. Para obtener más información sobre la configuración de las acciones de alarma, consulte Acciones de alarma en la Guía del usuario de Amazon CloudWatch.
10. Elija 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.

Direct ConnectCuotas de

En la siguiente tabla se muestran las cuotas relacionadas con Direct Connect.

Componente	Cuota	Comentarios
Interfaces virtuales públicas o privadas por conexión dedicada de Direct Connect	50	Este límite no se puede aumentar.
Interfaces virtuales de tránsito por conexión dedicada de Direct Connect. Las interfaces virtuales de tránsito se pueden utilizar para conectarse a una red central de la puerta de enlace de tránsito o de WAN en la nube de AWS. Para obtener más información, consulte Puertas de enlace.	4	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Interfaces virtuales privadas o públicas por conexión dedicada de Direct Connect e interfaces virtuales de tránsito por conexión dedicada de Direct Connect	51	Cuando se lanzó la compatibilidad de AWS Direct Connect con las puertas de enlace de tránsito de Amazon VPC, se agregó 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 de tránsito, públicas o privadas por conexión alojada de Direct Connect	1	Este límite no se puede aumentar.

Componente	Cuota	Comentarios
Conexiones de Direct Connect activas por ubicación de Direct Connect por región por 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 compatibilidad de AWS Direct Connect con las puertas de enlace de tránsito de Amazon VPC, se agregó una cuota de una (1) interfaz virtual de tránsito a la cuota 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 del protocolo de puerta de enlace fronteriza (BGP) en una interfaz virtual privada o de tránsito desde las instalaciones hasta 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	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Rutas por sesión de protocolo de puerta de enlace 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.
Puertas de enlace de Direct Connect 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 de Direct Connect	20	Este límite no se puede aumentar.
Puertas de enlace de tránsito por puerta de enlace de Direct Connect	6	Este límite no se puede aumentar.

Componente	Cuota	Comentarios
Número máximo de prefijos de ruta anunciados desde una puerta de enlace de Direct Connect de la red central WAN en la nube de AWS asociada en las instalaciones. **Note** Todas las interfaces virtuales de tránsito conectadas a esa puerta de enlace de Direct Connect recibirán todos los prefijos de ruta anunciados por la red central.	5 000	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Interfaces virtuales (privadas o de tránsito) por puerta de enlace de Direct Connect	30	Este límite no se puede aumentar.
Número de prefijos por AWS Transit Gateway desde AWS hasta las instalaciones en una interfaz virtual de tránsito	200 combinados en total para IPv4 e IPv6	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 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.

Componente	Cuota	Comentarios
Límite de prefijos de SiteLink	100	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.

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 y 400 Gbps: 400GBASE-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

Límites del ASN

Los siguientes límites se aplican a los números de sistema autónomo (ASN) que se utilizan con Direct Connect:

- Rango del ASN del lado del cliente: 1 a 4,294,967,294
  - ASN: 1 a 2147483647

  - ASN largos: 1 a 4294967294
- ASN del lado de Amazon: valores fijos asignados por AWS (normalmente 7224 para interfaces virtuales públicas)
- Rangos del ASN privado:
  - ASN privados: de 64,512 a 65,534
  - ASN privados largos: 4,200,000,000 a 4,294,967,294

> **Note**
>
> En el caso de las interfaces virtuales públicas, su ASN debe ser un ASN privado o debe estar registrado y permitir su uso con la interfaz virtual.

Consideraciones sobre el equilibrio de carga

Si desea utilizar el equilibrio de carga con varias interfaces virtuales públicas, todas las interfaces virtuales deben estar en la misma región.

Solucionar Direct Connect

La siguiente información de solución de problemas puede ayudarlo a diagnosticar y solucionar problemas con su conexión de Direct Connect.

Contenido

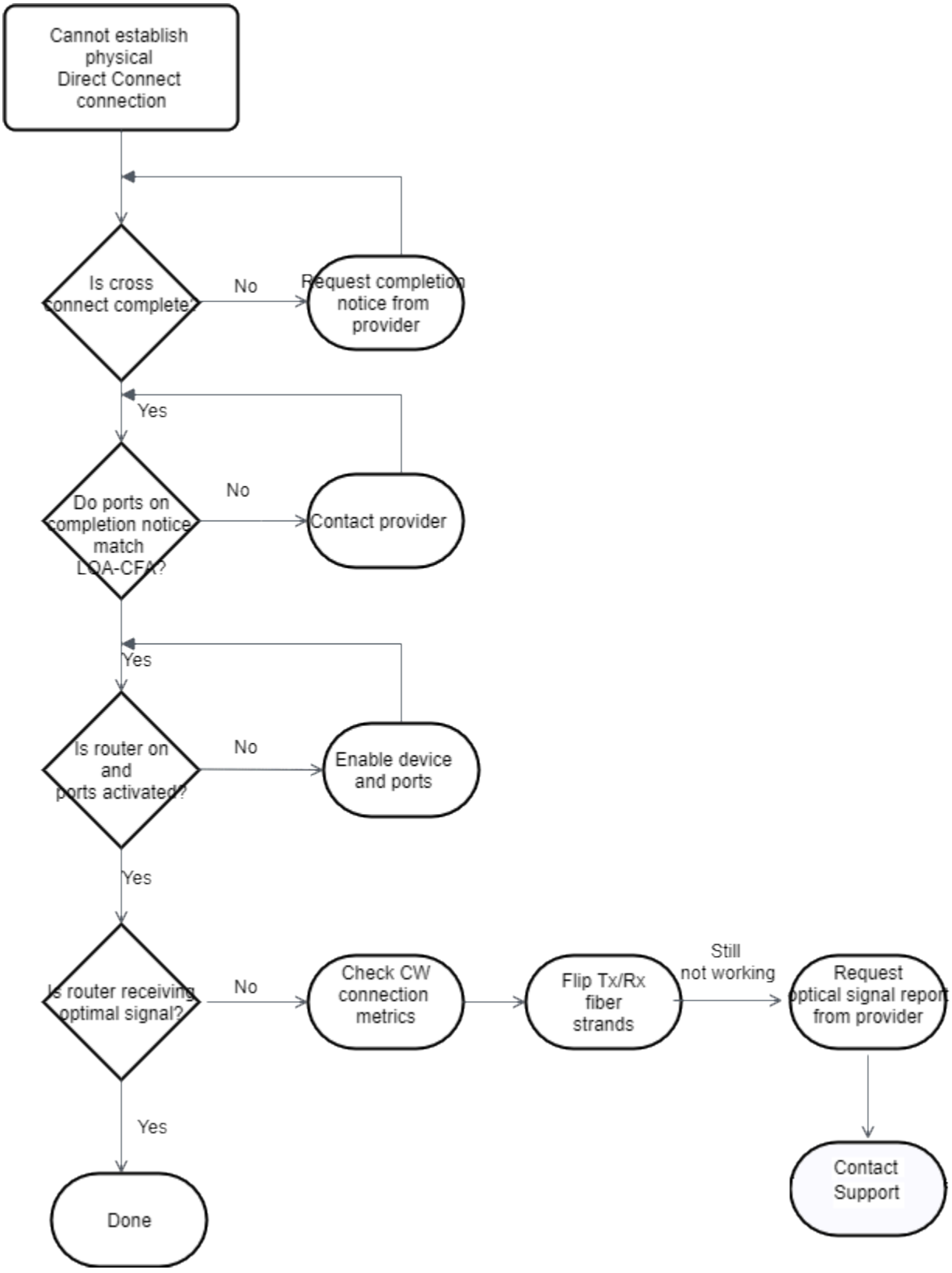
Solucione los problemas de capa 1 (físicos)

Si usted o su proveedor de red tienen dificultades para establecer una conectividad física con un dispositivo de Direct Connect, utilice los pasos siguientes 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, en función del punto de conexión de AWS Direct Connect que proporcione su conexión, es posible que sea necesario habilitar o deshabilitar 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). En función del punto de conexión de Direct Connect que proporcione su conexión, es posible que sea necesario habilitar o deshabilitar la negociación automática según corresponda.
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. Compruebe las métricas de Amazon CloudWatch para Direct Connect. Puede verificar las lecturas ópticas Tx/Rx del dispositivo de Direct Connect (tanto de 1 Gbps como de 10 Gbps), el recuento de errores físicos y el estado operativo. Para obtener más información, consulte Monitorización con 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.

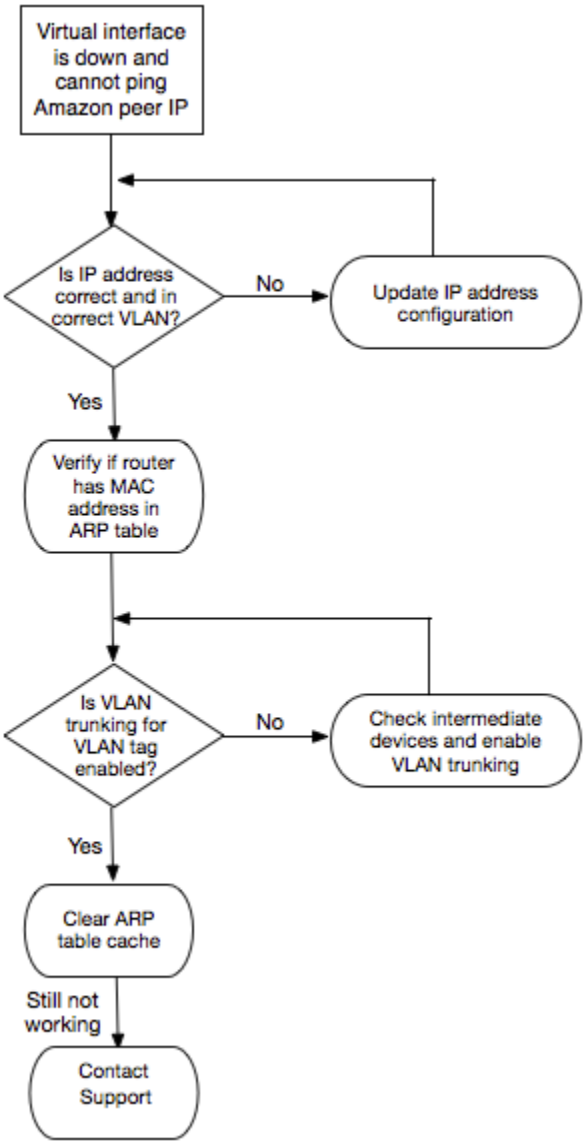

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check 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 física de Direct Connect está activa, pero la interfaz virtual no funciona, siga estos 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 está configurada en la subinterfaz VLAN y no en la interfaz física (por ejemplo, GigabitEthernet0/0.123 en lugar de GigabitEthernet0/0).
2. Compruebe si el enrutador tiene una entrada de dirección MAC para el punto de conexión de AWS en la tabla del protocolo 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 en el lado de AWS hasta que AWS reciba tráfico etiquetado.
4. Borre la caché de su tabla de ARP o de la del proveedor.
5. Si los pasos anteriores no permiten establecer el ARP o sigue sin poder hacer ping a la dirección IP de mismo nivel de Amazon, póngase en contacto con AWS Asistencia.

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 enrutamiento.

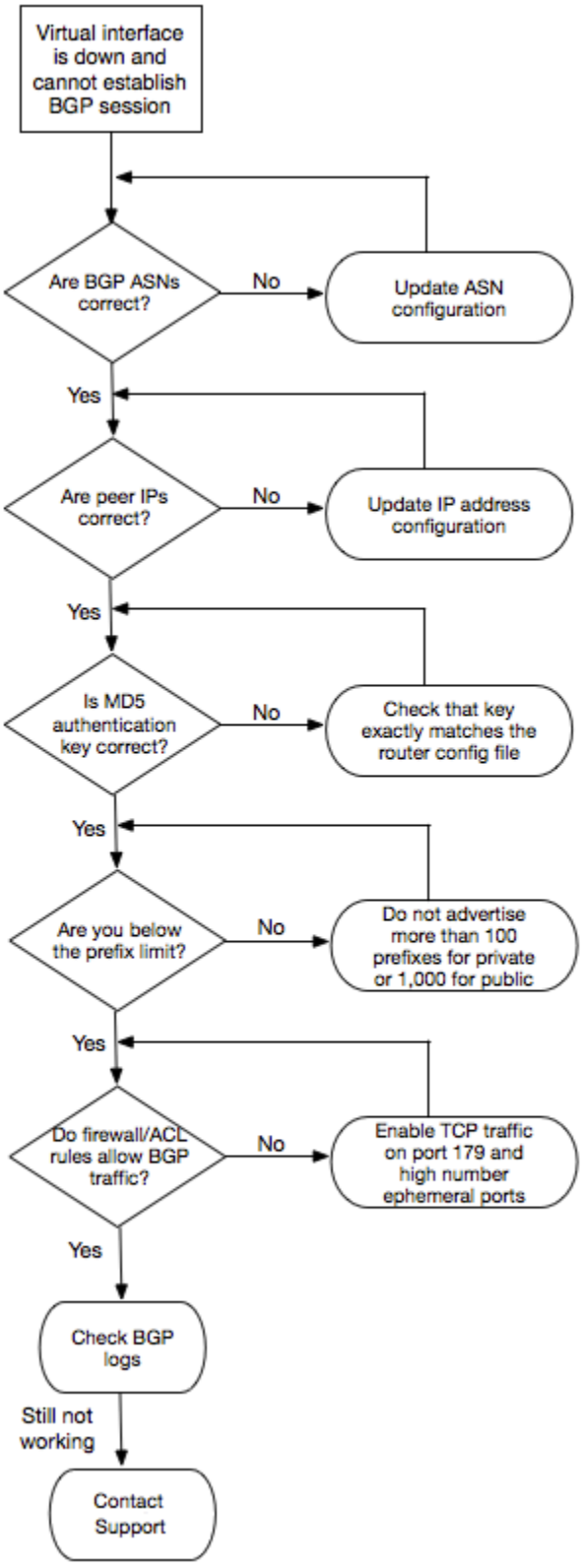
Solución de problemas de capa 3/4 (red/transporte)

Imagine una situación en la que su conexión física de Direct Connect está activa y puede hacer ping a la dirección IP de mismo nivel de Amazon. Si la interfaz virtual está activa 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 intercambio de tráfico del BGP, póngase en contacto con AWS Asistencia.

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 enrutamiento.

Solución de problemas de ASN largos

Si tiene problemas con las configuraciones del ASN largo, sigua los siguientes pasos para solucionarlas:

La sesión del BGP falla con un ASN largo

Síntomas: la sesión del BGP no se puede establecer después de configurar un ASN largo

Causa: es posible que el router local no admita la capacidad de ASN largo

Solución:

- Compruebe que su router sea compatible con RFC 6793
- Compruebe la configuración del BGP para ver si el formato ASN es coherente
- Revise los registros del BGP para ver si hay errores de negociación de capacidades

Las respuestas de la API muestran el ASN como 0

Síntomas: las respuestas de la API muestran el campo `asn` como 0

Causa: este es el comportamiento esperado cuando el ASN real supera 2,147,483,647

Solución: utilice el campo `asnLong` en las respuestas de la API para obtener el valor de ASN correcto

Migración de ASN a problemas de ASN largos

Síntomas: pérdida de conectividad durante la migración a un ASN

Causa: es necesario restablecer la sesión del BGP para los cambios en el ASN

Solución:

- Planifique la migración durante los periodos de mantenimiento
- Actualice una interfaz virtual a la vez
- Supervise el estado de la sesión del BGP durante los cambios
- Verifique la convergencia de la tabla de enrutamiento después de la migración

Si sigue teniendo problemas con las configuraciones de ASN largos después de seguir estos pasos, póngase en contacto con AWS Support con la siguiente información:

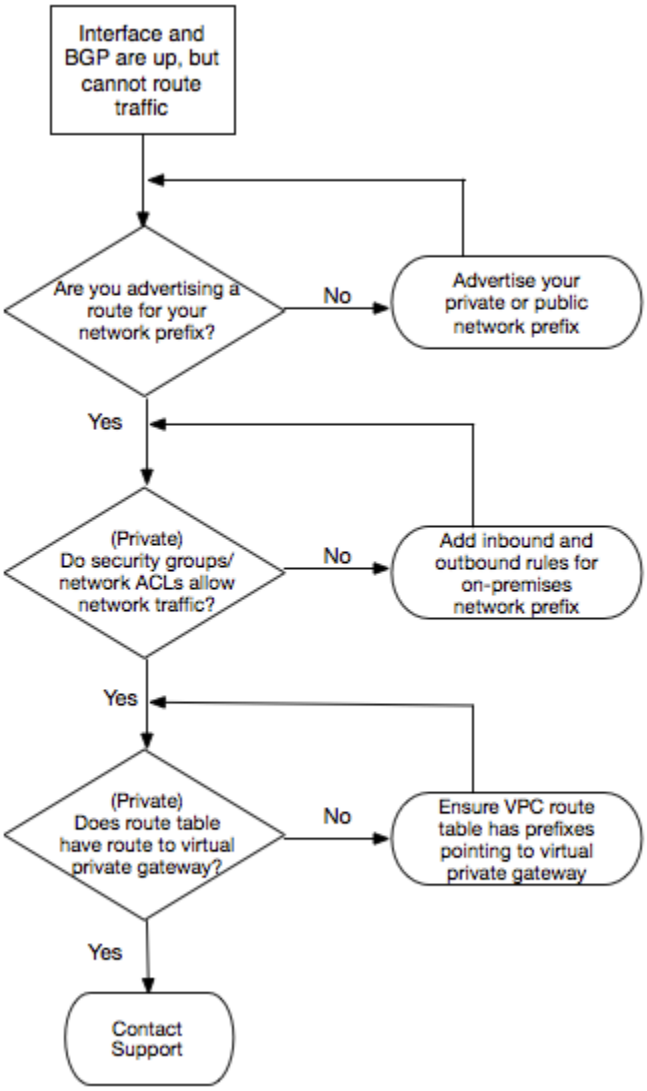
- ID de interfaz virtual o ID de par BGP
- Valores de ASN configurados (ASN y ASN largo)
- Modelo de router y versión de software
- Configuración y registros de BGP
- Se observaron mensajes de error o síntomas

Solución de problemas de enrutamiento

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 enrutamiento de la VPC tienen prefijos que apuntan a la puerta de enlace privada virtual a la que está conectada la 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 puerta de enlace privada virtual como destino en las tablas de enrutamiento 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 Asistencia.

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 de documentos

En la tabla siguiente se describen las versiones de las AWS Direct Connect. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Compatibilidad para ASN largo	Ahora puede usar los valores de ASN largos para las sesiones de BGP con las interfaces virtuales de Direct Connect.	24 de julio de 2025
Crear una asociación entre la puerta de enlace de Direct Connect y una red central de AWS Network Manager	Ahora puede crear una asociación de puerta de enlace Direct Connect directamente entre Direct Connect y una red principal de AWS Cloud WAN.	25 de noviembre de 2024
Compatibilidad con 400 G	Temas actualizados para incluir la compatibilidad con 400 G conexiones.	18 de julio de 2024
Se agregó un límite de prefijos de SiteLink	Se agregó un límite de prefijos de SiteLink para el tema de cuotas y límites.	15 de junio de 2023
Compatibilidad con SiteLink	Puede crear una interfaz privada virtual que habilite la conectividad entre dos puntos de presencia (PoP) de Direct Connect en la misma región de AWS.	1 de diciembre de 2021
Compatibilidad con la seguridad de MAC	Puede utilizar conexiones de Direct Connect compatibles con MACsec para cifrar los	31 de marzo de 2021

	datos desde el centro de datos corporativo hasta la ubicación de Direct Connect.	
Compatibilidad con 100 G	Temas actualizados para incluir la compatibilidad con conexiones dedicadas de 100 G.	12 de febrero de 2021
Ubicación nueva en Italia	Tema actualizado para incluir la ubicación nueva en Italia.	22 de enero de 2021
Nueva ubicación en Israel	Tema actualizado para incluir la ubicación nueva en Israel.	7 de julio de 2020
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.	3 de junio de 2020
Compatibilidad con métricas de interfaz virtual de CloudWatch	Puede monitorear las conexiones de Direct Connect físicas y las interfaces virtuales mediante CloudWatch.	11 de mayo de 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.	7 de octubre de 2019

Compatibilidad con regiones adicionales para permitir el uso de AWS Transit Gateway entre cuentas	Compatibilidad con regiones adicionales para el uso de AWS Transit Gateway entre cuentas.	30 de septiembre de 2019
Compatibilidad con AWS Direct Connect para AWS Transit Gateway	Puede utilizar una puerta de enlace de Direct Connect para conectar su conexión de 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 la conexión de Direct Connect con la puerta de enlace de Direct Connect.	27 de marzo de 2019
Compatibilidad con tramas gigantes	Puede enviar tramas gigantes (9001 MTU) sobre Direct Connect.	11 de octubre de 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.	6 de febrero de 2018

Direct Connect puerta de enlace	Puede usar una puerta de enlace de Direct Connect para establecer la conexión de Direct Connect con las VPC de regiones remotas.	1 de noviembre de 2017
Métricas de Amazon CloudWatch	Puede ver las métricas de CloudWatch de las conexiones de Direct Connect.	29 de junio de 2017
Grupos de agregación de enlaces (LAG	Puede crear un grupo de agregación de enlaces (LAG) para agregar varias conexione s de Direct Connect.	13 de febrero de 2017
Compatibilidad con IPv	La interfaz virtual ahora es compatible una sesión de intercambio de tráfico BGP IPv6.	1 de diciembre de 2016
Compatibilidad del etiquetado	A partir de ahora, puede etiquetar los recursos de Direct Connect.	4 de noviembre de 2016
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 Direct Connect.	22 de junio de 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).	3 de junio de 2016

Nueva ubicación en Ámsterdam	Tema actualizado para incluir la ubicación nueva en Ámsterdam en la región Europa (Fráncfort).	19 de mayo de 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 de abril de 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).	9 de diciembre de 2015
Nuevas ubicaciones en Dallas, Londres, Silicon Valley y Mumbai	Se actualizaron los temas para incluir las ubicaciones nuevas en Dallas (región Este de EE. UU. [Norte de Virginia]), Londres (región Europa [Irlanda]), Silicon Valley (región AWS GovCloud [Oeste de EE. UU.]) y Bombay (región Asia-Pacífico [Singapur]).	27 de noviembre de 2015
Ubicación nueva en la región China (Pekín	Temas actualizados para incluir la ubicación nueva en Pekín en la región China (Pekín).	14 de abril de 2015
Nueva ubicación en Las Vegas en la región EE. UU. Oeste (Oregón	Temas actualizados para incluir la nueva ubicación de Direct Connect en Las Vegas en la región EE. UU. Oeste (Oregón).	10 de noviembre de 2014

Nueva región UE (Fráncfort	Temas actualizados para incluir la nuevas ubicaciones de Direct Connect que sirven a la región UE (Fráncfort).	23 de octubre de 2014
Nuevas ubicaciones en la región Asia Pacífico (Sídney	Temas actualizados para incluir las nuevas ubicacion es de Direct Connect que sirven a la región Asia Pacífico (Sídney).	14 de julio de 2014
Compatibilidad con AWS CloudTrail	Se agregó un tema nuevo en el que se detalla cómo utilizar CloudTrail para registrar actividad en Direct Connect.	4 de abril de 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.	19 de diciembre de 2013
Compatibilidad con conexione s alojadas	Temas actualizados para incluir la compatibilidad con conexiones alojadas.	22 de octubre de 2013
Nueva ubicación en la región UE (Irlanda	Temas actualizados para incluir la nueva ubicación de Direct Connect que sirve a la región UE (Irlanda).	24 de junio de 2013
Nueva ubicación en Seattle en la región EE. UU. Oeste (Oregón	Temas actualizados para incluir la nueva ubicación de Direct Connect en Seattle en la región EE. UU. Oeste (Oregón).	8 de mayo de 2013

Compatibilidad para utilizar IAM con Direct Connect	Tema añadido que explica cómo utilizar AWS Identity and Access Management con Direct Connect.	21 de diciembre de 2012
Nueva región Asia Pacífico (Sídney	Temas actualizados para incluir la nueva ubicación de Direct Connect que sirve a la región Asia Pacífico (Sídney).	14 de diciembre de 2012
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 Direct Connect ha reemplazado a la Guía de introducción a Direct Connect. Nuevos temas añadidos sobre la nueva consola de Direct Connect. Además, se ha añadido un tema sobre facturación, información sobre la configura ción del router y se han actualizado temas para incluir las dos nuevas ubicaciones de Direct Connect que sirven a las regiones EE. UU. Este (Norte de Virginia) y América del Sur (São Paulo).	13 de agosto de 2012
Compatibilidad con las regiones UE (Irlanda), Asia Pacífico (Singapur) y Asia Pacífico (Tokio	Nueva sección de solución de problemas y temas actualiza dos para incluir las cuatro nuevas ubicaciones de Direct Connect que sirven a las regiones EE. UU. Oeste (Norte de California), UE (Irlanda), Asia Pacífico (Singapur) y Asia Pacífico (Tokio).	10 de enero de 2012

Compatibilidad con la región EE. UU. Oeste (Norte de California	Temas actualizados para la región EE. UU. Oeste (Norte de California).	8 de septiembre de 2011
Versión pública	La primera versión de Direct Connect.	3 de agosto de 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.