Guía del usuario

AWS Direct Connect

AWS Direct Connect: Guía del usuario

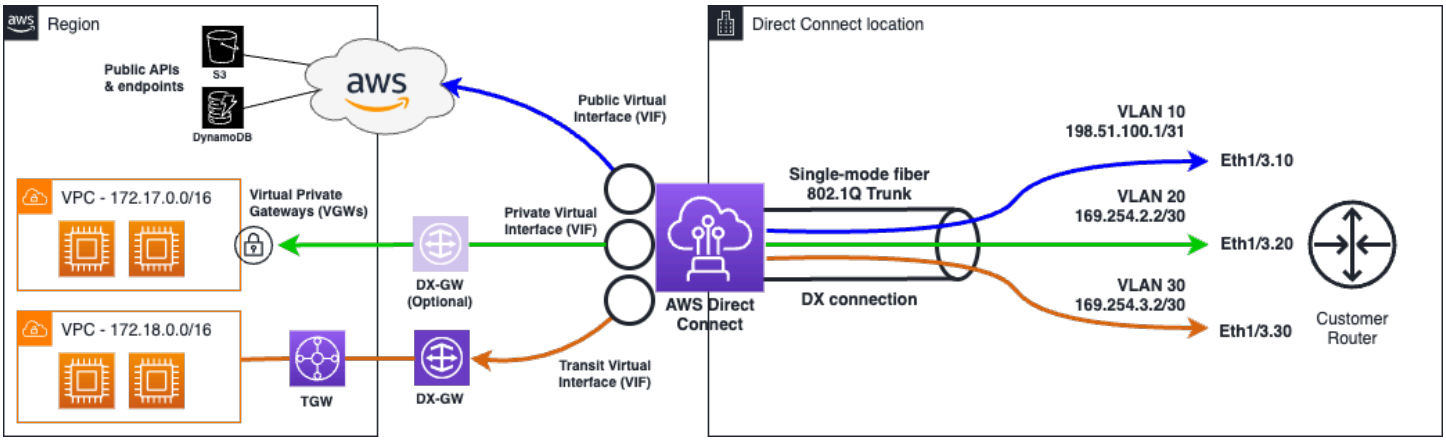
Table of Contents

¿Qué es AWS Direct Connect?

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

- Para obtener una lista de las ubicaciones de Direct Connect a las que puede conectarse, consulte Ubicaciones de AWS Direct Connect.
- Para obtener respuestas a las preguntas sobre Direct Connect, consulte Direct Connect FAQ.

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



Contenido

- AWS Direct Connect políticas y BGP comunidades de enrutamiento

AWS Direct Connect componentes

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

Conexiones

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

Interfaces virtuales

Cree una interfaz virtual para permitir el acceso a AWS los servicios. Una interfaz virtual pública lo habilita para acceder a servicios públicos, como Amazon S3. Una interfaz virtual privada permite el acceso a suVPC. Los tipos de interfaces compatibles se describen a continuación enthe section called “Tipos de interfaz virtual Direct Connect compatibles”. Para obtener más información sobre las interfaces compatibles, consulte AWS Direct Connect interfaces virtuales e interfaces virtuales alojadas yRequisitos previos de las interfaces virtuales.

Requisitos de red

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

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

Además, la red debe cumplir las siguientes condiciones:

- Su red debe utilizar fibra monomodo con un transceptor 1000 BASE -LX (1310 nm) para Ethernet de 1 gigabit, un transceptor 10 GBASE -LR (1310 nm) para 10 gigabits, uno 100 para Ethernet de 100 GBASE gigabit o un transceptor de 400 LR4 para Ethernet de 400 Gbps. GBASE LR4
- La negociación automática de un puerto debe estar deshabilitada para una conexión con una velocidad de puerto superior a 1 Gbps. Sin embargo, según el punto final de AWS Direct Connect que dé servicio a su conexión, es posible que sea necesario activar o desactivar la negociación automática para las conexiones de 1 Gbps. Si la interfaz virtual permanece inactiva, consulte Solución de problemas de capa 2 (enlace de datos).
- VLANLa encapsulación 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 su red. La función asíncrona BFD se habilita automáticamente para cada interfaz virtual. AWS Direct Connect Se habilita de forma automática en las interfaces virtuales de Direct Connect, pero no funcionará hasta que la configure en el enrutador. Para obtener más información, consulte BFDHabilitar una conexión Direct Connect.

AWS Direct Connect es compatible con los protocolos de IPv6 comunicación IPv4 y los protocolos de comunicación. IPv6se puede acceder a las direcciones proporcionadas por los AWS servicios AWS Direct Connect públicos a través de interfaces virtuales públicas.

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

Tipos de interfaz virtual Direct Connect compatibles

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

- Interfaz virtual privada

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

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

- Interfaz virtual pública

  Este tipo de interfaz virtual se utiliza para acceder a todos los servicios AWS públicos mediante direcciones IP públicas. Con una interfaz virtual pública, puede conectarse a todos los servicios y direcciones IP AWS públicos de todo el mundo.

- Interfaz virtual de tránsito

  Este tipo de interfaz se utiliza para acceder a una o más pasarelas de Amazon VPC Transit asociadas a las pasarelas de Direct Connect. Con una interfaz virtual de transporte, conectas múltiples Amazon VPC Transit Gateways a través de varias cuentas y Regiones de AWS (excepto en las regiones de AWS China).

> **Note**
>
> Hay límites en el número de tipos diferentes de asociaciones entre una puerta de enlace Direct Connect y una interfaz virtual. Para obtener más información sobre límites específicos, consulte la Cuotas de Direct Connect página.

Para obtener más información sobre las interfaces virtuales, consulteInterfaces virtuales e interfaces virtuales alojadas.

Precios de Direct Connect

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

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

En el caso de AWS los recursos direccionables públicamente (por ejemplo, cubos de Amazon S3, EC2 instancias clásicas o EC2 tráfico que pasa por una puerta de enlace de Internet), si el tráfico saliente se destina a prefijos públicos que pertenecen a la misma cuenta de AWS pagador y se anuncian activamente a AWS través de una interfaz virtual AWS Direct Connect pública, el uso de Data Transfer Out (DTO) se calcula en beneficio del propietario del recurso según la tasa de transferencia de datos. AWS Direct Connect

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

AWS Direct Connect mantenimiento

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

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

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

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

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

Le recomendamos que siga las Recomendaciones de resiliencia de AWS Direct Connect para poder transferir el tráfico de forma ágil y proactiva a su conexión redundante de Direct Connect durante

el mantenimiento. También le recomendamos que pruebe de forma proactiva la resiliencia de sus conexiones redundantes de manera periódica para comprobar que la conmutación por error funciona según lo previsto. Con esta the section called “Prueba de conmutación por error” funcionalidad, puede comprobar que el tráfico se enruta a través de una de sus interfaces virtuales redundantes.

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

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

Para obtener más información sobre los eventos de mantenimiento, consulte Eventos de mantenimiento en el AWS Direct Connect FAQs.

Acceso a AWS regiones remotas

AWS Direct Connect ubicaciones en regiones públicas o AWS GovCloud (US) puede acceder a los servicios públicos en cualquier otra región pública (excepto China (Beijing y Ningxia)). Además, AWS Direct Connect las conexiones se encuentran en regiones públicas o se AWS GovCloud (US) pueden configurar para acceder a una VPC de tus cuentas en cualquier otra región pública (excepto China (Pekín y Ningxia). Por lo tanto, puede utilizar una única conexión de AWS Direct Connect para crear servicios en varias regiones. Todo el tráfico de red permanece en la red troncal AWS global, independientemente de si accedes a AWS los servicios 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 BGP las comunidades compatibles para una AWS Direct Connect conexión, consultePolíticas y BGP comunidades de enrutamiento.

Acceso a los servicios públicos en una región remota

Para acceder a los recursos públicos en una región remota, debe configurar una interfaz virtual pública y establecer una sesión del Border Gateway Protocol (BGP). Para obtener más información, consulte Interfaces virtuales e interfaces virtuales alojadas.

Tras crear una interfaz virtual pública y establecer una BGP sesión en ella, el router aprende las rutas de las demás AWS regiones públicas. Para obtener más información sobre los prefijos anunciados actualmente por AWS, consulte Intervalos de direcciones AWS IP en. Referencia general de Amazon Web Services

Acceso a una VPCs región remota

Puede crear una gateway de Direct Connect en cualquier región pública. Úsala para conectar tu AWS Direct Connect conexión a través de una interfaz virtual privada a VPCs una cuenta ubicada en diferentes regiones o a una pasarela de transporte público. Para obtener más información, consulte AWS Direct Connect pasarelas.

Como alternativa, puedes crear una interfaz virtual pública para tu AWS Direct Connect conexión y, a continuación, establecer una VPN conexión con la tuya VPC en la región remota. Para obtener más información sobre la configuración de la VPN conectividad a unVPC, consulte Escenarios para el uso de Amazon Virtual Private Cloud en la Guía del VPC usuario de Amazon.

Opciones de conectividad de red a Amazon VPC

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

- Opciones de conectividad de Amazon Virtual Private Cloud

AWS Direct Connect políticas y BGP comunidades de enrutamiento

AWS Direct Connect aplica políticas de enrutamiento de entrada (desde su centro de datos local) y de salida (desde su AWS región) para una conexión pública. AWS Direct Connect También puedes usar etiquetas de comunidad del Border Gateway Protocol (BGP) en las rutas anunciadas por Amazon y aplicar etiquetas de BGP comunidad en las rutas que anuncies en Amazon.

Políticas de direccionamiento de interfaces virtuales públicas

Si las utilizas AWS Direct Connect para acceder a AWS servicios públicos, debes especificar los IPv4 prefijos o IPv6 prefijos públicos en los que quieres anunciarte. BGP

Se aplican las siguientes políticas de direccionamiento de entrada:

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

Se aplican las siguientes políticas de direccionamiento de salida:

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

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

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

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

BGPComunidades de interfaces virtuales públicas

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

ÁmbitoBGP: comunidades

Puedes aplicar etiquetas de BGP comunidad a los prefijos públicos que anuncies en Amazon para indicar hasta qué punto debes propagar tus prefijos en la red de Amazon, solo para la AWS región local, para todas las regiones de un continente o para todas las regiones públicas.

Región de AWS comunidades

En el caso de las políticas de enrutamiento entrante, puede utilizar las siguientes BGP comunidades como prefijos:

- `7224:9100`—Local 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 que están marcados con las mismas comunidades y que tienen PATH atributos AS_ idénticos son aptos para usar rutas múltiples.

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

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

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

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

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

`NO_EXPORT`BGPcomunidad

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

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

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

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

Si las utilizas AWS Direct Connect para acceder a tus AWS recursos privados, debes especificar los prefijos IPv4 o los IPv6 prefijos en los que quieres anunciarte. BGP Estos prefijos pueden ser públicos o privados.

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

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

Comunidades de interfaces virtuales privadas y de interfaces virtuales de tránsito BGP

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

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

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

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

> **Note**
>
> Esto no afecta a las ubicaciones locales ni ECMP desde ellas. Región de AWS

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

BGPComunidades de preferencias locales

Puede usar etiquetas de BGP comunidad de preferencias locales para lograr el equilibrio de carga y la preferencia de ruta para el tráfico entrante a su red. Para cada prefijo que anuncie durante una BGP sesión, puede aplicar una etiqueta de comunidad para indicar la prioridad de la ruta asociada para el tráfico de retorno.

Se admiten las siguientes etiquetas de BGP comunidad de preferencias locales:

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

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

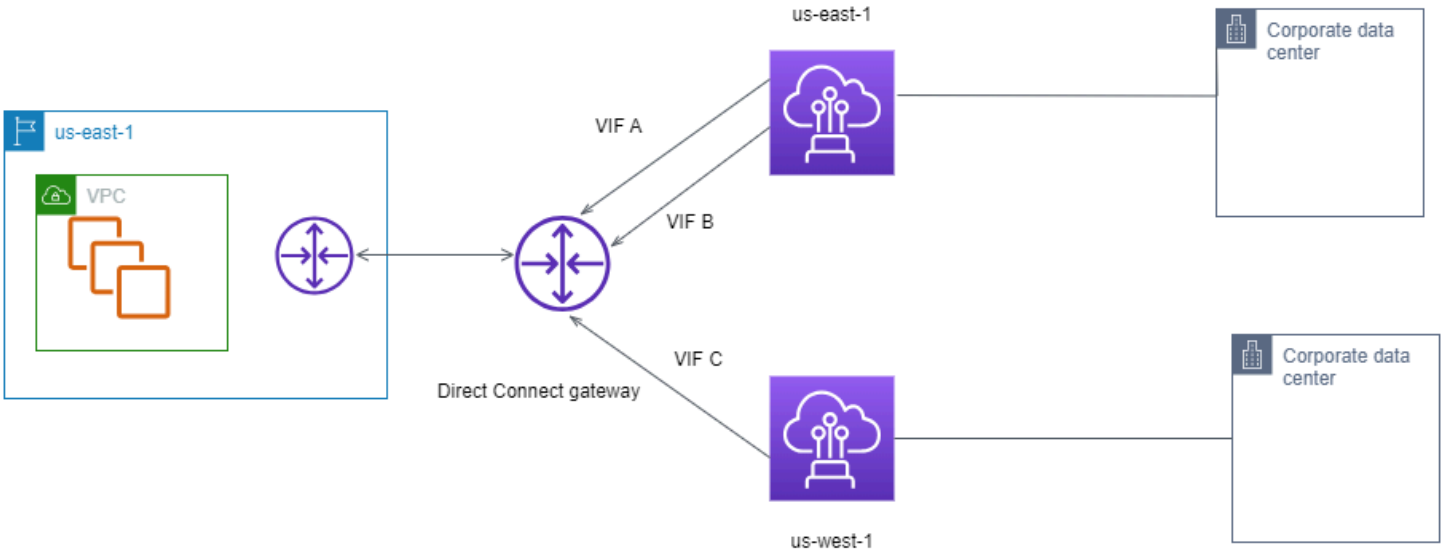
Las etiquetas de BGP comunidad de preferencias locales se evalúan antes que cualquier PATH atributo AS_ y se evalúan en orden de menor a mayor preferencia (donde se prefiere la preferencia más alta).

AWS Direct Connect Ejemplo de enrutamiento de interfaz virtual privada

Considere la configuración en la que la región de origen de la AWS Direct Connect ubicación 1 es la misma que la región de VPC origen. Hay una AWS Direct Connect ubicación redundante en una región diferente. Hay dos privadas VIFs (VIFA y VIF B) desde la AWS Direct Connect ubicación 1 (us-east-1) hasta la puerta de enlace Direct Connect. Hay una puerta privada VIF (VIFC) desde la AWS Direct Connect ubicación (us-west-1) hasta la puerta de enlace Direct Connect. Para que el tráfico de la AWS ruta pase por VIF B antes que por VIF A, establezca el PATH atributo AS_ de VIF B para que sea más corto que el atributo VIF A AS_. PATH

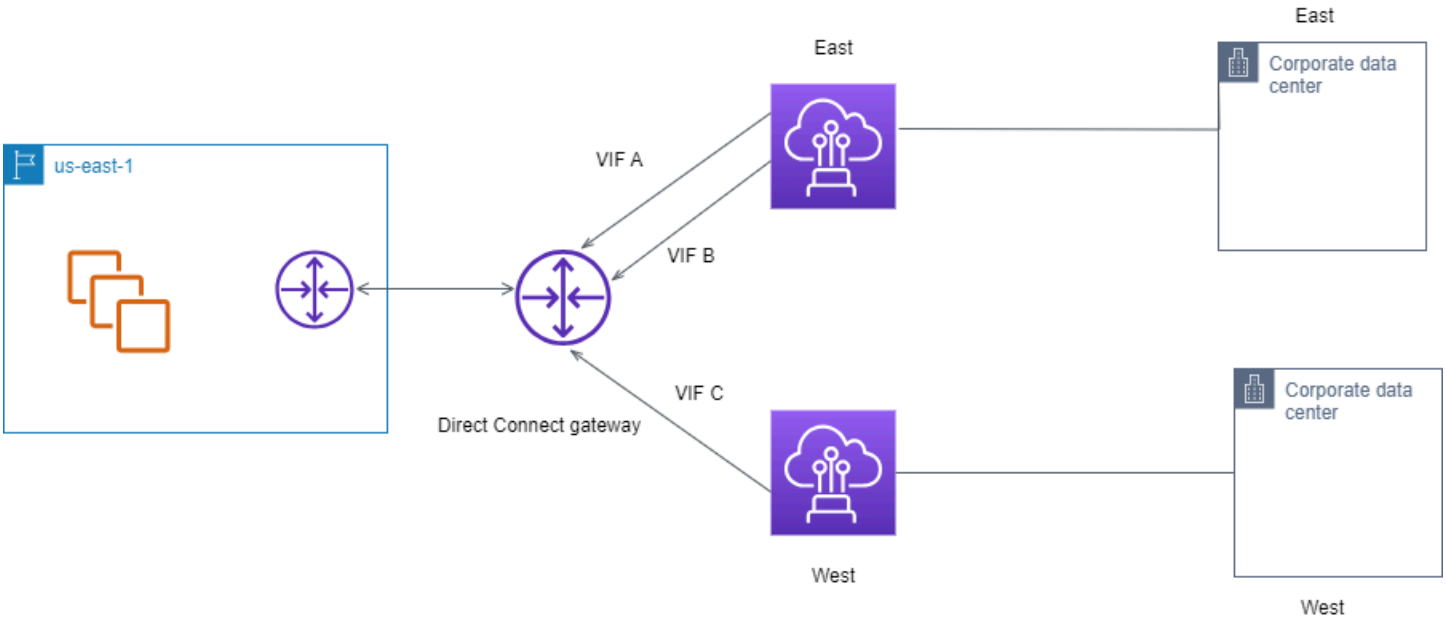
VIFsTienen las siguientes configuraciones:

- VIFA (en us-east-1) anuncia 172.16.0.0/16 y tiene un atributo AS_ de 65001, 65001, 65001 PATH
- VIFB (en us-east-1) anuncia 172.16.0.0/16 y tiene un atributo AS_ de 65001, 65001 PATH
- VIFC (en us-west-1) anuncia 172.16.0.0/16 y tiene un atributo AS_ de 65001 PATH



Si cambia la configuración de CIDR rango de VIF C, las rutas que entran en el CIDR rango VIF C usan VIF C porque tiene la longitud de prefijo más larga.

- VIFC (en us-west-1) anuncia 172.16.0.0/24 y tiene un atributo AS_ de 65001 PATH



AWS Direct Connect Kit de herramientas de resiliencia

AWS ofrece a los clientes la posibilidad de lograr conexiones de red altamente resilientes entre Amazon Virtual Private Cloud (AmazonVPC) 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, a ordenar el número de conexiones dedicadas para lograr su objetivo. SLA Usted selecciona un modelo de resiliencia y, a continuación, el kit de herramientas de AWS Direct Connect resiliencia lo guía a través del proceso específico de pedido de conexiones. Los modelos de resiliencia están diseñados para garantizar que dispone del número adecuado de conexiones dedicadas en varias ubicaciones.

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

- Proporciona directrices para determinar y después solicitar las conexiones dedicadas de AWS Direct Connect redundantes apropiadas.
- Garantiza que las conexiones dedicadas redundantes tengan la misma velocidad.
- Configura automáticamente los nombres de conexión dedicados.
- Aprueba automáticamente sus conexiones dedicadas cuando tiene una AWS cuenta existente y selecciona un socio conocido. AWS Direct Connect La carta de autorización (LOA) está disponible para su descarga inmediata.
- Crea automáticamente un ticket de soporte para la aprobación de la conexión exclusiva cuando eres un AWS cliente nuevo o seleccionas un socio desconocido (otro).
- Proporciona un resumen del pedido de las conexiones dedicadas SLA que puede obtener y el coste por hora de puerto de las conexiones dedicadas solicitadas.
- Crea grupos de agregación de enlaces (LAGs) y añade el número adecuado de conexiones dedicadas LAGs cuando eliges una velocidad distinta de 1 Gbps, 10 Gbps, 100 Gbps o 400 Gbps.
- Proporciona un LAG resumen con la conexión dedicada SLA que puede conseguir y el coste total por hora de puerto de cada conexión dedicada solicitada como parte de la misma. LAG
- Impide que se terminen las conexiones dedicadas en el mismo dispositivo de AWS Direct Connect .
- Proporciona una forma de probar la resiliencia de su configuración. Usted trabaja AWS para reducir la sesión de interconexión BGP a fin de comprobar que el tráfico se dirige a una de sus interfaces virtuales redundantes. Para obtener más información, consulte the section called “Prueba de conmutación por error”.

- Proporciona CloudWatch métricas de Amazon para conexiones e interfaces virtuales. Para obtener más información, consulte Supervise los recursos de Direct Connect.

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

- Máxima resiliencia: este modelo le proporciona una forma de solicitar conexiones dedicadas para lograr un 99,99%. SLA Requiere que cumpla con todos los requisitos para lograr lo especificado en SLA el acuerdo de nivel de AWS Direct Connect servicio.
- Alta resiliencia: este modelo le permite solicitar conexiones dedicadas para alcanzar un SLA 99,9%. Requiere que cumpla con todos los requisitos para lograr los requisitos SLA que se especifican en el acuerdo de nivel de AWS Direct Connect servicio.
- Desarrollo y pruebas: este modelo le ofrece una forma de conseguir resiliencia de desarrollo y pruebas para cargas de trabajo no críticas mediante el uso de conexiones independientes que terminan en dispositivos independientes en una ubicación.
- Classic. Este modelo está destinado a aquellos usuarios que tengan conexiones existentes y que deseen añadir otras. Este modelo no proporciona unSLA.

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

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

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

Requisitos previos

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

(1310 nm) para 10 gigabits, un transceptor 100 para Ethernet de 100 GBASE gigabit o un transceptor 400 LR4 para Ethernet de 400 Gbps. GBASE LR4

Puede configurar una conexión 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 AWS Direct Connect socio o un proveedor de red para conectar un router desde su centro de datos, oficina o entorno de colocación a una ubicación . AWS Direct Connect El proveedor de red no tiene que ser un AWS Direct Connect socio para conectarlo a una conexión dedicada. AWS Direct Connect Las conexione s dedicadas admiten estas velocidades de puerto a través de fibra monomodo: 1 Gbps: 1000 BASE -LX (1310 nm), 10 Gbps: 10 GBASE -LR (1310 nm), 100 GbpsGBASE: LR4 100 o 400 (para Ethernet de 400 Gbps). GBASE LR4
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 AWS Direct Connect socio del Programa de Socios para conectar un router desde su centro de datos, oficina o entorno de colocación a una ubicación. AWS Direct Connect

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

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

- La red debe utilizar fibra monomodo con un transceptor 1000 BASE -LX (1310 nm) para Ethernet de 1 gigabit, un transceptor 10 GBASE -LR (1310 nm) para 10 gigabits, uno 100 para Ethernet de 100 GBASE gigabits o un transceptor 400 para Ethernet de 400 Gbps. LR4 GBASE LR4
- La negociación automática de un puerto debe estar deshabilitada para una conexión con una velocidad de puerto superior a 1 Gbps. Sin embargo, según el punto final de AWS Direct Connect que dé servicio a su conexión, es posible que sea necesario activar o desactivar la negociación automática para las conexiones de 1 Gbps. Si la interfaz virtual permanece inactiva, consulte Solución de problemas de capa 2 (enlace de datos).
- VLANLa encapsulación 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 su red. La función asíncrona BFD se habilita automáticamente para cada interfaz virtual. AWS Direct Connect Se habilita de forma automática en las interfaces virtuales de Direct Connect, pero no funcionará hasta que la configure en el enrutador. Para obtener más información, consulte BFDHabilitar una conexión Direct Connect.

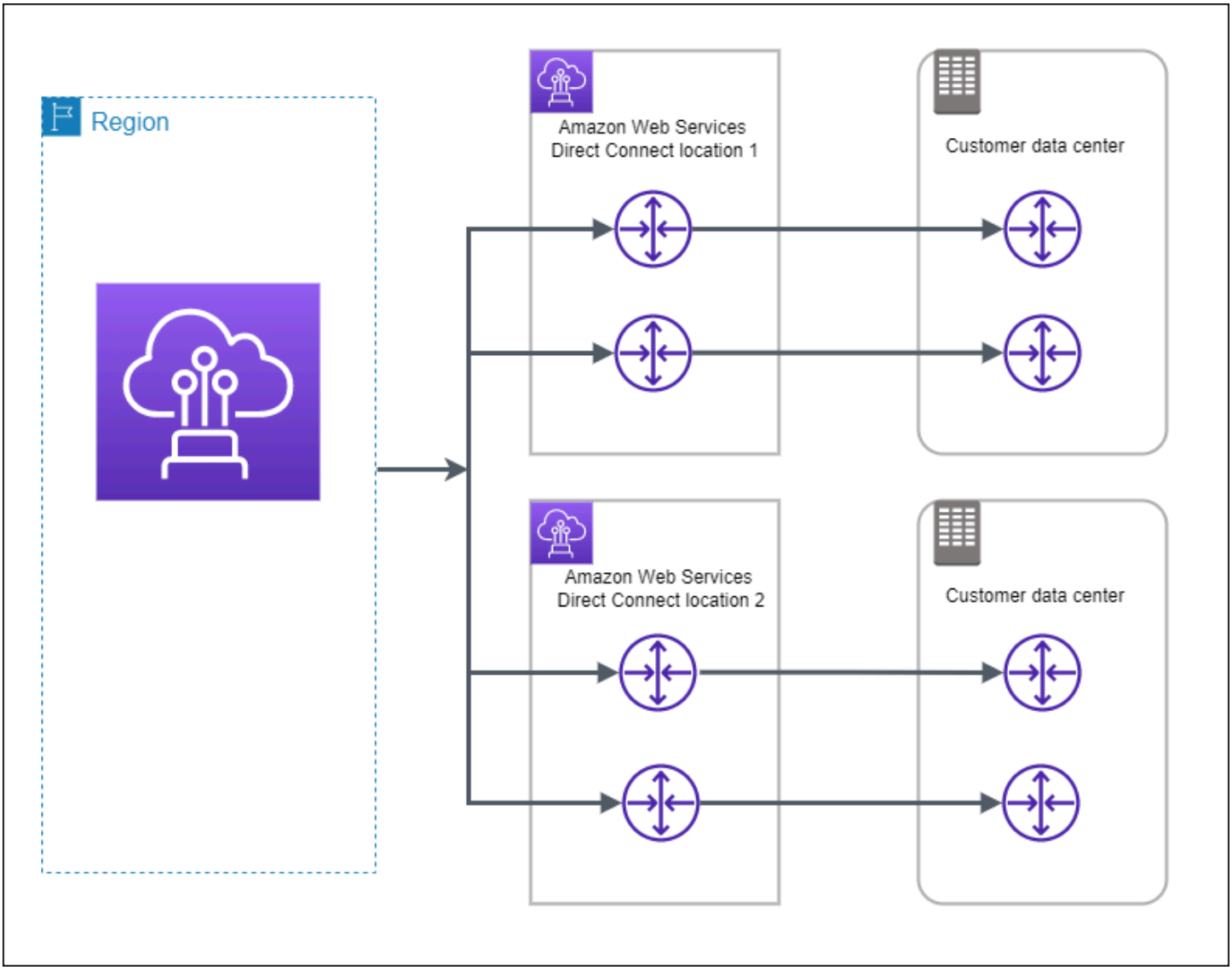
Asegúrese de que dispone de la siguiente información antes de comenzar la configuración:

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

  Solo necesita la velocidad para una conexión.

Resiliencia máxima

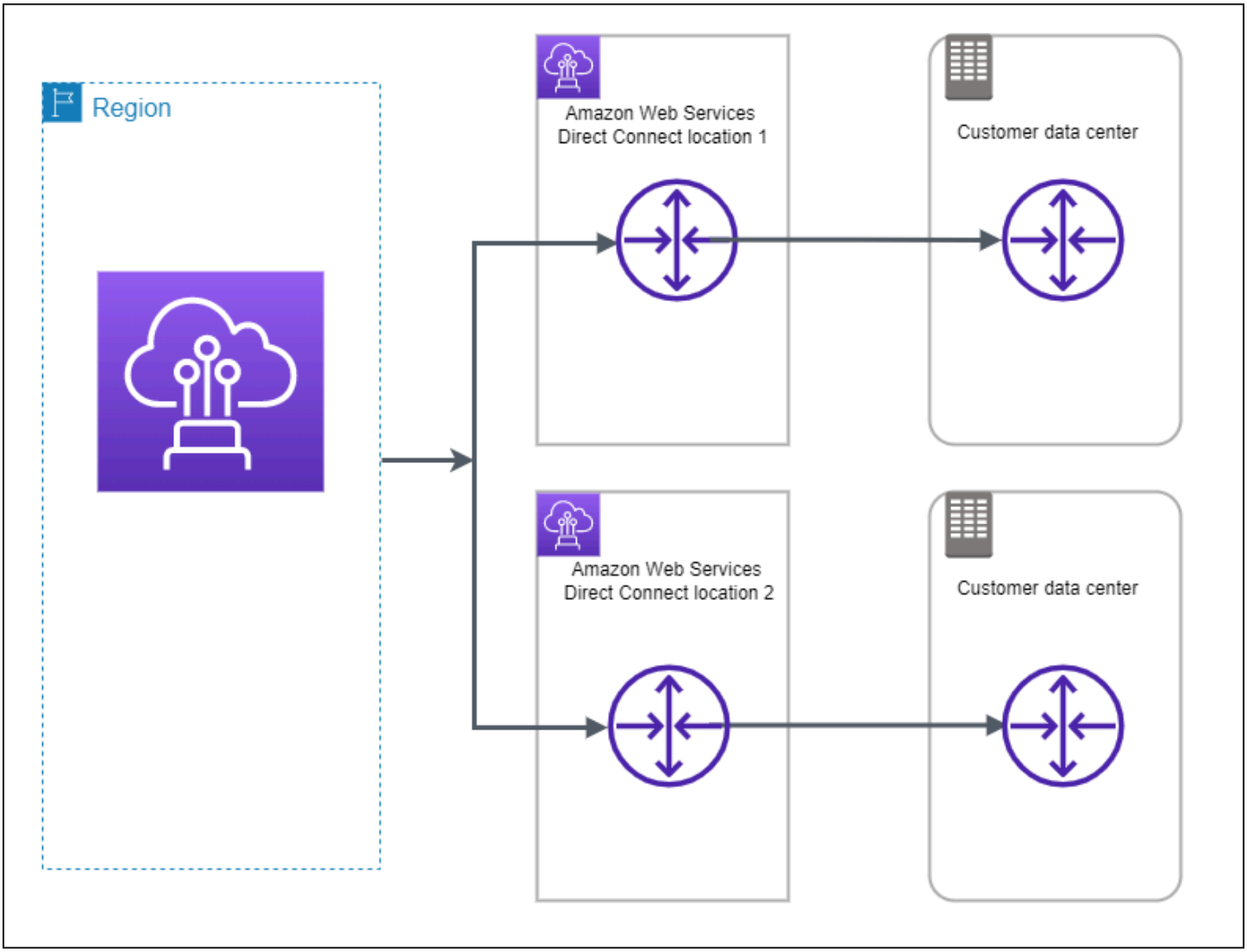
Puede conseguir la máxima resiliencia para cargas de trabajo críticas mediante el uso de conexiones independientes que terminan en dispositivos independientes en más de una ubicación (tal y como se muestra en la siguiente figura). Este modelo proporciona resistencia frente a errores de dispositivo, conectividad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



Para conocer el procedimiento de uso del kit de herramientas de AWS Direct Connect resiliencia para configurar un modelo de máxima resiliencia, consulte. Configure 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.

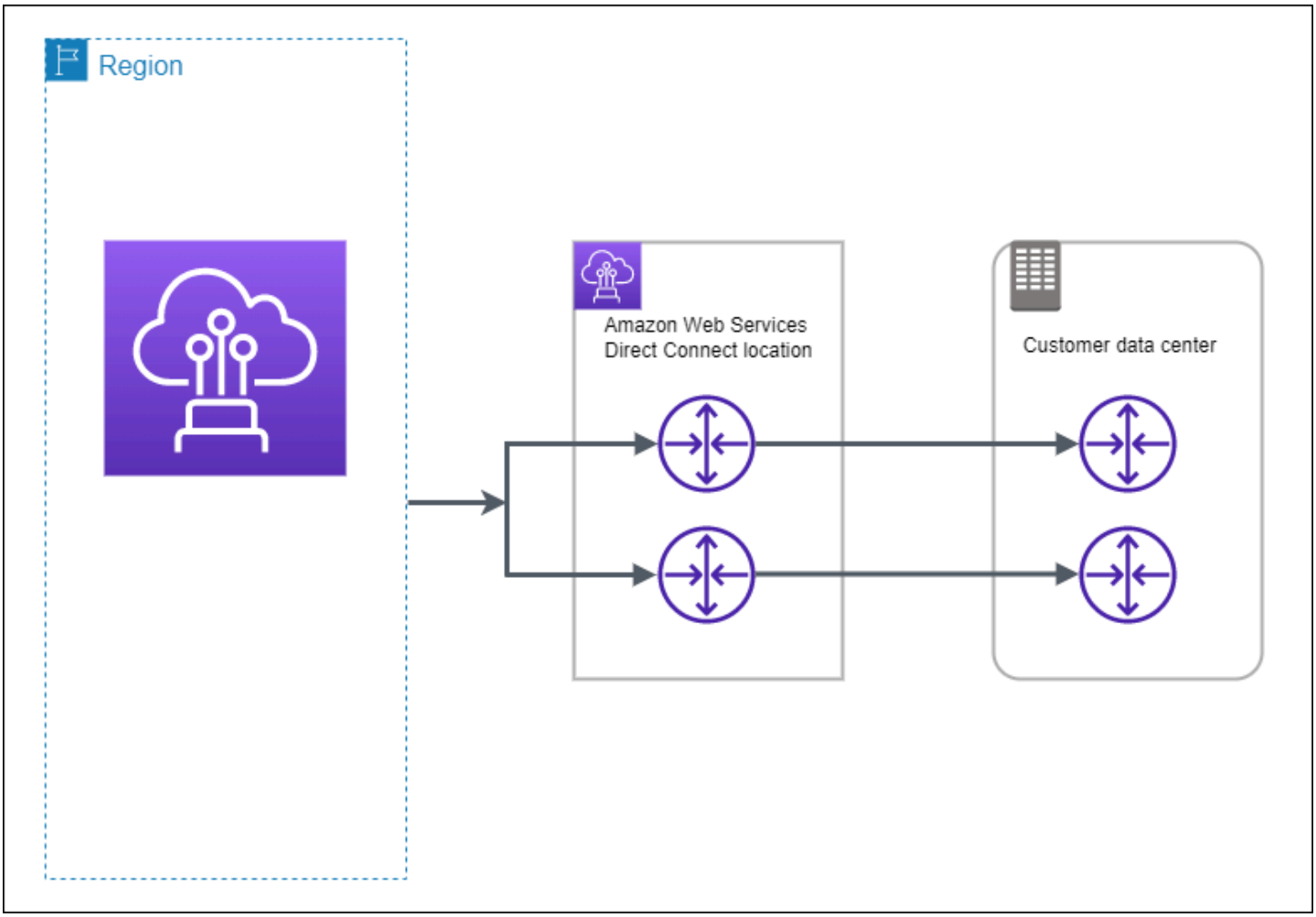


Para conocer el procedimiento de uso del kit de herramientas de AWS Direct Connect resiliencia para configurar un modelo de alta resiliencia, consulte. Configure una alta resiliencia

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 de uso del kit de herramientas de AWS Direct Connect resiliencia para configurar un modelo de máxima resiliencia, consulte. Configure la resiliencia de desarrollo y pruebe

Classic

Seleccione Classic si tiene conexiones existentes.

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

Requisitos previos

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

- La red debe utilizar fibra monomodo con un transceptor 1000 BASE -LX (1310 nm) para Ethernet de 1 gigabit, un transceptor 10 GBASE -LR (1310 nm) para 10 gigabits, uno 100 para Ethernet de 100 gigabits o un transceptor 400 LR4 para Ethernet de GBASE 400 Gbps. GBASE LR4
- La negociación automática de un puerto debe estar deshabilitada para una conexión con una velocidad de puerto superior a 1 Gbps. Sin embargo, según el punto final de AWS Direct Connect que dé servicio a su conexión, es posible que sea necesario activar o desactivar la negociación automática para las conexiones de 1 Gbps. Si la interfaz virtual permanece inactiva, consulte Solución de problemas de capa 2 (enlace de datos).
- VLANLa encapsulación 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 su red. La función asíncrona BFD se habilita automáticamente para cada interfaz virtual. AWS Direct Connect Se habilita de forma automática en las interfaces virtuales de Direct Connect, pero no funcionará hasta que la configure en el enrutador. Para obtener más información, consulte BFDHabilitar una conexión Direct Connect.

Para conocer el procedimiento de uso del kit de herramientas de AWS Direct Connect resiliencia para configurar una conexión clásica, consulte. Configure una conexión clásica

AWS Direct Connect FailoverTest

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

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

Utilice el kit de herramientas AWS Direct Connect de resiliencia para configurarlo y AWS Direct Connect obtener la máxima resiliencia

En este ejemplo, el kit de herramientas de AWS 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 AWS Direct Connect, necesitas una AWS cuenta si aún no la tienes.

Inscríbase en una Cuenta de AWS

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

Para suscribirte a una Cuenta de AWS

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

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .
2. Activa la autenticación multifactorial (MFA) para tu usuario root.

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

Creación de un usuario con acceso administrativo

1. Habilite 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 cómo usar el Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

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

Para obtener ayuda para iniciar sesión con un usuario de IAM Identity Center, 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 con 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. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Conexiones y, a continuación, Crear una conexión.
3. En Connection ordering type (Tipo de solicitud de conexión), elija Connection wizard (Asistente de conexión).
4. En Resiliency level (Nivel de resiliencia), elija Maximum Resiliency (Resiliencia máxima) y, a continuación, elija Next (Siguiente).
5. En el panel Configure connections (Configurar conexiones), en Connection settings (Configuración de conexión), proceda del modo siguiente:

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

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

   b. En First Location Service Provider, selecciona la AWS Direct Connect ubicación adecuada para la conexión dedicada.

c. Si procede, en First Sub location (Primera ubicación secundaria), elija el piso más cercano a usted o a su proveedor de red. Esta opción solo está disponible si la ubicación 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 AWS 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 Next (Siguiente).
7. Revise las conexiones y, a continuación, elija Continue (Continuar).

   Si LOAs está preparado, puede elegir Descargar y, a continuaciónLOA, hacer clic en Continuar.

   La revisión de la solicitud y el aprovisionamiento de un puerto para la conexión pueden tardar hasta 72 horas. AWS Durante este tiempo, es posible que reciba un correo electrónico con una solicitud de información adicional sobre su caso de uso o sobre la ubicación especificada. El correo electrónico se envía a la dirección de correo electrónico que utilizaste 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 conectarse a suVPC. O bien, puede crear una interfaz virtual pública para conectarse a AWS servicios públicos que no están en unVPC. Al crear una

interfaz virtual privada para unaVPC, necesitará una interfaz virtual privada para cada una de las interfaces a las VPC que se conecte. Por ejemplo, necesita tres interfaces virtuales privadas para conectarse a tresVPCs.

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

Recurso	Información necesaria
Conexión	El grupo de AWS Direct Connect conexiones 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 conectarte a una VPC de la misma AWS región, necesitas la puerta de enlace privada virtual para tuVPC. El ASN lado de Amazon de la BGP sesión se hereda de la puerta de enlace privada virtual. Al crear una puerta de enlace privada virtual, puede especificar su propia puerta privadaASN. De lo contrario, Amazon proporciona un valor predeterminadoASN. Para obtener más información, consulte Crear una puerta de enlace privada virtual en la Guía del VPC usuario de Amazon. Para conectarse a VPC través de una puerta de enlace Direct Connect, necesita la puerta de enlace Direct Connect. Para obtener más información, consulte Gateways de Direct Connect.
VLAN	Una etiqueta de red de área local virtual única (VLAN) que aún no esté en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de AWS Direct Connect . Si tiene una conexión alojada, su AWS Direct Connect socio le proporcionará este valor. No puede modificar el valor después de haber creado la interfaz virtual.
Direcciones IP de mismo nivel	Una interfaz virtual puede admitir una sesión de BGP emparejamiento para IPv4IPv6, o una de cada una de ellas (doble pila). No utilice Elastic IPs (EIPs) ni traiga sus propias direcciones IP (BYOIP) del Amazon Pool para crear una

Recurso	Información necesaria

	interfaz virtual pública. No puede crear varias BGP sesiones para la misma familia de direcciones IP en la misma interfaz virtual. Los rangos de direccion es IP se asignan a cada extremo de la interfaz virtual para la sesión de BGP emparejamiento.
	
	• IPv4:
	  • (Solo interfaz virtual pública) Debe especificar IPv4 direcciones públicas únicas de su propiedad. El valor puede ser uno de los siguientes:
	  • Propiedad del cliente IPv4 CIDR
	
	  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 oISP, junto con una LOA CFA autorización
	  • Un AWS CIDR /31 proporcionado. Póngase en contacto con AWS Support para solicitar una solicitud pública IPv4 CIDR (y proporcione un caso de uso en su solicitud)
	
	  Note
	  No podemos garantizar que podamos cumplir con todas las solicitudes AWS de IPv4 direcciones públicas 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

Recurso	Información necesaria
	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 /125. IPv6 CIDR No puede especificar sus propias direcciones homólogas. IPv6
Familia de direcciones	Si la sesión BGP de intercambio de pares terminará IPv4 oIPv6.
BGPinformación	• Un número de sistema autónomo del Border Gateway Protocol (BGPASN) público o privado para su parte de la BGP sesión. Si utiliza uno públicoAS N, debe ser su propietario. Si utilizas una privadaASN, puedes establecer un ASN valor personalizado. Para un archivo de 16 bitsASN, el valor debe estar en el rango de 64512 a 65534. En el caso de 32 bitsASN, el valor debe estar comprendido entre 1 y 2147483647. La función anteponer un sistema autónomo (AS) no funciona si se utiliza una interfaz virtual privada ASN para una pública. • AWS se habilita MD5 de forma predeterminada. Esta opción no se puede modificar. • Una clave MD5 BGP de autenticación. 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	IPv4Rutas públicas o IPv6 rutas sobre las que hacer publicidadBGP. Debe anunciar al menos un prefijo conBGP, hasta un máximo de 1000 prefijos.
	• IPv4: IPv4 CIDR Pueden superponerse con otro IPv4 CIDR anuncio público que se haya utilizado AWS Direct Connect cuando se dé alguna de las siguientes condiciones:
	  • CIDRsSon de diferentes AWS regiones. Asegúrese de aplicar etiquetas BGP comunitarias a los prefijos públicos.
	  • Utiliza AS_ PATH cuando tiene un público ASN en una configuración activa/pasiva.
	  Para obtener más información, consulte Políticas y comunidades de enrutamiento. BGP
	• IPv6: especifique una longitud de prefijo igual o inferior a /64.
	• Puedes añadir prefijos adicionales a un público existente VIF y anunciarl os poniéndote en contacto con el servicio de asistencia.AWS En su caso de soporte, proporcione una lista de CIDR prefijos adicionales que desee añadir al público VIF y anuncie.
	• Puede especificar cualquier longitud de prefijo en una interfaz virtual pública de Direct Connect. IPv4debería admitir cualquier valor comprendido entre /1 y /32 y IPv6 entre /1 y /64.

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

Si sus prefijos son públicos o ASNs pertenecen a uno de nuestros ISP operadores 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 en el que se compruebe que ASN puede utilizar el prefijo o prefijo de red.

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

Para aprovisionar una interfaz virtual pública a los que no son VPC servicios

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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. Para VLAN, introduzca el número de identificación de su red de área local virtual ()VLAN.

   d. Para ello BGPASN, introduzca el número de sistema autónomo (BGP) del protocolo de puerta de enlace fronteriza (ASN) de su puerta de enlace.

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

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

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

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

      [IPv6] Para configurar un IPv6 BGP par, 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 BGP clave, BGP MD5 introdúzcala.

      Si no introduce ningún valor, generamos una BGP clave.

c. Para anunciar prefijos en Amazon, en el caso de los prefijos que desee anunciar, introduzca las direcciones de IPv4 CIDR destino (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 un VPC

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Tipo de interfaz virtual, en Tipo, elija Privada.
5. En Configuración de la interfaz virtual privada, realice lo siguiente:

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

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

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

   d. En Propietario de la interfaz virtual, 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. Para VLAN, introduzca el número de identificación de su red de área local virtual (VLAN).

   g. BGPASNEn este caso, introduzca el número de sistema autónomo del protocolo Border Gateway del router homólogo local para la nueva interfaz virtual.

Los valores válidos son 1 a 2147483647.

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

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

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

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

      > **Important**
      >
      > Si permite la AWS asignación automática de IPv4 direcciones, se CIDR asignará un /29 desde IPv4 169.254.0.0/16 Link-Local de acuerdo con 3927 para la conectividad. RFC point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen o destino del tráfico. VPC En su lugar, debe usar RFC 1918 u otra dirección y especificar la dirección usted mismo.
      >
      > - Para obtener más información sobre RFC 1918, consulte Asignación de direcciones para Internet privadas.
      > - Para obtener más información acerca de RFC 3927, consulte Configuración dinámica de direcciones locales de IPv4 enlace.

      [IPv6] Para configurar un IPv6 BGP par, 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 Jumbo MTU (MTUtamaño 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 AmazonVPC, realice una prueba de conmutación por error de la interfaz virtual para comprobar que la configuración cumple con los requisitos de resiliencia. Para obtener más información, consulte the section called “Prueba de conmutación por error”.

Paso 5: Compruebe la conectividad de las interfaces virtuales

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

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

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

Para verificar la conexión de la interfaz virtual a Amazon VPC

1. Con un pingAMI, como Amazon LinuxAMI, lanza una EC2 instancia en la VPC que esté conectada a tu 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 incluya una regla que permita el ICMP tráfico 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.

Utilice el kit de herramientas AWS Direct Connect de resiliencia AWS Direct Connect para configurar una alta resiliencia

En este ejemplo, el kit de herramientas de AWS 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 AWS Direct Connect, necesitas una AWS cuenta si aún no la tienes.

Inscríbase en una Cuenta de AWS

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

Para suscribirte a una Cuenta de AWS

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

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .

2. Activa la autenticación multifactorial (MFA) para tu usuario root.

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

Creación de un usuario con acceso administrativo

1. Habilite 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 cómo usar el Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

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

  Para obtener ayuda para iniciar sesión con un usuario de IAM Identity Center, 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 con 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. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Conexiones y, a continuación, Crear una conexión.
3. En Connection ordering type (Tipo de solicitud de conexión), elija Connection wizard (Asistente de conexión).
4. En Resiliency level (Nivel de resiliencia), elija High Resiliency (Alta resiliencia), y, a continuación, elija Next (Siguiente).
5. En el panel Configure connections (Configurar conexiones), en Connection settings (Configuración de conexión), proceda del modo siguiente:

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

      Este ancho de banda se aplica a todas las conexiones creadas.
   b. En First Location Service Provider, seleccione la ubicación adecuada AWS 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 AWS 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 Next (Siguiente).

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

   Si LOAs está preparado, puede elegir Descargar y, a continuaciónLOA, hacer clic en Continuar.

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

Paso 3: Crear las interfaces virtuales

Puede crear una interfaz virtual privada para conectarse a suVPC. O bien, puede crear una interfaz virtual pública para conectarse a AWS servicios públicos que no están en unVPC. Al crear una interfaz virtual privada para unaVPC, necesitará una interfaz virtual privada para cada una de las interfaces a las VPC que se conecte. Por ejemplo, necesita tres interfaces virtuales privadas para conectarse a tresVPCs.

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

Recurso	Información necesaria
Conexión	El grupo de AWS Direct Connect conexiones 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 conectarte a una VPC de la misma AWS región, necesitas la puerta de enlace privada virtual para tuVPC. El ASN lado de Amazon de la BGP sesión se hereda de la puerta de enlace privada virtual. Al crear una puerta de enlace privada virtual, puede especificar su propia puerta privadaASN. De lo contrario, Amazon proporciona un valor predeterminadoASN. Para obtener más información, consulte Crear una puerta de enlace privada virtual en la Guía del VPC usuario de Amazon. Para conectarse a VPC través de una puerta de enlace Direct Connect, necesita la puerta de enlace Direct Connect. Para obtener más información, consulte Gateways de Direct Connect.
VLAN	Una etiqueta de red de área local virtual única (VLAN) que aún no esté en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de AWS Direct Connect . Si tiene una conexión alojada, su AWS Direct Connect socio le proporcionará este valor. No puede modificar el valor después de haber creado la interfaz virtual.
Direcciones IP de mismo nivel	Una interfaz virtual puede admitir una sesión de BGP emparejamiento para IPv4IPv6, o una de cada una de ellas (doble pila). No utilice Elastic IPs (EIPs) ni traiga sus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias BGP sesiones para la misma familia de direcciones IP en la misma interfaz virtual. Los rangos de direccion es IP se asignan a cada extremo de la interfaz virtual para la sesión de BGP emparejamiento.

Recurso	Información necesaria

	• IPv4:
	  • (Solo interfaz virtual pública) Debe especificar IPv4 direcciones públicas únicas de su propiedad. El valor puede ser uno de los siguientes:
	  • Propiedad del cliente IPv4 CIDR
	
	  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 oISP, junto con una LOA CFA autorización
	  • Un AWS CIDR /31 proporcionado. Póngase en contacto con AWS Support para solicitar una solicitud pública IPv4 CIDR (y proporcione un caso de uso en su solicitud)
	
	  Note
	  No podemos garantizar que podamos cumplir con todas las solicitudes AWS de IPv4 direcciones públicas 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` rango, por ejemplo, podría usarlo `192.168.0.1` para su IP homóloga y `192.168.0.2` para la IP AWS homóloga. `192.168.0.0/30`

Recurso	Información necesaria
	• IPv6: Amazon te asigna automáticamente un /125. IPv6 CIDR No puede especificar sus propias direcciones homólogas. IPv6
Familia de direcciones	Si la sesión BGP de intercambio de pares terminará IPv4 oIPv6.
BGPinformación	• Un número de sistema autónomo del Border Gateway Protocol (BGPASN) público o privado para su parte de la BGP sesión. Si utiliza uno públicoAS N, debe ser su propietario. Si utilizas una privadaASN, puedes establecer un ASN valor personalizado. Para un archivo de 16 bitsASN, el valor debe estar en el rango de 64512 a 65534. En el caso de 32 bitsASN, el valor debe estar comprendido entre 1 y 2147483647. La función anteponer un sistema autónomo (AS) no funciona si se utiliza una interfaz virtual privada ASN para una pública. • AWS se habilita MD5 de forma predeterminada. Esta opción no se puede modificar. • Una clave MD5 BGP de autenticación. 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	IPv4Rutas públicas o IPv6 rutas sobre las que anunciarseBGP. Debe anunciar al menos un prefijo conBGP, hasta un máximo de 1000 prefijos.
	• IPv4: IPv4 CIDR Pueden superponerse con otro IPv4 CIDR anuncio público que se haya utilizado AWS Direct Connect cuando se dé alguna de las siguientes condiciones:
	  • CIDRsSon de diferentes AWS regiones. Asegúrese de aplicar etiquetas BGP comunitarias a los prefijos públicos.
	  • Utiliza AS_ PATH cuando tiene un público ASN en una configuración activa/pasiva.
	  Para obtener más información, consulte Políticas y comunidades de enrutamiento. BGP
	• IPv6: especifique una longitud de prefijo igual o inferior a /64.
	• Puedes añadir prefijos adicionales a un público existente VIF y anunciarlos poniéndote en contacto con el servicio de asistencia.AWS En su caso de soporte, proporcione una lista de CIDR prefijos adicionales que desee añadir al público VIF y anuncie.
	• Puede especificar cualquier longitud de prefijo en una interfaz virtual pública de Direct Connect. IPv4debería admitir cualquier valor comprendido entre /1 y /32 y IPv6 entre /1 y /64.

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

Si sus prefijos son públicos o ASNs pertenecen a uno o varios ISP operadores de red, AWS le solicitará 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 en el que se compruebe que ASN puede utilizar el prefijo o prefijo de red.

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

Para aprovisionar una interfaz virtual pública a los que no son VPC servicios

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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. Para VLAN, introduzca el número de identificación de su red de área local virtual ()VLAN.

   d. Para ello BGPASN, introduzca el número de sistema autónomo (BGP) del protocolo de puerta de enlace fronteriza (ASN) de su puerta de enlace.

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

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

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

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

      [IPv6] Para configurar un IPv6 BGP par, 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 BGP clave, BGP MD5 introdúzcala.

      Si no introduce ningún valor, generamos una BGP clave.

c. Para anunciar prefijos en Amazon, en el caso de los prefijos que desee anunciar, introduzca las direcciones de IPv4 CIDR destino (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 un VPC

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Tipo de interfaz virtual, en Tipo, elija Privada.
5. En Configuración de la interfaz virtual privada, realice lo siguiente:

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

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

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

   d. En Propietario de la interfaz virtual, 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. Para VLAN, introduzca el número de identificación de su red de área local virtual (VLAN).

   g. BGPASNEn este caso, introduzca el número de sistema autónomo del protocolo Border Gateway del router homólogo local para la nueva interfaz virtual.

Los valores válidos son 1 a 2147483647.

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

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

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

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

      > **Important**
      >
      > Si permite la AWS asignación automática de IPv4 direcciones, se CIDR asignará un /29 desde IPv4 169.254.0.0/16 Link-Local de acuerdo con 3927 para la conectividad. RFC point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen o destino del tráfico. VPC En su lugar, debe usar RFC 1918 u otra dirección y especificar la dirección usted mismo.
      >
      > - Para obtener más información acerca de RFC 1918, consulte Asignación de direcciones para Internet privadas.
      > - Para obtener más información acerca de RFC 3927, consulte Configuración dinámica de direcciones locales de IPv4 enlace.

      [IPv6] Para configurar un IPv6 BGP par, 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 Jumbo MTU (MTUtamaño 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 AmazonVPC, realice una prueba de conmutación por error de la interfaz virtual para comprobar que la configuración cumple con los requisitos de resiliencia. Para obtener más información, consulte the section called “Prueba de conmutación por error”.

Paso 5: Compruebe la conectividad de las interfaces virtuales

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

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

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

Para verificar la conexión de la interfaz virtual a Amazon VPC

1. Con un pingAMI, como Amazon LinuxAMI, lanza una EC2 instancia en la VPC que esté conectada a tu 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 incluya una regla que permita el ICMP tráfico 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.

Utilice el kit de herramientas AWS Direct Connect de resiliencia AWS Direct Connect para configurar el desarrollo y probar la resiliencia

En este ejemplo, el kit de herramientas de AWS 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 AWS Direct Connect, necesitas una AWS cuenta si aún no la tienes.

Inscríbase en una Cuenta de AWS

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

Para suscribirte a una Cuenta de AWS

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

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .
2. Activa la autenticación multifactorial (MFA) para tu usuario root.

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

Creación de un usuario con acceso administrativo

1. Habilite 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 cómo usar el Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

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

Para obtener ayuda para iniciar sesión con un usuario de IAM Identity Center, 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 con 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. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Conexiones y, a continuación, Crear una conexión.
3. En Connection ordering type (Tipo de solicitud de conexión), elija Connection wizard (Asistente de conexión).
4. En Resiliency level (Nivel de resiliencia), elija Development and test (Desarrollo y pruebas) y, a continuación, elija Next (Siguiente).
5. En el panel Configure connections (Configurar conexiones), en Connection settings (Configuración de conexión), proceda del modo siguiente:

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

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

   b. En First Location Service Provider, seleccione la ubicación adecuada AWS 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 Next (Siguiente).
7. Revise las conexiones y, a continuación, elija Continue (Continuar).

   Si LOAs está preparado, puede elegir Descargar y, a continuaciónLOA, hacer clic en Continuar.

   La revisión de la solicitud y el aprovisionamiento de un puerto para la conexión pueden tardar hasta 72 horas. AWS Durante este tiempo, es posible que reciba un correo electrónico con una solicitud de información adicional sobre su caso de uso o sobre la ubicación especificada. El correo electrónico se envía a la dirección de correo electrónico que utilizaste 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 AWS Direct Connect la conexión, debe crear una interfaz virtual. Puede crear una interfaz virtual privada para conectarse a suVPC. O bien, puede crear una interfaz virtual pública para conectarse a AWS servicios públicos que no están en unVPC. Al crear una interfaz virtual privada para unaVPC, necesitará una interfaz virtual privada para cada una de las interfaces a las VPC que se conecte. Por ejemplo, necesita tres interfaces virtuales privadas para conectarse a tresVPCs.

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

Recurso	Información necesaria
Conexión	El grupo de AWS Direct Connect conexiones 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 conectarte a una VPC de la misma AWS región, necesitas la puerta de enlace privada virtual para tuVPC. El ASN lado de Amazon de la BGP sesión se hereda de la puerta de enlace privada virtual. Al crear una puerta de enlace privada virtual, puede especificar su propia puerta privadaASN. De lo contrario, Amazon proporciona un valor predeterminadoASN. Para obtener más información, consulte Crear una puerta de enlace privada virtual en la Guía del VPC usuario de Amazon. Para conectarse a VPC través de una puerta de enlace Direct Connect, necesita la puerta de enlace Direct Connect. Para obtener más información, consulte Gateways de Direct Connect.
VLAN	Una etiqueta de red de área local virtual única (VLAN) que aún no esté en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de AWS Direct Connect . Si tiene una conexión alojada, su AWS Direct Connect socio le proporcionará este valor. No puede modificar el valor después de haber creado la interfaz virtual.
Direcciones IP de mismo nivel	Una interfaz virtual puede admitir una sesión de BGP emparejamiento para IPv4IPv6, o una de cada una de ellas (doble pila). No utilice Elastic IPs (EIPs) ni traiga sus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias BGP sesiones para la misma familia de direcciones IP en la misma interfaz virtual. Los rangos de direccion es IP se asignan a cada extremo de la interfaz virtual para la sesión de BGP emparejamiento.

Recurso	Información necesaria

	• IPv4:
	  • (Solo interfaz virtual pública) Debe especificar IPv4 direcciones públicas únicas de su propiedad. El valor puede ser uno de los siguientes:
	  • Propiedad del cliente IPv4 CIDR
	
	  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 oISP, junto con una LOA CFA autorización
	  • Un AWS CIDR /31 proporcionado. Póngase en contacto con AWS Support para solicitar una solicitud pública IPv4 CIDR (y proporcione un caso de uso en su solicitud)
	
	  Note
	  No podemos garantizar que podamos cumplir con todas las solicitudes AWS de IPv4 direcciones públicas 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` rango, por ejemplo, podría usarlo `192.168.0.1` para su IP homóloga y `192.168.0.2` para la IP AWS homóloga. `192.168.0.0/30`

Recurso	Información necesaria
	• IPv6: Amazon te asigna automáticamente un /125. IPv6 CIDR No puede especificar sus propias direcciones homólogas. IPv6
Familia de direcciones	Si la sesión BGP de intercambio de pares terminará IPv4 oIPv6.
BGPinformación	• Un número de sistema autónomo del Border Gateway Protocol (BGPASN) público o privado para su parte de la BGP sesión. Si utiliza uno públicoAS N, debe ser su propietario. Si utilizas una privadaASN, puedes establecer un ASN valor personalizado. Para un archivo de 16 bitsASN, el valor debe estar en el rango de 64512 a 65534. En el caso de 32 bitsASN, el valor debe estar comprendido entre 1 y 2147483647. La función anteponer un sistema autónomo (AS) no funciona si se utiliza una interfaz virtual privada ASN para una pública. • AWS se habilita MD5 de forma predeterminada. Esta opción no se puede modificar. • Una clave MD5 BGP de autenticación. 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	IPv4Rutas públicas o IPv6 rutas sobre las que hacer publicidadBGP. Debe anunciar al menos un prefijo conBGP, hasta un máximo de 1000 prefijos.
	• IPv4: IPv4 CIDR Pueden superponerse con otro IPv4 CIDR anuncio público que se haya utilizado AWS Direct Connect cuando se dé alguna de las siguientes condiciones:
	  • CIDRsSon de diferentes AWS regiones. Asegúrese de aplicar etiquetas BGP comunitarias a los prefijos públicos.
	  • Utiliza AS_ PATH cuando tiene un público ASN en una configuración activa/pasiva.
	  Para obtener más información, consulte Políticas y comunidades de enrutamiento. BGP
	• IPv6: especifique una longitud de prefijo igual o inferior a /64.
	• Puedes añadir prefijos adicionales a un público existente VIF y anunciarl os poniéndote en contacto con el servicio de asistencia.AWS En su caso de soporte, proporcione una lista de CIDR prefijos adicionales que desee añadir al público VIF y anuncie.
	• Puede especificar cualquier longitud de prefijo en una interfaz virtual pública de Direct Connect. IPv4debería admitir cualquier valor comprendido entre /1 y /32 y IPv6 entre /1 y /64.

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

Si sus prefijos son públicos o ASNs pertenecen a uno de nuestros ISP operadores 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 en el que se compruebe que ASN puede utilizar el prefijo o prefijo de red.

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

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

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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. Para VLAN, introduzca el número de identificación de su red de área local virtual ()VLAN.

   d. Para ello BGPASN, introduzca el número de sistema autónomo (BGP) del protocolo de puerta de enlace fronteriza (ASN) de su puerta de enlace.

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

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

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

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

      [IPv6] Para configurar un IPv6 BGP par, 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 BGP clave, BGP MD5 introdúzcala.

      Si no introduce ningún valor, generamos una BGP clave.

c. Para anunciar prefijos en Amazon, en el caso de los prefijos que desee anunciar, introduzca las direcciones de IPv4 CIDR destino (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 un VPC

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Tipo de interfaz virtual, en Tipo, elija Privada.
5. En Configuración de la interfaz virtual privada, realice lo siguiente:

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

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

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

   d. En Propietario de la interfaz virtual, 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. Para VLAN, introduzca el número de identificación de su red de área local virtual (VLAN).

   g. Para BGPASNello, introduzca el número de sistema autónomo del protocolo Border Gateway del router homólogo local para la nueva interfaz virtual.

Los valores válidos son 1 a 2147483647.

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

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

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

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

      > **Important**
      >
      > Si permite la AWS asignación automática de IPv4 direcciones, se CIDR asignará un /29 desde IPv4 169.254.0.0/16 Link-Local de acuerdo con 3927 para la conectividad. RFC point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen o destino del tráfico. VPC En su lugar, debe usar RFC 1918 u otra dirección y especificar la dirección usted mismo.
      >
      > - Para obtener más información sobre RFC 1918, consulte Asignación de direcciones para Internet privadas.
      > - Para obtener más información acerca de RFC 3927, consulte Configuración dinámica de direcciones locales de IPv4 enlace.

      [IPv6] Para configurar un IPv6 BGP par, 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 Jumbo MTU (MTUtamaño 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 AmazonVPC, realice una prueba de conmutación por error de la interfaz virtual para comprobar que la configuración cumple con los requisitos de resiliencia. Para obtener más información, consulte the section called “Prueba de conmutación por error”.

Paso 5: Compruebe la interfaz virtual

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

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

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

Para verificar la conexión de la interfaz virtual a Amazon VPC

1. Con un pingAMI, como Amazon LinuxAMI, lanza una EC2 instancia en la VPC que esté conectada a tu 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 incluya una regla que permita el ICMP tráfico 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.

Configurar una conexión clásica

Configure una conexión clásica cuando tenga conexiones Direct Connect existentes.

Paso 1: Inscríbase en AWS

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

Inscríbase en una Cuenta de AWS

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

Para suscribirte a una Cuenta de AWS

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

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In .

2. Activa la autenticación multifactorial (MFA) para tu usuario root.

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

Creación de un usuario con acceso administrativo

1. Habilite 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 cómo usar el Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Iniciar sesión como usuario con acceso de administrador

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

  Para obtener ayuda para iniciar sesión con un usuario de IAM Identity Center, 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 con privilegios mínimos.

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

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

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

Paso 2: Solicita una conexión AWS Direct Connect dedicada

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

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

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

Para crear una AWS Direct Connect conexión nueva

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Conexiones y, a continuación, Crear una conexión.
3. Elija Classic.
4. En el panel Create Connection (Crear conexión), en Connection settings (Configuración de conexión) haga lo siguiente:
   a. En Name (Nombre), escriba un nombre para la conexión.
   b. En Location (Ubicación), seleccione la ubicación de AWS Direct Connect apropiada.
   c. Si procede, en Sub Location (Sububicación), elija el piso más cercano a usted o a su proveedor de red. Esta opción solo está disponible si la ubicación 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 AWS Direct Connect socio cuando utilice esta conexión para conectarse a su centro de datos.

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

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

h. (Opcional) Añada o elimine una etiqueta.

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

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

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

5. Elija Create Connection (Crear conexión).

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

Para obtener más información, consulte AWS Direct Connect conexiones dedicadas y alojadas.

Aceptación de la conexión alojada

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

Para aceptar una interfaz virtual alojada

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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: Descarga el - LOA CFA

Después de solicitar una conexión, ponemos a su disposición una carta de autorización y la asignación de la instalación de conexión (LOA-CFA) para que la descargue, o le enviaremos un correo electrónico con una solicitud de más información. El LOA - CFA es la autorización para conectarse a AWS, y el proveedor de alojamiento o su proveedor de red lo requieren para establecer la conexión entre redes (conexión cruzada).

Para descargar el - LOA CFA

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Connections (Conexiones).
3. Seleccione la conexión y elija View Details (Ver detalles).
4. Selecciona Descargar LOA -. CFA

   El LOA - CFA se descarga en su ordenador como un PDF archivo.

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

5. Tras descargar el LOA -CFA, realice una de las siguientes acciones:

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

AWS Direct Connect las ubicaciones que aparecen como sitios múltiples (por ejemplo, Equinix DC1 - DC6 y DC1 0-DC11) se configuran como campus. Si su equipo o el de su proveedor de red está ubicado en cualquiera de estos sitios, puede solicitar una conexión cruzada con el puerto asignado aunque este se encuentre en otro edificio del campus.

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

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

Paso 4: Crear una interfaz virtual

Para empezar a utilizar AWS Direct Connect la conexión, debe crear una interfaz virtual. Puede crear una interfaz virtual privada para conectarse a suVPC. O bien, puede crear una interfaz virtual pública para conectarse a AWS servicios públicos que no están en unVPC. Al crear una interfaz virtual privada para unaVPC, necesitará una interfaz virtual privada para cada una de ellas VPC a la que conectarse. Por ejemplo, necesita tres interfaces virtuales privadas para conectarse a tresVPCs.

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

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

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

Recurso	Información necesaria

Direcciones IP de mismo nivel	Una interfaz virtual puede admitir una sesión de BGP emparejamiento para IPv4IPv6, o una de cada una de ellas (doble pila). No utilice Elastic IPs (EIPs) ni traiga sus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias BGP sesiones para la misma familia de direcciones IP en la misma interfaz virtual. Los rangos de direccion es IP se asignan a cada extremo de la interfaz virtual para la sesión de BGP emparejamiento.
	
	• IPv4:
	  • (Solo interfaz virtual pública) Debe especificar IPv4 direcciones públicas únicas de su propiedad. El valor puede ser uno de los siguientes:
	  • Propiedad del cliente IPv4 CIDR
	
	  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 oISP, junto con una LOA CFA autorización
	  • Un AWS CIDR /31 proporcionado. Póngase en contacto con AWS Support para solicitar una solicitud pública IPv4 CIDR (y proporcione un caso de uso en su solicitud)
	
	  Note
	  No podemos garantizar que podamos cumplir con todas las solicitudes AWS de IPv4 direcciones públicas 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 /125. IPv6 CIDR No puede especificar sus propias direcciones homólogas. IPv6
Familia de direcciones	Si la sesión BGP de intercambio de pares terminará IPv4 oIPv6.
BGPinformación	• Un número de sistema autónomo del Border Gateway Protocol (BGPASN) público o privado para su parte de la BGP sesión. Si utiliza uno públicoAS N, debe ser su propietario. Si utilizas una privadaASN, puedes establecer un ASN valor personalizado. Para un archivo de 16 bitsASN, el valor debe estar en el rango de 64512 a 65534. En el caso de 32 bitsASN, el valor debe estar comprendido entre 1 y 2147483647. La función anteponer un sistema autónomo (AS) no funciona si se utiliza una interfaz virtual privada ASN para una pública. • AWS se habilita MD5 de forma predeterminada. Esta opción no se puede modificar. • Una clave MD5 BGP de autenticación. 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	IPv4Rutas públicas o IPv6 rutas sobre las que hacer publicidadBGP. Debe anunciar al menos un prefijo conBGP, hasta un máximo de 1000 prefijos.
	• IPv4: IPv4 CIDR Pueden superponerse con otro IPv4 CIDR anuncio público que se haya utilizado AWS Direct Connect cuando se dé alguna de las siguientes condiciones:
	  • CIDRsSon de diferentes AWS regiones. Asegúrese de aplicar etiquetas BGP comunitarias a los prefijos públicos.
	  • Utiliza AS_ PATH cuando tiene un público ASN en una configuración activa/pasiva.
	  Para obtener más información, consulte Políticas y comunidades de enrutamiento. BGP
	• IPv6: especifique una longitud de prefijo igual o inferior a /64.
	• Puedes añadir prefijos adicionales a un público existente VIF y anunciarl os poniéndote en contacto con el servicio de asistencia.AWS En su caso de soporte, proporcione una lista de CIDR prefijos adicionales que desee añadir al público VIF y anuncie.
	• Puede especificar cualquier longitud de prefijo en una interfaz virtual pública de Direct Connect. IPv4debería admitir cualquier valor comprendido entre /1 y /32 y IPv6 entre /1 y /64.

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

Le solicitamos información adicional si sus prefijos públicos ASNs pertenecen a uno o varios operadores de redISP. 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 ASN puede utilizar el prefijo o prefijo de red.

En el caso de las interfaces virtuales privadas y públicas, la unidad de transmisión máxima (MTU) de una conexión de red es el tamaño, en bytes, del paquete más grande permitido que se puede

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

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

Para aprovisionar una interfaz virtual pública a los que no son VPC servicios

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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. Para VLAN, introduzca el número de identificación de su red de área local virtual ()VLAN.

   d. Para BGPASNello, introduzca el número de sistema autónomo del protocolo The Border Gateway del router homólogo local para la nueva interfaz virtual.

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

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

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

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

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

[IPv6] Para configurar un IPv6 BGP par, 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 BGP clave, BGP MD5 introdúzcala.

Si no introduce ningún valor, generamos una BGP clave.

c. Para anunciar prefijos en Amazon, en el caso de los prefijos que desee anunciar, introduzca las direcciones de IPv4 CIDR destino (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 un VPC

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Tipo de interfaz virtual, en Tipo, elija Privada.
5. En Configuración de la interfaz virtual privada, realice lo siguiente:

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

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

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

d. En Propietario de la interfaz virtual, 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. Para VLAN, introduzca el número de identificación de su red de área local virtual (VLAN).

g. Para BGPASNello, introduzca el número de sistema autónomo del protocolo Border Gateway del router homólogo local para la nueva interfaz virtual.

   Los valores válidos son 1 a 2147483647.

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

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

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

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

      > **Important**
      >
      > Si permite la AWS asignación automática de IPv4 direcciones, se CIDR asignará un /29 desde IPv4 169.254.0.0/16 Link-Local de acuerdo con 3927 para la conectividad. RFC point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen o destino del tráfico. VPC En su lugar, debe usar RFC 1918 u otra dirección y especificar la dirección usted mismo.
      >
      > - Para obtener más información acerca de RFC 1918, consulte Asignación de direcciones para Internet privadas.
      > - Para obtener más información acerca de RFC 3927, consulte Configuración dinámica de direcciones locales de IPv4 enlace.

      [IPv6] Para configurar un IPv6 BGP par, 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 Jumbo MTU (MTUtamaño 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 usar su BGP dispositivo para anunciar la red que utiliza para la VIF conexión pública.

Paso 5: Descargar la configuración del enrutador

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

Para descargar una configuración del router

1. Abra la AWS Direct Connectconsola en 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 AWS Direct Connect.

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

Una vez que haya configurado el router, el estado de la interfaz virtual pasa a UP. Si la interfaz virtual permanece inactiva y no puede hacer ping a la dirección IP homóloga del AWS Direct Connect dispositivo, 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 BGP de interconexión está establecida pero no puede enrutar el tráfico, consulteSolución de problemas de direccionamiento.

Paso 6: Verificar la interfaz virtual

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

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

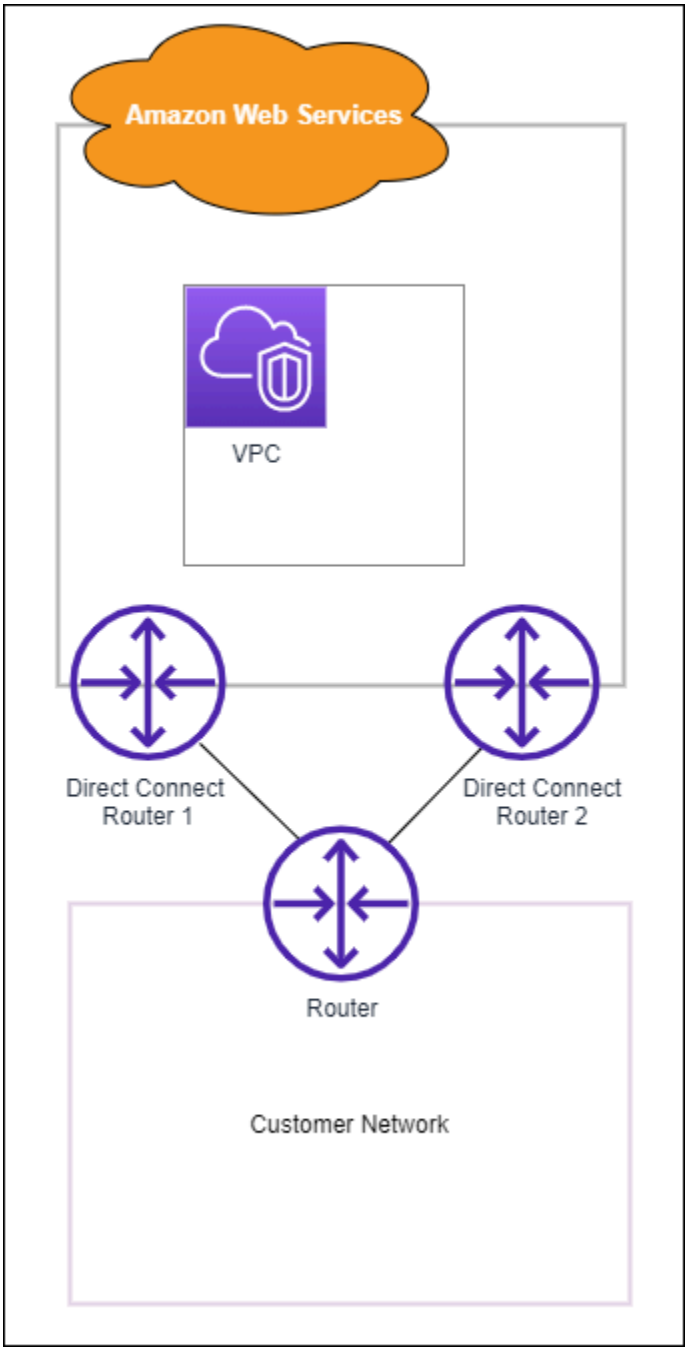
- Ejecute `traceroute` y verifique que el AWS Direct Connect identificador esté en el rastreo de la red.

Para verificar la conexión de la interfaz virtual a Amazon VPC

1. Con un pingAMI, como Amazon LinuxAMI, lanza una EC2 instancia en la VPC que esté conectada a tu 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 incluya una regla que permita el ICMP tráfico 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 (multiruta)BGP. Esta es la configuración predeterminada, en la que ambas conexiones están activas. AWS Direct Connect admite múltiples rutas a múltiples interfaces virtuales dentro de la misma ubicación y la carga del tráfico se comparte entre las interfaces en función del flujo. Si una conexión no se encuentra disponible, todo el tráfico se redirige a través de la otra conexión.

- Activa/Pasiva (conmutación por error). Una conexión gestiona el tráfico mientas que la otra está en modo de espera. Si la conexión activa no se encuentra disponible, todo el tráfico se redirige a través de la conexión pasiva. Deberá colocar la ruta de AS delante de la ruta de uno de los enlaces para convertirlo en el enlace pasivo.

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

Si utiliza una VPN conexión por redundancia, asegúrese de implementar un mecanismo de comprobación de estado y conmutación por error. Si utiliza una de las siguientes configuraciones, tendrá que comprobar el direccionamiento de la tabla de ruteo para direccionar a la nueva interfaz de red.

- Puede utilizar sus propias instancias para el direccionamiento; por ejemplo, la instancia es el firewall.
- Usas tu propia instancia para finalizar una conexión. VPN

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

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

AWS Direct Connect Prueba de conmutación por error

Los modelos de AWS Direct Connect resiliencia del Resiliency Toolkit están diseñados para garantizar que tenga la cantidad adecuada de conexiones de interfaz virtual en varias ubicaciones. Después de completar el asistente, utilice la prueba de conmutación por error del AWS Direct Connect Resiliency Toolkit para cerrar la sesión de BGP emparejamiento y comprobar que el tráfico se dirige a una de sus interfaces virtuales redundantes y cumple con sus 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 iniciar la prueba, debe seleccionar una interfaz virtual, una sesión de BGP emparejamiento y el tiempo durante el que se va a ejecutar la prueba. AWS coloca la sesión de BGP emparejamiento de la interfaz virtual seleccionada en estado inactivo. 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, se produce un error en la sesión de BGP emparejamiento y el tráfico no se enruta. Cuando se complete la prueba, o cuando la detenga manualmente, se AWS restaura la sesión. BGP Una vez finalizada la prueba, puede utilizar el kit de herramientas AWS Direct Connect de resiliencia para ajustar la configuración.

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

Historial de pruebas

AWS borra el historial de pruebas transcurridos 365 días. El historial de pruebas incluye el estado de las pruebas que se realizaron en todos los BGP compañeros. El historial incluye las sesiones de BGP intercambio de pares que se probaron, las horas de inicio y finalización y el 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 “Vea el historial de pruebas de conmutación por error de una 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 de AWS CloudTrail que se ha realizado una prueba en una interfaz virtual.

Temas

- Ver el historial de pruebas de conmutación por error de la interfaz virtual de AWS Direct Connect Resiliency Toolkit
- Detenga una prueba de AWS Direct Connect conmutación por error de la interfaz virtual de Resiliency Toolkit

Inicie una prueba de conmutación por error de la interfaz virtual AWS Direct Connect del Resiliency Toolkit

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

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

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/v2/home.
2. Elija Interfaces virtuales.
3. Seleccione las interfaces virtuales y, a continuación, elija Actions, Bring Down. 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. Para que los pares se reduzcan para probarlos, elija qué sesiones de emparejamiento desea probar, por ejemplo. IPv4
   b. En Tiempo máximo de la prueba, especifique el número de minutos que durará la prueba.

      El valor máximo es 4320 minutos (72 horas).

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

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

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

Utilice StartBgpFailoverTest.

Ver el historial de pruebas de conmutación por error de la interfaz virtual de AWS Direct Connect Resiliency Toolkit

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

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

1. Abra la AWS Direct Connectconsola en la versión 2/homehttps://console.aws.amazon.com/directconnect/.
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 ver el historial de pruebas de conmutación por error de la interfaz virtual mediante el AWS CLI

Utilice ListVirtualInterfaceTestHistory.

Detenga una prueba de AWS Direct Connect conmutación por error de la interfaz virtual de Resiliency Toolkit

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

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

1. Abra la AWS Direct Connectconsola en la versión 2/homehttps://console.aws.amazon.com/directconnect/.
2. Elija Interfaces virtuales.

3. Seleccione la interfaz virtual y, a continuación, elija Acciones, Cancelar prueba.
4. Elija Confirmar.

AWS restaura la sesión de BGP emparejamiento. El historial de pruebas muestra "cancelado" para la prueba.

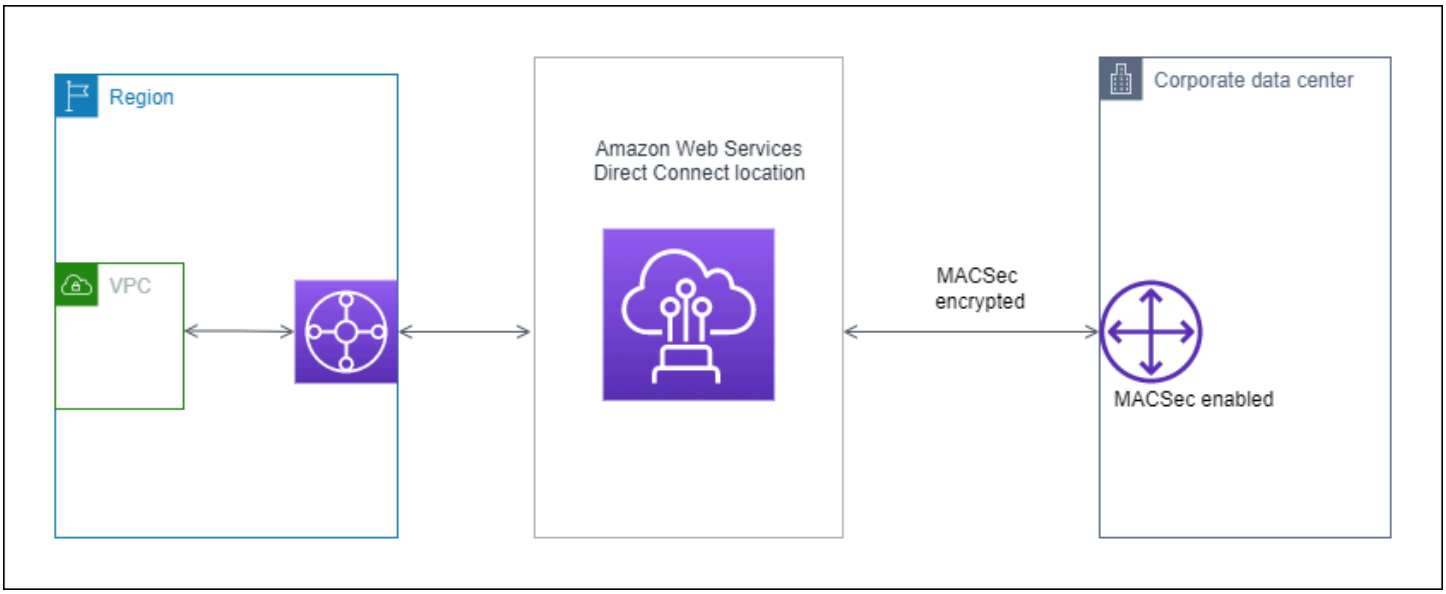
Para detener la prueba de conmutación por error de la interfaz virtual mediante el AWS CLI

Utilice StopBgpFailoverTest.

MACSeguridad

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

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



MACsecconceptos

Los siguientes son los conceptos clave paraMACsec:

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

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

MACsecrotación de teclas

Al girar las teclas, los llaveros admiten la rotación de las teclas. MACsec Direct Connect MACsec admite MACsec llaveros con capacidad para almacenar hasta tres CKN CAK pares. El `associate-mac-sec-key` comando se utiliza para asociar el CAK parCKN/a la conexión MACsec habilitada existente. A continuación, configuras el mismo CAK parCKN/en el dispositivo de tu parte de la AWS Direct Connect conexión. El dispositivo Direct Connect intentará usar la última clave almacenada para la conexión. Si esa clave no coincide con la clave del dispositivo, Direct Connect seguirá utilizando la tecla de trabajo anterior.

Para obtener información sobre el uso`associate-mac-sec-key`, consulte associate-mac-sec-key.

Conexiones compatibles

MACsecestá disponible en conexiones dedicadas. Para obtener información sobre cómo solicitar conexiones compatiblesMACsec, consulte AWS Direct Connect.

MACsecen conexiones dedicadas

Lo siguiente le ayudará a familiarizarse con MACsec las conexiones AWS Direct Connect dedicadas. No hay cargos adicionales por su usoMACsec.

Los pasos para configurar MACsec una conexión dedicada se encuentran enComience con MACsec una conexión dedicada. Antes de realizar MACsec la configuración en una conexión dedicada, tenga en cuenta lo siguiente:

- MACseces compatible con conexiones Direct Connect dedicadas de 10 Gbps, 100 Gbps y 400 Gbps en puntos de presencia seleccionados. Para estas conexiones, se admiten los siguientes MACsec conjuntos de cifrado:
  - Para conexiones de 10 Gbps, AES -256 y GCM GCM - - -256. AES XPN
  - Para conexiones de 100 Gbps y 400 Gbps, - - -256. GCM AES XPN

- Solo se admiten claves de 256 bitsMACsec.
- Se requiere la numeración de paquetes extendida (XPN) para las conexiones de 100 Gbps y 400 Gbps. Para conexiones de 10 Gbps, Direct Connect admite tanto GCM - AES -256 como - -256. GCM AES XPN Las conexiones de alta velocidad, como las dedicadas de 100 Gbps y 400 Gbps, pueden agotar rápidamente el espacio original MACsec de numeración de paquetes de 32 bits, lo que requeriría rotar las claves de cifrado cada pocos minutos para establecer una nueva asociación de conectividad. Para evitar esta situación, la modificación de la norma IEEE 802.1 de AEbw 2013 introdujo una numeración de paquetes ampliada, aumentando el espacio de numeración a 64 bits y reduciendo el requisito de puntualidad para la rotación de claves.
- El identificador de canal seguro (SCI) es obligatorio y debe estar activado. Esta configuración no se puede ajustar.
- IEEELa etiqueta 802.1Q (dot1Q/VLAN) offset/dot1 no q-in-clear se admite para mover una etiqueta fuera de una carga útil cifrada. VLAN

Para obtener información adicional sobre Direct Connect yMACsec, consulte la MACsec sección de AWS Direct Connect FAQs.

MACsecrequisitos previos para las conexiones dedicadas

Realice las siguientes tareas antes de configurar MACsec una conexión dedicada.

- Cree un CAK parCKN/para la clave MACsec secreta.

  Puede crear el par con una herramienta estándar abierta. El par debe cumplir los requisitos especificados de the section called “Configure su router local”.
- Asegúrese de tener un dispositivo en el extremo de la conexión que sea compatibleMACsec.
- El identificador de canal seguro (SCI) debe estar activado.
- Solo se admiten MACsec claves de 256 bits, lo que proporciona la protección de datos avanzada más reciente.

Roles vinculados a servicios

AWS Direct Connect utiliza AWS Identity and Access Management (IAM) funciones vinculadas al servicio. Un rol vinculado a un servicio es un tipo único de IAM rol al que se vincula directamente. AWS Direct Connect Los roles vinculados al servicio están predefinidos AWS Direct Connect e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en tu nombre.

Un rol vinculado a un servicio facilita la configuración AWS Direct Connect , ya que no es necesario añadir manualmente los permisos necesarios. AWS Direct Connect define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Direct Connect puede asumir sus funciones. Los permisos definidos incluyen la política de confianza y la política de permisos, y esa política de permisos no se puede adjuntar a ninguna otra IAM entidad. Para obtener más información, consulte the section called “Roles vinculados al servicio”.

MACsecconsideraciones CAK clave o CKN previamente compartidas

AWS Direct Connect utiliza claves AWS administradas CMKs para las claves previamente compartidas que asocias a las conexiones o. LAGs Secrets Manager guarda los CAK pares previamente compartidos CKN como un secreto que la clave raíz del Secrets Manager cifra. Para obtener más información, consulta la sección AWS Gestionado CMKs en la Guía AWS Key Management Service para desarrolladores.

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

- Si la conexión está en estado pendiente, la desasociamos 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 realizas ninguna acción en un plazo de 30 días, la desasociaremos CKN de tu conexión.

Cuando desasociamos lo último CKN de tu conexión y el modo de cifrado de la conexión está configurado en «debe cifrarse», configuramos el modo en «should_encrypt» para evitar la pérdida repentina de paquetes.

Comience a usarlo MACsec en una AWS Direct Connect conexión dedicada

La siguiente tarea le permitirá empezar a configurarlo MACsec para su uso en una conexión dedicada de Direct Connect.

Paso 1: Crear una conexión

Para empezar a utilizarlaMACsec, debes activar la función al crear una conexión dedicada.

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

Si utiliza varias conexiones para la redundancia, puede crear una LAG que sea compatibleMACsec. Para obtener más información, consulte MACsecconsideraciones Crear un LAG.

Paso 3: Asocie laCKN/CAKa la conexión o LAG

Después de crear la conexión o la LAG que la admiteMACsec, debe asociar unaCKN/CAKa la conexión. Para obtener más información, consulte una de las siguientes:

- Asocie una MACsecCKN/CAKa una conexión
- Asocie un MACsecCKN/CAKa un LAG

Paso 4: Configurar su enrutador en las instalaciones

Actualice su router local con la clave MACsec secreta. La clave MACsec secreta del router local y la de la AWS Direct Connect ubicación deben coincidir. Para obtener más información, consulte Descargar el archivo de configuración del enrutador.

Paso 5: (opcional) Elimine la asociación entreCKN/CAKy la conexión o LAG

Si lo desea, puede eliminar la asociación entreCKN/CAKy la conexión oLAG, si necesita eliminar la asociación, consulte una de las siguientes opciones:

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

AWS Direct Connect conexiones dedicadas y alojadas

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

Existen dos tipos de conexiones:

- Conexión dedicada: una conexión Ethernet física asociada a un solo cliente. Los clientes pueden solicitar una conexión dedicada a través de la AWS Direct Connect consolaCLI, el o elAPI. Para obtener más información, consulte Conexiones dedicadas.
- 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

AWS Direct Connect Conexiones dedicadas

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

AWS Direct Connect location

Trabaje con un AWS Direct Connect socio del Programa de Socios para que lo ayude a establecer circuitos de red entre una AWS Direct Connect ubicación y su centro de datos, oficina o entorno de colocación. También pueden contribuir a proporcionar una sala técnica de coubicación en las mismas instalaciones que la ubicación. Para obtener más información, consulte Soporte para APNsocios. AWS 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. Puedes crear una conexión independiente o puedes crear una conexión para asociarla a una LAG de tu cuenta. Si asocias una conexión a unaLAG, se crea con la misma velocidad de puerto y ubicación que se especifican en. LAG

Tras solicitar la conexión, ponemos a tu disposición una carta de autorización y la asignación de la instalación de conexión (LOA-CFA) para que la descargues o envíes un correo electrónico con una solicitud de más información. Si recibe una solicitud para obtener más información, deberá responder en un plazo de 7 días o se eliminará la conexión. El LOA - CFA es la autorización para conectarse AWS y su proveedor de red lo necesita para solicitar una conexión cruzada para usted. Si no tiene equipo en la AWS Direct Connect ubicación, no puede solicitar una conexión cruzada para usted en esa ubicación.

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

- Crear una conexión mediante el asistente de conexión
- Crear una conexión clásica
- the section called “Visualización de los detalles de la conexión”
- the section called “Actualizar una conexión”
- Asocie una MACsecCKN/CAKa una conexión
- the section called “Elimine la asociación entre una clave MACsec secreta y una conexión”
- the section called “Eliminar una conexión”

Puede añadir una conexión dedicada a un grupo de agregación de enlaces (LAG), lo que le permitirá tratar varias conexiones como una sola. Para obtener más información, consulte Asocie 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 AWS Direct Connect ubicación, póngase primero en contacto con un AWS Direct Connect AWS Direct Connect socio del Programa de socios. Para obtener más información, consulte APNPartners Supporting AWS 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 “MACsecrequisitos previos para las conexiones dedicadas”.

Carta de autorización y asignación de la instalación de conexión (LOA-CFA)

Una vez que hayamos procesado su solicitud de conexión, podrá descargar el archivo LOA -CFA. Si el enlace no está activado, el LOA - aún no CFA está disponible para su descarga. Compruebe su correo electrónico para ver si hay una solicitud de información.

La LoA descargada está firmada digitalmente y tiene una marca de agua para validar la autenticidad de la LoA emitida por. AWS La firma digital y la marca de agua en la LoA. El PDF documento evita que el proveedor de las instalaciones tome medidas en relación con una LoA modificada o potencialmente fraudulenta en los sitios de Direct Connect. La firma digital se puede autenticar abriendo el panel de firmas PDF y revisándolo. Un documento válido mostrará las palabras «La firma es válida» y «El documento no se ha modificado desde que se aplicó la firma». La marca de agua repite el panel de conexiones y las líneas asignadas a lo largo del cuerpo de la LoA como un indicador visual, aunque no seguro, de autenticidad.

La facturación comienza automáticamente cuando el puerto está activo o 90 días después de su emisión, lo que ocurra primero. LOA Para evitar los cargos de facturación, elimina el puerto antes de la activación o en un plazo de 90 días a partir de LOA su emisión.

Si tu conexión no funciona después de 90 días y no se CFA ha emitido el signo «LOA-», te enviaremos un correo electrónico informándote de que el puerto se eliminará en un plazo de 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 para descargar la LoA-CFA, consulte. Descarga el LOA - CFA

> **Note**
>
> Para obtener más información sobre los precios, consulte Precios de AWS Direct Connect. Si ya no desea la conexión después de volver a emitir el LOA -CFA, debe eliminarla usted mismo. Para obtener más información, consulte Eliminar una AWS Direct Connect conexión.

Temas

Cree una conexión AWS 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 AWS Direct Connect dedicada”.

Para crear una conexión mediante el asistente de conexión

1. Abra la AWS Direct Connectconsola en la versión 2/home. https://console.aws.amazon.com/directconnect/
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 AWS Direct Connect Kit de herramientas de resiliencia.
5. Elija Next (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. Esto puede oscilar entre 1 Gbps y 400 Gbps.

b. En Ubicación, elija la AWS Direct Connect ubicación adecuada y, a continuación, elija el proveedor de servicios de primera ubicación y, a continuación, seleccione el proveedor de servicios que proporciona conectividad para la conexión en esta ubicación.

c. En Segunda ubicación, elija la ubicación adecuada AWS Direct Connect en la segunda ubicación y, a continuación, elija el proveedor de servicios de segunda ubicación y, a continuación, seleccione el proveedor de servicios que proporciona conectividad para la conexión en esta segunda ubicación.

d. (Opcional) Configure MAC la seguridad (MACsec) para la conexión. En Configuración adicional, selecciona Solicitar un puerto MACsec compatible.

   MACsecsolo está disponible en conexiones dedicadas.

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

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

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

7. Elija Next (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 la asignación de la instalación de conexión (LOA-CFA). Para obtener más información, consultethe section called “Carta de autorización y asignación de la instalación de conexión (LOA-CFA)”.

Utilice uno de los siguientes comandos.

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

Cree una conexión AWS Direct Connect clásica

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

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

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

Para crear una AWS Direct Connect conexión nueva

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En la pantalla AWS Direct Connect, en Get started (Empezar), seleccione Create a connection (Crear una conexión).
3. Elija Classic.
4. En Name (Nombre), escriba un nombre para la conexión.
5. En Location (Ubicación), seleccione la ubicación de AWS Direct Connect apropiada.
6. Si procede, en Sub Location (Sububicación), elija el piso más cercano a usted o a su proveedor de red. Esta opción solo está disponible si la ubicación 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 AWS Direct Connect si utiliza esta conexión para conectarse a su centro de datos.

9. En el caso del proveedor de servicios, seleccione el AWS Direct Connect socio. Si utiliza un socio que no está en la lista, seleccione Other (Otro).
10. Si ha seleccionado Other (Otro) en Service provider (Proveedor de servicios), en Name of other provider (Nombre de otro proveedor), escriba el nombre del socio que utiliza.
11. (Opcional) Seleccione Agregar etiqueta para agregar pares clave/valor que ayuden a identificar aún más esta conexión.

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

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

La revisión de su solicitud y el aprovisionamiento de un puerto para su conexión pueden tardar hasta 72 horas. AWS Durante este tiempo, es posible que reciba un correo electrónico con una solicitud de información adicional sobre su caso de uso o sobre la ubicación especificada. El correo electrónico se envía a la dirección de correo electrónico que utilizaste al registrarte 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 AWS Direct Connect LOA - CFA

Puede descargar el LOA - CFA mediante la AWS Direct Connect consola o mediante la línea de comandos. Una vez que hayas descargado el LOA - CFA y se lo hayas proporcionado a tu proveedor de red o ubicación, ese proveedor podrá encargarte de la conexión cruzada.

Para descargar el - LOA CFA

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Connections (Conexiones).
3. Seleccione la conexión y, a continuación, elija Ver detalles.
4. Selecciona Descargar LOA -. CFA

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

5. Envía el LOA - CFA a tu proveedor de red o de colocación para que puedan solicitarte una conexión cruzada. El proceso de contacto puede variar en función del proveedor de coubicación. Para obtener más información, consulte Solicitud de conexiones cruzadas en AWS Direct Connect ubicaciones.

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

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

Asocie un MACsecCKN/CAKa una AWS Direct Connect conexión

Después de crear la conexión que admiteMACsec, puede asociar unaCKN/CAKa la conexión. Puede crear la asociación mediante la AWS Direct Connect consola o mediante la línea de comandos o. 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 AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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 CKN parCAK/] Elija el par de claves y, a continuación, haga lo siguiente:

   - Para la clave de asociación de conectividad (CAK), introduzca laCAK.
   - Para el nombre de la clave de asociación de conectividad (CKN), introduzca elCKN.

   [Use el secreto] Elija el secreto del administrador de secretos existente y, a continuación, en Secreto, seleccione la clave MACsec secreta.
6. Elija Asociar clave.

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

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

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

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

Para eliminar una asociación entre una conexión y una clave MACsec

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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 tecla mediante la línea de comandos o API

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

AWS Direct Connect Conexiones alojadas

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

AWS Direct Connect location

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

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

Velocidad del puerto

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

Tenga en cuenta lo siguiente:

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

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

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

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 AWS 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 AWS Direct Connect .

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

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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 API

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

Eliminar una AWS Direct Connect conexión

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

Antes de eliminar una conexión, descargue el LOA archivo correspondiente a la conexión que contiene la información de las cuentas cruzadas para disponer de la información pertinente sobre los circuitos que se van a desconectar. Para conocer los pasos para descargar la conexiónLOA, consulteCarta de autorización y asignación de la 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 su proveedor de alojamiento o circuito le siga cobrando los cargos de conexión cruzada o de circuito de red, ya que es posible que el cable de conexión cruzada siga conectado a su dispositivo de red. Estos cargos por la conexión cruzada son independientes de Direct Connect y deben cancelarse con el proveedor de colocación o circuito utilizando la información del. LOA

Si la conexión forma parte de un grupo de agregación de enlaces (LAG), no puede eliminar la conexión si, LAG al hacerlo, queda por debajo de su configuración de número mínimo de conexiones operativas.

Puede eliminar una conexión mediante la AWS Direct Connect consola o mediante la línea de comandos oAPI.

Para eliminar una conexión

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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 mediante la línea de comandos o API

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

Actualizar una AWS Direct Connect conexión

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

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

> **Note**
>
> MACsecsolo está disponible en conexiones dedicadas.

Los valores válidos son:

- `should_encrypt`
- `must_encrypt`

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

Para actualizar una conexión

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Connections (Conexiones).
3. Seleccione la conexión y, a continuación, elija Editar.
4. Modifique la conexión:

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

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

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

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

Para actualizar una conexión mediante la línea de comandos o API

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

Ver los detalles AWS Direct Connect de la conexión

Puede ver el estado actual de la conexión mediante la AWS Direct Connect consola o mediante la línea de comandos oAPI. También puedes ver tu ID de conexión (por ejemplo`dxcon-12nikabc`) y comprobar que coincide con el LOA ID de conexión CFA que recibiste o descargaste.

Para obtener información sobre la supervisión de conexiones, consulte Supervise los recursos de Direct Connect.

Para ver los detalles de una conexión

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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 API

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

Solicitud de conexiones cruzadas en AWS Direct Connect ubicaciones

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

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

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

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

> **Note**
>
> Si la conexión cruzada no se completa en un plazo de 90 días, la autorización otorgada por el LOA - CFA caduca. Para renovar unLOA... CFA que ha caducado, puedes volver a descargarlo desde la AWS Direct Connect consola. Para obtener más información, consulte Carta de autorización y asignación de la instalación de conexión (LOA-CFA).

Coubicaciones

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

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

Este de EE. UU. (Ohio)

Ubicación	Cómo solicitar una conexión
CologixCOL2, Colón	Póngase en contacto con Cologix en sales@cologix.com.
CologixMIN3, Minneapolis	Póngase en contacto con Cologix en sales@cologix.com.

Ubicación	Cómo solicitar una conexión
CyrusOne WestIII, Houston	Envíe una solicitud mediante el portal del cliente.
EquinixCH2, Chicago	Póngase en contacto con Equinix en awsdealreg@equinix.com.
QTS, Chicago	Póngase QTS en contacto con AConnect@qtsdatacenters .com.
Centros de datos de Netrality, 1102 Grand, Kansas City	Póngase en contacto con los Centros de datos de Netrality en support@netrality.com.

Este de EE. UU. (Norte de Virginia)

Ubicación	Cómo solicitar una conexión
165 Halsey Street, Newark	Póngase en contacto con operations@165halsey.com.
CoreSite 32k, Nueva York	Realice un pedido a través del Portal de CoreSite Clientes. Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web.
CoreSite VA1-VA2, Reston	Realice un pedido en el portal de CoreSite clientes. 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 RealtyIAD38, Ashburn	Póngase en contacto con Digital Realty en amazon.orders@digitalrealty.com.
Equinix DC1 - DC6 y 0-D12, Ashburn DC1	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix - y, Dallas DAA1 DC3 DC6	Póngase en contacto con Equinix en awsdealreg@equinix.com.
EquinixMI1, Miami	Póngase en contacto con Equinix en awsdealreg@equinix.com.

Ubicación	Cómo solicitar una conexión
EquinixNY5, Seacaucus	Póngase en contacto con Equinix en awsdealreg@equinix.com.
KIONetworks, Querétaro, MX QRO1	KIORedes de contacto».
Markley, One Summer Street, Boston	Para los clientes actuales, cree una solicitud mediante el portal de clientes. Para nuevas consultas, póngase en contacto con sales@markleygroup.com.
Netrality Data Centers, segundo pisoMMR, Filadelfia	Póngase en contacto con los Centros de datos de Netrality en support@netrality.com.
QTSATL1, Atlanta	Póngase QTS en contacto con AConnect@qtsdatacenters .com.

Oeste de EE. UU. (Norte de California)

Ubicación	Cómo solicitar una conexión
CoreSite,LA1, Los Ángeles	Realice un pedido a través del Portal de CoreSite Clientes. Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web.
CoreSite SV2, Milpitas	Realice un pedido a través del portal de CoreSiteclientes. Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web.
CoreSite SV4, Santa Clara	Realice un pedido a través del portal de CoreSite clientes. Después de completar el formulario, revise el pedido para comprobar que es correcto y, a continuación, apruebelo a través del MyCoreSite sitio web.
EdgeConneX, Phoenix	Haga un pedido con el Portal del cliente de EdgeOS. Una vez que haya enviado el formulario, EdgeConne X le proporcionará un formulario de solicitud de servicio para su aprobación. Puede enviar preguntas a cloudaccess@edgeconnex.com.

Ubicación	Cómo solicitar una conexión
EquinixLA3, El Segundo	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix &SV1, San José SV5	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Fénix, Fénix NAP	Póngase en contacto con phoenix NAP Provisioning en provisioning@phoenixnap.com.

Oeste de EE. UU. (Oregón)

Ubicación	Cómo solicitar una conexión
CoreSite DE1, Denver	Realice un pedido a través del Portal CoreSite del cliente. Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web.
Digital Realty SEA1 0, Westin Building, Seattle	Póngase en contacto con Digital Realty en amazon.orders@digitalrealty.com.
EdgeConneX, Portland	Haga un pedido con el Portal del cliente de EdgeOS. Una vez que haya enviado el formulario, EdgeConne X le proporcionará un formulario de solicitud de servicio para su aprobación. Puede enviar preguntas a cloudaccess@edgeconnex.com.
EquinixSE2, 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 TierPoint en contacto con nosotros en sales@tierpoint.com.

África (Ciudad del Cabo)

Ubicación	Cómo solicitar una conexión
Centros de datos de Cape Town Internet Exchange/ Teraco	Póngase en contacto con Teraco en support@teraco.co.za (si es cliente de Teraco) o en connect@teraco.co.za (para nuevos clientes).
TeracoJB1, 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
DCIJK3, Yakarta	Póngase en contacto con DCI Indonesia en jessie.w@dci-indonesia.com.com.
NTT2 Centro de datos, Yakarta	Póngase NTT en contacto con nosotros en tps.cms.presales@global.ntt.

Asia Pacific (Bombay)

Ubicación	Cómo solicitar una conexión
Equinix, Bombay	Póngase en contacto con Equinix en awsdealreg@equinix.com.
NetMagic DC2, Bangalore	Póngase en contacto con NetMagic Ventas y Marketing llamando al número gratuito 18001033130 o enviando un correo electrónico a marketing@netmagicsolutions.com.
Sify Rabale, Mumbai	Póngase en contacto con Sify en aws.directconnect@sifycorp.com.

Ubicación	Cómo solicitar una conexión
STTDelhi, Delhi DC2	Contacto STT en caso de consulta. AWSDX@sttelemediag dc .in.
STTGDCPvt. Ltd. VSB, Chennai	Contacto en STT caso de consulta. AWSDX@sttelemediag dc .in.
STTHyderabad, Hyderabad DC1	Contacto en consulta. STT AWSDX@sttelemediagdc .in.

Asia-Pacífico (Seúl)

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

Asia-Pacífico (Singapur)

Ubicación	Cómo solicitar una conexión
EquinixHK1, Tsuen Wan N.T., Hong Kong SAR	Póngase en contacto con Equinix en awsdealreg@equinix.com.
EquinixSG2, Singapur	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Global Switch, Singapur	Póngase en contacto con Global Switch en salessingapore@glo balswitch.com.

Ubicación	Cómo solicitar una conexión
GPX, Bombay	Póngase en contacto con GPX (Equinix) en awsdealreg@equinix.com.
iAdvantage Mega-i, Hong Kong	Póngase iAdvantage en contacto con cs@iadvantage.net o haga un pedido mediante el formulario electrónico de pedido iAdvantage de cableado.
Menara, Kuala Lumpur AIMS	Los clientes AIMS actuales pueden solicitar un pedido de X-Connect mediante el portal de servicio al cliente rellenando 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.
TCCCentro de datos, Bangkok	Póngase en contacto con TCC Technology Co., Ltd en gateway.ne@tcc-technology.com.

Asia-Pacífico (Sídney)

Ubicación	Cómo solicitar una conexión
CDCHume 2, Canberra	Inicie sesión en el portal de clientes en CDCCustomer Portal.
DatacomDH6, Auckland	Póngase en contacto con Datacom en Datacom Orbit, Auckland.
Equinix, Melbourne ME2	Póngase en contacto con Equinix en awsdealreg@equinix.com.
EquinixSY3, Sídney	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Global Switch, Sídney	Póngase en contacto con Global Switch en salessydney@globalswitch.com.
NEXTDCC1, Canberra	Póngase en contacto con nosotros NEXTDC en nxtops@nextdc.com.
NEXTDCM1, Melbourne	Póngase en contacto con nosotros NEXTDC en nxtops@nextdc.com.

Ubicación	Cómo solicitar una conexión
NEXTDCP1, Perth	Póngase en contacto con nosotros NEXTDC en nxtops@nextdc.com.
NEXTDCS2, Sídney	Póngase NEXTDC en contacto con nosotros en nxtops@nextdc.com.

Asia-Pacífico (Tokio)

Ubicación	Cómo solicitar una conexión
Centro de datos AT Tokyo Chuo, Tokio	Póngase en contacto con TOKYO AT en at-sales@attokyo.co.jp.
Chief Telecom LY, Taipei	Póngase en contacto con Chief Telecom en vicky_chan@chief.com.tw.
Chunghwa Telecom, Taipei	Póngase en contacto con CHT Taipéi IDC NOC en taipei_idc@cht.com.tw.
EquinixOS1, Osaka	Póngase en contacto con Equinix en awsdealreg@equinix.com.
EquinixTY2, Tokio	Póngase en contacto con Equinix en awsdealreg@equinix.com.
NECInzai, Inzai	Póngase en contacto con Inzai en connection_support@ices.jp.nec.comNEC.

Canadá (centro)

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

Ubicación	Cómo solicitar una conexión
CologixVAN2, Vancouver	Póngase en contacto con Cologix en sales@cologix.com.
eStruxture, Montreal	Póngase eStruxture en contacto con nosotros en directconnect@estruxture.com.

China (Pekín)

Ubicación	Cómo solicitar una conexión
CIDSJiachuangIDC, Pekín	Póngase en contacto con dx-order@sinnet.com.cn.
Sinnet Jiuxianqiao, Pekín IDC	Póngase en contacto con dx-order@sinnet.com.cn.
GDSCentro de datos número 3, Shanghái	Póngase en contacto con dx@nwcdcloud.cn.
GDSCentro de datos número 3, Shenzhen	Póngase en contacto con dx@nwcdcloud.cn.

China (Ningxia)

Ubicación	Cómo solicitar una conexión
Parque industrialIDC, Ningxia	Póngase en contacto con dx@nwcdcloud.cn.
ShapotouIDC, Ningxia	Póngase en contacto con dx@nwcdcloud.cn.

Europe (Fráncfort)

Ubicación	Cómo solicitar una conexión
CE Colo, Praga, República Checa	Póngase en contacto con CE Colo en info@cecolo.com.

Ubicación	Cómo solicitar una conexión
DigiPlex Ulven, Oslo, Noruega	Póngase en contacto con nosotros DigiPlex en helpme@digiplex.com.
EquinixAM3, Ámsterdam, Países Bajos	Póngase en contacto con Equinix en awsdealreg@equinix.com.
EquinixFR5, Frankfurt	Póngase en contacto con Equinix en awsdealreg@equinix.com.
EquinixHE6, Helsinki	Póngase en contacto con Equinix en awsdealreg@equinix.com.
EquinixMU1, Múnich	Póngase en contacto con Equinix en awsdealreg@equinix.com.
EquinixWA1, Varsovia	Póngase en contacto con Equinix en awsdealreg@equinix.com.
InterxionAMS7, Ámsterdam	Póngase en contacto con Interxion en customer.services@interxion.com.
InterxionCPH2, Copenhague	Póngase en contacto con Interxion en customer.services@interxion.com.
InterxionFRA6, Fráncfort	Póngase en contacto con Interxion en customer.services@interxion.com.
InterxionMAD2, Madrid	Póngase en contacto con Interxion en customer.services@interxion.com.
InterxionVIE2, Viena	Póngase en contacto con Interxion en customer.services@interxion.com.
InterxionZUR1, Zúrich	Póngase en contacto con Interxion en customer.services@interxion.com.
IPB, Berlín	Póngase IPB en contacto con nosotros en kontakt@ipb.de.
Equinix ITConicMD2, Madrid	Póngase en contacto con Equinix en awsdealreg@equinix.com.

Europe (Irlanda)

Ubicación	Cómo solicitar una conexión
Digital Realty (Reino Unido), Docklands	Póngase en contacto con Digital Realty (Reino Unido) en amazon.orders@digitalrealty.com.
Eircom Clonshaugh	Póngase en contacto con Eircom en datacentre@eirevo.ie.
EquinixDX1, Dublín	Póngase en contacto con Equinix en awsdealreg@equinix.com.
EquinixLD5, Londres (Slough)	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Interxion, Dublín DUB2	Póngase en contacto con Interxion en customer.services@interxion.com.
InterxionMRS1, Marsella	Póngase en contacto con Interxion en customer.services@interxion.com.

Europa (Milán)

Ubicación	Cómo solicitar una conexión
CDLANsrl Via Caldera 21, Milán	Póngase CDLAN en contacto con nosotros en sales@cdlan.it.
Equinix, MilánML2, Italia	Póngase en contacto con Equinix en awsdealreg@equinix.com.

Europe (Londres)

Ubicación	Cómo solicitar una conexión
Digital Realty (Reino Unido), Docklands	Póngase en contacto con Digital Realty (Reino Unido) en amazon.orders@digitalrealty.com.
EquinixLD5, Londres (Slough)	Póngase en contacto con Equinix en awsdealreg@equinix.com.

Ubicación	Cómo solicitar una conexión
Equinix, Manchester MA3	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
EquinixPA3, París	Póngase en contacto con Equinix en awsdealreg@equinix.com.
InterxionPAR7, París	Póngase en contacto con Interxion en customer.services@interxion.com.
Telehouse Voltaire, París	Póngase en contacto con Telehouse Paris Voltaire a través de la página de contacto.

Europa (Estocolmo)

Ubicación	Cómo solicitar una conexión
InterxionSTO1, Estocolmo	Póngase en contacto con Interxion en customer.services@interxion.com.

Europa (Zúrich)

Ubicación	Cómo solicitar una conexión
EquinixZRH51, Oberengstringen, Suiza	Póngase en contacto con Equinix en awsdealreg@equinix.com.

Israel (Tel Aviv)

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

Medio Oriente (Baréin)

Ubicación	Cómo solicitar una conexión
AWS BahréinDC53, Manama	Para realizar la conexión, puede colaborar con uno de nuestros socios proveedores de red de la ubicación para establecer la conectividad. Luego, entregará una carta de autorización (LOA) del proveedor de la red a AWS través del AWS Support Center. AWS completa la conexión cruzada en esta ubicación.
AWS BahréinDC52, Manama	Para realizar la conexión, puede colaborar con uno de nuestros socios proveedores de red de la ubicación para establecer la conectividad. Luego, entregará una carta de autorización (LOA) del proveedor de la red a AWS través del AWS Support Center. AWS completa la conexión cruzada en esta ubicación.

Oriente Medio () UAE

Ubicación	Cómo solicitar una conexión
EquinixDX1, Dubái, UAE	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Centro de SmartHub datos de Etisalat, Fujairah, UAE	Póngase en contacto con el centro de datos de Etisalat en -C&WS@etisalat.ae. SmartHub IntlSales

América del Sur (São Paulo)

Ubicación	Cómo solicitar una conexión
Cirion, Buenos Aires BNARAGMS	Póngase en contacto con Cirion en cloud.connect@ciriontechnologies.com.
EquinixRJ2, Río de Janeiro	Póngase en contacto con Equinix en awsdealreg@equinix.com.
EquinixSP4, São Paulo	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Tivit	Póngase en contacto con Tivit en aws@tivit.com.br.

AWS GovCloud (Este de EE. UU.)

No puede solicitar conexiones en esta región.

AWS GovCloud (Estados Unidos-Oeste)

Ubicación	Cómo solicitar una conexión
EquinixSV5, San José	Póngase en contacto con Equinix en awsdealreg@equinix.com.

AWS Direct Connect interfaces virtuales e interfaces virtuales alojadas

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

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

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

Reglas de anuncio de prefijo de interfaz virtual pública

Te anunciamos los prefijos de Amazon adecuados para que puedas acceder a tus AWS servicios VPCs o a otros. Puede acceder a todos los AWS prefijos a través de esta conexión; por ejemplo, AmazonEC2, Amazon S3 y Amazon.com. No tiene acceso a los prefijos que no son de Amazon. Para ver una lista actualizada de los prefijos anunciados por AWS, consulte Intervalos de direcciones AWS IP en. Referencia general de Amazon Web Services AWS no vuelve a anunciar a otros clientes los prefijos de los clientes que se recibieron a través de las interfaces virtuales públicas de Direct AWS Connect. Para obtener más información sobre las interfaces virtuales públicas y las políticas de enrutamiento, consulte the section called “Políticas de direccionamiento de interfaces virtuales públicas”.

> **Note**
>
> Le recomendamos que utilice un filtro de firewall (en función de la dirección de origen/destino de los paquetes) para controlar el tráfico que envía a algunos prefijos o que procede de ellos.

Si utiliza un filtro de prefijo (mapeado de ruta), asegúrese de que acepta prefijos con una coincidencia exacta o mayor. Los prefijos anunciados AWS Direct Connect pueden estar agregados y pueden diferir de los prefijos definidos en el filtro de prefijos.

SiteLink

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

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

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

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

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

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

Tipo de interfaz virtual	Admitido/No admitido
una puerta de enlace virtual o de tránsito	
Interfaz virtual privada adjunta a una puerta de enlace virtual	No compatible
Interfaz virtual privada	No compatible

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

SiteLink admite un MTU tamaño máximo de trama gigante de 8500 o 9001, según el tipo de interfaz virtual. Para obtener más información, consulte MTUspara 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 Crear una conexión mediante el asistente de conexión.
- Cree un grupo de agregación de enlaces (LAG) cuando tenga varias conexiones que desee tratar como una sola. Para obtener más información, consulte Asocie una conexión a un LAG.

Para crear una interfaz virtual, necesita la siguiente información:

Recurso	Información necesaria
Conexión	El grupo de AWS Direct Connect conexiones 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 conectarte a una VPC de la misma AWS región, necesitas la puerta de enlace privada virtual para tuVPC. El ASN lado de Amazon de la BGP sesión se hereda de la puerta de enlace privada virtual. Al crear una puerta de enlace privada virtual, puede especificar su propia puerta privadaASN. De lo contrario, Amazon proporciona un valor predeterminadoASN. Para obtener más información, consulte Crear una puerta de enlace privada virtual en la Guía del VPC usuario de Amazon. Para conectarse a VPC través de una puerta de enlace Direct Connect, necesita la puerta de enlace Direct Connect. Para obtener más información, consulte Gateways de Direct Connect.
VLAN	Una etiqueta de red de área local virtual única (VLAN) que aún no esté en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de AWS Direct Connect . Si tiene una conexión alojada, su AWS Direct Connect socio le proporcionará este valor. No puede modificar el valor después de haber creado la interfaz virtual.
Direcciones IP de mismo nivel	Una interfaz virtual puede admitir una sesión de BGP emparejamiento para IPv4IPv6, o una de cada una de ellas (doble pila). No utilice Elastic IPs (EIPs) ni traiga sus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias BGP sesiones para la misma familia de direcciones IP en la misma interfaz virtual. Los rangos de direccion es IP se asignan a cada extremo de la interfaz virtual para la sesión de BGP emparejamiento.

Recurso	Información necesaria

	• IPv4:
	  • (Solo interfaz virtual pública) Debe especificar IPv4 direcciones públicas únicas de su propiedad. El valor puede ser uno de los siguientes:
	  • Propiedad del cliente IPv4 CIDR
	
	  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 oISP, junto con una LOA CFA autorización
	  • Un AWS CIDR /31 proporcionado. Póngase en contacto con AWS Support para solicitar una solicitud pública IPv4 CIDR (y proporcione un caso de uso en su solicitud)
	
	  Note
	  No podemos garantizar que podamos cumplir con todas las solicitudes AWS de IPv4 direcciones públicas 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` rango, por ejemplo, podría usarlo `192.168.0.1` para su IP homóloga y `192.168.0.2` para la IP AWS homóloga. `192.168.0.0/30`

Recurso	Información necesaria
	• IPv6: Amazon te asigna automáticamente un /125. IPv6 CIDR No puede especificar sus propias direcciones homólogas. IPv6
Familia de direcciones	Si la sesión BGP de intercambio de pares terminará IPv4 oIPv6.
BGPinformación	• Un número de sistema autónomo del Border Gateway Protocol (BGPASN) público o privado para su parte de la BGP sesión. Si utiliza uno públicoAS N, debe ser su propietario. Si utilizas una privadaASN, puedes establecer un ASN valor personalizado. Para un archivo de 16 bitsASN, el valor debe estar en el rango de 64512 a 65534. En el caso de 32 bitsASN, el valor debe estar comprendido entre 1 y 2147483647. La función anteponer un sistema autónomo (AS) no funciona si se utiliza una interfaz virtual privada ASN para una pública. • AWS se habilita MD5 de forma predeterminada. Esta opción no se puede modificar. • Una clave MD5 BGP de autenticación. 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	IPv4Rutas públicas o IPv6 rutas sobre las que hacer publicidadBGP. Debe anunciar al menos un prefijo conBGP, hasta un máximo de 1000 prefijos.
	• IPv4: IPv4 CIDR Pueden superponerse con otro IPv4 CIDR anuncio público que se haya utilizado AWS Direct Connect cuando se dé alguna de las siguientes condiciones:
	  • CIDRsSon de diferentes AWS regiones. Asegúrese de aplicar etiquetas BGP comunitarias a los prefijos públicos.
	  • Utiliza AS_ PATH cuando tiene un público ASN en una configuración activa/pasiva.
	  Para obtener más información, consulte Políticas y comunidades de enrutamiento. BGP
	• IPv6: especifique una longitud de prefijo igual o inferior a /64.
	• Puedes añadir prefijos adicionales a un público existente VIF y anunciarl os poniéndote en contacto con el servicio de asistencia.AWS En su caso de soporte, proporcione una lista de CIDR prefijos adicionales que desee añadir al público VIF y anuncie.
	• Puede especificar cualquier longitud de prefijo en una interfaz virtual pública de Direct Connect. IPv4debería admitir cualquier valor comprendido entre /1 y /32 y IPv6 entre /1 y /64.

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

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

- En el caso de las VIFs redes privadas y de tránsitoVIFs, la cuenta se aplica a la interfaz virtual y al destino de la puerta de enlace privada virtual o la puerta de enlace Direct Connect.

- En el caso de las cuentas públicasVIFs, la cuenta se utiliza para la facturación de la interfaz virtual. El uso de Data Transfer Out (DTO) se calcula en beneficio del propietario del recurso según la velocidad de transferencia de AWS Direct Connect datos.

> **Note**
>
> Los prefijos de 31 bits se admiten en todos los tipos de interfaz virtual de Direct Connect. Consulte RFC3021: Uso de prefijos de 31 bits en enlaces IPv4 punto a punto para obtener más información.

MTUspara interfaces virtuales privadas o interfaces virtuales de tránsito

AWS Direct Connect admite un tamaño de trama Ethernet de 1522 o 9023 bytes (encabezado Ethernet de 14 bytes + VLAN etiqueta de 4 bytes + bytes para el datagrama IP + 4 bytesFCS) en la capa de enlace.

La unidad de transmisión máxima (MTU) de una conexión de red es el tamaño, en bytes, del paquete más grande permitido que se puede pasar a través de la conexión. El MTU de una interfaz privada virtual puede ser de 1500 o 9001 (tramas gigantes). La interfaz virtual MTU de tránsito puede ser de 1500 u 8500 (tramas gigantes). Puede especificarlo MTU al crear la interfaz o actualizarla después de crearla. Si se establece una interfaz virtual en 8500 (tramas gigantes) o 9001 (tramas jumbo), se puede producir una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. MTU Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Jumbo Frame Capable en la pestaña Resumen.

Después de habilitar los marcos gigantes para su interfaz virtual privada o interfaz virtual de tránsito, solo podrá asociarlos a una conexión o LAG que sea compatible con marcos 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 MTU valores diferentes, o si tiene una interfaz de sitio a sitio VPN que anuncia la misma ruta, se utilizará 1500. MTU

> **Important**
>
> Las tramas gigantes solo se aplicarán a las rutas propagadas AWS Direct Connect y a las rutas estáticas a través de pasarelas de tránsito. Las tramas gigantes de las puertas de enlace de tránsito solo admiten 8500 bytes.
> Si una EC2 instancia no admite tramas gigantes, descarta las tramas jumbo de Direct Connect. Todos los tipos de EC2 instancias admiten tramas gigantes, excepto las C1CC1, T1 y M1. Para obtener más información, consulte Unidad máxima de transmisión de red (MTU) para su EC2 instancia en la Guía del EC2 usuario de Amazon.
> 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 ver los pasos MTU para configurar una interfaz virtual privada, consulteConfigure la MTU de una interfaz virtual privada.

AWS Direct Connect interfaces virtuales

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

Para crear una interfaz virtual para las cuentas propias AWS Organizations o AWS Organizations distintas de la suya, cree una interfaz virtual alojada.

Consulte lo siguiente para crear una interfaz virtual:

- Crear una interfaz virtual pública
- Crear una interfaz virtual privada
- Crear 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 el tránsito de interfaces virtuales a una puerta de enlace Direct Connect

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

La unidad de transmisión máxima (MTU) de una conexión de red es el tamaño, en bytes, del paquete más grande permitido que se puede pasar a través de la conexión. El MTU de una interfaz privada virtual puede ser de 1500 o 9001 (tramas gigantes). La interfaz virtual MTU de tránsito puede ser de 1500 u 8500 (tramas gigantes). Puede especificarlo MTU al crear la interfaz o actualizarla después de crearla. Si se establece una interfaz virtual en 8500 (tramas gigantes) o 9001 (tramas jumbo), se puede producir una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. MTU Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la consola de AWS Direct Connect y busque Jumbo Frame Capable (Con capacidad de tramas gigantes) en la pestaña Summary (Resumen).

> **Important**
>
> Si asocias tu pasarela de transporte a una o más pasarelas de Direct Connect, el número de sistema autónomo (ASN) utilizado por la pasarela de transporte y la pasarela de Direct Connect deben ser diferentes. Por ejemplo, si usa el ASN 64512 predeterminado tanto para la puerta de enlace de tránsito como para la puerta de enlace Direct Connect, se produce un error en la solicitud de asociación.

Crear una interfaz virtual AWS Direct Connect pública

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

Para aprovisionar una interfaz virtual pública

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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. Para VLAN, introduzca el número de identificación de su red de área local virtual ()VLAN.

   d. BGPASNEn este caso, introduzca el número de sistema autónomo del protocolo Border Gateway del router homólogo local para la nueva interfaz virtual.

      Los valores válidos son 1-2.147.483.647.

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

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

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

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

      [IPv6] Para configurar un IPv6 BGP par, 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 BGP clave, BGP MD5 introdúzcala.

      Si no introduce ningún valor, generamos una BGP clave. Si ha proporcionado su propia clave o si la hemos generado nosotros, ese valor se muestra en la columna de claves de BGP autenticación de la página de detalles de la interfaz virtual de Virtual Interfaces.

   c. Para anunciar prefijos en Amazon, en el caso de los prefijos que desee anunciar, introduzca las direcciones de IPv4 CIDR destino (separadas por comas) a las que se debe enrutar el tráfico a través de la interfaz virtual.

      > **Important**
      >
      > Puedes añadir prefijos adicionales a un público existente VIF y anunciarlos poniéndote en contacto con el servicio de asistencia.AWS En su caso de soporte,

proporcione una lista de CIDR prefijos adicionales que desee añadir al público VIF y anuncie.

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 API

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

Crear una interfaz virtual AWS Direct Connect privada

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

Si utiliza el VPC asistente para crear unaVPC, la propagación de rutas se habilita automáticamente. Con la propagación de rutas, las rutas se rellenan automáticamente en las tablas de rutas de suVPC. Si lo prefiere, puede deshabilitar la propagación de rutas. Para obtener más información, consulte Habilitar la propagación de rutas en su tabla de rutas en la Guía del VPC usuario de Amazon.

La unidad de transmisión máxima (MTU) de una conexión de red es el tamaño, en bytes, del paquete más grande permitido que se puede pasar a través de la conexión. El MTU de una interfaz privada virtual puede ser de 1500 o 9001 (tramas gigantes). La interfaz virtual MTU de tránsito puede ser de 1500 u 8500 (tramas gigantes). Puede especificarlo MTU al crear la interfaz o actualizarla después de crearla. Si se establece una interfaz virtual en 8500 (tramas gigantes) o 9001 (tramas jumbo), se puede producir una actualización de la conexión física subyacente si no se actualizó para

admitir tramas gigantes. MTU Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la consola de AWS Direct Connect y busque Jumbo Frame Capable (Con capacidad de tramas gigantes) en la pestaña Summary (Resumen).

Para aprovisionar una interfaz virtual privada a un VPC

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Tipo de interfaz virtual, elija Privada.
5. En Configuración de la interfaz virtual privada, realice lo siguiente:
   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.
   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.
   c. Como propietario de la interfaz virtual, elija Mi AWS cuenta si la interfaz virtual es para su AWS cuenta.
   d. En Direct Connect gateway (Gateway de Direct Connect), seleccione la gateway de Direct Connect.
   e. Para VLAN, introduzca el número de identificación de su red de área local virtual (VLAN).
   f. BGPASNEn este caso, introduzca el número de sistema autónomo del protocolo Border Gateway del router homólogo local para la nueva interfaz virtual.

      Los valores válidos son 1 a 2147483647.
6. En Additional Settings (Configuración adicional), haga lo siguiente:
   a. Para configurar un par IPv4 BGP o un IPv6 par, haga lo siguiente:

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

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

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

> **Important**
>
> Si permite la AWS asignación automática de IPv4 direcciones, se CIDR asignará un /29 desde IPv4 169.254.0.0/16 Link-Local de acuerdo con 3927 para la conectividad. RFC point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen o destino del tráfico. VPC En su lugar, debe usar RFC 1918 u otra dirección (distinta de RFC 1918) y especificar la dirección usted mismo.
>
> - Para obtener más información acerca de RFC 1918, consulte Asignación de direcciones para Internet privadas.
> - Para obtener más información acerca de RFC 3927, consulte Configuración dinámica de direcciones locales de IPv4 enlace.

[IPv6] Para configurar un IPv6 BGP par, 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 Jumbo MTU (MTUtamaño 9001).

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

d. (Opcional) Añada o elimine una etiqueta.

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

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

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

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

8. Descargue la configuración del router para su dispositivo. Para obtener más información, consulte Descargar el archivo de configuración del enrutador.

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

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

Cree una interfaz virtual de tránsito para la AWS Direct Connect puerta de enlace

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

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

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Virtual interface type (Tipo de interfaz virtual) en Type (Tipo), elija Transit (Tránsito).
5. En Transit virtual interface settings (Configuración de la interfaz virtual de tránsito), haga lo siguiente:

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

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

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

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

   e. Para VLAN, introduzca el número de identificación de su red de área local virtual (VLAN).

   f. Para BGPASNello, introduzca el número de sistema autónomo del protocolo Border Gateway del router homólogo local para la nueva interfaz virtual.

      Los valores válidos son 1 a 2147483647.

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

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

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

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

> **Important**
>
> Si permite la AWS asignación automática de IPv4 direcciones, se CIDR asignará un /29 desde IPv4 169.254.0.0/16 Link-Local de acuerdo con 3927 para la conectividad. RFC point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen o destino del tráfico. VPC En su lugar, debe usar RFC 1918 u otra dirección (distinta de RFC 1918) y especificar la dirección usted mismo.
>
> - Para obtener más información acerca de RFC 1918, consulte Asignación de direcciones para Internet privadas.
> - Para obtener más información acerca de RFC 3927, consulte Configuración dinámica de direcciones locales de IPv4 enlace.

[IPv6] Para configurar un IPv6 BGP par, 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 8500 (tramas gigantes), seleccione Jumbo MTU (MTUtamaño 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 API

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

Para ver las interfaces virtuales que están conectadas a una puerta de enlace de Direct Connect mediante la línea de comandos o API

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

Descargar el archivo de configuración del AWS Direct Connect router

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 que están MACsec activadas, crearemos automáticamente el archivo de configuración para su enrutador:

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

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Seleccione la interfaz virtual y, a continuación, elija View details (Ver detalles).
4. Elija Download router configuration (Descargar configuración del router).
5. En Download router configuration (Descargar configuración del router), haga lo siguiente:
   a. En Vendor (Proveedor), seleccione el fabricante del router.
   b. En Platform, seleccione el modelo del router.

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

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

7. Si necesita configurar su router manualmenteMACsec, utilice la siguiente tabla como guía.

Parámetro	Descripción
CKNlongitud	Se trata de una cadena de 64 caracteres hexadecimales (0–9, A–E). Utilice la longitud completa para maximizar la compatibilidad multiplat aforma.
CAKlongitud	Se trata de una cadena de 64 caracteres hexadecimales (0–9, A–E). Utilice la longitud completa para maximizar la compatibilidad multiplat aforma.
Algoritmo criptográfico	AES_256_ CMAC
SAKSuite de cifrado	• Para conexiones de 100 Gbps: GCM _ _ _256 AES XPN • Para conexiones de 10 Gbps: GCM _ _ _256 o AES _ XPN _256 GCM AES
Conjunto de cifrado de claves	16
Desplazamiento de confidenc ialidad	0
ICVIndicador	No
SAKHora de volver a introducir	Sustitución de PN>

Interfaces AWS Direct Connect virtuales alojadas

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

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

Para crear una interfaz virtual, necesita la siguiente información:

Recurso	Información necesaria
Conexión	El grupo de AWS Direct Connect conexiones 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 conectarte a una VPC de la misma AWS región, necesitas la puerta de enlace privada virtual para tuVPC. El ASN lado de Amazon de la BGP sesión se hereda de la puerta de enlace privada virtual. Al crear una puerta de enlace privada virtual, puede especificar su propia puerta privadaASN. De lo contrario, Amazon proporciona un valor predeterminadoASN. Para obtener más información, consulte Crear una puerta de enlace privada virtual en la Guía del VPC usuario de Amazon. Para conectarse a VPC través de una puerta de enlace Direct Connect, necesita la puerta de enlace Direct Connect. Para obtener más información, consulte Gateways de Direct Connect.
VLAN	Una etiqueta de red de área local virtual única (VLAN) que aún no esté en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de AWS Direct Connect .

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 BGP emparejamiento para IPv4IPv6, o una de cada una de ellas (doble pila). No utilice Elastic IPs (EIPs) ni traiga sus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias BGP sesiones para la misma familia de direcciones IP en la misma interfaz virtual. Los rangos de direccion es IP se asignan a cada extremo de la interfaz virtual para la sesión de BGP emparejamiento.
	
	• IPv4:
	  • (Solo interfaz virtual pública) Debe especificar IPv4 direcciones públicas únicas de su propiedad. El valor puede ser uno de los siguientes:
	  • Propiedad del cliente IPv4 CIDR
	
	  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 oISP, junto con una LOA CFA autorización
	  • Un AWS CIDR /31 proporcionado. Póngase en contacto con AWS Support para solicitar una solicitud pública IPv4 CIDR (y proporcione un caso de uso en su solicitud)
	
	  Note
	  No podemos garantizar que podamos cumplir con todas las solicitudes AWS de IPv4 direcciones públicas 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 /125. IPv6 CIDR No puede especificar sus propias direcciones homólogas. IPv6
Familia de direcciones	Si la sesión BGP de intercambio de pares terminará IPv4 oIPv6.
BGPinformación	• Un número de sistema autónomo del Border Gateway Protocol (BGPASN) público o privado para su parte de la BGP sesión. Si utiliza uno públicoAS N, debe ser su propietario. Si utilizas una privadaASN, puedes establecer un ASN valor personalizado. Para un archivo de 16 bitsASN, el valor debe estar en el rango de 64512 a 65534. En el caso de 32 bitsASN, el valor debe estar comprendido entre 1 y 2147483647. La función anteponer un sistema autónomo (AS) no funciona si se utiliza una interfaz virtual privada ASN para una pública. • AWS se habilita MD5 de forma predeterminada. Esta opción no se puede modificar. • Una clave MD5 BGP de autenticación. 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	IPv4Rutas públicas o IPv6 rutas sobre las que anunciarseBGP. Debe anunciar al menos un prefijo conBGP, hasta un máximo de 1000 prefijos.
	• IPv4: IPv4 CIDR Pueden superponerse con otro IPv4 CIDR anuncio público que se haya utilizado AWS Direct Connect cuando se dé alguna de las siguientes condiciones:
	  • CIDRsSon de diferentes AWS regiones. Asegúrese de aplicar etiquetas BGP comunitarias a los prefijos públicos.
	  • Utiliza AS_ PATH cuando tiene un público ASN en una configuración activa/pasiva.
	  Para obtener más información, consulte Políticas y comunidades de enrutamiento. BGP
	• IPv6: especifique una longitud de prefijo igual o inferior a /64.
	• Puedes añadir prefijos adicionales a un público existente VIF y anunciarlos poniéndote en contacto con el servicio de asistencia.AWS En su caso de soporte, proporcione una lista de CIDR prefijos adicionales que desee añadir al público VIF y anuncie.
	• Puede especificar cualquier longitud de prefijo en una interfaz virtual pública de Direct Connect. IPv4debería admitir cualquier valor comprendido entre /1 y /32 y IPv6 entre /1 y /64.

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

Cree una interfaz virtual privada alojada en AWS 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 AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Tipo de interfaz virtual, en Tipo, elija Privada.
5. En Configuración de la interfaz virtual privada, realice lo siguiente:

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

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

   c. En Propietario de la interfaz virtual, elija Otra cuenta de AWS y, a continuación, en Propietario de la interfaz virtual, ingrese el ID de la cuenta propietaria de esta interfaz virtual.

   d. Para VLAN, introduzca el número de identificación de su red de área local virtual ()VLAN.

   e. Para BGPASNello, introduzca el número de sistema autónomo del protocolo Border Gateway del router homólogo local para la nueva interfaz virtual.

      Los valores válidos son 1-2.147.483.647.

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

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

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

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

      > **Important**
      >
      > Si permite la AWS asignación automática de direcciones IP, se CIDR asignará un /29 a partir de 169.254.0.0/16. AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen y destino del tráfico. En su lugar, debe usar RFC 1918 u otra dirección (distinta de RFC 1918)

y especificar la dirección usted mismo. Para obtener más información sobre RFC 1918, consulte Asignación de direcciones para Internet privadas.

[IPv6] Para configurar un IPv6 BGP par, 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 Jumbo MTU (MTUtamaño 9001).

c. (Opcional) Añada o elimine una etiqueta.

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

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

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

7. Una vez que el propietario de la otra AWS cuenta acepte 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 API

- allocate-private-virtual-interface (AWS CLI)
- AllocatePrivateVirtualInterface (AWS Direct Connect API)

Cree una interfaz virtual pública alojada en AWS 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 AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).

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

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

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

   c. En Propietario de la interfaz virtual, elija Otra AWS cuenta y, a continuación, en Propietario de la interfaz virtual, introduzca el ID de la cuenta propietaria de esta interfaz virtual.

   d. Para VLAN, introduzca el número de identificación de su red de área local virtual (VLAN).

   e. BGPASNEn este caso, introduzca el número de sistema autónomo del protocolo Border Gateway del router homólogo local para la nueva interfaz virtual.

      Los valores válidos son 1-2.147.483.647.
6. Para configurar un par IPv4 BGP o un IPv6 par, haga lo siguiente:

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

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

   > **Important**
   >
   > Si permite la AWS asignación automática de direcciones IP, se CIDR asignará un /29 a partir de 169.254.0.0/16. AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen y destino del tráfico. En su lugar, debe usar RFC 1918 u otra dirección y especificar la dirección usted mismo. Para obtener más información sobre RFC 1918, consulte Asignación de direcciones para Internet privadas.

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

7. Para anunciar prefijos en Amazon, en el caso de los prefijos que desee anunciar, introduzca las direcciones de IPv4 CIDR destino (separadas por comas) a las que se debe enrutar el tráfico a través de la interfaz virtual.
8. Para proporcionar su propia clave para autenticar la BGP sesión, en Configuración adicional, introduzca la clave de autenticación como clave de BGP autenticación.

   Si no introduce ningún valor, generaremos una BGP clave.
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 AWS cuenta acepte 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 API

- allocate-public-virtual-interface (AWS CLI)
- AllocatePublicVirtualInterface (AWS Direct Connect API)

Cree una interfaz virtual de tránsito AWS Direct Connect alojada

Para crear una interfaz virtual de tránsito alojada

> **Important**
>
> Si asocias tu pasarela de transporte a una o más pasarelas de Direct Connect, el número de sistema autónomo (ASN) utilizado por la pasarela de transporte y la pasarela de Direct Connect deben ser diferentes. Por ejemplo, si usa el ASN 64512 predeterminado tanto para la puerta de enlace de tránsito como para la puerta de enlace Direct Connect, se produce un error en la solicitud de asociación.

1. Abre la AWS Direct Connectconsola en la versión 2/homehttps://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 Transit (Tránsito).
5. En Transit virtual interface settings (Configuración de la interfaz virtual de tránsito), haga lo siguiente:

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

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

   c. En Propietario de la interfaz virtual, elija Otra AWS cuenta y, a continuación, en Propietario de la interfaz virtual, introduzca el ID de la cuenta propietaria de esta interfaz virtual.

   d. Para VLAN, introduzca el número de identificación de su red de área local virtual (VLAN).

   e. Para BGPASNello, introduzca el número de sistema autónomo del protocolo Border Gateway del router homólogo local para la nueva interfaz virtual.

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

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

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

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

      > **Important**
      >
      > Si permite la AWS asignación automática de direcciones IP, se CIDR asignará un /29 a partir de 169.254.0.0/16. AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen y destino del tráfico. En su lugar, debe usar RFC 1918 u otra dirección y especificar la dirección

usted mismo. Para obtener más información sobre RFC 1918, consulte Asignación de direcciones para Internet privadas.

[IPv6] Para configurar un IPv6 BGP par, 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 8500 (tramas gigantes), seleccione Jumbo MTU (MTUtamaño 8500).

c. [Opcional] Añada una etiqueta. Haga lo siguiente:

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

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

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

7. Elija Create virtual interface (Crear interfaz virtual).
8. Una vez que el propietario de la otra AWS cuenta acepte la interfaz virtual alojada, podrá descargar el archivo de configuración del router para su 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 API

- allocate-transit-virtual-interface (AWS CLI)
- AllocateTransitVirtualInterface (AWS Direct Connect API)

Ver detalles de la interfaz AWS Direct Connect virtual

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

- Estado de la conexión
- Nombre
- Ubicación
- VLAN
- BGPdetalles

- Direcciones IP de mismo nivel

Para ver los detalles de una interfaz virtual

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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 las interfaces virtuales mediante la línea de comandos o API

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

Añadir un BGP par a una interfaz AWS Direct Connect virtual

Agregue o elimine una IPv4 sesión de IPv6 BGP emparejamiento a su interfaz virtual mediante la AWS Direct Connect consola o la línea de comandos o. API

Una interfaz virtual puede admitir una sola sesión de IPv4 BGP interconexión y una sola sesión de interconexión IPv6BGP. No puede especificar sus propias IPv6 direcciones de pares para una sesión de IPv6 BGP emparejamiento. Amazon te asigna automáticamente un /125. IPv6 CIDR

No se admite el uso de varios protocolos. BGP IPv4y IPv6 funcionan en modo de doble pila para la interfaz virtual.

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

Utilice el siguiente procedimiento para añadir un BGP par.

Para añadir un BGP par

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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 agregar IPv4 BGP pares, haga lo siguiente:
   - Elija IPv4.
   - Para especificar estas direcciones IP usted mismo, en Your router peer ip, introduzca la IPv4 CIDR dirección de destino a la que Amazon debe enviar el tráfico. En el caso de la IP del mismo nivel del router Amazon, introduce la IPv4 CIDR dirección a la que se va a enviar el tráfico AWS.
6. (Interfaz virtual pública) Para agregar IPv4 BGP pares, haga lo siguiente:
   - En el caso de la IP del mismo nivel de su router, introduzca la dirección de IPv4 CIDR destino a la que se debe enviar el tráfico.
   - En el caso de la IP homóloga del router Amazon, introduce la IPv4 CIDR dirección a la que se va a enviar el tráfico AWS.

   > **Important**
   >
   > Si permite la AWS asignación automática de direcciones IP, se CIDR asignará un /29 a partir de 169.254.0.0/16. AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen y destino del tráfico. En su lugar, debe usar RFC 1918 u otra dirección y especificar la dirección usted mismo. Para obtener más información sobre RFC 1918, consulte Asignación de direcciones para Internet privadas.

7. (Interfaz virtual privada o pública) Para agregar IPv6 BGP pares, elija IPv6. Las IPv6 direcciones homólogas se asignan automáticamente desde el conjunto de IPv6 direcciones de Amazon; no puedes especificar IPv6 direcciones personalizadas.
8. O BGPASNbien, introduzca el número de sistema autónomo del protocolo Border Gateway de su router homólogo local para la nueva interfaz virtual.

   En el caso de una interfaz virtual pública, ASN debe ser privada o estar ya incluida en la lista de interfaces virtuales permitidas.

   Los valores válidos son 1-2.147.483.647.

   Tenga en cuenta que si no ingresa un valor, le asignaremos uno de forma automática.
9. Para proporcionar su propia BGP clave, en Clave de BGP autenticación, BGP MD5 introdúzcala.
10. Elija Add peering (Añadir intercambio).

Para crear un BGP par mediante la línea de comandos o API

- create-bgp-peer (AWS CLI)
- reateBGPPeer(CAWS Direct Connect API)

Eliminar un BGP par de interfaz AWS Direct Connect virtual

Si su interfaz virtual tiene una sesión de IPv4 IPv6 BGP emparejamiento y otra, puede eliminar una de las sesiones de BGP emparejamiento (pero no ambas). Puede eliminar un BGP par de interfaz virtual mediante la AWS Direct Connect consola o mediante la línea de comandos o. API

Para eliminar un BGP par

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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 par mediante la línea de comandos o API

- delete-bgp-peer (AWS CLI)
- eleteBGPPeer(DAWS Direct Connect API)

Configurar MTU una interfaz virtual AWS Direct Connect privada

Si la interfaz virtual tiene una sesión de IPv6 BGP interconexión IPv4 y otra, puede eliminar una de las sesiones de BGP interconexión (pero no ambas). Para obtener más información sobre las interfaces virtuales privadas MTUs y las interfaces virtuales privadas, consulte MTUslas interfaces virtuales privadas o las interfaces virtuales de tránsito.

Puede configurar una interfaz virtual privada mediante la AWS Direct Connect consola o mediante la línea de comandos oAPI. MTU

Para configurar MTU una interfaz virtual privada

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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 (MTUtamaño 9001) o Jumbo MTU (MTUtamaño 8500), selecciona Activado.
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 configurar una interfaz virtual privada mediante la línea de comandos o MTU API

- update-virtual-interface-attributes (AWS CLI)
- UpdateVirtualInterfaceAttributes (AWS Direct Connect API)

Agregar o quitar etiquetas de interfaz AWS Direct Connect virtual

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

Para añadir o eliminar una etiqueta de interfaz virtual

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/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 AWS Direct Connect virtual

Puede eliminar una o varias interfaces virtuales. Antes de poder eliminar una conexión, debe eliminar la interfaz virtual. Al eliminar una interfaz virtual, se detienen AWS Direct Connect los gastos de transferencia de datos asociados a la interfaz virtual.

Puede eliminar una interfaz virtual mediante la AWS Direct Connect consola o la línea de comandos oAPI.

Para eliminar una interfaz virtual

1. Abra la AWS Direct Connectconsola en la versión 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 API

- delete-virtual-interface (AWS CLI)
- DeleteVirtualInterface (AWS Direct Connect API)

Aceptar una interfaz AWS Direct Connect virtual alojada

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

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

Para aceptar una interfaz virtual alojada

1. Abra la AWS Direct Connectconsola en la versión https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Seleccione la interfaz virtual y, a continuación, elija View details (Ver detalles).
4. Elija Aceptar.
5. Esto se aplica a las interfaces virtuales privadas y a las interfaces virtuales de tránsito.

   (Interfaz virtual de tránsito) En el cuadro de diálogo Accept virtual interface (Aceptar interfaz virtual), seleccione una gateway de Direct Connect y, a continuación, elija Accept virtual interface (Aceptar interfaz virtual).

   (Interfaz virtual privada) En el cuadro de diálogo Accept virtual interface (Aceptar interfaz virtual), seleccione una gateway privada virtual o de Direct Connect y, a continuación, elija Accept (Aceptar).
6. Una vez que acepte la interfaz virtual alojada, el propietario de la conexión de AWS Direct Connect puede descargar el archivo de configuración del router. La opción Download router configuration (Descargar configuración del router) no está disponible para la cuenta que acepta la interfaz virtual alojada.

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

- confirm-private-virtual-interface (AWS CLI)
- ConfirmPrivateVirtualInterface (AWS Direct Connect API)

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

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

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

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

Migrar una interfaz AWS Direct Connect virtual

Utilice este procedimiento cuando desee realizar cualquiera de las siguientes operaciones de migración de interfaz virtual:

- Migre una interfaz virtual existente asociada a una conexión a otraLAG.
- Migre una interfaz virtual existente asociada a una existente LAG a una nuevaLAG.
- 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 preconfigurar la configuración de la conexión y, a continuación, actualizarlaBGP.
> - No puede migrar VIF de una conexión alojada a otra conexión alojada. VLANIDsson únicas; por lo tanto, migrar una de esta VIF manera significaría que VLANs no coinciden. Tienes que eliminar la conexión oVIF, y luego volver a crearla, utilizando una VLAN que sea igual tanto para la conexión como para 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. Abre la AWS Direct Connectconsola en la versión 2/homehttps://console.aws.amazon.com/directconnect/.
2. En el panel de navegación, elija Virtual Interfaces.
3. Seleccione la interfaz virtual y, a continuación, elija Edit (Editar).
4. En Conexión, selecciona la conexión LAG o.
5. Elija Edit virtual interface (Editar interfaz virtual).

Para migrar una interfaz virtual mediante la línea de comandos o API

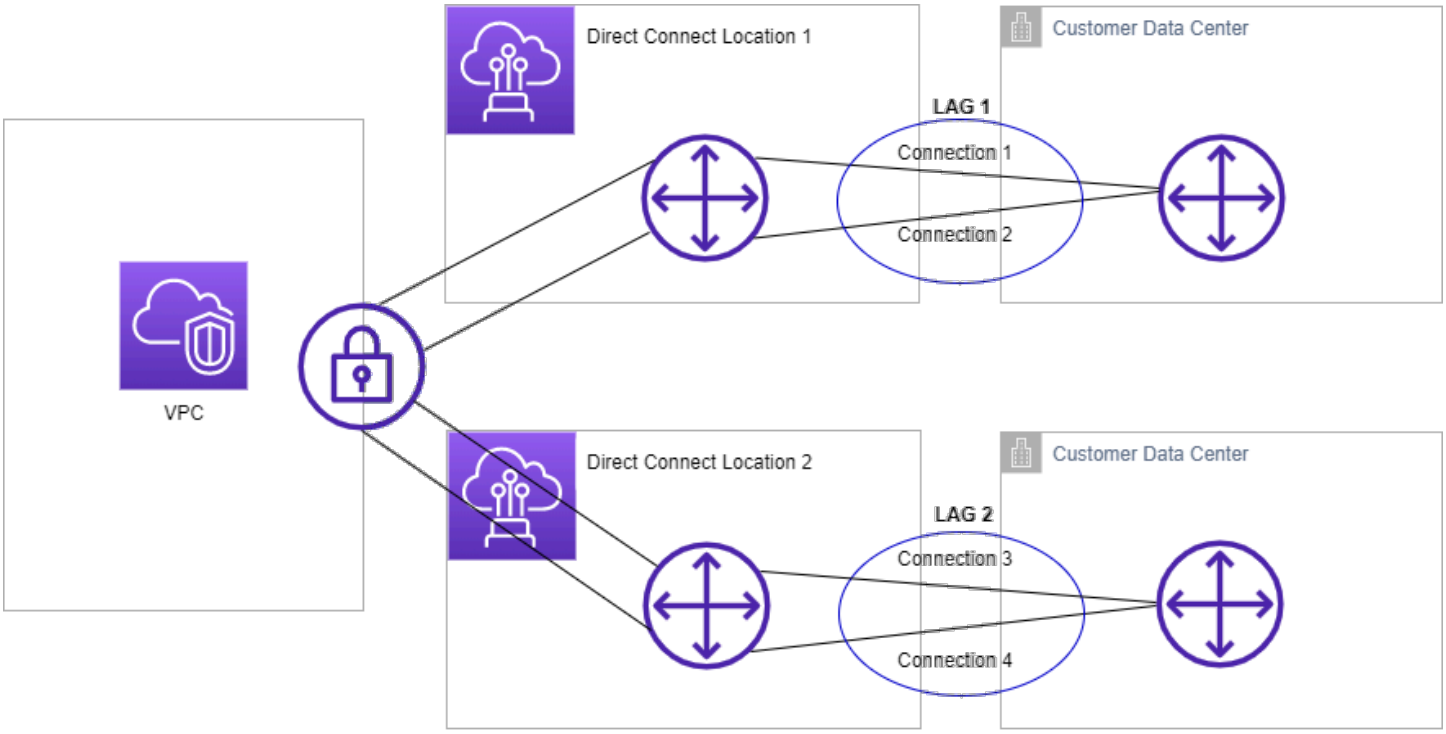
- associate-virtual-interface (AWS CLI)
- AssociateVirtualInterface (AWS Direct Connect API)

Grupos de agregación de enlaces (LAGs)

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 agregación de enlaces (LACP) para agregar varias conexiones en un único AWS Direct Connect punto final, lo que le permite tratarlas como una única conexión administrada. LAGsagiliza la configuración porque la LAG configuración se aplica a todas las conexiones del grupo.

> **Note**
>
> El multichasis LAG (MLAG) no es compatible AWS con.

En el siguiente diagrama, tiene cuatro conexiones, con dos conexiones a cada ubicación. Puede crear un LAG cuatro conexiones que terminen en el mismo AWS dispositivo y en la misma ubicación y, a continuación, utilizar las dos conexiones LAGs en lugar de las cuatro para la configuración y la administración.



Puede crear una LAG a partir de conexiones existentes o aprovisionar conexiones nuevas. Una vez creada laLAG, puede asociar las conexiones existentes (ya sean independientes o parte de otraLAG) a laLAG.

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 LAG deben usar 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 Gbps en una. LAG Cada conexión de la región se tiene en LAG cuenta para el límite total de conexiones de la región.
- Todas las conexiones de la LAG deben terminar en el mismo AWS Direct Connect punto final.
- LAGsson compatibles con todos los tipos de interfaces virtuales: públicas, privadas y de tránsito.

Al crear unaLAG, puede descargar la carta de autorización y la asignación de la instalación de conexión (LOA-CFA) para una nueva conexión física de forma individual desde la consola. AWS Direct Connect Para obtener más información, consulte Carta de autorización y asignación de la instalación de conexión (LOA-CFA).

Todas LAGs tienen un atributo que determina el número mínimo de conexiones LAG que deben estar operativas para que la LAG propia esté operativa. De forma predeterminada, los nuevos LAGs tienen este atributo establecido en 0. Puede actualizarlo LAG para especificar un valor diferente; si el número de conexiones operativas cae por debajo de este LAG umbral, todas sus conexiones dejarán de estar operativas. Este atributo se puede utilizar para evitar la utilización excesiva de las otras conexiones.

Todas las conexiones de un LAG funcionan en modo activo/activo.

> **Note**
>
> Al crear LAG o asociar más conexiones a élLAG, es posible que no podamos garantizar que haya suficientes puertos disponibles en un punto final determinado AWS Direct Connect .

Temas

- Asociar una conexión LAG a un AWS Direct Connect punto final
- Desasociar una conexión de un LAG punto final AWS Direct Connect
- Asociar un MACsecCKN/CAKa un AWS Direct Connect punto final LAG
- Eliminar la asociación entre una clave MACsec secreta y un AWS Direct Connect punto final LAG
- Eliminar un AWS Direct Connect punto final LAG

MACsecconsideraciones para AWS Direct Connect

Tenga en cuenta lo siguiente cuando desee configurar MACsec enLAGs:

- Al crear una LAG a partir de conexiones existentes, desasociamos todas las MACsec claves de las conexiones. A continuaciónLAG, añadimos las conexiones a y asociamos la LAG MACsec clave a las conexiones.
- Al asociar una conexión existente aLAG, las MACsec claves que están asociadas actualmente a la conexión LAG se asocian a la conexión. Por lo tanto, desasociamos las MACsec claves de la conexión, añadimos la conexión a la yLAG, a continuación, asociamos la LAG MACsec clave a la conexión.

Crear un LAG en un AWS Direct Connect punto final

Puede crear una LAG mediante el aprovisionamiento de nuevas conexiones o la agregación de las conexiones existentes.

No puede crear una LAG con conexiones nuevas si, por lo tanto, supera el límite total de conexiones de la región.

Para crear una a LAG partir de conexiones existentes, las conexiones deben estar en el mismo AWS dispositivo (terminar en el mismo AWS Direct Connect punto final). También deben utilizar el mismo ancho de banda. No se puede migrar una conexión desde una existente LAG si, al eliminarla, la conexión original LAG queda por debajo de su configuración de número mínimo de conexiones operativas.

> **Important**
>
> En el caso de las conexiones existentes, la conectividad a AWS se interrumpe durante la creación delLAG.

Para crear una LAG con nuevas conexiones

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija. LAGs
3. Elija Crear LAG.
4. En Lag creation type (Tipo de creación de LAG), elija Request new connections (Solicitar conexiones nuevas) y proporcione la información siguiente:
   - LAGnombre: un nombre paraLAG.
   - Ubicación: La ubicación delLAG.
   - Port speed (Velocidad del puerto): la velocidad del puerto para las conexiones.
   - Number of new connections (Número de conexiones nuevas): el número de conexiones nuevas que se van a crear. Puede tener un máximo de cuatro conexiones cuando la velocidad del puerto es de 1 G o 10 G, o dos cuando la velocidad del puerto es de 100 Gbps o 400 Gbps.
   - (Opcional) Configure la MAC seguridad (MACsec) para la conexión. En Configuración adicional, selecciona Solicitar un puerto MACsec compatible.

     MACsecsolo está 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. Selecciona Crear LAG.

Para crear una a LAG partir de conexiones existentes

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija. LAGs
3. Elija Crear LAG.

4. En Lag creation type (Tipo de creación de LAG), elija Use existing connections (Usar conexiones existentes) y proporcione la información siguiente:
   - LAGnombre: un nombre paraLAG.
   - Conexiones existentes: la conexión Direct Connect que se utilizará paraLAG.
   - (Opcional) Número de conexiones nuevas: el número de conexiones nuevas que se van a crear. Puede tener un máximo de cuatro conexiones cuando la velocidad del puerto es de 1 G o 10 G, o dos cuando la velocidad del puerto es de 100 Gbps o 400 Gbps.
   - Enlaces mínimos: el número mínimo de conexiones que deben estar operativas para que el LAG propio servidor esté operativo. Si no especifica un valor, se asignará el valor predeterminado (0).
5. (Opcional) Añada o elimine una etiqueta.

   [Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:
   - En Key (Clave), escriba el nombre de la clave.
   - En Valor, escriba el valor de la clave.

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

Para crear una LAG mediante la línea de comandos o API

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

Para describir su LAGs uso de la línea de comandos o API

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

Para descargar elLOA... CFA mediante la línea de comandos o API

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

Después de crear unLAG, puede asociar o desasociar las conexiones del mismo. Para obtener más información, consulte Asociar una conexión a LAG y Desasociar una conexión de a. LAG

Ver LAG detalles en un AWS Direct Connect punto final

Después de crear unaLAG, puede ver sus detalles mediante la AWS Direct Connect consola o mediante la línea de comandos oAPI.

Para ver la información de sus LAG

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija. LAGs
3. Seleccione LAG y elija Ver detalles.
4. Puede ver información sobre el LAG AWS Direct Connect punto final en el que terminan las conexiones, incluido su ID.

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

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

Actualizar un LAG en un AWS Direct Connect punto final

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

- El nombre delLAG.
- El valor del número mínimo de conexiones que deben estar operativas para que el LAG propio dispositivo esté operativo.
- LAGEs el modo MACsec de cifrado.

  MACsecsolo está disponible en conexiones dedicadas.

  AWS asigna este valor a cada conexión que forma parte deLAG.

  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 valor umbral para el número mínimo de conexiones operativas, asegúrese de que el nuevo valor no provoque que caigan por debajo del umbral y dejen de funcionar. LAG

Para actualizar un LAG

1. Abra la AWS Direct Connectconsola en la versión 2/homehttps://console.aws.amazon.com/directconnect/.
2. En el panel de navegación, elija. LAGs
3. Seleccione yLAG, a continuación, elija Editar.
4. Modifique el LAG

   [Cambiar el nombre] En LAGNombre, introduzca un LAG nombre nuevo.

   [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. Seleccione Editar LAG.

Para actualizar un LAG mediante la línea de comandos o API

- update-lag (AWS CLI)
- UpdateLag (AWS Direct Connect API)

Asociar una conexión LAG a un AWS Direct Connect punto final

Puede asociar una conexión existente a una LAG mediante la AWS Direct Connect consola o mediante la línea de comandos oAPI. La conexión puede ser independiente o puede formar parte de otraLAG. La conexión debe estar en el mismo AWS dispositivo y debe utilizar el mismo ancho de banda que elLAG. Si la conexión ya está asociada a otraLAG, no podrá volver a asociarla si, al eliminar la conexión, la conexión original LAG queda por debajo del límite mínimo de conexiones operativas.

Al asociar una conexión a una, LAG se vuelven a asociar automáticamente sus interfaces virtuales a. LAG

> **Important**
>
> La conectividad a AWS través de la conexión se interrumpe durante la asociación.

Para asociar una conexión a un LAG

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija. LAGs
3. Seleccione yLAG, a continuación, elija Ver detalles.
4. En Connections (Conexiones), elija Associate connection (Asociar conexión).
5. En Conexión, elija la conexión Direct Connect que se va a utilizar paraLAG.
6. Elija Associate Connection (Asociar conexión).

Para asociar una conexión mediante la línea de comandos o API

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

Desasociar una conexión de un LAG punto final AWS Direct Connect

Convierta una conexión en independiente desasociándola de una LAG mediante la AWS Direct Connect consola o la línea de comandos o. API No puedes desasociar una conexión si esto hace que caiga por debajo de su umbral para el número mínimo de conexiones operativas. LAG

Al desasociar una conexión de una, LAG no se desasocia automáticamente ninguna interfaz virtual.

> **Important**
>
> La conexión a AWS se interrumpe durante la disociación.

Para desasociar una conexión de un LAG

1. Abra la AWS Direct Connectconsola en la versión 2/homehttps://console.aws.amazon.com/directconnect/.
2. En el panel de la izquierda, elija LAGs.
3. Seleccione yLAG, 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 API

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

Asociar un MACsecCKN/CAKa un AWS Direct Connect punto final LAG

Después de crear la LAG que sea compatibleMACsec, puede asociar unaCKN/CAKa la conexión mediante la AWS Direct Connect consola o mediante la línea de comandos oAPI.

> **Note**
>
> No puede modificar una clave MACsec secreta después de asociarla aLAG. 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 “Elimine la asociación entre una clave MACsec secreta y un LAG”.

Para asociar una MACsec clave a un LAG

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija. LAGs
3. Seleccione LAG y elija Ver detalles.
4. Elija Asociar clave.
5. Introduzca la MACsec clave.

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

   - Para la clave de asociación de conectividad (CAK), introduzca laCAK.
   - Para el nombre de la clave de asociación de conectividad (CKN), introduzca elCKN.

   [Use el secreto] Elija el secreto del administrador de secretos existente y, a continuación, en Secreto, seleccione la clave MACsec secreta.
6. Elija Asociar clave.

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

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

Eliminar la asociación entre una clave MACsec secreta y un AWS Direct Connect punto final LAG

Puede eliminar la asociación entre la clave LAG y la MACsec tecla mediante la AWS Direct Connect consola o la línea de comandos oAPI.

Para eliminar una asociación entre una LAG y una MACsec tecla

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija. LAGs
3. Seleccione LAG y elija Ver detalles.
4. Seleccione el MACsec secreto que desee eliminar y, a continuación, elija Desasociar la clave.
5. En el cuadro de diálogo de confirmación, ingrese disociar y, a continuación, elija Desasociar.

Para eliminar una asociación entre una LAG y una MACsec tecla mediante la línea de comandos o API

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

Eliminar un AWS Direct Connect punto final LAG

Si ya no los necesitaLAGs, puede eliminarlos. No puede eliminar una LAG si tiene interfaces virtuales asociadas. Primero debe eliminar las interfaces virtuales o asociarlas a una conexión LAG OR diferente. Al eliminar una, LAG no se eliminan las conexiones de laLAG; debe eliminarlas usted mismo. Para obtener más información, consulte Eliminar una conexión.

Puede eliminar una LAG mediante la AWS Direct Connect consola o mediante la línea de comandos oAPI.

Para eliminar un LAG

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija. LAGs

3. Seleccione yLAGs, a continuación, elija Eliminar.
4. En el cuadro de diálogo de confirmación, elija Eliminar.

Para eliminar un LAG mediante la línea de comandos o API

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

AWS Direct Connect pasarelas

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

- Gateways de Direct Connect

  Con una puerta de enlace Direct Connect, puede asociar la puerta de enlace Direct Connect a una puerta de enlace de tránsito con múltiples conexiones VPCs o a una puerta de enlace privada virtual.

- Asociaciones de la gateway privada virtual

  Con una puerta de enlace privada virtual, puede asociar la puerta de enlace de Direct Connect a través de una interfaz virtual privada a una o más VPCs cuentas ubicadas en la misma región o en regiones diferentes.

- Asociaciones de la puerta de enlace de tránsito

  Use una puerta de enlace Direct Connect para conectar su conexión de Direct Connect a través de una interfaz virtual de tránsito a la puerta de enlace de tránsito VPCs o VPNs que esté conectada a su puerta de enlace de tránsito.

- Interacciones de prefijos permitidos

  Usa los prefijos permitidos para interactuar con las pasarelas de tránsito y las pasarelas privadas virtuales.

AWS Direct Connect pasarelas

Utilice la AWS Direct Connect puerta de enlace para conectar suVPCs. Puede asociar una puerta de enlace de AWS Direct Connect con cualquiera de las siguientes puertas de enlace:

- Una pasarela de tránsito cuando tienes varias VPCs en la misma región
- Una gateway privada virtual

También puede utilizar una puerta de enlace privada virtual para ampliar su zona local. Esta configuración permite que los VPC asociados a la zona local se conecten 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 Acceder a las Zonas Locales mediante una puerta de enlace Direct Connect en la Guía del VPC usuario de Amazon.

Una gateway de Direct Connect es un recurso disponible en todo el mundo. Puede conectarse a cualquier región del mundo mediante una puerta de enlace de Direct Connect. Esto incluye AWS GovCloud (US) , pero no incluye, las regiones de AWS China.

Los clientes que utilicen Direct Connect y VPCs que actualmente omitan una zona de disponibilidad principal no podrán migrar sus conexiones de Direct Connect ni sus interfaces virtuales.

A continuación se describen escenarios en los que puede utilizar una puerta de enlace de Direct Connect.

Una gateway de Direct Connect no permite que las asociaciones de gateway que se encuentran en la misma gateway de Direct Connect se envíen tráfico entre sí (por ejemplo, una gateway privada virtual a otra gateway privada virtual). Una excepción a esta regla, implementada en noviembre de 2021, es cuando se anuncia una superred en dos o másVPCs, que tienen sus puertas de enlace privadas virtuales adjuntas (VGWs) asociadas a la misma puerta de enlace de Direct Connect y en la misma interfaz virtual. En este caso, VPCs pueden comunicarse entre sí a través del punto final 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 la conectada VPCs 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, es decir, desde la red local, pueden comunicarse entre sí. VPCs

Si desea bloquear la VPC comunicación VPC entre direcciones dentro de una puerta de enlace de Direct Connect, haga lo siguiente:

1. Configure grupos de seguridad en las instancias y otros recursos que desee VPC bloquear el tráfico entre ellas VPCs y utilícelos también como parte del grupo de seguridad predeterminado de laVPC.
2. Evite anunciar una superred desde su red local que se superponga a la suya. VPCs En su lugar, puede anunciar rutas más específicas desde su red local que no se superpongan con la suya. VPCs
3. Aprovisione una sola puerta de enlace de Direct Connect para cada una de las VPC que desee conectarse a la red local en lugar de utilizar la misma puerta de enlace de Direct Connect para variasVPCs. Por ejemplo, en lugar de utilizar una sola puerta de enlace de Direct Connect para el desarrollo y la producciónVPCs, utilice puertas de enlace de Direct Connect independientes para cada una de ellasVPCs.

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 puertas de enlace VPCs conectadas a tránsito asociadas a la misma puerta de enlace de Direct Connect, VPCs podrían comunicarse. Para evitar que se VPCs comuniquen, asocie una tabla de rutas a los VPC archivos adjuntos que tengan configurada la opción de agujero negro.

Temas

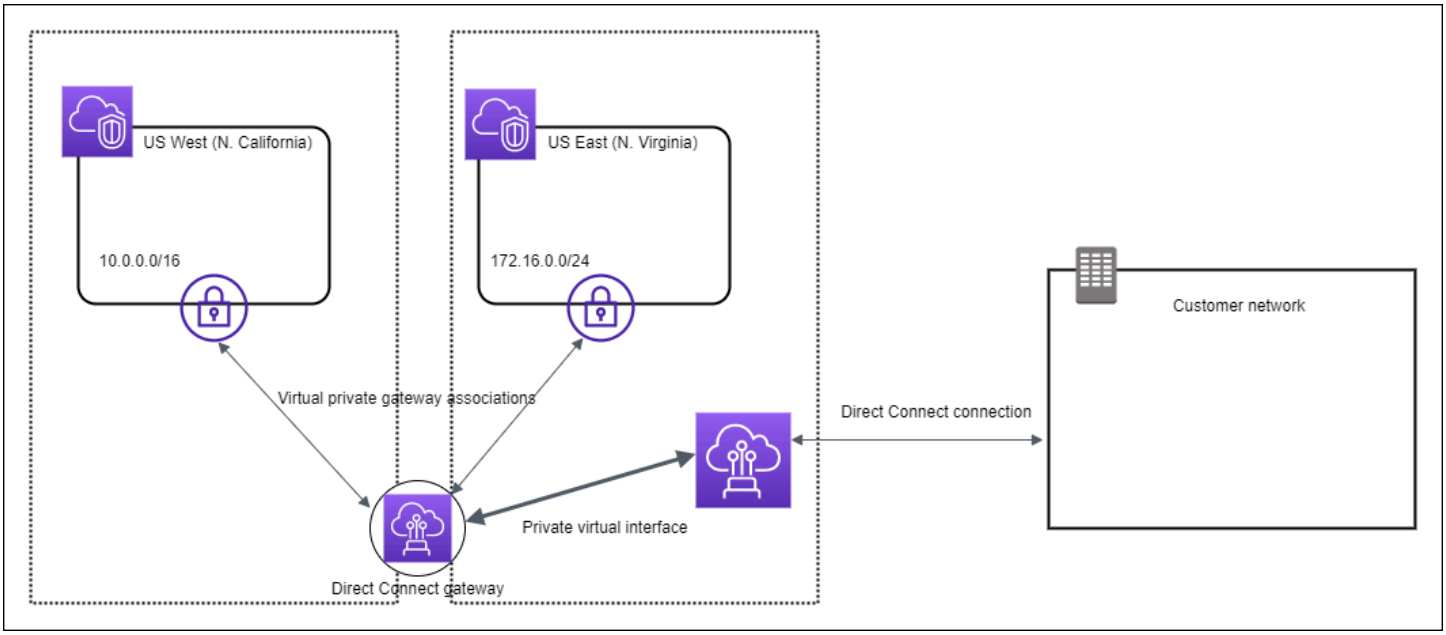
Escenarios

A continuación se describen solo algunos escenarios para usar las puertas de enlace Direct Connect.

Escenario: asociaciones de pasarelas privadas virtuales

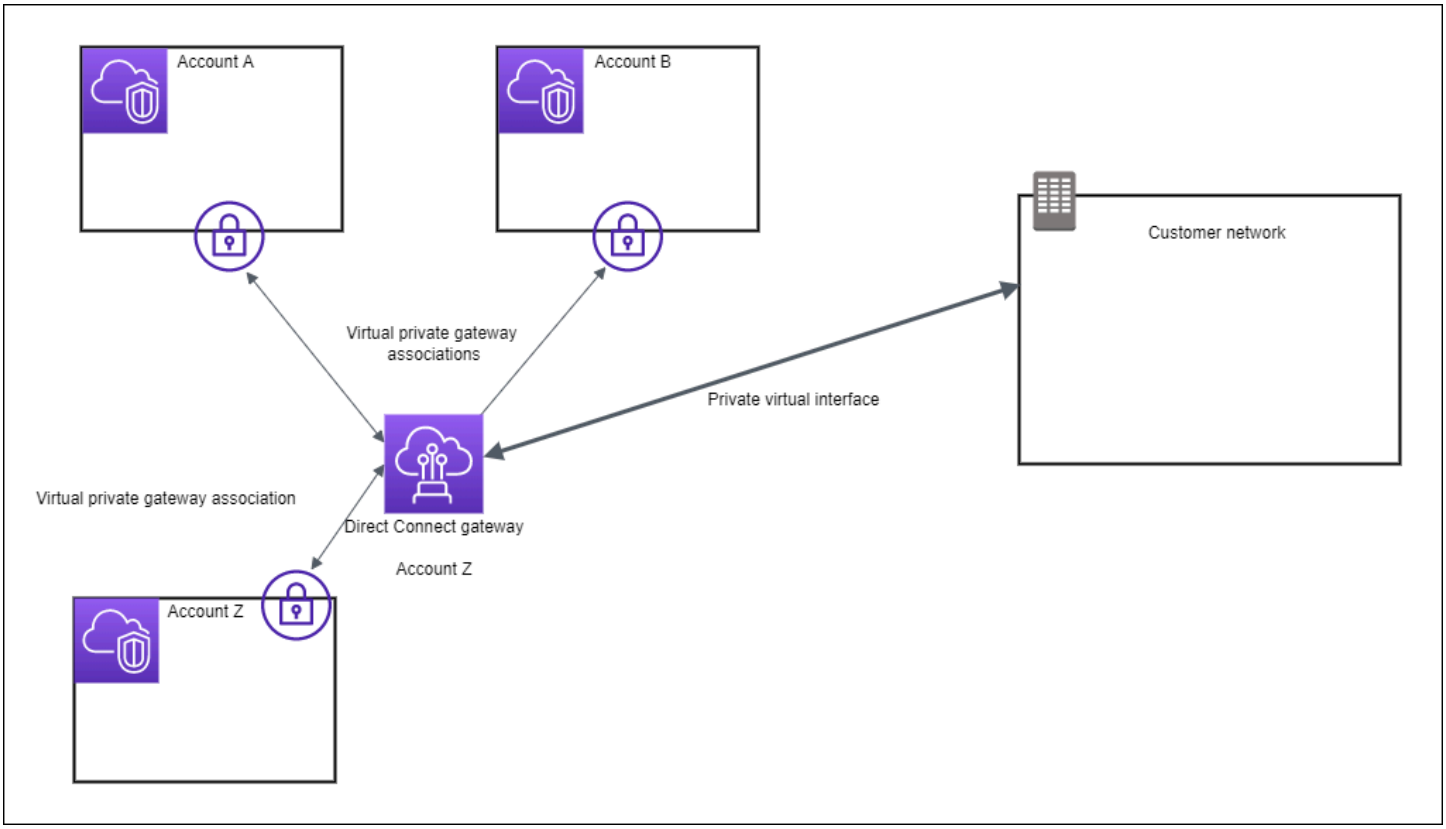
En el siguiente diagrama, la puerta de enlace Direct Connect le permite usar su AWS Direct Connect conexión en la región EE.UU. Este (Norte de Virginia) para acceder VPCs a su cuenta en las regiones EE.UU. Este (Norte de Virginia) y EE.UU. Oeste (Norte de California).

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



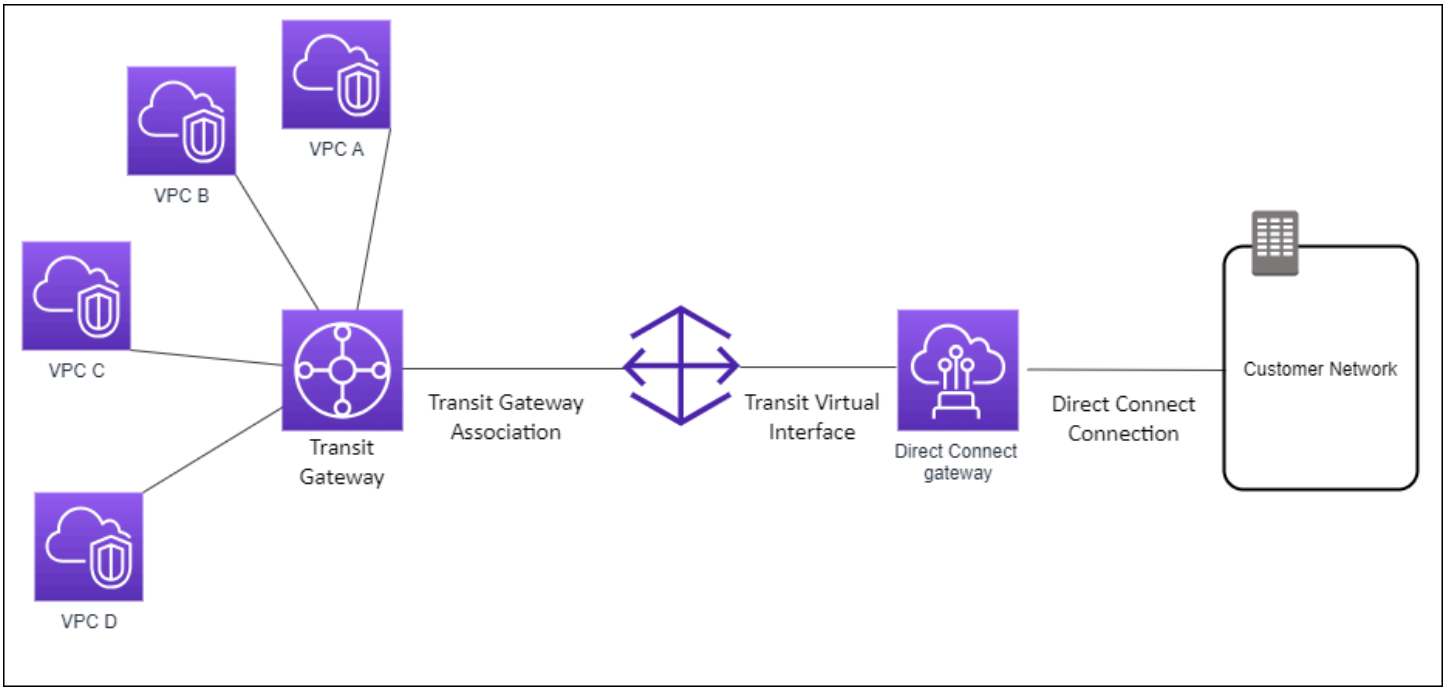
Escenario: asociaciones de pasarelas privadas virtuales entre cuentas

Considere este escenario en el que el propietario de una gateway de Direct Connect es la cuenta Z (account Z). Las cuentas A y B desean utilizar la gateway de Direct Connect. Las cuentas A y B envían sus respectivas propuestas de asociación a la cuenta Z. La cuenta Z acepta las propuestas de asociación y, si lo desea, puede actualizar los prefijos permitidos desde la gateway privada virtual de la cuenta A o desde la gateway privada virtual de la cuenta B. Cuando la cuenta Z acepta las propuestas, la cuenta A y la cuenta B pueden dirigir tráfico desde su gateway privada virtual a la gateway de Direct Connect. La cuenta Z también es propietaria del direccionamiento a los clientes, ya que la cuenta Z es la propietaria de la gateway.



Escenario: asociaciones de pasarelas de tránsito

El siguiente diagrama ilustra cómo la puerta de enlace Direct Connect le permite crear una única conexión a su conexión Direct Connect que todos VPCs pueden usar.



La solución implica los siguientes componentes:

- Una pasarela de tránsito que tiene VPC archivos adjuntos.
- Una gateway de Direct Connect.
- Una asociación entre la gateway de Direct Connect y la gateway de tránsito.
- Una interfaz virtual de tránsito vinculada a la gateway de Direct Connect.

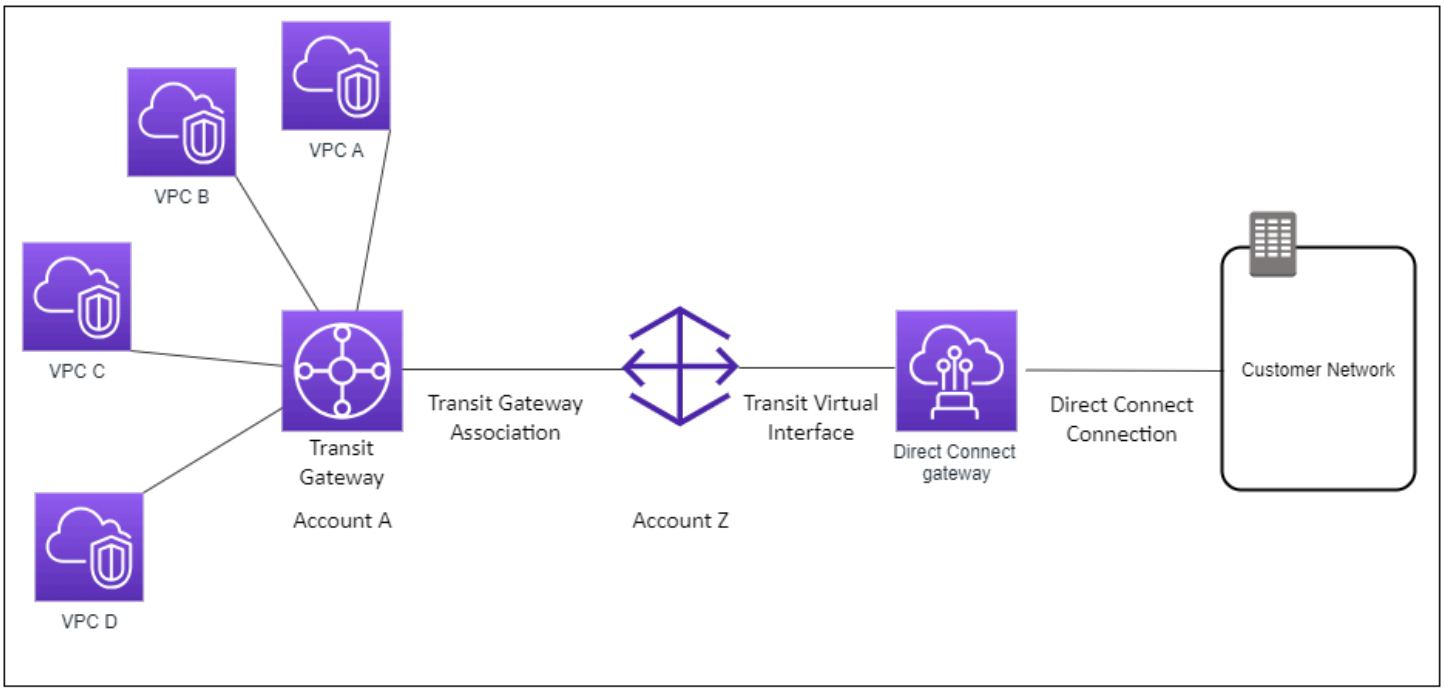
Esta configuración ofrece los siguientes beneficios. Puede hacer lo siguiente:

- Administre una sola conexión para varias VPCs o VPNs que estén en la misma región.
- Anuncie prefijos desde las instalaciones locales hacia AWS y desde AWS las instalaciones locales.

Para obtener información sobre la configuración de las pasarelas de tránsito, consulte Cómo trabajar con pasarelas de tránsito en la Guía de pasarelas de VPC tránsito de Amazon.

Escenario: asociaciones de pasarelas de tránsito entre cuentas

Considere este escenario en el que el propietario de una gateway de Direct Connect es la cuenta Z (account Z). La cuenta A posee la puerta de enlace de tránsito y desea utilizar la puerta de enlace de Direct Connect. La cuenta Z acepta las propuestas de asociación y puede actualizar de forma opcional los prefijos permitidos de la puerta de enlace de tránsito de la cuenta A. Una vez que la cuenta Z acepte las propuestas, el dispositivo VPCs adjunto a la puerta de enlace de tránsito puede enrutar el tráfico desde la puerta de enlace de tránsito a la puerta de enlace Direct Connect. La cuenta Z también es propietaria del direccionamiento a los clientes, ya que la cuenta Z es la propietaria de la gateway.



Crear una AWS Direct Connect puerta de enlace

Puede crear una puerta de enlace Direct Connect en cualquier región compatible mediante la AWS Direct Connect consola o la línea de comandos oAPI.

Para crear una gateway de Direct Connect

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Direct Connect Gateways.
3. Elija Create Direct Connect gateway (Crear gateway de Direct Connect).
4. Especifique la información siguiente y elija Create Direct Connect gateway (Crear gateway de Direct Connect).
   - Name (Nombre): escriba un nombre que le ayude a identificar la gateway de Direct Connect.
   - Amazon side ASN: especifique ASN el lado Amazon de la BGP sesión. ASNDebe estar en el rango de 64.512 a 65.534 o de 4.200 000 000 a 4.294.967.294.
   - Virtual private gateway (Gateway privada virtual): para asociar una gateway privada virtual, elija la gateway privada virtual.

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

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

Migre de una puerta de enlace privada virtual a una AWS Direct Connect puerta de enlace

Puede migrar una puerta de enlace privada virtual conectada a una interfaz virtual a una puerta de enlace de Direct Connect.

Si utiliza Direct Connect y actualmente VPCs evita una zona de disponibilidad principal, no podrá migrar sus conexiones de Direct Connect ni sus interfaces virtuales.

Los siguientes pasos describen los pasos que debe seguir para migrar una puerta de enlace privada virtual a una puerta de enlace de Direct Connect.

Para migrar a una gateway de Direct Connect

1. Cree una gateway de Direct Connect.

   Si la puerta de enlace Direct Connect aún no existe, tendrá que crearla. Para conocer los pasos para crear una puerta de enlace de Direct Connect, consulteCrear una puerta de enlace Direct Connect.
2. Cree una interfaz virtual para la gateway de Direct Connect.

   Se requiere una interfaz virtual para la migración. Si la interfaz no existe, tendrá que crearla. Para conocer los pasos para crear la interfaz virtual, consulteInterfaces virtuales.
3. Asocie cada gateway privada virtual con la gateway de Direct Connect.

   Tanto la puerta de enlace Direct Connect como una puerta de enlace privada virtual deben estar asociadas. Para conocer los pasos para crear la asociación, consulteAsocie o desasocie las puertas de enlace privadas virtuales.
4. Elimine la interfaz virtual que estaba asociada a la gateway privada virtual. Para obtener más información, consulte Eliminar una interfaz virtual.

Eliminar una AWS Direct Connect puerta de enlace

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

- Para conocer los pasos para desasociar una puerta de enlace privada virtual, consulte. Asocie o desasocie las puertas de enlace privadas virtuales
- Para conocer los pasos para eliminar una interfaz virtual, consulte. Eliminar una interfaz virtual

Para eliminar una gateway de Direct Connect

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Direct Connect Gateways.
3. Seleccione las gateways y elija Delete (Eliminar).

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

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

AWS Direct Connect asociaciones de pasarelas privadas virtuales

Puede usar una AWS Direct Connect puerta de enlace para conectar su AWS Direct Connect conexión a través de una interfaz virtual privada a una o más VPCs cuentas que estén ubicadas en la misma región o en regiones diferentes. Debe asociar una puerta de enlace Direct Connect a la puerta de enlace privada virtual paraVPC. A continuación, crea una interfaz virtual privada para la AWS Direct Connect conexión a la puerta de enlace Direct Connect. Puede adjuntar varias interfaces virtuales privadas a su gateway de Direct Connect.

Las siguientes reglas se aplican a las asociaciones de puerta de enlace privada virtual:

- No habilite la propagación de rutas hasta que haya asociado una puerta de enlace virtual a una puerta de enlace de Direct Connect. Si habilita la propagación de rutas antes de asociar las puertas de enlace, es posible que las rutas se propaguen incorrectamente.
- Existen límites para la creación y el uso de gateways de Direct Connect. Para obtener más información, consulte Cuotas 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.
- El elemento VPCs al que se conecta a través de una puerta de enlace de Direct Connect no puede tener CIDR bloques superpuestos. Si agrega un IPv4 CIDR bloque a uno VPC que está asociado a una puerta de enlace de Direct Connect, asegúrese de que el CIDR bloque no se superponga con un CIDR bloque existente de ningún otro asociadoVPC. Para obtener más información, consulta Cómo añadir IPv4 CIDR bloques a un VPC en la Guía del VPC usuario de Amazon.
- No se puede crear una interfaz virtual pública a una gateway de Direct Connect.
- Una puerta de enlace de Direct Connect solo admite la comunicación entre interfaces virtuales privadas adjuntas y puertas de enlace privadas virtuales asociadas; puede habilitar una puerta de enlace privada virtual a otra puerta de enlace privada. No se admiten los siguientes flujos de tráfico:
  - Comunicación directa entre las VPCs que están asociadas a una única puerta de enlace Direct Connect. Esto incluye el tráfico de uno VPC a otro mediante el uso de una horquilla a través de una red local a través de una única puerta de enlace Direct Connect.
  - Comunicación directa entre las interfaces virtuales que están asociadas a la gateway única de Direct Connect.
  - Comunicación directa entre las interfaces virtuales que están conectadas a una única puerta de enlace de Direct Connect y una VPN conexión de una puerta de enlace privada virtual que está asociada a la misma puerta de enlace de Direct Connect.
- No se puede asociar una gateway privada virtual con más de una gateway de Direct Connect ni tampoco se puede adjuntar una interfaz virtual privada a más de una gateway de Direct Connect.
- Una puerta de enlace privada virtual que asocie a una puerta de enlace de Direct Connect debe estar conectada a unVPC.
- Una propuesta de asociación de gateways privadas virtuales caduca 7 días después de crearla.
- Una propuesta de gateway privada virtual aceptada o eliminada permanece visible durante 3 días.
- Una gateway privada virtual se puede asociar a una gateway de Direct Connect y también se puede asociar a una interfaz virtual.

- Al separar una puerta de enlace privada virtual de una, VPC también se disocia la puerta de enlace privada virtual de una puerta de enlace Direct Connect.

Para conectar su AWS Direct Connect conexión únicamente a una VPC de la misma región, puede crear una puerta de enlace Direct Connect. O bien, puede crear una interfaz virtual privada y adjuntarla a la puerta de enlace privada virtual delVPC. Para obtener más información, consulte Crear una interfaz virtual privada y VPN CloudHub.

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

Temas

Cree una puerta de enlace privada AWS Direct Connect virtual

La puerta de enlace privada virtual debe estar conectada VPC a la que desee conectarse. Puede crear una puerta de enlace privada virtual y conectarla a una VPC mediante la AWS Direct Connect consola o mediante la línea de comandos oAPI.

> **Note**
>
> Si planea usar la puerta de enlace privada virtual para una puerta de enlace Direct Connect y una VPN conexión dinámica, configure la puerta de enlace privada virtual ASN en el valor que necesite para la VPN conexión. De lo contrario, ASN el valor de la puerta de enlace privada virtual se puede establecer en cualquier valor permitido. La puerta de enlace Direct Connect anuncia todas las conexiones a VPCs través de las que tiene ASN asignadas.

Después de crear una puerta de enlace privada virtual, debe adjuntarla a suVPC.

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

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Puertas de enlace privadas virtuales y, a continuación, elija Crear una puerta de enlace privada virtual.
3. (Opcional) Escriba un nombre para la gateway privada virtual. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
4. Para ASN, deja la selección por defecto para usar Amazon por defectoASN. De lo contrario, selecciona Personalizado ASN e introduce un valor. Para un archivo de 16 bitsASN, el valor debe estar en el rango de 64512 a 65534. Para un archivo de 32 bitsASN, el valor debe estar en el rango de 4200000000 a 4294967294.
5. Elija Create Virtual Private Gateway.
6. Seleccione la puerta de enlace privada virtual que creó y, a continuación, elija Acciones, Adjuntar a. VPC
7. Seleccione la suya VPC de la lista y elija Sí, adjuntar.

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

- CreateVpnGateway(EC2Consulta de AmazonAPI)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

Para adjuntar una puerta de enlace privada virtual a una VPC mediante la línea de comandos o API

- AttachVpnGateway(EC2Consulta de AmazonAPI)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (AWS Tools for Windows PowerShell)

Asociar o desasociar puertas de AWS Direct Connect enlace privadas virtuales

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

Para asociar una gateway privada virtual

1. Abra la AWS Direct Connectconsola en la versión 2/homehttps://console.aws.amazon.com/directconnect/.
2. En el panel de navegación, elija Puertas de enlace de Direct Connect y, a continuación, elija la puerta de enlace de Direct Connect.
3. Elija Ver detalles.
4. Elija Asociaciones de puerta de enlace y, a continuación, elija Asociar puerta de enlace.
5. En Gateways, elija las gateways privadas virtuales que desea asociar y, a continuación, elija Associate gateway (Asociar gateway).

Puede ver todas las gateways privadas virtuales que están asociados con la gateway de Direct Connect. Para ello, elija Gateway Associations (Asociaciones de gateways).

Para desasociar una gateway privada virtual

1. Abre la AWS Direct Connectconsola en la v2/home. https://console.aws.amazon.com/directconnect/
2. En el panel de navegación, elija Direct Connect Gateways (Gateways de Direct Connect) y, a continuación, seleccione la gateway de Direct Connect.
3. Elija Ver detalles.
4. Elija Gateway associations (Asociaciones de gateway) y, a continuación, seleccione la gateway privada virtual.
5. Elija Desasociar.

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

- create-direct-connect-gateway-asociación ()AWS CLI

- CreateDirectConnectGatewayAssociation (AWS Direct Connect API)

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

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

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

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

Cree una interfaz virtual privada para la AWS Direct Connect puerta de enlace

Para conectar la AWS Direct Connect conexión al control remotoVPC, debe crear una interfaz virtual privada para la conexión. Especifique la gateway de Direct Connect a la que se va a conectar. Puede crear una interfaz virtual privada mediante la AWS Direct Connect consola o mediante la línea de comandos oAPI.

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

Para provisionar una interfaz virtual privada en una gateway de Direct Connect

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

5. En Configuración de la interfaz virtual privada, realice lo siguiente:

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

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

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

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

   e. Para VLAN, introduzca el número de identificación de su red de área local virtual (VLAN).

   f. BGPASNEn este caso, introduzca el número de sistema autónomo del protocolo Border Gateway del router homólogo local para la nueva interfaz virtual.

      Los valores válidos son 1 a 2147483647.

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

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

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

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

      > **Important**
      >
      > Si permite la AWS asignación automática de IPv4 direcciones, se CIDR asignará un /29 desde IPv4 169.254.0.0/16 Link-Local de acuerdo con 3927 para la conectividad. RFC point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen o destino del tráfico. VPC En su lugar, debe usar RFC 1918 u otra dirección (distinta de RFC 1918) y especificar la dirección usted mismo.
      >
      > - Para obtener más información acerca de RFC 1918, consulte Asignación de direcciones para Internet privadas.

- Para obtener más información acerca de RFC 3927, consulte Configuración dinámica de direcciones locales de IPv4 enlace.

[IPv6] Para configurar un IPv6 BGP par, 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 Jumbo MTU (MTUtamaño 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 API

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

Para ver las interfaces virtuales que están conectadas a una puerta de enlace de Direct Connect mediante la línea de comandos o API

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

Asocie una puerta de enlace privada AWS Direct Connect virtual a todas las cuentas

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

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

Prefijos permitidos

Cuando asocias una puerta de enlace privada virtual a una puerta de enlace de Direct Connect, especificas una lista de VPC prefijos de Amazon para anunciarlos en la puerta de enlace de Direct Connect. La lista de prefijos actúa como un filtro que permite anunciar lo mismo CIDRs o uno menor CIDRs en la puerta de enlace de Direct Connect. Debe establecer los prefijos permitidos en un rango igual o más amplio que el anterior, VPC CIDR ya que los aprovisionamos íntegramente en la puerta de VPC CIDR enlace privada virtual.

Considere el caso en el que VPC CIDR es 10.0.0.0/16. Puede establecer los prefijos permitidos en 10.0.0.0/16 (el valor) o en 10.0.0.0/15 (VPCCIDRun valor más ancho que el). VPC CIDR

Cualquier interfaz virtual incluida en los prefijos de red anunciados a través de Direct Connect solo se propaga a las pasarelas de tránsito de todas las regiones, no dentro de la misma región. Para obtener más información sobre cómo interactúan los prefijos permitidos con las puertas de enlace privadas virtuales y las puertas de enlace de tránsito, consulte Interacciones de prefijos permitidos.

AWS Direct Connect pasarelas y asociaciones de pasarelas de tránsito

Puede usar la AWS Direct Connect puerta de enlace para conectar su conexión Direct Connect a través de una interfaz virtual de tránsito a la puerta de enlace de tránsito VPCs o VPNs que esté conectada a ella. Asocie una puerta de enlace de Direct Connect con la puerta de enlace de tránsito. A continuación, cree una interfaz virtual de tránsito para su AWS Direct Connect conexión a la puerta de enlace Direct Connect.

Las siguientes reglas se aplican a las asociaciones de puerta de enlace de tránsito:

- No puede adjuntar una puerta de enlace de Direct Connect en una puerta de enlace de tránsito cuando la puerta de enlace de Direct Connect ya se encuentra asociada a una puerta de enlace privada virtual o adjunta a una interfaz virtual privada.
- Existen límites para la creación y el uso de gateways de Direct Connect. Para obtener más información, consulte Cuotas de Direct Connect.
- Una puerta de enlace Direct Connect admite la comunicación entre las interfaces virtuales de tránsito conectadas y las puertas de enlace de tránsito asociadas.
- Si se conecta a varias pasarelas de tránsito que se encuentran en diferentes regiones, utilice una única ASNs para cada pasarela de tránsito.
- Cualquier interfaz virtual incluida en los prefijos de red anunciados a través de Direct Connect solo se propaga a las pasarelas de tránsito de todas las regiones, pero no dentro de la misma región

Asociación de una gateway de tránsito entre cuentas

Puede asociar una puerta de enlace Direct Connect existente o una nueva puerta de enlace de Direct Connect a una puerta de enlace de tránsito que sea propiedad de cualquier AWS cuenta. El propietario de la puerta de enlace de tránsito crea una propuesta de asociación y el propietario de la puerta de enlace de Direct Connect debe aceptar la propuesta de asociación.

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

Prefijos permitidos

En el caso de una asociación de puerta de enlace de tránsito, aprovisione la lista de prefijos permitidos de la puerta de enlace de Direct Connect. La lista se usa para enrutar el tráfico desde las instalaciones hasta AWS la puerta de enlace de tránsito, incluso si las personas VPCs conectadas a la puerta de enlace de tránsito no tienen una asignaciónCIDRs. Los prefijos de la lista de prefijos permitidos de la gateway de Direct Connect se originan en la gateway de Direct Connect y se publican en la red local. Para obtener más información sobre cómo interactúan los prefijos permitidos con las pasarelas de tránsito y las pasarelas privadas virtuales, consulte. Interacciones de prefijos permitidos

Temas

- Asociar o desasociar AWS Direct Connect con una pasarela de tránsito

- Cree una interfaz virtual de tránsito para la AWS Direct Connect puerta de enlace
- Cree una pasarela de tránsito y una propuesta AWS Direct Connect de asociación
- Aceptar o rechazar una propuesta de pasarela de tránsito y AWS Direct Connect asociación
- Actualizar los prefijos permitidos para una pasarela de tránsito y AWS Direct Connect una asociación
- Eliminar una propuesta de pasarela de tránsito y AWS Direct Connect asociación

Asociar o desasociar AWS Direct Connect con una pasarela de tránsito

Asocie o desasocie una pasarela de tránsito mediante la AWS Direct Connect consola o la línea de comandos o. API

Para asociar una puerta de enlace de tránsito

1. Abre la AWS Direct Connectconsola en la versión 2/homehttps://console.aws.amazon.com/directconnect/.
2. En el panel de navegación, elija Direct Connect Gateways (Gateways de Direct Connect) y, a continuación, seleccione la gateway de Direct Connect.
3. Elija Ver detalles.
4. Elija Gateway associations (Asociaciones de gateway) y, a continuación, elija Associate gateway (Asociar gateway).
5. En Puertas de enlace, elija la puerta de enlace de tránsito que desee asociar.
6. En Prefijos permitidos, ingrese los prefijos (separados por una coma o en una línea nueva) que la puerta de enlace de Direct Connect anuncia en el centro de datos en las instalaciones. Para obtener más información sobre los prefijos permitidos, consulte Interacciones de prefijos permitidos.
7. Elija Asociar puerta de enlace

Puede ver todas las gateways que están asociadas con la gateway de Direct Connect. Para ello, elija Gateway associations (Asociaciones de gateways).

Desasociación de una puerta de enlace de tránsito

1. Abre la AWS Direct Connectconsola en la v2/home. https://console.aws.amazon.com/directconnect/

2. En el panel de navegación, elija Direct Connect gateways (Gateways de Direct Connect) y, a continuación, seleccione la gateway de Direct Connect.
3. Elija Ver detalles.
4. Elija Gateway associations (Asociaciones de gateway) y, a continuación, seleccione la gateway de tránsito.
5. Elija Desasociar.

Actualización de los prefijos permitidos para una puerta de enlace de tránsito

Puede agregar o eliminar prefijos permitidos en la puerta de enlace de tránsito.

1. Abre la AWS Direct Connectconsola en la v2/home. https://console.aws.amazon.com/directconnect/
2. En el panel de navegación, elija Puertas de enlace de Direct Connect y, a continuación, elija la puerta de enlace de Direct Connect para la que desee agregar o eliminar los prefijos permitidos.
3. Seleccione la pestaña de Asociaciones de puerta de enlace.
4. Elija la puerta de enlace que desee modificar y, a continuación, elija Editar.
5. En Prefijos permitidos, ingrese los prefijos que la puerta de enlace de Direct Connect anuncia en el centro de datos en las instalaciones. En el caso de varios prefijos, separe cada prefijo con una coma o coloque cada prefijo en una línea nueva. Los prefijos que añada deben coincidir con Amazon VPC CIDRs para 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.
7. Elija Desasociar.
8. Vuelva a elegir Desasociar para confirmar que desea desasociar la puerta de enlace.

   En la sección de Asociación de puerta de enlace, el Estado muestra desasociando. Al finalizar, aparece un mensaje de confirmación y la puerta de enlace se elimina de la sección. Esto puede tardar varios minutos o más tiempo en completarse.

Para asociar una pasarela de tránsito mediante la línea de comandos o API

- create-direct-connect-gateway-asociación ()AWS CLI

- CreateDirectConnectGatewayAssociation (AWS Direct Connect API)

Para ver las puertas de enlace de tránsito asociadas a una puerta de enlace de Direct Connect mediante la línea de comandos o API

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

Para desasociar una pasarela de tránsito mediante la línea de comandos o API

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

Para actualizar los prefijos permitidos para una pasarela de tránsito mediante la línea de comandos o API

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

Cree una interfaz virtual de tránsito para la AWS Direct Connect puerta de enlace

Para conectar su AWS Direct Connect conexión a la pasarela de tránsito, debe crear una interfaz de tránsito para su conexión. Especifique la gateway de Direct Connect a la que se va a conectar. Puede usar la AWS Direct Connect consola o la línea de comandos oAPI.

> **Important**
>
> Si asocias tu pasarela de transporte a una o más pasarelas de Direct Connect, el número de sistema autónomo (ASN) utilizado por la pasarela de transporte y la pasarela de Direct Connect deben ser diferentes. Por ejemplo, si usa el ASN 64512 predeterminado tanto para la puerta de enlace de tránsito como para la puerta de enlace Direct Connect, se produce un error en la solicitud de asociación.

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

1. Abre la AWS Direct Connectconsola en la versión 2/homehttps://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 Transit (Tránsito).
5. En Transit virtual interface settings (Configuración de la interfaz virtual de tránsito), haga lo siguiente:

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

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

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

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

   e. Para VLAN, introduzca el número de identificación de su red de área local virtual (VLAN).

   f. Para BGPASNello, introduzca el número de sistema autónomo del protocolo Border Gateway del router homólogo local para la nueva interfaz virtual.

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

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

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

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

> **Important**
>
> Si permite la AWS asignación automática de IPv4 direcciones, se CIDR asignará un /29 desde IPv4 169.254.0.0/16 Link-Local de acuerdo con 3927 para la conectividad. RFC point-to-point AWS no recomienda esta opción si pretende utilizar la dirección IP homóloga del router del cliente como origen o destino del tráfico. VPC En su lugar, debe usar RFC 1918 u otra dirección (distinta de RFC 1918) y especificar la dirección usted mismo.
>
> - Para obtener más información acerca de RFC 1918, consulte Asignación de direcciones para Internet privadas.
> - Para obtener más información acerca de RFC 3927, consulte Configuración dinámica de direcciones locales de IPv4 enlace.

[IPv6] Para configurar un IPv6 BGP par, 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 8500 (tramas gigantes), seleccione Jumbo MTU (MTUtamaño 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 API

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

Para ver las interfaces virtuales que están conectadas a una puerta de enlace de Direct Connect mediante la línea de comandos o API

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

Cree una pasarela de tránsito y una propuesta AWS Direct Connect de asociación

Si es el propietario de la puerta de enlace de tránsito, debe crear la propuesta de asociación. La pasarela de transporte público debe estar asociada a una VPC o VPN en tu AWS cuenta. El propietario de la puerta de enlace de Direct Connect debe compartir el ID de la puerta de enlace de Direct Connect y el ID de su cuenta de AWS . Después de crear la propuesta, el propietario de la gateway de Direct Connect debe aceptarla, para que usted pueda tener acceso a la red local a través de AWS Direct Connect. Puede crear una propuesta de asociación mediante la AWS Direct Connect consola o mediante la línea de comandos oAPI.

Para crear una propuesta de asociación

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Puertas de enlace de tránsito y, a continuación, seleccione la puerta de enlace de tránsito.
3. Elija Ver detalles.
4. Elija Direct Connect gateway associations (Asociaciones de gateways de Direct Connect) y, a continuación, elija Associate Direct Connect gateway (Asociar gateway de Direct Connect).
5. En Association account type (Tipo de cuenta para la asociación), en Account owner (Propietario de la cuenta), elija Another account (Otra cuenta).
6. En Propietario de la puerta de enlace de Direct Connect, ingrese el ID de la cuenta a la que pertenece la puerta de enlace de Direct Connect.

7. En Association settings (Configuración de la asociación), haga lo siguiente:
   a. En Direct Connect gateway ID (ID de la gateway de Direct Connect), escriba el ID de la gateway de Direct Connect.
   b. En Propietario de la interfaz virtual, ingrese el ID de la cuenta a la que pertenece la interfaz virtual para la asociación.
   c. (Opcional) Para especificar una lista de los prefijos que se permitirán desde la puerta de enlace de tránsito, agregue los prefijos a Prefijos permitidos utilizando comas a fin de separarlos o introduciéndolos en diferentes líneas.
8. Elija Associate Direct Connect gateway (Asociar gateway de Direct Connect).

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

- create-direct-connect-gateway-propuesta de asociación ()AWS CLI
- CreateDirectConnectGatewayAssociationProposal (AWS Direct Connect API)

Aceptar o rechazar una propuesta de pasarela de tránsito y AWS Direct Connect asociación

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

Para aceptar una propuesta de asociación

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Direct Connect gateways (Gateways de Direct Connect).
3. Seleccione la gateway de Direct Connect que tiene propuestas pendientes y, a continuación, elija View details (Ver detalles).
4. En la pestaña Pending proposals (Propuestas pendientes), seleccione la propuesta y, a continuación, elija Accept proposal (Aceptar propuesta).

5. (Opcional) Para especificar una lista de los prefijos que se permitirán desde la puerta de enlace de tránsito, agregue los prefijos a Prefijos permitidos utilizando comas para separarlos o introduciéndolos en diferentes líneas.
6. Elija Accept proposal (Aceptar propuesta).

Para rechazar una propuesta de asociación

1. Abre la AWS Direct Connectconsola en la v2/home. https://console.aws.amazon.com/directconnect/
2. En el panel de navegación, elija Direct Connect gateways (Gateways de Direct Connect).
3. Seleccione la gateway de Direct Connect que tiene propuestas pendientes y, a continuación, elija View details (Ver detalles).
4. En la pestaña Pending proposals (Propuestas pendientes), seleccione la gateway de tránsito y, a continuación, elija Reject proposal (Rechazar propuesta).
5. En el cuadro de diálogo Reject proposal (Rechazar propuesta), escriba Delete y, a continuación, elija Reject proposal (Rechazar propuesta).

Para ver las propuestas de asociación mediante la línea de comandos o API

- describe-direct-connect-gateway-propuestas de asociación ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposals (AWS Direct Connect API)

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

- accept-direct-connect-gateway-propuesta de asociación ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposal (AWS Direct Connect API)

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

- delete-direct-connect-gateway-propuesta de asociación ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal (AWS Direct Connect API)

Actualizar los prefijos permitidos para una pasarela de tránsito y AWS Direct Connect una asociación

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

- Si eres el propietario de la puerta de enlace de tránsito, tendrás que crear una nueva propuesta de asociación para esa puerta de enlace de Direct Connect, especificando los prefijos que deseas permitir. Para conocer los pasos para crear una nueva propuesta de asociación, consulteCree una propuesta de asociación de pasarelas de tránsito.
- Si es el propietario de la puerta de enlace Direct Connect, puede actualizar los prefijos permitidos al aceptar la propuesta de asociación o si actualiza los prefijos permitidos para una asociación existente. Para conocer los pasos para actualizar los prefijos permitidos al aceptar la asociación, consulte. Acepte o rechace una propuesta de asociación de pasarelas de tránsito

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

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

Eliminar una propuesta de pasarela de tránsito y AWS Direct Connect asociación

El propietario de la puerta de enlace de tránsito puede eliminar la propuesta de asociación de la puerta de enlace de Direct Connect si todavía se encuentra pendiente de aceptación. Una vez aceptada una propuesta de asociación, no es posible eliminarla, pero se puede desasociar la gateway de tránsito de la gateway de Direct Connect. Para obtener más información, consulte Cree una propuesta de asociación de pasarelas de tránsito.

Puede eliminar una propuesta de asociación entre una pasarela de tránsito y Direct Connect mediante la AWS Direct Connect consola o la línea de comandos oAPI.

Para eliminar una propuesta de asociación

1. Abra la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Puertas de enlace de tránsito y, a continuación, seleccione la puerta de enlace de tránsito.
3. Elija Ver detalles.
4. Elija Pending gateway associations (Asociaciones pendientes de la gateway), seleccione la asociación y, a continuación, elija Delete association (Eliminar asociación).
5. En el cuadro de diálogo Delete association proposal (Eliminar propuesta de asociación), escriba Delete y, a continuación, elija Delete (Eliminar).

Para eliminar una propuesta de asociación pendiente mediante la línea de comandos o API

- delete-direct-connect-gateway-asociación-propuesta ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal (AWS Direct Connect API)

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

Aprenda cómo los prefijos permitidos interactúan con las pasarelas de tránsito y las pasarelas privadas virtuales. Para obtener más información, consulte Políticas y BGP comunidades de enrutamiento.

Asociaciones de la gateway privada virtual

La lista de prefijos (IPv4yIPv6) actúa como un filtro que permite anunciar lo mismo CIDRs o un rango menor en la puerta de CIDRs enlace de Direct Connect. Debe establecer los prefijos en un rango igual o más amplio que el bloque. VPC CIDR

> **Note**
>
> La lista de permitidos solo funciona como filtro y solo la asociada se VPC CIDR anunciará en la pasarela de clientes.

Considere el escenario en el que un VPC CIDR 10.0.0.0/16 está conectado 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 el tráfico que utiliza ese prefijo.

Asociaciones de la puerta de enlace de tránsito

En el caso de una asociación de puerta de enlace de tránsito, aprovisione la lista de prefijos permitidos de la puerta de enlace de Direct Connect. La lista enruta el tráfico local hacia o desde una puerta de enlace de Direct Connect a la puerta de enlace de tránsito, incluso cuando las personas VPCs conectadas a la puerta de enlace de tránsito no tienen una asignaciónCIDRs. 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 de la puerta de enlace Direct ConnectASN.
- En el caso de las pasarelas privadas virtuales, los prefijos permitidos introducidos actúan como un filtro para permitir que los prefijos sean iguales o menores. CIDRs

Considere el escenario en el que tiene un CIDR 10.0.0.0/16 VPC conectado a una puerta de enlace de tránsito.

- Si la lista de prefijos permitidos se establece en 22.0.0.0/24, recibirá el 22.0.0.0/24 a través de su interfaz virtual de tránsito. BGP No recibe 10.0.0.0/16 porque aprovisionamos directamente los prefijos que se encuentran en la lista de prefijos permitidos.
- Si la lista de prefijos permitidos se establece en 10.0.0.0/24, recibirá 10.0.0.0/24 a través de su interfaz virtual de tránsito. BGP No recibe 10.0.0.0/16 porque aprovisionamos directamente los prefijos que se encuentran en la lista de prefijos permitidos.

- Si la lista de prefijos permitidos se establece en 10.0.0.0/8, recibirá 10.0.0.0/8 a través de su interfaz virtual de tránsito. BGP

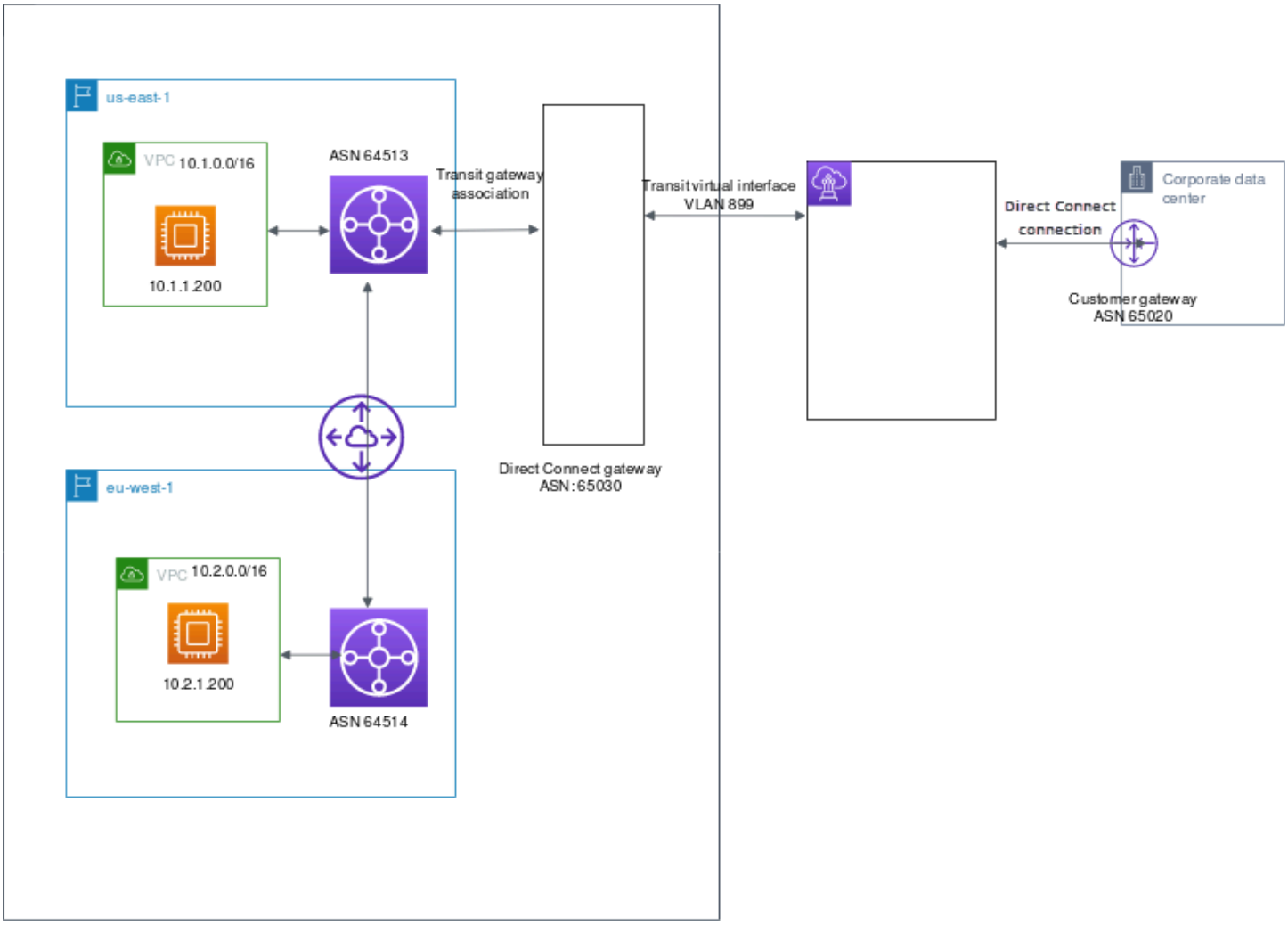
No se permiten las superposiciones de prefijos permitidos cuando hay varias puertas de enlace de tránsito asociadas a una puerta de enlace de Direct Connect. Por ejemplo, si tiene una puerta de enlace de tránsito con una lista de prefijos permitidos que incluye 10.1.0.0/16 y una segunda puerta de enlace 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. Dado que 0.0.0.0/0 incluye todas IPv4 las redes, no puede configurar 0.0.0.0/0 si hay varias puertas de enlace de tránsito asociadas a una puerta de enlace de Direct Connect. Se devuelve un error que indica que las rutas permitidas se superponen a una o más rutas permitidas existentes en la puerta de enlace de Direct Connect.

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

Ejemplo: Prefijos permitidos en una configuración de puerta de enlace de tránsito

Considere la configuración en la que tiene instancias en dos AWS regiones diferentes que necesitan acceder al centro de datos corporativo. Puede utilizar los siguientes recursos para esta configuración:

- Una puerta de enlace de tránsito en cada región.
- Una conexión de intercambio de tráfico de puerta de enlace de tránsito.
- Una puerta de enlace de Direct Connect.
- Una asociación de puerta de enlace de tránsito entre una de las puertas de enlace de tránsito (la de us-east-1) y la puerta de enlace de Direct Connect.
- Una interfaz virtual de tránsito desde la ubicación en las instalaciones y la ubicación de AWS Direct Connect .



Configure las siguientes opciones para los recursos.

- Puerta de enlace Direct Connect: establezca el ASN valor para 65030. Para obtener más información, consulte Crear una puerta de enlace Direct Connect.
- Interfaz virtual de tránsito: establezca el en VLAN 899 y el ASN en 65020. Para obtener más información, consulte Crear una interfaz virtual de tránsito en la puerta de enlace de Direct Connect.
- Asociación de la puerta de enlace de Direct Connect con la puerta de enlace de tránsito: establezca los prefijos permitidos en 10.0.0.0/8.

  Este CIDR bloque cubre ambos VPC CIDR bloques. Para obtener más información, consulte Asocie o desasocie una pasarela de tránsito con Direct Connect..
- VPCruta: para enrutar el tráfico desde la versión 10.2.0.0VPC, cree una ruta en la tabla de VPC rutas que tenga el destino 0.0.0.0/0 y el ID de la puerta de enlace de tránsito como destino. Para

obtener más información sobre el enrutamiento a una puerta de enlace de tránsito, consulta Enrutamiento para una puerta de enlace de tránsito en la Guía del VPC usuario de Amazon.

Etiquetar AWS Direct Connect recursos

Una etiqueta es una etiqueta que el propietario de un recurso asigna a sus AWS Direct Connect recursos. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario. Las etiquetas permiten al propietario del recurso clasificar AWS Direct Connect los recursos de diferentes maneras, por ejemplo, por propósito 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, tiene dos AWS Direct Connect conexiones en una región, cada una en ubicaciones diferentes. La conexión `dxcon-11aa22bb` es una conexión que sirve tráfico de producción y que está asociada a la interfaz virtual `dxvif-33cc44dd`. La conexión `dxcon-abcabcab` es una conexión redundante (backup) asociada a la interfaz virtual `dxvif-12312312`. Para ayudar a distinguirlas, puede etiquetar las conexiones e interfaces virtuales tal y como se indica a continuación:

ID de recurso	Clave de etiqueta	Valor de etiqueta
`dxcon-11aa22bb`	Finalidad	Producción
	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 de más fácilmente. Las etiquetas no tienen ningún significado semántico AWS Direct Connect y se interpretan estrictamente como una cadena 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 AWS Direct Connect recursos mediante la AWS Direct Connect consola, la AWS Direct Connect API, la AWS CLI AWS Tools for Windows PowerShell, la o una AWS SDK. Cuando utilice estas herramientas para administrar etiquetas, debe especificar el nombre del recurso de Amazon (ARN) para el recurso. Para obtener más información al respectoARNs, consulte Amazon Resource Names (ARNs) en Referencia general de Amazon Web Services.

Recurso	Admite etiquetas	Admite etiquetas en la creación	Admite etiquetas que controlan el acceso y la asignación de recursos	Admite la asignación de costos
Conexiones	Sí	Sí	Sí	Sí
Interfaces virtuales	Sí	Sí	Sí	No
Grupos de agregación de enlaces (LAG)	Sí	Sí	Sí	Sí
Interconexiones	Sí	Sí	Sí	Sí
Gateways de Direct Connect	No	No	No	No

Restricciones de las etiquetas

Las siguientes reglas y restricciones se aplican a las etiquetas:

- Número máximo de etiquetas por recurso: 50
- Longitud máxima de la clave: 128 caracteres Unicode
- Longitud máxima del valor: 265 caracteres Unicode
- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.

- El `aws:` prefijo está reservado para su AWS uso. 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 costes solo se admiten para conexiones, interconexiones y. LAGs Para obtener información sobre cómo usar las etiquetas en la administración de costos, consulte Uso de etiquetas de asignación de costos en la Guía del AWS Billing and Cost Management usuario.

Trabajar con etiquetas mediante CLI o 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. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza AWS Direct Connect. Los siguientes temas muestran cómo configurarlo AWS 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 AWS Direct Connect recursos.

Temas

Protección de datos en AWS Direct Connect

El modelo de responsabilidad AWS compartida modelo se aplica a la protección de datos en AWS Direct Connect. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte la sección Privacidad de datos FAQ. Para obtener información sobre la protección de datos en Europa, consulte el modelo de responsabilidad AWS compartida y la entrada del GDPR blog sobre AWS seguridad.

Para proteger los datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactorial (MFA) con cada cuenta.
- UseSSL/TLSpara comunicarse con AWS los recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad del usuario con AWS CloudTrail.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita entre FIPS 140 y 3 módulos criptográficos validados para acceder a AWS través de una interfaz de línea de comandos o unaAPI, utilice un FIPS terminal. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la Norma federal de procesamiento de información () 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 cuando trabaja con AWS Direct Connect o Servicios de AWS utiliza la consola, API AWS CLI, o. AWS SDKs Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, le recomendamos encarecidamente que no incluya la información sobre las credenciales URL para validar la solicitud a ese servidor.

Para obtener más información sobre la protección de datos, consulte el modelo de responsabilidad AWS compartida y la entrada del GDPR blog sobre AWS seguridad.

Temas

Privacidad del tráfico entre redes en AWS Direct Connect

Tráfico entre el servicio y las aplicaciones y clientes locales

Dispone de 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 aVPCs. Para obtener más información, consulte Asociaciones de la gateway privada virtual y Asociaciones de la puerta de enlace de tránsito.

Tráfico entre AWS recursos de 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 paraVPCs. Para obtener más información, consulte Asociaciones de la gateway privada virtual y Asociaciones de la puerta de enlace de tránsito.

Cifrado en tránsito AWS Direct Connect

AWS Direct Connect no cifra el tráfico en tránsito de forma predeterminada. Para cifrar los datos en tránsito que los atraviesan AWS Direct Connect, debe utilizar las opciones de cifrado de tránsito de ese servicio. Para obtener más información sobre el cifrado del tráfico de EC2 instancias, consulta Encryption in Transit en la Guía del EC2 usuario de Amazon.

Con AWS Direct Connect y AWS Site-to-Site VPN, puedes combinar una o más conexiones de red AWS Direct Connect dedicadas con Amazon VPCVPN. Esta combinación proporciona una

conexión privada IPsec cifrada que también reduce los costes de red, aumenta el rendimiento del ancho de banda y proporciona una experiencia de red más uniforme que las conexiones basadas en InternetVPN. Para obtener más información, consulta Opciones de VPC conectividad VPC entre Amazon y Amazon.

MACLa seguridad (MACsec) es un IEEE estándar que proporciona confidencialidad, integridad y autenticidad del origen de los datos. Puede utilizar AWS Direct Connect conexiones compatibles MACsec con el cifrado de los datos desde el centro de datos corporativo hasta la AWS Direct Connect ubicación. Para obtener más información, consulte MACseguridad (MACsec).

Identity and Access Management para Direct Connect

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. IAMlos administradores controlan quién puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar los recursos de Direct Connect. IAMes una Servicio de AWS que puede utilizar sin coste adicional.

Temas

Público

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

Usuario de servicio: si utiliza el servicio de Direct Connect para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Direct Connect para realizar su trabajo, es posible que necesite otros permisos. Entender cómo

se administra el acceso puede ayudarlo a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Direct Connect, consulte Solución de problemas de identidad y acceso de Direct Connect.

Administrador de servicio: si está a cargo de los recursos de Direct Connect de su empresa, es probable que tenga acceso completo a Direct Connect. Su trabajo consiste en determinar a qué características y recursos de Direct Connect deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos deIAM. Para obtener más información sobre cómo su empresa puede utilizar IAM Direct Connect, consulteCómo funciona Direct Connect con IAM.

IAMadministrador: si es IAM administrador, es posible que desee obtener información sobre cómo escribir políticas para administrar el acceso a Direct Connect. Para ver ejemplos de políticas basadas en la identidad de Direct Connect que puede utilizarIAM, consulte. Ejemplos de políticas basadas en identidades de Direct Connect

Autenticación con identidades

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

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAMIdentity Center), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accede AWS mediante la federación, asume indirectamente un rol.

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

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

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

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de tareas que requieren que inicie sesión como usuario root, consulte Tareas que requieren credenciales de usuario root en la Guía del IAM usuario.

Identidad federada

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

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utilice AWS IAM Identity Center. Puede crear usuarios y grupos en IAM Identity Center, o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones Cuentas de AWS . Para obtener información sobre IAM Identity Center, consulte ¿Qué es IAM Identity Center? en la Guía AWS IAM Identity Center del usuario.

Usuarios y grupos de IAM

Un IAMusuario es una identidad dentro de ti Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos utilizar credenciales

temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener más información, consulte Rotar las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración en la Guía del IAM usuario.

Un IAMgrupo es una identidad que especifica un conjunto de IAM usuarios. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar IAM los recursos.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Cuándo crear un IAM usuario (en lugar de un rol) en la Guía del IAM usuario.

IAMroles

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

IAMlos roles con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información sobre los roles para la federación, consulte Creación de un rol para un proveedor de identidad externo en la Guía del IAM usuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en. IAM Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos IAM de usuario temporales: un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.

- Acceso multicuenta: puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulta el tema sobre el acceso a los recursos entre cuentas IAM en la Guía del IAM usuario.
- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros. Servicios de AWS Por ejemplo, cuando realizas una llamada en un servicio, es habitual que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un IAM usuario o un rol para realizar acciones en AWS ellas, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del principal que llama a an Servicio de AWS, junto con los que solicitan, Servicio de AWS para realizar solicitudes a los servicios descendentes. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros recursos Servicios de AWS o para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener detalles sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar sesiones de acceso.
  - Función de servicio: una función de servicio es una IAMfunción que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos Servicio de AWS en un rol en el IAMManual del usuario.
  - Función vinculada a un servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.
- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y que realizan AWS CLI o AWS API solicitan. Esto es preferible a almacenar las claves de acceso dentro de la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales

temporales. Para obtener más información, consulte Uso de un IAM rol para conceder permisos a aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del IAM usuario.

Para saber si se deben usar IAM roles o IAM usuarios, consulte Cuándo crear un IAM rol (en lugar de un usuario) en la Guía del IAM usuario.

Administración de acceso mediante políticas

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

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

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

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

Políticas basadas en identidad

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, 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 información sobre cómo crear una política basada en la identidad, consulte Creación de IAM políticas en la Guía del usuario. IAM

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo

o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y funciones de su empresa. Cuenta de AWS Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para saber cómo elegir entre una política gestionada o una política integrada, consulte Elegir entre políticas gestionadas y políticas integradas en la Guía del IAM usuario.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No puede usar políticas AWS administradas desde una política IAM basada en recursos.

Listas de control de acceso () ACLs

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

Amazon S3 AWS WAF y Amazon VPC son ejemplos de servicios compatiblesACLs. Para obtener más informaciónACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

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

- Límites de permisos: un límite de permisos es una función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (IAMusuario o rol). Puede establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites

de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte los límites de los permisos para IAM las entidades en la Guía del IAMusuario.

- Políticas de control de servicios (SCPs): SCPs son JSON políticas que especifican los permisos máximos para una organización o unidad organizativa (OU) en AWS Organizations. AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. SCPLimita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre OrganizationsSCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte las políticas de sesión en la Guía del IAM usuario.

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 IAM usuario.

Cómo funciona Direct Connect con IAM

Antes de usar IAM para administrar el acceso a Direct Connect, infórmese sobre las IAM funciones disponibles para usar con Direct Connect.

IAMfunciones que puede usar con Direct Connect

IAMfunción	Compatibilidad de Direct Connect
Políticas basadas en identidades	Sí

IAMfunción	Compatibilidad de Direct Connect
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACLs	No
ABAC(etiquetas en las 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 IAM funciones, consulte AWS los servicios con los que funcionan IAM en la Guía del IAM usuario.

Políticas basadas en identidades de Direct Connect

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, 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 información sobre cómo crear una política basada en la identidad, consulte Creación de IAM políticas en la Guía del usuario. IAM

Con las políticas IAM basadas en la identidad, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica

al usuario o rol al que está adjunto. Para obtener más información sobre todos los elementos que puede utilizar en una JSON política, consulte la referencia sobre los elementos de la IAM JSON política en la Guía del IAMusuario.

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 JSON de política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar una cuenta completa o IAM entidades de otra cuenta como principales en una política basada en recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el IAM administrador de la cuenta de confianza también debe conceder permiso a la entidad principal (usuario o rol) para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte el tema Acceso a recursos entre cuentas IAM en la Guía del IAM usuario.

Acciones de políticas de Direct Connect

Compatibilidad con las acciones de política: sí

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

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de política suelen tener el mismo nombre que

la AWS API operación asociada. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

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

Para ver una lista de las acciones de Direct Connect, consulte Acciones definidas por Direct Connect en la Referencia de autorización del servicio.

Las acciones de políticas de Direct Connect utilizan el siguiente prefijo antes de la acción:

```
Direct Connect
```

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

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

Recursos de políticas de Direct Connect

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar AWS JSON políticas 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` JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso mediante su nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de Direct Connect y sus ARNs respectivos tipos, consulte Recursos definidos por Direct Connect en la AWS Direct Connect APIreferencia. Para saber con qué acciones puede especificar cada recurso, consulte Acciones definidas por Direct Connect. ARN

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 AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

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

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

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

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

Para ver una lista de claves de condición de Direct Connect, consulte Claves de condición de Direct Connect en la AWS Direct Connect APIreferencia. Para saber con qué acciones y recursos puede

usar una clave de condición, consulte Acciones, recursos y claves de condición de Direct Connect en la Referencia de autorización de servicio.

Para ver ejemplos de políticas basadas en identidades de Direct Connect, consulte Ejemplos de políticas basadas en identidades de Direct Connect.

ACLsen Direct Connect

SoportesACLs: 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. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

ABACcon Direct Connect

Soportes ABAC (etiquetas en las políticas): parciales

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define los permisos en función de los atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a IAM entidades (usuarios o roles) y a muchos AWS recursos. Etiquetar entidades y recursos es el primer paso deABAC. Luego, diseñe ABAC políticas para permitir las operaciones cuando la etiqueta del principal coincida con la etiqueta del recurso al que está intentando acceder.

ABACes útil en entornos de rápido crecimiento y ayuda en situaciones en las que la administración de políticas se vuelve engorrosa.

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

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

Para obtener más información al respectoABAC, consulte ¿Qué es? ABAC en la Guía IAM del usuario. Para ver un tutorial con los pasos de configuraciónABAC, consulte Usar el control de acceso basado en atributos (ABAC) en la Guía del IAMusuario.

Uso de credenciales temporales con Direct Connect

Compatibilidad con credenciales temporales: sí

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

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

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

Permisos de entidad principal entre servicios de Direct Connect

Admite sesiones de acceso directo (FAS): Sí

Cuando utilizas un IAM usuario o un rol para realizar acciones en AWSél, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del principal que llama a una Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros recursos Servicios de AWS o para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener detalles sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar sesiones de acceso.

Roles de servicio de Direct Connect

Compatibilidad con roles de servicio: sí

Una función de servicio es una IAMfunción que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos Servicio de AWS en un rol en el IAMManual del usuario.

> **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 IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.

Para obtener más información sobre la creación o la administración de funciones vinculadas a un servicio, consulte los AWS servicios que funcionan con. IAM Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidades de Direct Connect

De forma predeterminada, los usuarios y los roles no tienen permiso para crear ni modificar los recursos de Direct Connect. Tampoco pueden realizar tareas con AWS Management Console, AWS Command Line Interface (AWS CLI) o. AWS API Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

Para obtener información sobre cómo crear una política IAM basada en la identidad mediante estos documentos de JSON política de ejemplo, consulte Creación de IAM políticas en la Guía del IAMusuario.

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
- Acciones, recursos y condiciones de Direct Connect
- Uso de la consola de Direct Connect
- Cómo permitir a los usuarios consultar sus propios permisos
- Acceso de solo lectura a AWS Direct Connect
- Acceso completo a AWS Direct Connect
- Ejemplos de políticas basadas en identidades de Direct Connect que utilizan condiciones basadas en etiquetas

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. Para obtener más información, consulte las políticas AWS gestionadas o las políticas AWS gestionadas para las funciones laborales en la Guía del IAM usuario.
- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, 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. Para obtener más información sobre cómo IAM aplicar permisos, consulte Políticas y permisos IAM en la IAM Guía del usuario.
- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse medianteSSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte los elementos IAM JSON de la política: Condición en la Guía del IAM usuario.

- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAMAccess Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte la validación de políticas de IAM Access Analyzer en la Guía del IAM usuario.
- Requerir autenticación multifactorial (MFA): si se encuentra en una situación en la que se requieren IAM usuarios o un usuario raíz Cuenta de AWS, actívela MFA para aumentar la seguridad. Para solicitarlo MFA cuando se convoque a API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte Configuración del API acceso MFA protegido en la Guía del IAM usuario.

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

Acciones, recursos y condiciones de Direct Connect

Con las políticas IAM basadas en la identidad, 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 más información sobre todos los elementos que se utilizan en una JSON política, consulte la Referencia sobre los elementos IAM JSON de la política en la Guía del IAMusuario.

Acciones

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

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de política suelen tener el mismo nombre que la AWS API operación asociada. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

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

Las acciones de políticas de Direct Connect utilizan el siguiente prefijo antes de la acción: `directconnect:`. Por ejemplo, para conceder permiso a alguien para ejecutar una EC2

instancia de Amazon con la EC2 `DescribeVpnGateways` API operación 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 AWS Direct Connect.

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

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

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

Para ver una lista de las acciones de Direct Connect, consulte Acciones definidas por Direct Connect en la Guía del IAM usuario.

Recursos

Los administradores pueden usar AWS JSON políticas 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` JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso mediante su nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Direct Connect utiliza lo siguienteARNs:

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 deARNs, consulte Amazon Resource Names (ARNs) y AWS Service Namespaces.

Por ejemplo, para especificar la `dxcon-11aa22bb` interfaz en su declaración, utilice lo 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 tiposARNs, consulte los tipos de recursos definidos por AWS Direct Connect en la Guía del IAM usuario. Para saber con qué acciones puede especificar cada recurso, consulte SERVICE - ACTIONS -URL;. ARN

Claves de condición

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

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

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

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder a un IAM usuario permiso para acceder a un recurso solo si está etiquetado con

su nombre de IAM usuario. Para obtener más información, consulte los elementos de IAM política: variables y etiquetas en la Guía del IAM usuario.

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

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 IAM usuario.

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 IAM usuario. Para saber con qué acciones y recursos puede utilizar una clave condicionada, consulte SERVICE - ACTIONS -URL;.

Uso de la consola de Direct Connect

Para acceder a la consola de Direct Connect, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle 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 Añadir permisos a un usuario en la Guía del IAM usuario:

```
directconnect
```

No es necesario conceder permisos mínimos de consola a los usuarios que realicen llamadas únicamente al AWS CLI o al AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la API operación que está intentando realizar.

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo se puede crear una política que permita a IAM los usuarios ver las políticas integradas y administradas asociadas a su identidad de usuario. Esta política incluye

permisos para completar esta acción en la consola o mediante programación mediante la tecla o. AWS CLI AWS API

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Acceso de solo lectura a AWS Direct Connect

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

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

```
        {
            "Effect": "Allow",
            "Action": [
                "directconnect:Describe*",
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

Acceso completo a AWS Direct Connect

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

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

Ejemplos de políticas basadas en identidades de Direct Connect que utilizan condiciones basadas en etiquetas

Puede controlar el acceso a los recursos y las solicitudes mediante condiciones de clave de etiqueta. También puede usar una condición en su IAM política para controlar si se pueden usar claves de etiqueta específicas en un recurso o en una solicitud.

Para obtener información sobre cómo usar etiquetas con IAM políticas, consulte Control del acceso mediante etiquetas en la Guía del IAM usuario.

Asociación de interfaces virtuales de Direct Connect basada en etiquetas

En el ejemplo siguiente se muestra cómo puede crear una política que permita asociar una interfaz virtual solo si la etiqueta contiene la clave de entorno y los valores preprod o production.

```
     {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "directconnect:AssociateVirtualInterface"
        ],
        "Resource": "arn:aws:directconnect:*:*:dxvif/*",
        "Condition": {
          "StringEquals": {
            "aws:ResourceTag/environment": [
              "preprod",
              "production"
            ]
          }
        }
      },
      {
        "Effect": "Allow",
        "Action": "directconnect:DescribeVirtualInterfaces",
        "Resource": "*"
      }
    ]
  }
```

Control del acceso a solicitudes basado en etiquetas

Puede usar condiciones en sus IAM políticas para controlar qué pares clave-valor de etiquetas se pueden transferir en una solicitud que etiqueta un AWS recurso. En el siguiente ejemplo, se muestra cómo se puede crear una política que permita utilizar la AWS Direct Connect TagResource acción para adjuntar etiquetas a una interfaz virtual únicamente si la etiqueta contiene la clave de entorno y los valores de preproducción o producción. Le recomendamos que utilice el modificador `ForAllValues` con la clave de condición `aws:TagKeys` para indicar que solo se permite la clave environment en la solicitud.

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "directconnect:TagResource",
        "Resource": "arn:aws:directconnect:*:*:dxvif/*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/environment": [
                    "preprod",
                    "production"
                ]
            },
            "ForAllValues:StringEquals": {"aws:TagKeys": "environment"}
        }
    }
}
```

Control de claves de etiqueta

Puedes usar una condición en tus IAM políticas para controlar si se pueden usar claves de etiqueta específicas en un recurso o en una solicitud.

En el ejemplo siguiente se muestra cómo puede crear una política que le permita etiquetar recursos, pero solo con la clave de etiqueta environment.

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

Funciones vinculadas al servicio para AWS Direct Connect

AWS Direct Connect usa AWS Identity and Access Management (IAM) roles vinculados al servicio. Un rol vinculado a un servicio es un tipo único de IAM rol al que se vincula directamente. AWS Direct Connect Los roles vinculados al servicio están predefinidos AWS Direct Connect e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en tu nombre.

Un rol vinculado a un servicio facilita la configuración AWS Direct Connect , ya que no es necesario añadir manualmente los permisos necesarios. AWS Direct Connect define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Direct Connect puede asumir sus funciones. Los permisos definidos incluyen la política de confianza y la política de permisos, y esa política de permisos no se puede adjuntar a ninguna otra IAM entidad.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege sus AWS Direct Connect recursos porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Para obtener información sobre otros servicios que admiten funciones vinculadas a servicios, consulte AWS Servicios con los que funcionan IAM y busque los servicios con los que se indica Sí en la columna Función vinculada a servicios. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

Permisos de rol vinculados al servicio para AWS Direct Connect

AWS Direct Connect usa un rol vinculado a un servicio denominado. `AWSServiceRoleForDirectConnect` Esto permite AWS Direct Connect recuperar los MACSec secretos almacenados 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 de `AWSDirectConnectServiceRolePolicy`.

Debe configurar los permisos para permitir que una IAM entidad (como un usuario, un grupo o un rol) cree, edite o elimine un rol vinculado a un servicio. Para que el rol `AWSServiceRoleForDirectConnect` vinculado al servicio se cree correctamente, la IAM

identidad que utilice debe tener los AWS Direct Connect permisos necesarios. Para conceder los permisos necesarios, adjunte la siguiente política a la IAM identidad.

```
{
    "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 los permisos de funciones vinculadas a un servicio en la Guía del IAMusuario.

Crear un rol vinculado a un servicio para AWS 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 AWS Direct Connect recuperar los MACsec secretos almacenados en su nombre AWS Secrets Manager en el AWS Management Console, el o el. AWS CLI AWS API

> **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 Apareció un nuevo rol en mi IAM cuenta.

Si eliminas este rol vinculado al servicio y luego necesitas volver a crearlo, puedes usar el mismo proceso para volver a crear el rol en tu cuenta. AWS Direct Connect vuelve a crear el rol vinculado al servicio para ti.

También puede usar la IAM consola para crear un rol vinculado a un servicio con el caso de uso de AWS Direct Connect. En AWS CLI o en AWS API, cree un rol vinculado a un servicio con el nombre del servicio. `directconnect.amazonaws.com` Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario. 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 AWS Direct Connect

AWS 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 utilizando. IAM Para obtener más información, consulte Edición de un rol vinculado a un servicio en la Guía del IAMusuario.

Eliminar un rol vinculado a un servicio para AWS Direct Connect

No es necesario eliminar manualmente el rol de `AWSServiceRoleForDirectConnect`. Al eliminar el rol vinculado al servicio, debe eliminar todos los recursos asociados que están almacenados en el servicio AWS Secrets Manager web. El AWS Management Console AWS CLI, el o el AWS API AWS Direct Connect limpian los recursos y eliminan automáticamente el rol vinculado al servicio.

También puede usar la IAM consola 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 AWS Direct Connect servicio utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En ese caso, espere unos minutos e intente de nuevo la operación.

Para eliminar AWS 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 yLAGs. Para obtener más información, consulte the section called “Elimine la asociación entre una clave MACsec secreta y un LAG”

Para eliminar manualmente el rol vinculado al servicio mediante IAM

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

Regiones compatibles con los roles vinculados a un AWS Direct Connect servicio

AWS Direct Connect admite el uso de funciones vinculadas al servicio en todos los Regiones de AWS lugares donde esté disponible la función de MAC seguridad. 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 haya nuevas API operaciones disponibles para los servicios existentes.

Para obtener más información, consulte las políticas AWS administradas en la Guía del IAM usuario.

AWS política gestionada: AWSDirectConnectFullAccess

Puede adjuntar la `AWSDirectConnectFullAccess` política a sus IAM identidades. Esta política otorga permisos que permiten el acceso total a AWS Direct Connect.

Para ver los permisos de esta política, consulte AWSDirectConnectFullAccessen AWS Management Console.

AWS política gestionada: AWSDirectConnectReadOnlyAccess

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

Para ver los permisos de esta política, consulte AWSDirectConnectReadOnlyAccessen. AWS Management Console

AWS política gestionada: AWSDirectConnectServiceRolePolicy

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

Para ver los permisos de esta política, consulte AWSDirectConnectServiceRolePolicyen. AWS Management Console

AWS Direct Connect actualizaciones de las políticas AWS gestionadas

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

Cambio	Descripción	Fecha
AWSDirectConnectServiceRolePolicy: política nueva	Para respaldar MAC la seguridad, se agregó la función AWSServiceRoleForDirectConnectvinculada al servicio.	31 de marzo de 2021

Cambio	Descripción	Fecha
AWS Direct Connect comenzó a rastrear los cambios	AWS 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

Use la siguiente información como ayuda para diagnosticar y solucionar problemas comunes que pueden surgir al trabajar con Direct Connect yIAM.

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.

El siguiente ejemplo de error se produce cuando el `mateojackson` IAM usuario intenta usar la consola para ver los detalles de un *`my-example-widget`* recurso ficticio, pero no tiene los `directconnect:`*`GetWidget`* permisos ficticios.

```
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 AWS el 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 el rol al servicio.

El siguiente ejemplo de error se produce cuando un IAM usuario llamado `marymajor` intenta usar 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 AWS el 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

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que 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 más información, consulte lo siguiente:

- Para obtener información acerca de si Direct Connect admite estas características, consulte Cómo funciona Direct Connect con IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a través de los Cuentas de AWS que eres propietario, consulta Cómo proporcionar acceso a un IAM usuario en otro de tu Cuenta de AWS propiedad en la Guía del IAMusuario.

- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo permitir el acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del IAM usuario.
- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del IAM usuario.
- Para saber la diferencia entre el uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte el acceso a recursos entre cuentas IAM en la Guía del usuario. IAM

Inicio de sesión y supervisión AWS Direct Connect

Puede utilizar las siguientes herramientas de monitorización automatizado para vigilar AWS Direct Connect e informar cuando haya algún problema:

- Amazon CloudWatch Alarms: observa una única métrica durante un período de tiempo que especifiques. Realiza una o varias acciones según el valor de la métrica con respecto a un umbral dado durante varios períodos de tiempo. La acción es una notificación que se envía a un SNS tema de Amazon. CloudWatch las alarmas no invocan acciones simplemente porque estén en un estado determinado; el estado debe haber cambiado y mantenido durante un número específico de períodos. Para obtener más información, consulte Monitoriza con Amazon CloudWatch.
- AWS CloudTrail Supervisión de registros: comparta archivos de registro entre cuentas y supervise los archivos de CloudTrail registro en tiempo real enviándolos a CloudWatch Logs. También puede escribir aplicaciones de procesamiento de registros en Java y validar que sus archivos de registro no hayan cambiado después de su entrega CloudTrail. Para obtener más información, consulte la AWS Direct Connect APIRegistra llamadas usando AWS CloudTrail sección Cómo trabajar con archivos de CloudTrail registro en la Guía del AWS CloudTrail usuario.

Para obtener más información, consulte Supervise los recursos de Direct Connect.

Validación de conformidad para AWS Direct Connect

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

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

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.
- Diseñando una arquitectura basada en la HIPAA seguridad y el cumplimiento en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar las empresas AWS para crear HIPAA aplicaciones aptas.

> **Note**
>
> No todos son aptos. Servicios de AWS HIPAA Para obtener más información, consulta la Referencia de servicios HIPAA aptos.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde la perspectiva del cumplimiento. En las guías se resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y se orientan a los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar

actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, por ejemplo PCIDSS, cumpliendo con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.

- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en AWS Direct Connect

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre 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 AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, AWS Direct Connect ofrece varias funciones para ayudarlo a satisfacer sus necesidades de respaldo y resiliencia de datos.

Para obtener información sobre cómo usarlo VPN con AWS Direct Connect, consulte AWS Direct Connect Plus VPN.

Conmutación por error

El kit de herramientas de AWS Direct Connect resiliencia proporciona un asistente de conexión con varios modelos de resiliencia que le ayuda a solicitar conexiones específicas para lograr su objetivo. SLA Usted selecciona un modelo de resiliencia y, a continuación, el kit de herramientas de AWS Direct Connect resiliencia lo guía a través del proceso específico de pedido de conexiones. 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 AWS Direct Connect Kit de herramientas de resiliencia.

Seguridad de la infraestructura en AWS Direct Connect

Como servicio gestionado, AWS Direct Connect está protegido por los procedimientos de seguridad de la red AWS global. Utiliza las API llamadas AWS publicadas para acceder a AWS Direct Connect través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.2 o una versión posterior. Recomendamos la versión TLS 1.3. Los clientes también deben admitir conjuntos de cifrado con total confidencialidad (PFS), como Ephemeral Diffie-Hellman () o Elliptic Curve Ephemeral Diffie-Hellman (DHE). ECDHE La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben firmarse con un identificador de clave de acceso y una clave de acceso secreta asociada a un director. IAM También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Puede API realizar estas operaciones desde cualquier ubicación de la red, pero AWS Direct Connect admite políticas de acceso basadas en los recursos, que pueden incluir restricciones basadas en la dirección IP de origen. También puede utilizar AWS Direct Connect políticas para controlar el acceso desde puntos de enlace específicos o específicos VPCs de Amazon Virtual Private Cloud (AmazonVPC). En efecto, esto aísla el acceso a la red a un AWS Direct Connect recurso determinado únicamente de los recursos específicos VPC de la AWS red. Por ejemplo, consulte the section called “Ejemplos de políticas basadas en identidades de Direct Connect”.

Seguridad del Border Gateway Protocol (BGP)

Internet se basa en gran medida en el enrutamiento BGP de la información entre los sistemas de red. BGPel enrutamiento a veces puede ser susceptible a ataques maliciosos o BGP secuestros. Para saber cómo proteger AWS de forma más segura su red contra el BGP secuestro, consulte Cómo AWS se ayuda a proteger el enrutamiento de Internet.

Usa el AWS CLI

Puede usarlo AWS CLI para crear AWS Direct Connect recursos y trabajar con ellos.

En el siguiente ejemplo, se utilizan los AWS CLI comandos para crear una AWS Direct Connect conexión. También puede descargar la carta de autorización y la asignación de la instalación de conexión (LOA-CFA) o proporcionar 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 AWS Command Line Interface Guía del usuario de .

Contenido

Paso 1: Crear una conexión

El primer paso es enviar una solicitud de conexión. Asegúrese de conocer la velocidad del puerto que necesita y la AWS Direct Connect ubicación. Para obtener más información, consulte Conexiones dedicadas y alojadas.

Para crear una solicitud de conexión

1. Describa las AWS Direct Connect ubicaciones 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. Necesitarás el identificador para obtener elLOA... 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: Descarga el LOA - CFA

Una vez que hayas solicitado una conexión, puedes obtener el LOA - CFA mediante el `describe-loa` comando. El resultado aparece codificado en base64. Debe extraer el LOA contenido relevante, decodificarlo y crear un PDF archivo.

Para obtener el LOA - CFA usando Linux o macOS

En este ejemplo, la parte final del comando decodifica el contenido mediante la utilidad base64 y envía el resultado a un PDF archivo.

```
aws directconnect describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent|base64 --decode > myLoaCfa.pdf
```

Para obtener el LOA - usando Windows CFA

En este ejemplo, el resultado se extrae a un archivo llamado myLoaCfa .base64. El segundo comando usa la `certutil` utilidad 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
```

Después de descargar el LOA -CFA, envíelo a su proveedor de red o de colocación.

Paso 3: Crear una interfaz virtual y obtener la configuración del enrutador

Tras realizar el pedido de una AWS Direct Connect conexión, debe crear una interfaz virtual para empezar a utilizarla. Puede crear una interfaz virtual privada para conectarse a suVPC. O bien, puede crear una interfaz virtual pública para conectarse a AWS servicios que no están en unVPC. Puede crear una interfaz virtual que admita IPv4 nuestro IPv6 tráfico.

Antes de comenzar, asegúrese de que ha leído todos los requisitos previos que detallan en ???.

Al crear una interfaz virtual mediante el AWS CLI, el resultado incluye información genérica de configuración del router. Para crear una configuración de router específica para su dispositivo, utilice la AWS Direct Connect consola. Para obtener más información, consulte Descargar el archivo de configuración del enrutador.

Para crear una interfaz virtual privada

1. Obtén el ID de la puerta de enlace privada virtual (vgw- xxxxxxxx) que está conectada a tu cuenta. 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, una VLAN identificación y un número de sistema BGP autónomo (). ASN

   Para IPv4 el tráfico, necesita IPv4 direcciones privadas para cada extremo de la sesión de BGP interconexión. Puedes especificar tus propias IPv4 direcciones o puedes dejar que Amazon genere las direcciones por ti. En el siguiente ejemplo, las IPv4 direcciones se generan para 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 admita el IPv6 tráfico, utilice el mismo comando anterior y especifique `ipv6` el `addressFamily` parámetro. No puedes especificar tus propias IPv6 direcciones para la sesión de BGP peering; Amazon te asigna las direcciones. IPv6

3. Para ver la información de configuración del router en XML formato, describa la interfaz virtual que creó. 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 VLAN ID y un número de sistema BGP autónomo (ASN).

   En cuanto al IPv4 tráfico, también debes especificar IPv4 las direcciones públicas para cada final de la BGP sesión de interconexión y IPv4 las rutas públicas por BGP las que anunciarás. En el siguiente ejemplo, se crea una interfaz virtual pública para el IPv4 tráfico.

```
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 admita IPv6 el tráfico, puedes especificar IPv6 las rutas por las que harás publicidadBGP. No puedes especificar IPv6 direcciones para la sesión de interconexión; Amazon te asigna IPv6 las direcciones. 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 XML formato, describa la interfaz virtual que creó. 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>
```

AWS Direct Connect APIRegistra llamadas usando AWS CloudTrail

AWS Direct Connect está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en AWS Direct Connect. CloudTrail captura todas API las llamadas AWS Direct Connect como eventos. Las llamadas capturadas incluyen las llamadas desde la AWS Direct Connect consola y las llamadas en código a las AWS Direct Connect API operaciones. Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para AWS Direct Connect. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por usted CloudTrail, puede determinar a AWS Direct Connect qué dirección IP se realizó la solicitud, quién la realizó, cuándo se realizó y detalles adicionales.

Para obtener más información, consulte la AWS CloudTrail Guía del usuario de .

AWS Direct Connect información en CloudTrail

CloudTrail está habilitada en su AWS cuenta al crear la cuenta. Cuando se produce una actividad en AWS Direct Connect, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el 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 CloudTrail eventos.

Para tener un registro continuo de los eventos de tu AWS cuenta, incluidos los eventos de tu cuenta AWS Direct Connect, crea una ruta. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando crea una ruta en la consola, la ruta se aplica a todas AWS las regiones. La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail Integraciones y servicios compatibles
- Configuración de Amazon SNS Notifications para CloudTrail

- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas AWS Direct Connect las acciones se registran CloudTrail y se documentan en la AWS Direct Connect APIReferencia. Por ejemplo, las llamadas a las `CreatePrivateVirtualInterface` acciones `CreateConnection` y las llamadas generan entradas en los archivos de CloudTrail registro.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales raíz o AWS Identity and Access Management (IAMde usuario).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.

Para obtener más información, consulte el CloudTrailuserIdentityElemento.

Comprenda las entradas de los archivos de AWS Direct Connect registro

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las API llamadas públicas, por lo que no aparecen en ningún orden específico.

A continuación se muestran ejemplos de CloudTrail registros de AWS Direct Connect.

Example Ejemplo: CreateConnection

```
{
    "Records": [
    {
        "eventVersion": "1.0",
```

```
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:28:16Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreateConnection",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "location": "EqSE2",
            "connectionName": "MyExampleConnection",
            "bandwidth": "1Gbps"
        },
        "responseElements": {
            "location": "EqSE2",
            "region": "us-west-2",
            "connectionState": "requested",
            "bandwidth": "1Gbps",
            "ownerAccount": "123456789012",
            "connectionId": "dxcon-fhajolyy",
            "connectionName": "MyExampleConnection"
        }
    },
    ...
  ]
}
```

Example Ejemplo: CreatePrivateVirtualInterface

```
{
    "Records": [
```

```
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:39:55Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "CreatePrivateVirtualInterface",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy",
            "newPrivateVirtualInterface": {
                "virtualInterfaceName": "MyVirtualInterface",
                "customerAddress": "[PROTECTED]",
                "authKey": "[PROTECTED]",
                "asn": -1,
                "virtualGatewayId": "vgw-bb09d4a5",
                "amazonAddress": "[PROTECTED]",
                "vlan": 123
            }
        },
        "responseElements": {
            "virtualInterfaceId": "dxvif-fgq61m6w",
            "authKey": "[PROTECTED]",
            "virtualGatewayId": "vgw-bb09d4a5",
            "customerRouterConfig": "[PROTECTED]",
            "virtualInterfaceType": "private",
            "asn": -1,
            "routeFilterPrefixes": [],
            "virtualInterfaceName": "MyVirtualInterface",
            "virtualInterfaceState": "pending",
```

```
            "customerAddress": "[PROTECTED]",
            "vlan": 123,
            "ownerAccount": "123456789012",
            "amazonAddress": "[PROTECTED]",
            "connectionId": "dxcon-fhajolyy",
            "location": "EqSE2"
        }
    },
    ...
  ]
}
```

Example Ejemplo: DescribeConnections

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:27:28Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeConnections",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": null,
        "responseElements": null
    },
    ...
  ]
```

```
}
```

Example Ejemplo: DescribeVirtualInterfaces

```
{
    "Records": [
    {
        "eventVersion": "1.0",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "EX_PRINCIPAL_ID",
            "arn": "arn:aws:iam::123456789012:user/Alice",
            "accountId": "123456789012",
            "accessKeyId": "EXAMPLE_KEY_ID",
            "userName": "Alice",
            "sessionContext": {
                "attributes": {
                    "mfaAuthenticated": "false",
                    "creationDate": "2014-04-04T12:23:05Z"
                }
            }
        },
        "eventTime": "2014-04-04T17:37:53Z",
        "eventSource": "directconnect.amazonaws.com",
        "eventName": "DescribeVirtualInterfaces",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "Coral/Jakarta",
        "requestParameters": {
            "connectionId": "dxcon-fhajolyy"
        },
        "responseElements": null
    },
    ...
  ]
}
```

Supervise AWS Direct Connect los recursos

La supervisión es una parte importante del mantenimiento de la confiabilidad, la disponibilidad y el rendimiento de los recursos de Direct Connect. Debe recopilar los datos de supervisión de todas las partes de la AWS solución para poder depurar más fácilmente una falla multipunto en caso de que se produzca. Sin embargo, antes de empezar a monitorear Direct Connect, debe crear un plan de monitoreo que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la supervisión?
- ¿Qué recursos deben monitorizarse?
- ¿Con qué frecuencia debe monitorizar estos recursos?
- ¿Qué herramientas de monitorización puede utilizar?
- ¿Quién se encarga de realizar las tareas de monitorización?
- ¿Quién debería recibir una notificación cuando surjan problemas?

El siguiente paso es establecer una línea base para el rendimiento normal de Direct Connect en su entorno, midiendo el rendimiento en distintos momentos y bajo diferentes condiciones de carga. Mientras monitorea Direct Connect, almacene los datos históricos de monitoreo. De este modo, puede compararlos con los datos de rendimiento actuales, identificar patrones de rendimiento normal y anomalías en el rendimiento, así como desarrollar métodos para la resolución de problemas.

Para establecer una línea base, debe supervisar el uso, el estado y el estado de las conexiones físicas de Direct Connect.

Contenido

Herramientas de monitoreo

AWS proporciona varias herramientas que puede utilizar para supervisar una AWS Direct Connect conexión. Puede configurar algunas de estas herramientas para que monitoricen por usted, pero otras herramientas requieren intervención manual. Le recomendamos que automatice las tareas de monitorización en la medida de lo posible.

Herramientas de monitoreo automatizadas

Puede usar las siguientes herramientas de monitoreo automatizadas para ver Direct Connect e informar cuando algo vaya mal:

- Amazon CloudWatch Alarms: observa una única métrica durante un período de tiempo que especifiques. Realiza una o varias acciones según el valor de la métrica con respecto a un umbral dado durante varios períodos de tiempo. La acción es una notificación que se envía a un SNS tema de Amazon. CloudWatch las alarmas no invocan acciones simplemente porque estén en un estado determinado; el estado debe haber cambiado y mantenido durante un número específico de períodos. Para obtener información sobre las métricas y dimensiones disponibles, consulte Monitoriza con Amazon CloudWatch.
- AWS CloudTrail Supervisión de registros: comparta archivos de registro entre cuentas y supervise los archivos de CloudTrail registro en tiempo real enviándolos a CloudWatch Logs. También puede escribir aplicaciones de procesamiento de registros en Java y validar que sus archivos de registro no hayan cambiado después de su entrega CloudTrail. Para obtener más información, consulte la Registra API llamadas sección Cómo trabajar con archivos de CloudTrail registro en la Guía del AWS CloudTrail usuario.

Herramientas de monitoreo manuales

Otra parte importante de la supervisión de una AWS Direct Connect conexión implica la supervisión manual de los elementos que CloudWatch las alarmas no cubren. Los paneles de Direct Connect y de la CloudWatch consola proporcionan una at-a-glance vista del estado de su AWS entorno.

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

  Además, puede CloudWatch hacer lo siguiente:

  - Cree paneles personalizados para monitorizar los servicios que le interesen.

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

Monitoriza con Amazon CloudWatch

Puede monitorear AWS Direct Connect las conexiones físicas y las interfaces virtuales mediante CloudWatch. CloudWatch recopila datos sin procesar de Direct Connect y los procesa para convertirlos en métricas legibles. De forma predeterminada, CloudWatch proporciona datos de métricas de Direct Connect en intervalos de 5 minutos. Los datos métricos de cada intervalo son una agregación de al menos dos muestras recopiladas durante ese intervalo.

Para obtener información detallada al respecto CloudWatch, consulta la Guía del CloudWatch usuario de Amazon. También puedes monitorear tus servicios CloudWatch para ver cuáles están consumiendo recursos. Para obtener más información, consulta AWS los servicios que publican CloudWatch métricas.

Contenido

AWS Direct Connect métricas y dimensiones

Las métricas están disponibles para las conexiones AWS Direct Connect físicas y las interfaces virtuales.

AWS Direct Connect Métricas de conexión

Las siguientes métricas están disponibles en las conexiones dedicadas de Direct Connect.

Métrica	Descripción
`ConnectionState`	El estado de la conexión.1 indica activa y 0 indica inactiva.

Métrica	Descripción
	Esta métrica está disponible para conexiones dedicadas y alojadas. **Note** Esta métrica también se encuentra disponibl e en las cuentas de propietario de la interfaz virtual alojada, al igual que en las cuentas de propietario de la conexión. Unidades: booleano
`ConnectionBpsEgress`	La velocidad de bits de los datos salientes desde el AWS lado de la conexión. El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especific ado (5 minutos de forma predeterminada y 1 minuto como mínimo). Puede cambiar el valor acumulado predeterminado. Es posible que esta métrica no esté disponible para una nueva conexión o cuando se reinicie un dispositi vo. La métrica se inicia cuando la conexión se utiliza para enviar o recibir tráfico. Unidades: bits por segundo

Métrica	Descripción
`ConnectionBpsIngress`	La velocidad de bits de los datos entrantes al AWS lado de la conexión. Es posible que esta métrica no esté disponible para una nueva conexión o cuando se reinicie un dispositivo. La métrica se inicia cuando la conexión se utiliza para enviar o recibir tráfico. Unidades: bits por segundo
`ConnectionPpsEgress`	` La velocidad de paquetes de los datos salientes desde el AWS lado de la conexión. El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especificado (5 minutos de forma predeterminada y 1 minuto como mínimo). Puede cambiar el valor acumulado predeterminado. Es posible que esta métrica no esté disponible para una nueva conexión o cuando se reinicie un dispositivo. La métrica se inicia cuando la conexión se utiliza para enviar o recibir tráfico. Unidades: paquetes por segundo

Métrica	Descripción
`ConnectionPpsIngress`	La velocidad de paquetes de datos entrantes al AWS lado de la conexión. El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especific ado (5 minutos de forma predeterminada y 1 minuto como mínimo). Puede cambiar el valor acumulado predeterminado. Es posible que esta métrica no esté disponible para una nueva conexión o cuando se reinicie un dispositi vo. La métrica se inicia cuando la conexión se utiliza para enviar o recibir tráfico. Unidades: paquetes por segundo
`ConnectionCRCErrorCount`	Este recuento ya no está en uso. En su lugar, use `ConnectionErrorCount` .

Métrica	Descripción
`ConnectionErrorCount`	El recuento total de errores de todos los tipos de errores de MAC nivel del AWS dispositivo. El total incluye los errores de comprobación de redundancia cíclica (CRC). Esta métrica es el recuento de errores que se han producido desde el último punto de datos registrado. Cuando hay errores en la interfaz, la métrica muestra valores distintos de cero. Para obtener el recuento total de todos los errores del intervalo seleccionado en CloudWatch, por ejemplo, 5 minutos, aplique la estadística de «suma». 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 saliente (de salida) procedente del AWS lado 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 entrante (de entrada) al AWS lado 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 se aplica esta métrica aLAG, 1 indica que todas las conexiones del mismo están LAG cifradasup. 0 indica que hay al menos una LAG conexión cifradadown.

AWS Direct Connect métricas de interfaz virtual

Las siguientes métricas están disponibles en las interfaces AWS Direct Connect virtuales.

Métrica	Descripción
`VirtualInterfaceBpsEgress`	La velocidad de bits de los datos salientes desde el AWS lateral de la interfaz virtual. El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especificado (5 minutos de forma predeterminada). Unidades: bits por segundo
`VirtualInterfaceBpsIngress`	La velocidad de bits de los datos entrantes al AWS lateral de la interfaz virtual.

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 paquetes de los datos salientes desde el AWS lado de la interfaz virtual. El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especificado (5 minutos de forma predeterminada). Unidades: paquetes por segundo
`VirtualInterfacePpsIngress`	La velocidad de paquetes de los datos entrantes al AWS lado de la interfaz virtual. El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especificado (5 minutos de forma predeterminada). Unidades: paquetes por segundo

AWS Direct Connect dimensiones disponibles

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

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

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

Temas

- Ver AWS Direct Connect CloudWatch métricas
- Crea CloudWatch alarmas de Amazon para monitorear AWS Direct Connect las conexiones

Ver AWS Direct Connect CloudWatch métricas

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

> **Note**
>
> Si estableces un intervalo de 1 minuto, Direct Connect hará todo lo posible por escribir las métricas para CloudWatch usar este intervalo, pero no siempre se puede garantizar.

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

Para ver las métricas mediante la CloudWatch consola

Las métricas se agrupan en primer lugar por el espacio de nombres de servicio y, a continuación, por las diversas combinaciones de dimensiones dentro de cada espacio de nombres. Para obtener más información sobre cómo Amazon CloudWatch ver las métricas de Direct Connect, incluida la adición de funciones matemáticas o consultas prediseñadas, consulte Uso de Amazon CloudWatch métricas en la Guía del CloudWatch usuario de Amazon.

1. Abra la CloudWatch consola en. https://console.aws.amazon.com/cloudwatch/
2. En el panel de navegación, elija Metrics (Métricas) y, a continuación, All metrics (Todas las métricas).
3. En la sección de Métricas, elija DX.

4. Elija un ConnectionIdnombre de métrica y, a continuación, elija una de las siguientes opciones para definir mejor la métrica:
   - Agregar a la búsqueda: agrega esta métrica a los resultados de la búsqueda.
   - Solo buscar esta: solo busca esta métrica.
   - Eliminar del gráfico: elimina esta métrica del gráfico.
   - Solo graficar esta métrica: solo grafica esta métrica.
   - Graficar todos los resultados de la búsqueda: grafica todas las métricas.
   - Gráfica con SQL consulta: abre el generador de consultas de Metric Insights, que te permite elegir qué quieres graficar creando una SQL consulta. Para obtener más información sobre el uso de Metric Insights, consulta Consulta tus métricas con CloudWatch Metrics Insights en la Guía del CloudWatch usuario de Amazon.

Para ver las métricas mediante la AWS Direct Connect consola

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. En el panel de navegación, elija Connections (Conexiones).
3. Seleccione la conexión.
4. Elija la pestaña de Monitoreo para visualizar las métricas de su conexión.

Para ver las métricas mediante el AWS CLI

En el símbolo del sistema, ejecute el siguiente comando.

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

Crea CloudWatch alarmas de Amazon para monitorear AWS Direct Connect las conexiones

Puedes crear una CloudWatch alarma que envíe un SNS mensaje de Amazon cuando la alarma cambie de estado. Una alarma vigila una métrica determinada durante el periodo especificado. Envía una notificación a un SNS tema de Amazon en función del valor de la métrica en relación con un umbral determinado durante varios períodos de tiempo.

Por ejemplo, puede crear una alarma que monitorice el estado de una conexión de AWS Direct Connect . Envía una notificación cuando el estado de conexión esté inactivo durante cinco periodos consecutivos de un minuto. Para obtener más información sobre lo que debe saber para crear una alarma y obtener más información sobre cómo crear una alarma, consulte Uso de Amazon CloudWatch Alarms en la Guía del CloudWatch usuario de Amazon.

Para crear una CloudWatch alarma.

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Alarms (Alarmas) y, a continuación, elija All Alarms (Todas las alarmas).
3. Seleccione Crear alarma.
4. Elija Seleccionar métrica y, a continuación, elija DX.
5. Elija la métrica de Métricas de conexión.
6. Seleccione la AWS Direct Connect conexión y, a continuación, elija la métrica Seleccionar métrica.
7. En la página Especificar la métrica y las condiciones, configure los parámetros de la alarma. Para obtener información más específica sobre las métricas y las condiciones, consulte Uso de Amazon CloudWatch Alarms en la Guía del CloudWatch usuario de Amazon.
8. Elija Next (Siguiente).
9. Configure las acciones de alarma en la página Configurar acciones. Para obtener más información sobre la configuración de las acciones de alarma, consulta Acciones de alarma en la Guía del CloudWatch usuario de Amazon.
10. Elija Next (Siguiente).
11. En la página Agregar nombre y descripción, ingrese un Nombre y una Descripción de alarma opcional para describir esta alarma y, a continuación, elija Siguiente.
12. Verifique la alarma propuesta en la página Vista previa y creación.
13. Si es necesario, elija Editar para cambiar cualquier información y, a continuación, elija Crear alarma.

    En la página Alarmas se muestra una fila nueva con información sobre la alarma nueva. En el estado de Acciones se muestran las Acciones habilitadas, lo que indica que la alarma se encuentra activa.

AWS Direct Connect cuotas

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

Componente	Cuota	Comentarios
Interfaces virtuales públicas o privadas por conexión AWS Direct Connect dedicada	50	Este límite no se puede aumentar.
Interfaces virtuales de tránsito por conexión AWS Direct Connect dedicada	4	Este límite no se puede aumentar.
Interfaces virtuales privadas o públicas por conexión AWS Direct Connect dedicada e interfaces virtuales de tránsito por conexión AWS Direct Connect dedicada	51	Cuando se lanzó la AWS Direct Connect compatibilidad con Amazon VPC Transit Gateways, se añadió una cuota de una (1) interfaz virtual de tránsito a la cuota de 50 interfaces virtuales públicas o privadas por conexión dedicada. El número de interfaces virtuales de tránsito permitido ahora es de cuatro (4) y se tiene en cuenta para el máximo de 51 interface s virtuales por conexión dedicada. Este límite no se puede aumentar.
Interfaces virtuales privadas, públicas o de tránsito por conexión AWS Direct Connect alojada	1	Este límite no se puede aumentar.
AWS Direct Connect Conexiones activas por ubicación de Direct Connect por región y cuenta	10	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Número de interfaces virtuales por grupo de agregación de enlaces (LAG)	51	Cuando se lanzó la AWS Direct Connect compatibilidad con Amazon VPC Transit Gateways, se añadió una cuota de una (1) interfaz virtual de tránsito a la cuota de

Componente	Cuota	Comentarios
		50 interfaces virtuales públicas o privadas por cada LAG una. La cantidad de interfaces virtuales de tránsito permitida s ahora es de cuatro (4) y se tiene en cuenta para el máximo de 51 interfaces virtuales por cada LAG una. Este límite no se puede aumentar.
Rutas por sesión del Border Gateway Protocol (BGP) en una interfaz virtual privada o en una interfaz virtual de tránsito desde una instalación local a AWS otra. Si anuncia más de 100 rutas para la BGP sesión IPv4 y IPv6 durante la misma, la BGP sesión pasará a un estado inactivo junto con la BGP sesiónDOWN.	100 cada una para IPv4 y IPv6	Este límite no se puede aumentar.
Rutas por sesión del Border Gateway Protocol (BGP) en una interfaz virtual pública	1 000	Este límite no se puede aumentar.

Componente	Cuota	Comentarios
Conexiones dedicadas por grupo de agregación de enlaces (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 (LAGs) por región	10	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
AWS Direct Connect pasarelas 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 AWS Direct Connect puerta de enlace	20	Este límite no se puede aumentar.
Pasarelas de tránsito por puerta de enlace AWS Direct Connect	6	Este límite no se puede aumentar.

Componente	Cuota	Comentarios
Interfaces virtuales (privadas o de tránsito) por AWS Direct Connect puerta de enlace	30	Este límite no se puede aumentar.
Número de prefijos por AWS Transit Gateway trayecto AWS y local en una interfaz virtual de tránsito	200 en total combinads para y IPv4 IPv6	Este límite no se puede aumentar.
Número de interfaces virtuales por puerta de enlace privada virtual	No hay límite.	
Número de puertas de enlace de Direct Connect asociadas a una puerta de enlace de tránsito	20	Este límite no se puede aumentar.
SiteLink límite de prefijos	100	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.

AWS Direct Connect admite las siguientes velocidades de puerto a través de fibra monomodo: 1 Gbps: 1000 BASE -LX (1310 nm), 10 Gbps: 10 GBASE -LR (1310 nm) y 100 Gbps: 100 -. GBASE LR4

BGPcuotas

Las siguientes son BGP cuotas. Los BGP temporizadores se negocian hasta el valor más bajo entre los enrutadores. Los BFD intervalos 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 un reinicio correcto y BFD al mismo tiempo.
- BFDintervalo mínimo de detección de vitalidad: 300 ms
- BFDmultiplicador mínimo: 3

Consideraciones sobre el equilibrio de carga

Si quieres utilizar el equilibrio de carga con varios públicosVIFs, todos VIFs deben estar en la misma región.

Solución de problemas AWS Direct Connect

La siguiente información de solución de problemas puede ayudarlo a diagnosticar y solucionar problemas con su conexión de AWS Direct Connect .

Contenido

Solución de problemas de capa 1 (físicos)

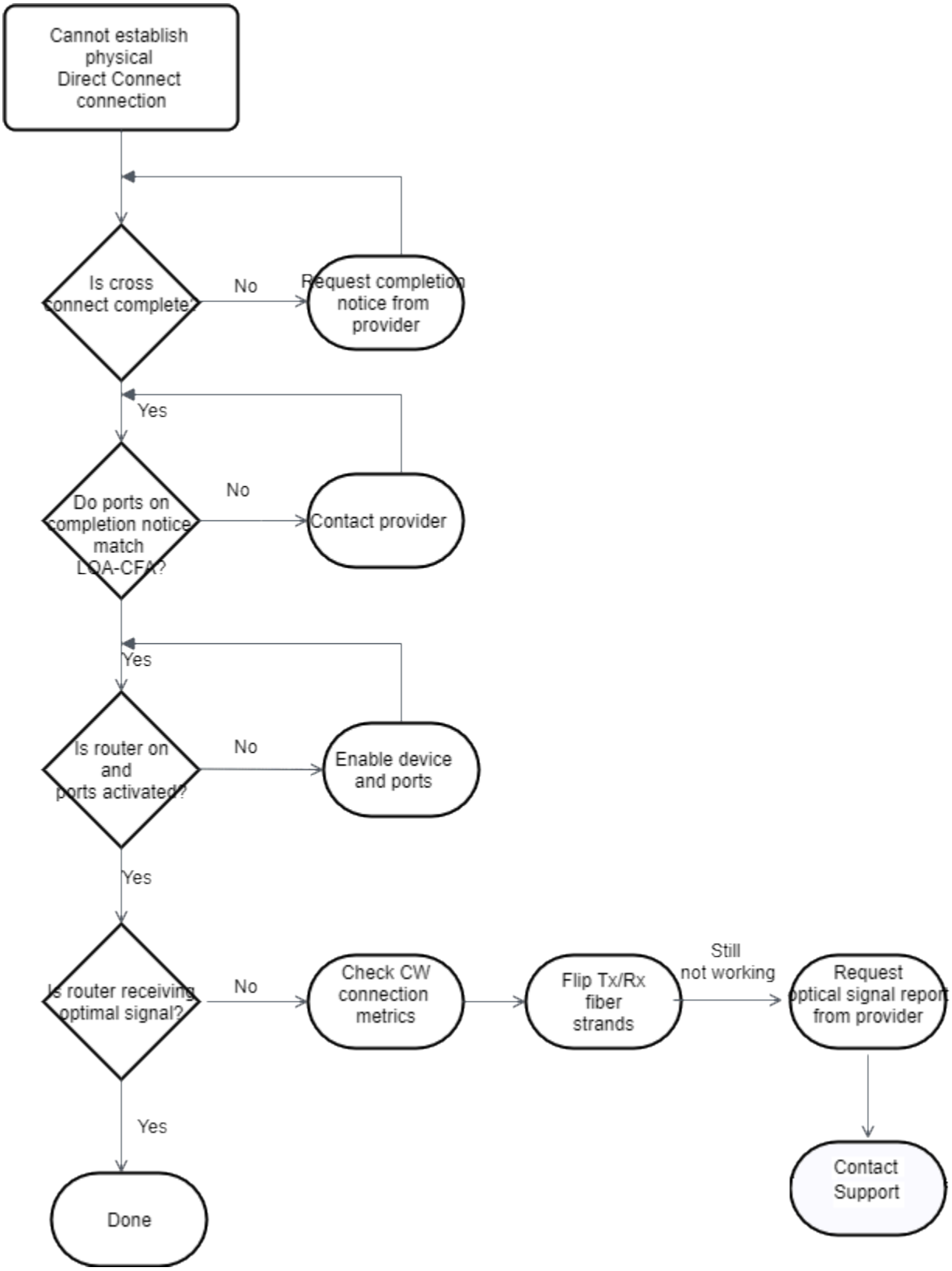
Si usted o su proveedor de red tienen dificultades para establecer la conectividad física con un AWS Direct Connect dispositivo, siga los siguientes pasos para solucionar el problema.

1. Con la ayuda del proveedor de coubicación, compruebe que la conexión cruzada se ha completado. Pídeles a ellos o a tu proveedor de red que te envíen un aviso de finalización de la conexión cruzada y que comparen los puertos con los que aparecen en tu LOA -CFA.
2. Compruebe que su router o el router del proveedor está encendido y que los puertos están activados.
3. Asegúrese de que los enrutadores utilicen el transceptor óptico correcto. La negociación automática del puerto debe estar deshabilitada si tiene una conexión con una velocidad de puerto superior a 1 Gbps. Sin embargo, según el punto final de AWS Direct Connect que dé servicio a su conexión, es posible que sea necesario activar o desactivar la negociación automática para las conexiones de 1 Gbps. Si es necesario deshabilitar la negociación automática para sus conexiones, la velocidad del puerto y el modo dúplex completo se deben configurar de forma manual. Si la interfaz virtual permanece inactiva, consulte Solución de problemas de capa 2 (enlace de datos).
4. Compruebe que el router está recibiendo una señal óptica aceptable a través de la conexión cruzada.
5. Intente voltear (o girar) las hebras de fibra de transmisión/recepción.
6. Consulta las CloudWatch estadísticas de Amazon para AWS Direct Connect. Puede verificar las lecturas ópticas de Tx/Rx del AWS Direct Connect dispositivo (tanto de 1 Gbps como de 10 Gbps),

el recuento de errores físicos y el estado operativo. Para obtener más información, consulta Monitoring with Amazon CloudWatch.

7. Póngase en contacto con el proveedor de coubicación y solicite un informe escrito para la señal óptica de transmisión/recepción a través de la conexión cruzada.
8. Si los pasos anteriores no resuelven los problemas de conectividad física, póngase en contacto con AWS Support y facilite la notificación de finalización de la conexión cruzada y el informe de la señal óptica que le ha proporcionado el proveedor de coubicación.

El siguiente diagrama contiene los pasos para diagnosticar problemas con la conexión física.

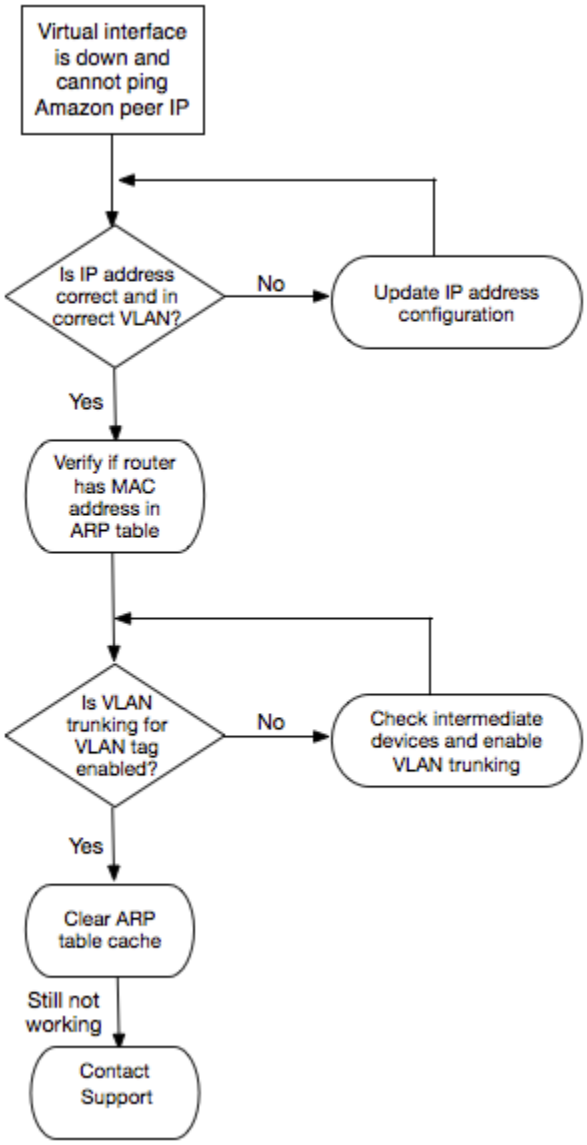

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check CW connection metrics
Flip Tx/Rx fiber strands
Still not working
Request optical signal report from provider
Contact Support
Yes
Done

Solución de problemas de capa 2 (enlace de datos)

Si la conexión AWS Direct Connect física está activa pero la interfaz virtual no funciona, siga los siguientes pasos para solucionar el problema.

1. Si no puedes hacer ping a la dirección IP del mismo nivel de Amazon, comprueba que la dirección IP del mismo nivel esté configurada correctamente y sea correctaVLAN. Asegúrese de que la dirección IP esté configurada en la VLAN subinterfaz y no en la interfaz física (por ejemplo, GigabitEthernet 0/0.123 en lugar de GigabitEthernet 0/0).
2. Compruebe si el router tiene una entrada de MAC dirección desde el AWS punto final en la tabla de protocolos de resolución de direcciones (). ARP
3. Asegúrese de que todos los dispositivos intermedios entre los puntos finales tengan habilitada la VLAN conexión troncal para la etiqueta VLAN 802.1Q. ARPno se puede establecer de forma AWS lateral hasta que reciba el tráfico etiquetado AWS .
4. Borra tu caché de ARP tablas o la de tu proveedor.
5. Si los pasos anteriores no permiten establecer ARP o sigues sin poder hacer ping a la IP del mismo nivel de Amazon, ponte en contacto con AWS Support.

El siguiente diagrama contiene los pasos para diagnosticar problemas con el enlace de datos.



Si la BGP sesión sigue sin establecerse después de verificar estos pasos, consulte. Solución de problemas de capa 3/4 (red/transporte) Si la BGP sesión está establecida pero tiene problemas de enrutamiento, consulteSolución de problemas de direccionamiento.

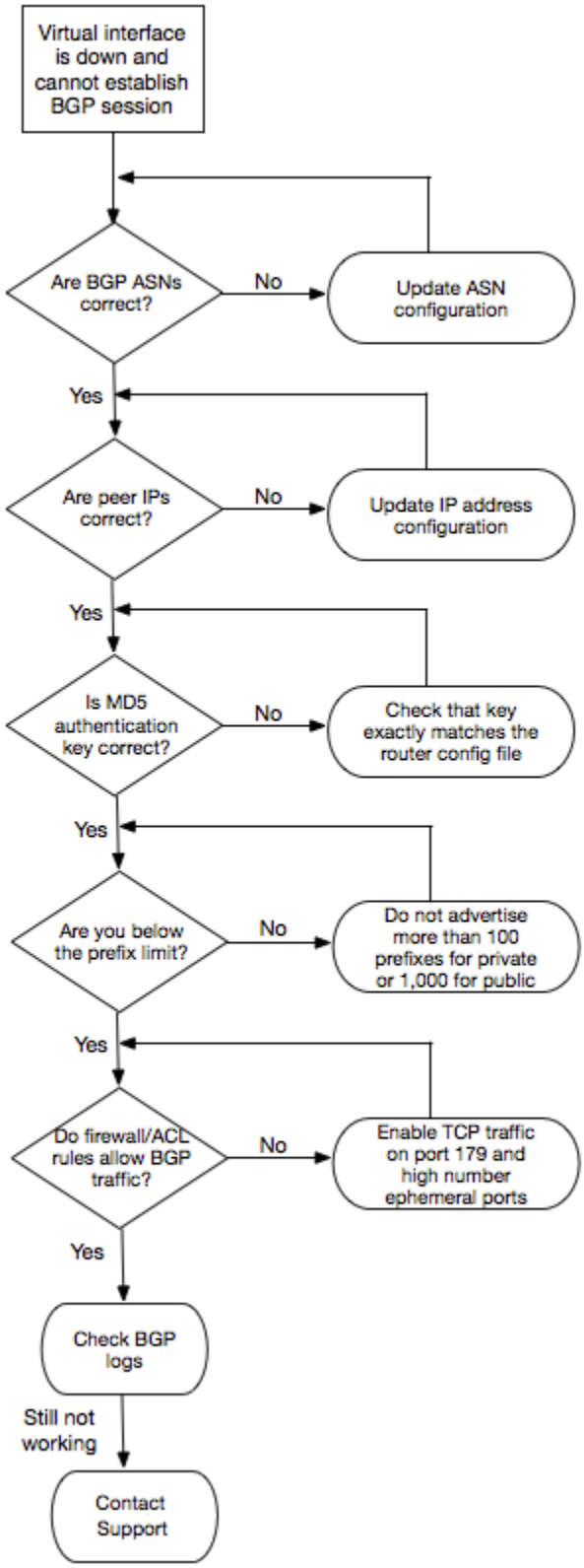
Solución de problemas de capa 3/4 (red/transporte)

Imagina una situación en la que tu conexión AWS Direct Connect física esté activa y puedas hacer ping a la dirección IP del mismo nivel de Amazon. Si la interfaz virtual está activa y no se puede establecer la BGP sesión de interconexión, siga los siguientes pasos para solucionar el problema:

1. Asegúrese de que su número de sistema autónomo BGP local (ASN) y el de Amazon ASN estén configurados correctamente.

2. Asegúrese de que los pares IPs de ambos lados de la sesión de BGP emparejamiento estén configurados correctamente.
3. Asegúrese de que la clave de MD5 autenticación esté configurada y coincida exactamente con la clave del archivo de configuración del router 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 haya ningún firewall o ACL reglas que bloqueen el TCP puerto 179 o cualquier puerto efímero TCP con números altos. Estos puertos son necesarios BGP para establecer una TCP conexión entre los pares.
6. Revise sus BGP registros para ver si hay errores o mensajes de advertencia.
7. Si los pasos anteriores no establecen la sesión de intercambio entre BGP pares, ponte en contacto con AWS Support.

El siguiente diagrama de flujo contiene los pasos para diagnosticar los problemas relacionados con la sesión de BGP emparejamiento.



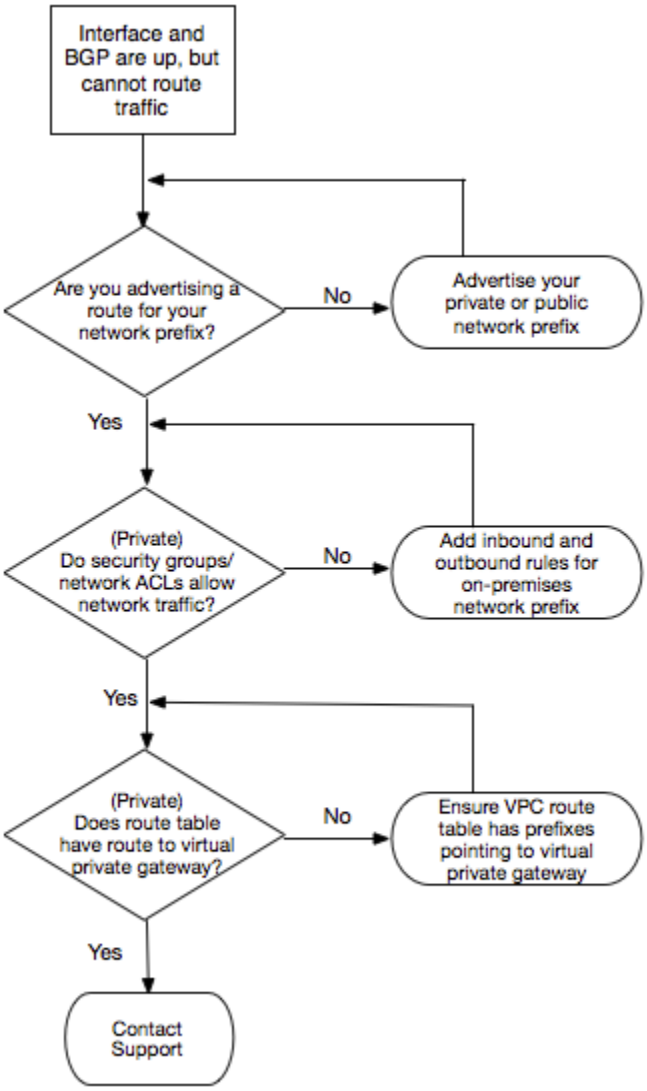
Si la sesión BGP de interconexión está establecida pero tiene problemas de enrutamiento, consulte. [Solución de problemas de direccionamiento]

Solución de problemas de direccionamiento

Considere una situación en la que su interfaz virtual esté activa y haya establecido una sesión de BGP emparejamiento. Si no puede dirigir el tráfico a través de la interfaz virtual, siga estos pasos para solucionar el problema:

1. Asegúrese de anunciar una ruta para el prefijo de la red local durante la sesión. 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 el caso de una interfaz virtual privada, asegúrese de que los grupos de VPC seguridad y la red ACLs permitan el tráfico entrante y saliente para el prefijo de la red local. Para obtener más información, consulte Grupos de seguridad y redes ACLs en la Guía del VPC usuario de Amazon.
3. En el caso de una interfaz virtual privada, asegúrese de que las tablas de VPC enrutamiento tengan prefijos que apunten a la puerta de enlace privada virtual a la que está conectada la interfaz virtual privada. Por ejemplo, si prefiere que todo el tráfico se dirija hacia la 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. VPC
   - Como alternativa, habilite la propagación de rutas para actualizar automáticamente las rutas de sus tablas de rutas en función de su anuncio dinámico de rutas. BGP Puede tener hasta 100 rutas propagadas por tabla de rutas. Este límite no se puede aumentar. Para obtener más información, consulte Habilitar y deshabilitar la propagación de rutas en la Guía del VPC usuario de Amazon.
4. Si los pasos anteriores no resuelven sus problemas de enrutamiento, póngase en contacto con AWS Support.

El siguiente diagrama contiene los pasos para diagnosticar problemas de direccionamiento.


Interface and BGP are up, but cannot route traffic
Are you advertising a route for your network prefix?
No
Advertise your private or public network prefix
Yes
(Private) Do security groups/ network ACLs allow network traffic?
No
Add inbound and outbound rules for on-premises network prefix
Yes
(Private) Does route table have route to virtual private gateway?
No
Ensure VPC route table has prefixes pointing to virtual private gateway
Yes
Contact Support

Historial de documentos

En la siguiente tabla se describen las versiones de AWS Direct Connect.

Característica	Descripción	Fecha
Support para SiteLink	Puede crear una interfaz privada virtual que permita la conectividad entre dos puntos de presencia de Direct Connect (PoPs) en la misma AWS región. Para obtener más información, consulte Interfaces AWS Direct Connect virtuales alojadas.	01/12/2021
Support MAC Security	Puede utilizar AWS Direct Connect conexiones compatibles MACsec con el cifrado de los datos desde el centro de datos corporativo hasta la AWS Direct Connect ubicación. Para obtener más información, consulte MACseguridad (MACsec).	31 de marzo de 2021
Compatibilidad con 100 G	Temas actualizados para incluir la compatibilidad con conexiones dedicadas de 100 G.	2021-02-12
Ubicación nueva en Italia	Tema actualizado para incluir la ubicación nueva en Italia. Para obtener más información, consulte the section called “Europa (Milán)”.	2021-01-22
Nueva ubicación en Israel	Tema actualizado para incluir la ubicación nueva en Israel. Para obtener más información, consulte the section called “Israel (Tel Aviv)”.	2020-07-07
Compatibilidad de la prueba de conmutación por error del conjunto de herramientas de resiliencia	Utilice la característica de prueba de conmutación por error del conjunto de herramientas de resiliencia para probar la resiliencia de sus conexiones. Para obtener más información, consulte the section called “Prueba de conmutación por error”.	03-06-2020

Característica	Descripción	Fecha
CloudWatch VIFsoporte métrico	Puede monitorear AWS Direct Connect las conexiones físicas y las interfaces virtuales mediante CloudWatch. Para obtener más información, consulte the section called “Monitoriza con Amazon CloudWatch”.	11-05-2020
AWS Direct Connect Kit de herramientas de resiliencia	El kit de herramientas de AWS Direct Connect resiliencia proporciona un asistente de conexión con varios modelos de resiliencia que le ayuda a solicitar conexiones específicas para lograr su objetivo. SLA Para obtener más información, consulte AWS Direct Connect Kit de herramientas de resiliencia.	07-10-2019
Compatibilidad con regiones adicionales para permitir el uso de AWS Transit Gateway entre cuentas	Para obtener más información, consulte the section called “Asociaciones de la puerta de enlace de tránsito”.	30-09-2019
AWS Direct Connect Support para AWS Transit Gateway	Puede usar una AWS Direct Connect puerta de enlace para conectar su AWS Direct Connect conexión a través de una interfaz virtual de tránsito a VPCs o VPNs conectada a su puerta de enlace de tránsito. Asocia una puerta de enlace Direct Connect a la puerta de enlace de tránsito Luego, crea una interfaz virtual de tránsito para su AWS Direct Connect conexión a la puerta de enlace Direct Connect. Para obtener más información, consulte the section called “Asociaciones de la puerta de enlace de tránsito”.	27-03-2019
Compatibilidad con tramas gigantes	Puede enviar tramas gigantes (9001MTU). AWS Direct Connect Para obtener más información, consulte MTUspara interfaces virtuales privadas o interfaces virtuales de tránsito.	11/10/2018

Característica	Descripción	Fecha
Comunidades de preferencias BGP locales	Puede usar etiquetas de BGP comunidad de preferencias locales para lograr el equilibrio de carga y la preferencia de ruta para el tráfico entrante a su red. Para obtener más información, consulte BGPComunidades de preferencias locales.	06/02/2018
AWS Direct Connect gateway	Puede usar una puerta de enlace Direct Connect para conectar su AWS Direct Connect conexión VPCs en regiones remotas. Para obtener más información, consulte AWS Direct Connect pasarelas.	01/11/2017
CloudWatch Métricas de Amazon	Puedes ver CloudWatch las métricas de tus AWS Direct Connect conexiones. Para obtener más información, consulte Monitoriza con Amazon CloudWatch.	2017-06-29
Grupos de agregación de enlaces (LAG)	Puede crear un grupo de agregación de enlaces (LAG) para agregar varias AWS Direct Connect conexiones. Para obtener más información, consulte Grupos de agregación de enlaces (LAGs).	13/02/2017
IPv6soporte	Su interfaz virtual ahora puede admitir una sesión de IPv6 BGP emparejamiento. Para obtener más información, consulte Añadir un BGP par a una interfaz AWS Direct Connect virtual.	01/12/2016
Compatibilidad del etiquetado	Ahora puede etiquetar sus AWS Direct Connect recursos. Para obtener más información, consulte Etiquetar AWS Direct Connect recursos.	04/11/2016
Autoservicio - LOA CFA	Ahora puede descargar su carta de autorización y la asignación de la instalación de conexión (LOA-CFA) utilizando la AWS Direct Connect consola oAPI.	22/06/2016
Nueva ubicación en Silicon Valley	Tema actualizado para incluir la ubicación nueva en Silicon Valley en la región Oeste de EE. UU. (Norte de California).	03/06/2016

Característica	Descripción	Fecha
Nueva ubicación en Ámsterdam	Tema actualizado para incluir la ubicación nueva en Ámsterdam en la región Europa (Fráncfort).	19/05/2016
Nuevas ubicaciones en Portland, Oregón y Singapur	Tema actualizado para incluir las ubicaciones nuevas en Portland, Oregón y Singapur en las regiones Oeste de EE. UU. (Oregón) y Asia-Pacífico (Singapur).	27/04/2016
Nueva ubicación en São Paulo, Brasil	Tema actualizado para incluir la ubicación nueva en São Paulo en la región América del Sur (São Paulo).	09/12/2015
Nuevas ubicaciones en Dallas, Londres, Silicon Valley y Mumbai	Se actualizaron los temas para incluir la incorporación de nuevas ubicaciones en Dallas (región EE.UU. Este (Norte de Virginia)), Londres (región Europa (Irlanda)), Silicon Valley AWS GovCloud (región EE.UU. Oeste) y Bombay (región Asia Pacífico (Singapur)).	27/11/2015
Ubicación nueva en la región China (Pekín)	Temas actualizados para incluir la ubicación nueva en Pekín en la región China (Pekín).	14/04/2015
Nueva ubicación en Las Vegas en la región EE. UU. Oeste (Oregón)	Se actualizaron los temas para incluir la incorporación de la nueva sucursal de AWS Direct Connect Las Vegas en la región de EE. UU. Oeste (Oregón).	10/11/2014

Característica	Descripción	Fecha
Nueva región UE (Fráncfort)	Se actualizaron los temas para incluir la incorporación de nuevas AWS Direct Connect ubicaciones que prestan servicio a la región de la UE (Fráncfort).	23/10/2014
Nuevas ubicaciones en la región Asia Pacífico (Sídney)	Se actualizaron los temas para incluir la incorporación de nuevas AWS Direct Connect ubicaciones que prestan servicio a la región de Asia Pacífico (Sídney).	14/07/2014
Support para AWS CloudTrail	Se ha añadido un nuevo tema para explicar cómo se puede utilizar CloudTrail para registrar la actividad AWS Direct Connect. Para obtener más información, consulte AWS Direct Connect APIRegistra llamadas usando AWS CloudTrail.	04/04/2014
Support para acceder a AWS regiones remotas	Nuevo tema añadido que explica cómo puede acceder a los recursos públicos de una región remota. Para obtener más información, consulte Acceso a AWS regiones remotas.	19/12/2013
Compatibilidad con conexiones alojadas	Temas actualizados para incluir la compatibilidad con conexiones alojadas.	22/10/2013
Nueva ubicación en la región UE (Irlanda)	Se actualizaron los temas para incluir la adición de una nueva AWS Direct Connect ubicación que presta servicio a la región de la UE (Irlanda).	24/06/2013

Característica	Descripción	Fecha
Nueva ubicación en Seattle en la región EE. UU. Oeste (Oregón)	Se actualizaron los temas para incluir la incorporación de una nueva AWS Direct Connect sucursal en Seattle, que presta servicio a la región de EE. UU. Oeste (Oregón).	08/05/2013
Support para su uso IAM con AWS Direct Connect	Se ha añadido un tema sobre el uso AWS Identity and Access Management con AWS Direct Connect. Para obtener más información, consulte the section called “Identity and Access Management”.	21/12/2012
Nueva región Asia Pacífico (Sídney)	Se actualizaron los temas para incluir la adición de una nueva AWS Direct Connect ubicación que presta servicio a la región de Asia Pacífico (Sídney).	14/12/2012
Nueva AWS Direct Connect consola y regiones de EE. UU. Este (Norte de Virginia) y Sudamérica (São Paulo)	Se sustituyó la AWS Direct Connect Guía de introducción por la Guía AWS Direct Connect del usuario. Se agregaron nuevos temas relacionados con la nueva AWS Direct Connect consola, se agregó un tema de facturación, se agregó información sobre la configuración del router y se actualizaron los temas para incluir la adición de dos nuevas AWS Direct Connect ubicacion es que prestan servicio a las regiones de EE. UU. Este (Virginia del Norte) y Sudamérica (São Paulo).	13/08/2012

Característica	Descripción	Fecha
Compatibilidad con las regiones UE (Irlanda), Asia Pacífico (Singapur) y Asia Pacífico (Tokio)	Se agregó una nueva sección de solución de problemas y se actualizaron los temas para incluir la adición de cuatro nuevas AWS Direct Connect ubicaciones que prestan servicio a las regiones de EE. UU. Oeste (Norte de California), UE (Irlanda), Asia Pacífico (Singapur) y Asia Pacífico (Tokio).	10/01/2012
Compatibilidad con la región EE. UU. Oeste (Norte de California)	Temas actualizados para la región EE. UU. Oeste (Norte de California).	08/09/2011
Versión pública	La primera versión de AWS Direct Connect.	03/08/2011

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.