Guía del usuario

AWS Direct Connect

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Direct Connect: Guía del usuario

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es AWS Direct Connect? ... 1
Componentes de Direct Connect ... 2
Requisitos de red ... 2
Tipos de interfaz virtual de Direct Connect admitidos ... 3
Precios de Direct Connect ... 4
Acceso a AWS regiones remotas ... 5
Acceda a servicios públicos en una región remota ... 5
Acceso a una VPCs región remota ... 5
Network-to-Amazon Opciones de conectividad de VPC ... 6
Routing policies and BGP communities ... 6
Políticas de enrutamiento de interfaces virtuales públicas ... 6
Comunidades BGP de interfaces virtuales públicas ... 8
Políticas de enrutamiento de interfaces virtuales privadas e interfaces virtuales de tránsito ... 10
Ejemplo de enrutamiento de interfaz virtual privada ... 12
AWS Direct Connect Kit de herramientas de resiliencia ... 15
Requisitos previos ... 16
Resiliencia máxima ... 19
Alta resiliencia ... 20
Desarrollo y pruebas ... 20
Classic ... 21
Requisitos previos ... 22
Prueba de conmutación por error ... 22
Configuración de la máxima resiliencia ... 23
Paso 1: Inscríbase en AWS ... 23
Paso 2: Configurar el modelo de resiliencia ... 25
Paso 3: Crear las interfaces virtuales ... 26
Paso 4: Compruebe la configuración de resiliencia de la interfaz virtual ... 34
Paso 5: Compruebe la conectividad de las interfaces virtuales ... 34
Configuración de alta resiliencia ... 35
Paso 1: Inscríbase en AWS ... 35
Paso 2: Configurar el modelo de resiliencia ... 37
Paso 3: Crear las interfaces virtuales ... 39
Paso 4: Compruebe la configuración de resiliencia de la interfaz virtual ... 47
Paso 5: Compruebe la conectividad de las interfaces virtuales ... 47

Configuración de la resiliencia de las pruebas y el desarrollo ... 48
Paso 1: Inscríbase en AWS ... 48
Paso 2: Configurar el modelo de resiliencia ... 50
Paso 3: Crear una interfaz virtual ... 52
Paso 4: Compruebe la configuración de resiliencia de la interfaz virtual ... 60
Paso 5: Compruebe la interfaz virtual ... 60
Configurar una conexión clásica ... 61
Paso 1: Inscríbase en AWS ... 61
Paso 2: Solicita una conexión AWS Direct Connect dedicada ... 63
(Conexión dedicada) Paso 3: Descargar el documento LOA-CFA ... 65
Paso 4: Crear una interfaz virtual ... 66
Paso 5: Descargar la configuración del enrutador ... 74
Paso 6: Verificar la interfaz virtual ... 75
(Recomendado) Paso 7: Configurar conexiones redundantes ... 76
Prueba de conmutación por error de Direct Connect ... 78
Historial de pruebas ... 79
Permisos de validación ... 79
Iniciar la prueba de conmutación por error de interfaz virtual ... 80
Consulte un historial de pruebas de conmutación por error de la interfaz virtual ... 81
Detener la prueba de conmutación por error de interfaz virtual ... 81
Mantenimiento de Direct Connect ... 83
Mantenimiento planificado ... 83
... 83
Mantenimiento de emergencia ... 84
Mantenimiento por parte de terceros ... 85
Preparación de eventos de mantenimiento ... 85
Validación de resiliencia ... 86
Aplazamiento de un evento de mantenimiento ... 86
Seguridad MAC (MACsec) ... 87
MACsec conceptos ... 87
MACsec rotación de teclas ... 88
Conexiones compatibles ... 89
Conexiones dedicadas de ... 90
LAGs ... 91
Interconexiones de socios ... 91
Roles vinculados a servicios ... 92

MACsec consideraciones clave previamente compartidas CKN/CAK 92
Comience con MACsec una conexión dedicada 93
Cree una conexión de 93
(Opcional) Cree un grupo de agregación de enlaces (LAG) 93
Asociar el CKN/CAK a la conexión o al LAG 93
Configure el enrutador en las instalaciones 93
Eliminar la asociación entre el CKN/CAK y la conexión o el LAG 93
Conexiones dedicadas y alojadas 95
Conexiones dedicadas de 95
Carta de autorización y asignación de instalación de conexión (LOA-CFA) 97
Cree una conexión mediante el asistente de conexión 98
Cree una conexión clásica 100
Descargar la LOA-CFA 101
Asocie un MACsec CKN/CAK a una conexión 102
Elimine la asociación entre una clave MACsec secreta y una conexión 103
Conexiones alojadas 104
Aceptar una conexión alojada 105
Eliminar una conexión 106
Actualizar una conexión 107
Ver los detalles de la conexión de 108
Conexiones cruzadas 110
Opciones de conectividad 111
Este de EE. UU. (Ohio) 112
Este de EE. UU. (Norte de Virginia) 113
Oeste de EE. UU. (Norte de California) 114
Oeste de EE. UU. (Oregón) 115
África (Ciudad del Cabo) 115
Asia-Pacífico (Yakarta) 116
Asia-Pacífico (Bombay) 116
Asia-Pacífico (Seúl) 117
Asia-Pacífico (Singapur) 117
Asia-Pacífico (Sídney) 118
Asia-Pacífico (Tokio) 119
Canadá (centro) 119
China (Pekín) 120
China (Ningxia) 120

Europa (Fráncfort) ... 120
Europa (Irlanda) ... 121
Europa (Milán) ... 122
Europa (Londres) ... 122
Europa (París) ... 123
Europa (Estocolmo) ... 123
Europa (Zúrich) ... 123
Israel (Tel Aviv) ... 123
Medio Oriente (Baréin) ... 124
Medio Oriente (EAU) ... 124
América del Sur (São Paulo) ... 125
AWS GovCloud (Este de EE. UU.) ... 125
AWS GovCloud (Estados Unidos-Oeste) ... 125
Interfaces virtuales e interfaces virtuales alojadas ... 126
Reglas de anuncio de prefijo de interfaz virtual pública ... 126
SiteLink ... 127
Requisitos previos de las interfaces virtuales ... 129
MTUs para interfaces virtuales privadas o interfaces virtuales de tránsito ... 136
Interfaces virtuales ... 137
Requisitos previos para interfaces virtuales de tránsito a una puerta de enlace de Direct Connect ... 137
Cree una interfaz virtual pública ... 138
Crear una interfaz virtual privada ... 140
Cree una interfaz virtual de tránsito en la puerta de enlace de Direct Connect ... 143
Descargar el archivo de configuración del enrutador de ... 145
Interfaces virtuales alojadas de ... 147
Crear una interfaz virtual privada alojada ... 152
Crear una interfaz virtual pública alojada ... 154
Cree una interfaz virtual de tránsito alojada ... 156
Consultar los detalles de la interfaz virtual de ... 158
Agregar un BGP de mismo nivel ... 159
Eliminar un BGP de mismo nivel ... 161
Establecer las MTU de una interfaz virtual privada ... 161
Agregar o eliminar etiquetas de interfaz virtual de ... 162
Eliminar una interfaz virtual ... 163
Aceptar una interfaz virtual de alojada ... 164

Migrar una interfaz virtual ... 165
Grupos de agregación de enlaces (LAGs) ... 167
MACsec consideraciones ... 169
Cree un LAG ... 169
Ver los detalles del LAG ... 172
Actualizar un LAG ... 172
Asociar una conexión a un LAG ... 174
Desasociar una conexión de un LAG ... 175
Asocie un MACsec CKN/CAK a un LAG ... 176
Elimine la asociación entre una clave MACsec secreta y un LAG ... 177
Eliminar un LAG ... 177
Puertas de enlace ... 179
Puertas de enlace de Direct Connect ... 180
Escenarios ... 182
Cree una puerta de enlace de Direct Connect ... 185
Migrar de una puerta de enlace privada virtual a una puerta de enlace de Direct Connect ... 186
Eliminar una puerta de enlace de Direct Connect ... 187
Asociaciones de la puerta de enlace privada virtual ... 187
Creación de una puerta de enlace privada virtual ... 190
Asociar o desasociar puertas de enlace privadas virtuales ... 191
Crear una interfaz virtual privada a la puerta de enlace de Direct Connect ... 192
Asociar una puerta de enlace privada virtual entre cuentas ... 195
Asociaciones de la puerta de enlace de tránsito ... 196
Asociación de una puerta de enlace de tránsito entre cuentas ... 197
Asociar una puerta de enlace de tránsito a Direct Connect o desasociarla de este. ... 197
Cree una interfaz virtual de tránsito en la puerta de enlace de Direct Connect ... 200
Crear una propuesta de asociación de puerta de enlace de tránsito ... 202
Aceptar o rechazar una propuesta de asociación de puerta de enlace de tránsito ... 204
Actualizar los prefijos permitidos de una asociación de puerta de enlace de tránsito ... 205
Eliminar una propuesta de asociación de puerta de enlace de tránsito ... 206
asociaciones de redes principales de WAN en la nube ... 207
Requisitos previos ... 209
Consideraciones ... 209
Asociaciones de pasarelas Direct Connect a una red central de Cloud WAN ... 210
Verificar la asociación de una puerta de enlace de Direct Connect ... 210
Interacciones de prefijos permitidos ... 211

Asociaciones de la puerta de enlace privada virtual ... 211
Asociaciones de la puerta de enlace de tránsito ... 212
Ejemplo: Prefijos permitidos en una configuración de puerta de enlace de tránsito ... 213
Etiquetar recursos ... 216
Restricciones de las etiquetas ... 217
Uso de etiquetas mediante la CLI o la API ... 218
Ejemplos ... 218
Seguridad ... 220
Protección de los datos ... 221
Privacidad del tráfico entre redes ... 222
Cifrado ... 222
Identity and Access Management ... 223
Público ... 224
Autenticación con identidades ... 224
Administración de acceso mediante políticas ... 228
Funcionamiento de Direct Connect con IAM ... 231
Ejemplos de políticas basadas en identidades de Direct Connect ... 238
Roles vinculados a servicios ... 250
AWS políticas gestionadas ... 253
Solución de problemas ... 255
Registro y supervisión ... 257
Validación de conformidad ... 258
Resiliencia en Direct Connect ... 259
Conmutación por error ... 259
Seguridad de la infraestructura ... 260
Protocolo de puerta de enlace fronteriza ... 261
Utilice la AWS CLI ... 262
Paso 1: Cree una conexión ... 262
Paso 2: Descargar el documento LOA-CFA ... 263
Paso 3: Crear una interfaz virtual y obtener la configuración del enrutador ... 264
Registro de llamadas a la API de ... 270
AWS Direct Connect información en CloudTrail ... 270
Comprenda las entradas de los archivos de AWS Direct Connect registro ... 271
Supervisar los recursos de Direct Connect ... 276
Herramientas de supervisión ... 276
Herramientas de supervisión automatizadas ... 277

Herramientas de supervisión manuales 277
Monitoriza con Amazon CloudWatch 278
AWS Direct Connect métricas y dimensiones 278
Ver las CloudWatch métricas de Direct Connect 285
Cree alarmas para supervisar conexiones 286
Cuotas de Direct Connect 288
Cuotas del BGP 292
Consideraciones sobre el equilibrio de carga 292
Solución de problemas 293
Problemas de capa 1 (físicos) 293
Problemas de capa 2 (enlace de datos) 296
Problemas de capa 3/4 (red/transporte) 297
Problemas de enrutamiento 300
Historial de documentos 302
..... cccx

¿Qué es AWS Direct Connect?

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

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

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

Contenido

- AWS Direct Connect componentes
- Requisitos de red
- Tipos de interfaz virtual de Direct Connect admitidos
- Precios de Direct Connect
- Acceso a AWS Direct Connect regiones remotas

- AWS Direct Connect políticas de enrutamiento y comunidades BGP

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 su VPC. Los tipos de interfaces admitidas se describen a continuación en the section called “Tipos de interfaz virtual de Direct Connect admitidos”. Para obtener más información sobre las interfaces admitidas, consulte AWS Direct Connect interfaces virtuales e interfaces virtuales alojadas y Requisitos 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 información, consulte Socios de APN que trabajan con AWS Direct Connect.
- Está trabajando con un proveedor de servicios independientes para conectarse a AWS Direct Connect.

Además, la red debe cumplir las siguientes condiciones:

- Su red debe utilizar fibra monomodo con un transceptor 1000BASE-LX (1310 nm) para Ethernet de 1 gigabit, un transceptor 10GBASE-LR (1310 nm) para 10 gigabits, un 100GBASE- para Ethernet de 100 gigabit o un transceptor 400GBASE- para Ethernet de 400 Gbps. LR4 LR4
- Según el punto de conexión de AWS Direct Connect que dé servicio a su conexión, es posible que sea necesario habilitar o deshabilitar la negociación automática de los dispositivos locales para cualquier conexión dedicada. Si una interfaz virtual permanece inactiva cuando hay una conexión Direct Connect activa, consulteSolución de problemas de capa 2 (enlace de datos).
- La encapsulación de VLAN 802.1Q debe ser compatible en toda la conexión, incluidos los dispositivos intermedios.
- El dispositivo debe ser compatible con el protocolo Border Gateway (BGP) y la autenticación BGP MD5 .
- (Opcional) Puede configurar la detección de reenvío bidireccional (BFD) en la red. El BFD asíncrono se habilita automáticamente para cada interfaz virtual. AWS Direct Connect Se habilita de forma automática en las interfaces virtuales de Direct Connect, pero no funcionará hasta que la configure en el enrutador. A fin de obtener más información, consulte Habilitar la BFD para una conexión de Direct Connect.

AWS Direct Connect es compatible con los protocolos de comunicación y los protocolos de comunicación IPv4 . IPv6 IPv6 se 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 la trama Ethernet de 1522 o 9023 bytes (encabezado de Ethernet de 14 bytes + etiqueta VLAN de 4 bytes + bytes para el datagrama IP + FCS de 4 bytes) en la capa de enlace. Puede establecer la MTU de sus interfaces virtuales privadas. Para obtener más información, consulte MTUs para interfaces virtuales privadas o interfaces virtuales de tránsito.

Tipos de interfaz virtual de Direct Connect admitidos

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

- Interfaz virtual privada

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

  - Conéctese directamente a una sola VPC por interfaz virtual privada para acceder a esos recursos mediante el uso privado de IPs 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 privada

  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 varias puertas de enlace de tránsito de Amazon VPC asociadas a puertas de enlace de Direct Connect. Con una interfaz virtual de tránsito, puede conectar varias pasarelas de tránsito de Amazon VPC a través de varias cuentas y Regiones de AWS (excepto en las regiones de AWS China).

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

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

Precios de Direct Connect

AWS Direct Connect tiene dos elementos de facturación: 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 puerta de enlace 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 transferencia de datos salientes (DTO) se mide al propietario del recurso según la velocidad de transferencia de datos. AWS Direct Connect

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

Acceso a AWS Direct Connect 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 su cuenta en cualquier otra región pública (excepto China (Pekín y Ningxia). Por lo tanto, puede utilizar una única conexión de AWS Direct Connect para crear servicios en varias regiones. Todo el tráfico de red permanece en la red troncal AWS global, independientemente de si accede 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 sobre las comunidades de BGP admitidas para las conexiones de AWS Direct Connect , consulte Routing policies and BGP communities.

Acceda a servicios públicos en una región remota

Para obtener acceso a los recursos públicos de una región remota, debe configurar una interfaz virtual pública y establecer una sesión de protocolo de puerta de enlace fronteriza (BGP). Para obtener más información, consulte Interfaces virtuales e interfaces virtuales alojadas.

Tras crear una interfaz virtual pública y establecer una sesión de BGP en ella, el router aprende las rutas de las demás regiones públicas AWS . 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 puerta de enlace 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, puede crear una interfaz virtual pública para su AWS Direct Connect conexión y, a continuación, establecer una conexión VPN con su VPC en la región remota. A fin de obtener más información sobre la configuración de la conectividad de la VPN con una VPC, consulte Escenarios para el uso de Amazon Virtual Private Cloud en la Guía del usuario de Amazon VPC.

Network-to-Amazon Opciones de conectividad de VPC

La siguiente configuración se puede utilizar para conectar redes remotas con su entorno de Amazon VPC. 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 de enrutamiento y comunidades BGP

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

Políticas de enrutamiento de interfaces virtuales públicas

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

Se aplican las siguientes políticas de enrutamiento de entrada:

- Debe poseer los prefijos públicos y deben estar registrados como tales en el registro de Internet regional correspondiente.
- El tráfico debe estar destinado a los prefijos públicos de Amazon. No se admite el enrutamiento transitivo entre las conexiones.
- 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 enrutamiento de salida:

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

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

- AWS Direct Connect anuncia prefijos con una longitud de ruta mínima de 3.
- AWS Direct Connect anuncia todos los prefijos públicos en la conocida comunidad BGP. `NO_EXPORT`
- Si anuncias los mismos prefijos desde dos regiones diferentes mediante dos interfaces virtuales públicas diferentes y ambas tienen los mismos atributos de BGP y la longitud de prefijo más larga, se AWS dará prioridad a la región de origen para el tráfico saliente.
- Si tiene varias AWS Direct Connect conexiones, puede ajustar la distribución de la carga del tráfico entrante anunciando prefijos con los mismos atributos de ruta.
- Los prefijos anunciados por no AWS Direct Connect deben anunciarse más allá de los límites de la red de su conexión. Por ejemplo, estos prefijos no se deben incluir en ninguna tabla de enrutamiento de Internet pública.
- AWS Direct Connect conserva los prefijos anunciados por los clientes dentro de la red de Amazon. No volvemos a anunciar los prefijos de los clientes que se obtienen de una interfaz virtual pública en ninguno de los siguientes sitios:
  - Otros clientes AWS Direct Connect
  - Redes compatibles con la red AWS global
  - Proveedores de conexión de Amazon

- Al utilizar una interfaz pública, puede utilizar una ASN pública o privada. Sin embargo, hay consideraciones importantes:
  - Público ASNs: debes ser el propietario de la ASN y tener derecho a anunciarla. AWS verificará que eres el propietario de la ASN.
  - Privado ASNs: puedes usar el modo privado ASNs (64512-65534, 4200000000-4294967294). Sin embargo, AWS Direct Connect sustituirá el ASN privado por el AWS ASN (7224) cuando anuncie sus prefijos a otros clientes o a través de Internet. AWS
  - SAN antepecho:
    - En el caso de un ASN público, la preposición funcionará según lo previsto, y tu ASN antedicho estará visible en otras redes.
    - En el caso de un ASN privado, se eliminarán todas las suposiciones que realices cuando sustituyas tu ASN privado por el 7224 AWS . Esto significa que la sumisión a un ASN no es eficaz para influir en las decisiones de enrutamiento si no AWS se utiliza un ASN privado en una interfaz virtual pública.
- Al establecer una sesión de emparejamiento de BGP a AWS través de una interfaz virtual pública, utilice 7224 como números de sistema autónomo (ASN) para establecer la sesión de BGP de forma paralela. AWS El ASN del router o dispositivo de puerta de enlace del cliente debe ser diferente al de ese ASN.

Comunidades BGP de interfaces virtuales públicas

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

Ámbito de las comunidades BGP

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

Región de AWS comunidades

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

- `7224:9100`—Locales Regiones de AWS
- `7224:9200`—Todo Regiones de AWS para un continente:
  - En toda América del Norte
  - Asia Pacífico
  - Europa, Medio Oriente y África
- `7224:9300`—Global (todas las regiones públicas AWS)

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

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

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

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

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

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

Comunidad BGP de **NO_EXPORT**

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

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

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

Políticas de enrutamiento de interfaces virtuales privadas e interfaces virtuales de tránsito

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

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

- AWS evalúa primero la longitud más larga del prefijo. AWS recomienda anunciar rutas más específicas mediante varias interfaces virtuales de Direct Connect si las rutas de enrutamiento deseadas están destinadas a conexiones activas/pasivas. Consulte Influencing Traffic over Hybrid Networks using Longest Prefix Match para obtener más información.
- La preferencia local es el atributo de BGP que se recomienda utilizar cuando las rutas de enrutamiento deseadas están previstas para conexiones activas/pasivas y las longitudes de prefijo anunciadas son las mismas. Este valor se establece por región para preferir las AWS Direct Connect ubicaciones que tengan lo mismo asociado Región de AWS mediante el valor de comunidad de preferencias locales `7224:7200` —Medium. Si la región local no está asociada a la ubicación de Direct Connect, se establece en un valor inferior. Esto únicamente se aplica si no hay asignadas etiquetas de comunidad de preferencia local.
- La longitud AS_PATH se puede utilizar para determinar la ruta de enrutamiento si la longitud del prefijo y la preferencia local son iguales.
- El discriminador de salidas múltiples (MED) se puede utilizar para determinar la ruta de enrutamiento cuando la longitud del prefijo, la preferencia local y AS_PATH coinciden. AWS no recomienda el uso de valores MED debido a su menor prioridad en la evaluación.

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

Comunidades BGP de interfaces virtuales privadas e interfaces virtuales de tránsito

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

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

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

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

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

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

Comunidades de BGP de preferencia local

Puede utilizar las etiquetas de comunidad de BGP de preferencia local para lograr el equilibrio entre el balanceo de carga y las preferencias de ruta del tráfico entrante a la red. Para cada prefijo que

usted comunica en una sesión de BGP, puede aplicar una etiqueta de comunidad para indicar la prioridad de la ruta asociada en el tráfico de retorno.

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

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

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

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

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

VIFs Tienen las siguientes configuraciones:

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

Si cambia la configuración del rango de CIDR de la interfaz virtual C, las rutas que se encuentren dentro del rango de CIDR de la interfaz virtual C utilizarán la interfaz virtual C porque tiene la longitud de prefijo más larga.

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

East
East
Corporate data center
us-east-1
VIF A
VIF B
VIF C
Direct Connect gateway
Corporate data center
West
West

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

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

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

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

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

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

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

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

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

Requisitos previos

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

nm) para 10 gigabits, 100GBASE- para Ethernet de 100 gigabit o 400GBASE- para Ethernet de 400 Gbps. LR4 LR4

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

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 AWS Direct Connect ubicación. 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: 1000BASE-LX (1310 nm), 10 Gbps: 10GBASE-LR (1310 nm), 100 Gbps: 100 GBASE o 400 GBASE para Ethernet de 400 Gbps. LR4 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 socio del programa de socios para conectar un router desde su centro de datos, oficina o entorno de colocación a AWS Direct Connect una ubicación. 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 1000BASE-LX (1310 nm) para Ethernet de 1 gigabit, un transceptor 10GBASE-LR (1310 nm) para 10 gigabits, un transceptor 100GBASE- para Ethernet de 100 gigabit o un transceptor 400GBASE- para Ethernet de 400 Gbps. LR4 LR4
- Según el punto de conexión de AWS Direct Connect que dé servicio a su conexión, es posible que sea necesario habilitar o deshabilitar la negociación automática de los dispositivos locales para cualquier conexión dedicada. Si una interfaz virtual permanece inactiva cuando hay una conexión Direct Connect activa, consulteSolución de problemas de capa 2 (enlace de datos).
- La encapsulación de VLAN 802.1Q debe ser compatible en toda la conexión, incluidos los dispositivos intermedios.
- El dispositivo debe ser compatible con el protocolo Border Gateway (BGP) y la autenticación BGP MD5 .
- (Opcional) Puede configurar la detección de reenvío bidireccional (BFD) en la red. El BFD asíncrono se habilita automáticamente para cada interfaz virtual. AWS Direct Connect Se habilita de forma automática en las interfaces virtuales de Direct Connect, pero no funcionará hasta que la configure en el enrutador. A fin de obtener más información, consulte Habilitar la BFD para una conexión de Direct Connect.

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

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

  Solo necesita la velocidad para una conexión.

Resiliencia máxima

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

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

Alta resiliencia

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

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

Desarrollo y pruebas

Puede conseguir resiliencia de desarrollo y pruebas para cargas de trabajo no críticas mediante el uso de conexiones independientes que terminan en dispositivos independientes en una ubicación

(tal y como se muestra en la siguiente figura). Este modelo proporciona resiliencia frente a errores de dispositivos, pero no ofrece resiliencia frente a errores de ubicación.

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

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:

- Su red debe utilizar fibra monomodo con un transceptor 1000BASE-LX (1310 nm) para Ethernet de 1 gigabit, un transceptor 10GBASE-LR (1310 nm) para 10 gigabits, un transceptor 100GBASE- para Ethernet de 100 gigabit o un transceptor 400GBASE- para Ethernet de 400 Gbps. LR4 LR4
- Según el punto de conexión de AWS Direct Connect que dé servicio a su conexión, es posible que sea necesario habilitar o deshabilitar la negociación automática de los dispositivos locales para cualquier conexión dedicada. Si una interfaz virtual permanece inactiva cuando hay una conexión Direct Connect activa, consulteSolución de problemas de capa 2 (enlace de datos).
- La encapsulación de VLAN 802.1Q debe ser compatible en toda la conexión, incluidos los dispositivos intermedios.
- El dispositivo debe ser compatible con el protocolo Border Gateway (BGP) y la autenticación BGP MD5 .
- (Opcional) Puede configurar la detección de reenvío bidireccional (BFD) en la red. El BFD asíncrono se habilita automáticamente para cada interfaz virtual. AWS Direct Connect Se habilita de forma automática en las interfaces virtuales de Direct Connect, pero no funcionará hasta que la configure en el enrutador. A fin de obtener más información, consulte Habilitar la BFD para una conexión de Direct Connect.

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

Utilice el kit de herramientas AWS Direct Connect de resiliencia AWS Direct Connect para configurar 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 o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

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

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

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

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión 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. Active la autenticación multifactor (MFA) para el usuario raíz.

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

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

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

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

Inicio de sesión como usuario con acceso de administrador

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

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

Concesión de acceso a usuarios adicionales

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

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

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

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

Paso 2: Configurar el modelo de resiliencia

Para configurar un modelo de resiliencia máxima

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

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

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

   b. En First Location Service Provider, selecciona la 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 Siguiente.
7. Revise las conexiones y, a continuación, elija Continue (Continuar).

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

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

Paso 3: Crear las interfaces virtuales

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

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

Recurso	Información necesaria
Conexión	El grupo de AWS Direct Connect conexión o agregación de enlaces (LAG) para el que va a crear la interfaz virtual.
Nombre de la interfaz virtual	Un nombre para la interfaz virtual.
Propietario de la interfaz virtual	Si va a crear la interfaz virtual para otra cuenta, necesitará el ID de AWS cuenta de la otra cuenta.
(Solo para la interfaz virtual privada) Conexión	Para conectarse a una VPC de la misma AWS región, necesita la puerta de enlace privada virtual para su VPC. El ASN del lado de Amazon de la sesión del BGP se hereda de la puerta de enlace privada virtual. Al crear una puerta de enlace privada virtual, puede especificar su propio ASN privado. De lo contrario, Amazon proporciona un ASN predeterminado. Para obtener información, consulte Crear una puerta de enlace privada virtual en la Guía del usuario de Amazon VPC. Para conectarse a una VPC a través de una puerta de enlace de Direct Connect, se necesita la puerta de enlace de Direct Connect. Para obtener más información, consulte Puertas de enlace de Direct Connect.
VLAN	Una etiqueta de red de área local virtual (VLAN) única que aún no se encuentra en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de 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 interconexión BGP para IPv4 cada sesión o una de ellas (doble pila). IPv6 No utilices Elastic IPs (EIPs) ni traigas tus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias sesiones de BGP para la misma familia de enrutamiento IP en la misma interfaz virtual. Los rangos de

Recurso	Información necesaria

	las direcciones IP que se asignan a cada extremo de la interfaz virtual para la sesión de intercambio de tráfico del BGP.
	
	• IPv4:
	  • (Solo interfaz virtual pública) Debe especificar IPv4 direcciones públicas únicas de su propiedad. El valor puede ser uno de los siguientes:
	  • Un CIDR propiedad del cliente IPv4
	
	  Puede ser cualquier tipo de máscara pública IPs (propiedad del cliente o proporcionada por él AWS), pero se debe usar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del router. AWS Por ejemplo, si asigna un `/31` rango, por ejemplo, podría usarlo `203.0.113.0` para su IP homóloga y `203.0.113.1` para la AWS IP homóloga. `203.0.113.0/31` O bien, si asignas un `/24` rango, por ejemplo`198.51.100.0/24` , puedes usarlo `198.51.100.10` para tu IP homóloga y `198.51.100.20` para la IP AWS homóloga.
	  • Un rango de IP propiedad de su AWS Direct Connect socio o ISP, junto con una autorización LOA-CFA
	  • Un AWS CIDR /31 proporcionado. Ponte en contacto con AWS Support para solicitar un IPv4 CIDR público (y proporciona un caso de uso en tu solicitud)
	
	  Note
	  No podemos garantizar que podamos tramitar todas las solicitudes AWS de direcciones públicas IPv4 proporcionadas.
	  • (Solo interfaz virtual privada) Amazon puede generar IPv4 direcciones privadas para usted. Si especifica la suya propia, asegúrese de especific ar privada únicamente CIDRs para la interfaz de su router y la interfaz AWS Direct Connect. Por ejemplo, no especifique otras direcciones IP de su red local. Al igual que en una interfaz virtual pública, se debe utilizar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del AWS router. Por ejemplo, si asigna un `/30`

Recurso	Información necesaria
	rango, por ejemplo, podría usarlo `192.168.0.1` para su IP homóloga y `192.168.0.2` para la IP AWS homóloga. `192.168.0.0/30` • IPv6: Amazon te asigna automáticamente un CIDR de IPv6 /125. No puede especificar sus propias direcciones homólogas. IPv6
Familia de direcciones	Si la sesión de emparejamiento de BGP finalizará o. IPv4 IPv6
Información sobre el BGP	• Un número de sistema autónomo (ASN) para el protocolo de puerta de enlace fronteriza (BGP) público o privado en su lado de la sesión del BGP. Si utiliza un ASN público, debe tener uno propio. Si utiliza un ASN privado, puede establecer un valor de ASN personalizado. Para un ASN de 16 bits ASN, el valor debe estar dentro del rango de 64 512 a 65 534. En el caso de un ASN de 32 bits, el valor debe estar dentro del rango de 1 a 2147483647. El sistema autónomo (AS) que se antepone no funciona si utiliza un ASN privado para una interfaz virtual pública. • AWS se habilita de forma MD5 predeterminada. Esta opción no se puede modificar. • Una clave de autenticación MD5 BGP. Puede proporcionar su propia clave o dejar que Amazon genere una en su nombre.

Recurso	Información necesaria

(Solo para la interfaz virtual pública) Prefijos que desea anunciar	IPv4 Rutas públicas o IPv6 rutas para anunciar a través de BGP. Debe comunicar al menos un prefijo a través del BGP, hasta un máximo de 1 000 prefijos.
	• IPv4: El IPv4 CIDR puede superponerse con otro IPv4 CIDR público que se haya anunciado que AWS Direct Connect se utilice cuando se dé alguna de las siguientes condiciones:
	  • CIDRs Son de diferentes regiones. AWS Asegúrese de aplicar etiquetas de comunidad del BGP a los prefijos públicos.
	  • Utiliza AS_PATH cuando tiene un ASN público en una configuración. active/passive
	  Para obtener más información, consulte Políticas de enrutamiento y comunidades de BGP.
	• A través de una interfaz virtual pública de Direct Connect, puede especificar cualquier longitud de prefijo de /1 a /32 IPv4 y de /1 a /64 para. IPv6
	• Puede agregar prefijos adicionales a una interfaz virtual pública existente y anunciarlos si se pone en contacto con AWS Asistencia. En su caso de soporte, proporcione una lista de los prefijos de CIDR adicionales que desee agregar a la interfaz virtual pública y anunciar.

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

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

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

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

1. Abre la 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 VLAN, escriba el número de ID de la red de área local virtual (VLAN).
   d. En BGP ASN, escriba el número de sistema autónomo (ASN) para protocolo de puerta de enlace fronteriza (BGP) de la puerta de enlace.

      Los valores válidos son 1-2.147.483.647.
6. En Additional settings (Configuración adicional), haga lo siguiente:
   a. Para configurar un IPv4 BGP o un IPv6 peer, haga lo siguiente:

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

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

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

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

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

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

d. (Opcional) Añada o elimine una etiqueta.

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

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

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

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

Para aprovisionar una interfaz virtual privada a una VPC

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

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

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

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

   d. En Propietario de la interfaz virtual, selecciona Otra AWS cuenta y, a continuación, introduce la AWS cuenta.

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

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

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

   Los valores válidos son 1 a 2147483647.

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

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

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

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

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

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

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

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

d. (Opcional) Añada o elimine una etiqueta.

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

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

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

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

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

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

Paso 5: Compruebe la conectividad de las interfaces virtuales

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

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

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

Para verificar la conexión de la interfaz virtual a Amazon VPC

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

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 o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

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

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

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

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión 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. Active la autenticación multifactor (MFA) para el usuario raíz.

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

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

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

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

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

Inicio de sesión como usuario con acceso de administrador

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

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

Concesión de acceso a usuarios adicionales

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

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

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

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

Paso 2: Configurar el modelo de resiliencia

Para configurar un modelo de alta resiliencia

1. Abra la AWS Direct Connectconsola en la versión 2/homehttps://console.aws.amazon.com/directconnect/.
2. En el panel de navegación, elija Conexiones y, a continuación, Crear una conexión.

3. En Connection ordering type (Tipo de solicitud de conexión), elija Connection wizard (Asistente de conexión).
4. En Resiliency level (Nivel de resiliencia), elija High Resiliency (Alta resiliencia), y, a continuación, elija Next (Siguiente).
5. En el panel Configure connections (Configurar conexiones), en Connection settings (Configuración de conexión), proceda del modo siguiente:

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

      Este ancho de banda se aplica a todas las conexiones creadas.
   b. En First Location Service Provider, seleccione la ubicación adecuada 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 Siguiente.
7. Revise las conexiones y, a continuación, elija Continue (Continuar).

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

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

Paso 3: Crear las interfaces virtuales

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

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

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

Recurso	Información necesaria
VLAN	Una etiqueta de red de área local virtual (VLAN) única que aún no se encuentra en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de 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 interconexión BGP para IPv4 cada sesión o una de ellas (doble pila). IPv6 No utilices Elastic IPs (EIPs) ni traigas tus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias sesiones de BGP para la misma familia de enrutamiento IP en la misma interfaz virtual. Los rangos de las direcciones IP que se asignan a cada extremo de la interfaz virtual para la sesión de intercambio de tráfico del BGP.
	
	• IPv4:
	  • (Solo interfaz virtual pública) Debe especificar IPv4 direcciones públicas únicas de su propiedad. El valor puede ser uno de los siguientes:
	  • Un CIDR propiedad del cliente IPv4
	
	  Puede ser cualquier tipo de máscara pública IPs (propiedad del cliente o proporcionada por él AWS), pero se debe usar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del router. AWS Por ejemplo, si asigna un `/31` rango, por ejemplo, podría usarlo `203.0.113.0` para su IP homóloga y `203.0.113.1` para la AWS IP homóloga. `203.0.113.0/31` O bien, si asignas un `/24` rango, por ejemplo`198.51.100.0/24` , puedes usarlo `198.51.100.10` para tu IP homóloga y `198.51.100.20` para la IP AWS homóloga.
	  • Un rango de IP propiedad de su AWS Direct Connect socio o ISP, junto con una autorización LOA-CFA
	  • Un AWS CIDR /31 proporcionado. Ponte en contacto con AWS Support para solicitar un IPv4 CIDR público (y proporciona un caso de uso en tu solicitud)
	
	  Note
	  No podemos garantizar que podamos tramitar todas las solicitudes AWS de direcciones públicas IPv4 proporcionadas.
	
	  • (Solo interfaz virtual privada) Amazon puede generar IPv4 direcciones privadas para usted. Si especifica la suya propia, asegúrese de especific ar privada únicamente CIDRs para la interfaz de su router y la interfaz

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

Recurso	Información necesaria

(Solo para la interfaz virtual pública) Prefijos que desea anunciar	IPv4 Rutas públicas o IPv6 rutas para anunciar a través de BGP. Debe comunicar al menos un prefijo a través del BGP, hasta un máximo de 1 000 prefijos.
	• IPv4: El IPv4 CIDR puede superponerse con otro IPv4 CIDR público que se haya anunciado que AWS Direct Connect se utilice cuando se dé alguna de las siguientes condiciones:
	  • CIDRs Son de diferentes regiones. AWS Asegúrese de aplicar etiquetas de comunidad del BGP a los prefijos públicos.
	  • Utiliza AS_PATH cuando tiene un ASN público en una configuración. active/passive
	  Para obtener más información, consulte Políticas de enrutamiento y comunidades de BGP.
	• A través de una interfaz virtual pública de Direct Connect, puede especificar cualquier longitud de prefijo de /1 a /32 IPv4 y de /1 a /64 para. IPv6
	• Puede agregar prefijos adicionales a una interfaz virtual pública existente y anunciarlos si se pone en contacto con AWS Asistencia. En su caso de soporte, proporcione una lista de los prefijos de CIDR adicionales que desee agregar a la interfaz virtual pública y anunciar.

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

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

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

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

1. Abre la 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 VLAN, escriba el número de ID de la red de área local virtual (VLAN).
   d. En BGP ASN, escriba el número de sistema autónomo (ASN) para protocolo de puerta de enlace fronteriza (BGP) de la puerta de enlace.

      Los valores válidos son 1-2.147.483.647.
6. En Additional settings (Configuración adicional), haga lo siguiente:
   a. Para configurar un IPv4 BGP o un IPv6 peer, haga lo siguiente:

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

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

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

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

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

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

d. (Opcional) Añada o elimine una etiqueta.

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

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

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

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

Para aprovisionar una interfaz virtual privada a una VPC

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

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

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

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

   d. En Propietario de la interfaz virtual, selecciona Otra AWS cuenta y, a continuación, introduce la AWS cuenta.

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

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

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

   Los valores válidos son 1 a 2147483647.

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

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

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

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

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

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

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

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

d. (Opcional) Añada o elimine una etiqueta.

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

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

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

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

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

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

Paso 5: Compruebe la conectividad de las interfaces virtuales

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

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

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

Para verificar la conexión de la interfaz virtual a Amazon VPC

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

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 suscribirse a una Cuenta de AWS

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

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

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

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

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

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión 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. Active la autenticación multifactor (MFA) para el usuario raíz.

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

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

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

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

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

Inicio de sesión como usuario con acceso de administrador

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

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

Concesión de acceso a usuarios adicionales

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

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

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

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

Paso 2: Configurar el modelo de resiliencia

Para configurar el modelo de resiliencia

1. Abra la AWS Direct Connectconsola en la versión 2/homehttps://console.aws.amazon.com/directconnect/.
2. En el panel de navegación, elija Conexiones y, a continuación, Crear una conexión.

3. En Connection ordering type (Tipo de solicitud de conexión), elija Connection wizard (Asistente de conexión).
4. En Resiliency level (Nivel de resiliencia), elija Development and test (Desarrollo y pruebas) y, a continuación, elija Next (Siguiente).
5. En el panel Configure connections (Configurar conexiones), en Connection settings (Configuración de conexión), proceda del modo siguiente:

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

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

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

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

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

Paso 3: Crear una interfaz virtual

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

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

Recurso	Información necesaria
Conexión	El grupo de AWS Direct Connect conexión o agregación de enlaces (LAG) para el que va a crear la interfaz virtual.
Nombre de la interfaz virtual	Un nombre para la interfaz virtual.
Propietario de la interfaz virtual	Si va a crear la interfaz virtual para otra cuenta, necesitará el ID de AWS cuenta de la otra cuenta.
(Solo para la interfaz virtual privada) Conexión	Para conectarse a una VPC de la misma AWS región, necesita la puerta de enlace privada virtual para su VPC. El ASN del lado de Amazon de la sesión del BGP se hereda de la puerta de enlace privada virtual. Al crear una puerta de enlace privada virtual, puede especificar su propio ASN privado. De lo contrario, Amazon proporciona un ASN predeterminado. Para obtener información, consulte Crear una puerta de enlace privada virtual en la Guía del usuario de Amazon VPC. Para conectarse a una VPC a través de una puerta de enlace de Direct Connect, se necesita la puerta de enlace de Direct Connect. Para obtener más información, consulte Puertas de enlace de Direct Connect.
VLAN	Una etiqueta de red de área local virtual (VLAN) única que aún no se encuentra en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de 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 interconexión BGP para IPv4 cada sesión o una de ellas (doble pila). IPv6 No utilices Elastic IPs (EIPs) ni traigas tus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias sesiones de BGP para la misma familia de enrutamiento IP en la misma interfaz virtual. Los rangos de las direcciones IP que se asignan a cada extremo de la interfaz virtual para la sesión de intercambio de tráfico del BGP.
	
	• IPv4:
	  • (Solo interfaz virtual pública) Debe especificar IPv4 direcciones públicas únicas de su propiedad. El valor puede ser uno de los siguientes:
	  • Un CIDR propiedad del cliente IPv4
	
	  Puede ser cualquier tipo de máscara pública IPs (propiedad del cliente o proporcionada por él AWS), pero se debe usar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del router. AWS Por ejemplo, si asigna un `/31` rango, por ejemplo, podría usarlo `203.0.113.0` para su IP homóloga y `203.0.113.1` para la AWS IP homóloga. `203.0.113.0/31` O bien, si asignas un `/24` rango, por ejemplo`198.51.100.0/24` , puedes usarlo `198.51.100.10` para tu IP homóloga y `198.51.100.20` para la IP AWS homóloga.
	  • Un rango de IP propiedad de su AWS Direct Connect socio o ISP, junto con una autorización LOA-CFA
	  • Un AWS CIDR /31 proporcionado. Ponte en contacto con AWS Support para solicitar un IPv4 CIDR público (y proporciona un caso de uso en tu solicitud)
	
	  Note
	  No podemos garantizar que podamos tramitar todas las solicitudes AWS de direcciones públicas IPv4 proporcionadas.
	
	  • (Solo interfaz virtual privada) Amazon puede generar IPv4 direcciones privadas para usted. Si especifica la suya propia, asegúrese de especific ar privada únicamente CIDRs para la interfaz de su router y la interfaz

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

Recurso	Información necesaria

(Solo para la interfaz virtual pública) Prefijos que desea anunciar	IPv4 Rutas públicas o IPv6 rutas para anunciar a través de BGP. Debe comunicar al menos un prefijo a través del BGP, hasta un máximo de 1 000 prefijos.
	• IPv4: El IPv4 CIDR puede superponerse con otro IPv4 CIDR público que se haya anunciado que AWS Direct Connect se utilice cuando se dé alguna de las siguientes condiciones:
	  • CIDRs Son de diferentes regiones. AWS Asegúrese de aplicar etiquetas de comunidad del BGP a los prefijos públicos.
	  • Utiliza AS_PATH cuando tiene un ASN público en una configuración. active/passive
	  Para obtener más información, consulte Políticas de enrutamiento y comunidades de BGP.
	• A través de una interfaz virtual pública de Direct Connect, puede especificar cualquier longitud de prefijo de /1 a /32 IPv4 y de /1 a /64 para. IPv6
	• Puede agregar prefijos adicionales a una interfaz virtual pública existente y anunciarlos si se pone en contacto con AWS Asistencia. En su caso de soporte, proporcione una lista de los prefijos de CIDR adicionales que desee agregar a la interfaz virtual pública y anunciar.

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

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

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

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

1. Abre la 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 VLAN, escriba el número de ID de la red de área local virtual (VLAN).
   d. En BGP ASN, escriba el número de sistema autónomo (ASN) para protocolo de puerta de enlace fronteriza (BGP) de la puerta de enlace.

      Los valores válidos son 1-2.147.483.647.
6. En Additional settings (Configuración adicional), haga lo siguiente:
   a. Para configurar un IPv4 BGP o un IPv6 peer, haga lo siguiente:

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

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

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

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

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

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

d. (Opcional) Añada o elimine una etiqueta.

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

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

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

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

Para aprovisionar una interfaz virtual privada a una VPC

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

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

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

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

   d. En Propietario de la interfaz virtual, selecciona Otra AWS cuenta y, a continuación, introduce la AWS cuenta.

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

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

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

   Los valores válidos son 1 a 2147483647.

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

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

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

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

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

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

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

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

d. (Opcional) Añada o elimine una etiqueta.

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

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

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

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

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

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

Paso 5: Compruebe la interfaz virtual

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

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

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

Para verificar la conexión de la interfaz virtual a Amazon VPC

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

Configurar una conexión AWS Direct Connect clásica

Configure una conexión clásica cuando tenga conexiones de 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 o mensaje de texto e indicar un código de verificación en el teclado del teléfono.

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

AWS te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

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

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión 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. Active la autenticación multifactor (MFA) para el usuario raíz.

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

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

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

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

Inicio de sesión como usuario con acceso de administrador

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

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

Concesión de acceso a usuarios adicionales

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

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

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

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

Paso 2: Solicita una conexión AWS Direct Connect dedicada

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

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

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

Para crear una AWS Direct Connect conexión nueva

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

Para obtener más información, consulte 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/versión 2/home.
2. En el panel de navegación, elija Connections (Conexiones).
3. Seleccione la conexión alojada y, a continuación, elija Aceptar.

   Elija Aceptar.

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

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

Para descargar el documento LOA-CFA

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

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

   > **Note**
   >
   > Si el enlace no está habilitado, significa que aún no puede descargar el documento LOA-CFA. Busque una solicitud para obtener más información el correo electrónico. Si sigue

sin estar disponible o no has recibido ningún correo electrónico después de 72 horas laborables, ponte en contacto con AWS Support.

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

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

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

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

Recurso	Información necesaria
Conexión	El grupo de AWS Direct Connect conexión o agregación de enlaces (LAG) para el que va a crear la interfaz virtual.
Nombre de la interfaz virtual	Un nombre para la interfaz virtual.
Propietario de la interfaz virtual	Si va a crear la interfaz virtual para otra cuenta, necesitará el ID de AWS cuenta de la otra cuenta.
(Solo para la interfaz virtual privada) Conexión	Para conectarse a una VPC de la misma AWS región, necesita la puerta de enlace privada virtual para su VPC. El ASN del lado de Amazon de la sesión del BGP se hereda de la puerta de enlace privada virtual. Al crear una puerta de enlace privada virtual, puede especificar su propio ASN privado. De lo contrario, Amazon proporciona un ASN predeterminado. Para obtener información, consulte Crear una puerta de enlace privada virtual en la Guía del usuario de Amazon VPC. Para conectarse a una VPC a través de una puerta de enlace de Direct Connect, se necesita la puerta de enlace de Direct Connect. Para obtener más información, consulte Puertas de enlace de Direct Connect.
VLAN	Una etiqueta de red de área local virtual (VLAN) única que aún no se encuentra en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de 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 interconexión BGP para IPv4 cada sesión o una de ellas (doble pila). IPv6 No utilices Elastic IPs (EIPs) ni traigas tus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias sesiones de BGP para la misma familia de enrutamiento IP en la misma interfaz virtual. Los rangos de las direcciones IP que se asignan a cada extremo de la interfaz virtual para la sesión de intercambio de tráfico del BGP.

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:
	  • Un CIDR propiedad del cliente IPv4
	
	  Puede ser cualquier tipo de máscara pública IPs (propiedad del cliente o proporcionada por él AWS), pero se debe usar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del router. AWS Por ejemplo, si asigna un `/31` rango, por ejemplo, podría usarlo `203.0.113.0` para su IP homóloga y `203.0.113.1` para la AWS IP homóloga. `203.0.113.0/31` O bien, si asignas un `/24` rango, por ejemplo`198.51.100.0/24` , puedes usarlo `198.51.100.10` para tu IP homóloga y `198.51.100.20` para la IP AWS homóloga.
	  • Un rango de IP propiedad de su AWS Direct Connect socio o ISP, junto con una autorización LOA-CFA
	  • Un AWS CIDR /31 proporcionado. Ponte en contacto con AWS Support para solicitar un IPv4 CIDR público (y proporciona un caso de uso en tu solicitud)
	
	  Note
	  No podemos garantizar que podamos tramitar todas las solicitudes AWS de direcciones públicas IPv4 proporcionadas.
	  • (Solo interfaz virtual privada) Amazon puede generar IPv4 direcciones privadas para usted. Si especifica la suya propia, asegúrese de especific ar privada únicamente CIDRs para la interfaz de su router y la interfaz AWS Direct Connect. Por ejemplo, no especifique otras direcciones IP de su red local. Al igual que en una interfaz virtual pública, se debe utilizar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del AWS router. Por ejemplo, si asigna un `/30` 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 CIDR de IPv6 /125. No puede especificar sus propias direcciones homólogas. IPv6
Familia de direcciones	Si la sesión de emparejamiento de BGP finalizará o. IPv4 IPv6
Información sobre el BGP	• Un número de sistema autónomo (ASN) para el protocolo de puerta de enlace fronteriza (BGP) público o privado en su lado de la sesión del BGP. Si utiliza un ASN público, debe tener uno propio. Si utiliza un ASN privado, puede establecer un valor de ASN personalizado. Para un ASN de 16 bits ASN, el valor debe estar dentro del rango de 64 512 a 65 534. En el caso de un ASN de 32 bits, el valor debe estar dentro del rango de 1 a 2147483647. El sistema autónomo (AS) que se antepone no funciona si utiliza un ASN privado para una interfaz virtual pública. • AWS se habilita de forma MD5 predeterminada. Esta opción no se puede modificar. • Una clave de autenticación MD5 BGP. Puede proporcionar su propia clave o dejar que Amazon genere una en su nombre.

Recurso	Información necesaria

(Solo para la interfaz virtual pública) Prefijos que desea anunciar	IPv4 Rutas públicas o IPv6 rutas para anunciar a través de BGP. Debe comunicar al menos un prefijo a través del BGP, hasta un máximo de 1 000 prefijos.
	• IPv4: El IPv4 CIDR puede superponerse con otro IPv4 CIDR público que se haya anunciado que AWS Direct Connect se utilice cuando se dé alguna de las siguientes condiciones:
	  • CIDRs Son de diferentes regiones. AWS Asegúrese de aplicar etiquetas de comunidad del BGP a los prefijos públicos.
	  • Utiliza AS_PATH cuando tiene un ASN público en una configuración. active/passive
	  Para obtener más información, consulte Políticas de enrutamiento y comunidades de BGP.
	• A través de una interfaz virtual pública de Direct Connect, puede especificar cualquier longitud de prefijo de /1 a /32 IPv4 y de /1 a /64 para. IPv6
	• Puede agregar prefijos adicionales a una interfaz virtual pública existente y anunciarlos si se pone en contacto con AWS Asistencia. En su caso de soporte, proporcione una lista de los prefijos de CIDR adicionales que desee agregar a la interfaz virtual pública y anunciar.

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

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

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

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

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

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 Public (Pública).
5. En Public virtual interface settings (Configuración de la interfaz virtual pública), haga lo siguiente:
   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.
   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.
   c. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).
   d. En BGP ASN, introduzca el número de sistema autónomo de protocolo de puerta de enlace fronteriza del enrutador del mismo nivel de las instalaciones de la nueva interfaz virtual.

Los valores válidos son 1-2.147.483.647.

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

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

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

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

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

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

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

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

   d. (Opcional) Añada o elimine una etiqueta.

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

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

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

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

Para aprovisionar una interfaz virtual privada a una VPC

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

4. En Tipo de interfaz virtual, en Tipo, elija Privada.
5. En Configuración de la interfaz virtual privada, realice lo siguiente:
   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.
   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.
   c. En Tipo de puerta de enlace, elija Puerta de enlace privada virtual o Puerta de enlace de Direct Connect.
   d. En Propietario de la interfaz virtual, selecciona Otra AWS cuenta y, a continuación, introduce la AWS cuenta.
   e. En Puerta de enlace privada virtual, elija la puerta de enlace privada virtual para utilizar con esta interfaz.
   f. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).
   g. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

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

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

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

      > **Important**
      >
      > Al configurar las interfaces virtuales de AWS Direct Connect, puede especificar sus propias direcciones IP mediante RFC 1918, utilizar otros esquemas de direccionamiento u optar por direcciones CIDR asignadas de IPv4 /29 direcciones CIDR AWS asignadas desde el rango Link-Local RFC 3927 IPv4 169.254.0.0/16 para la conectividad. point-to-point Estas point-to-point conexiones deben usarse exclusivamente para la interconexión eBGP entre el router de puerta de enlace del

cliente y el punto final de Direct Connect. Para el tráfico de VPC o la creación de túneles, como AWS Site-to-Site Private IP VPN o Transit Gateway Connect, AWS recomienda utilizar una interfaz de bucle invertido o LAN en el router de puerta de enlace del cliente como dirección de origen o destino en lugar de las conexiones. point-to-point

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

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

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

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

d. (Opcional) Añada o elimine una etiqueta.

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

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

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

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

Paso 5: Descargar la configuración del enrutador

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

Para descargar una configuración del router

1. Abra la AWS Direct Connectconsola en 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 obtener más información sobre la configuración manual del router, consulte. Descargar el archivo de configuración del enrutador de

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

Paso 6: Verificar la interfaz virtual

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

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

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

Para verificar su conexión de interfaz+interfaz virtual a Amazon VPC

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

(Recomendado) Paso 7: Configurar conexiones redundantes

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

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

- Activa/Activa (múltiples rutas de BGP). Esta es la configuración predeterminada, en la que ambas conexiones están activas. AWS Direct Connect admite múltiples rutas a múltiples interfaces virtuales dentro de la misma ubicación y la carga del tráfico se comparte entre las interfaces en función del flujo. Si una conexión no se encuentra disponible, todo el tráfico se redirige a través de la otra conexión.

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

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

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

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

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

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 interconexión de BGP 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 interconexión de BGP y cuánto tiempo se va a ejecutar la prueba. AWS coloca la sesión de interconexión BGP 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, la sesión de

interconexión de BGP produce un error y el tráfico no se enruta. Cuando se complete la prueba, o cuando la detenga manualmente, AWS restaura la sesión de BGP. Una vez finalizada la prueba, puede utilizar el kit de herramientas de AWS Direct Connect resiliencia para ajustar la configuración.

> **Note**
>
> No utilice esta característica durante un periodo de mantenimiento de Direct Connect, ya que es posible que la sesión BGP se restablezca prematuramente durante o después del mantenimiento.

Historial de pruebas

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

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

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

Permisos de validación

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

Temas

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

- 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 Acciones, Reducir BGP.

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

   a. Para que los pares se reduzcan para probarlos, elige qué sesiones de emparejamiento quieres probar, por ejemplo. IPv4
   b. En Tiempo máximo de la prueba, especifique el número de minutos que durará la prueba.

      El valor máximo es de 4320 minutos (72 horas laborables).

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

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

Para 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 emparejamiento de BGP. 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.

AWS Direct Connect mantenimiento

AWS Direct Connect se compromete a garantizar la seguridad, la disponibilidad y la escalabilidad del servicio. Para mantener estos estándares, se requiere un mantenimiento periódico de los dispositivos de red de hardware. El mantenimiento de Direct Connect se divide en dos tipos: planificado y de emergencia.

Estos eventos de mantenimiento incluyen abordar las vulnerabilidades de seguridad y los problemas de hardware, realizar migraciones de dispositivos para cumplir con las normas, corregir los defectos y ofrecer nuevas funciones. Si sigue las prácticas descritas enPreparación de eventos de mantenimiento, puede preparar mejor su entorno de Direct Connect para evitar interrupciones durante los eventos de mantenimiento. Si tiene una configuración de red no resiliente o una conexión única, experimentará una interrupción en la conectividad entre la red local y los recursos. AWS

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

Eventos de mantenimiento

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

Mantenimiento planificado de Direct Connect

Los eventos de mantenimiento planificados incluyen actualizaciones de la red, como la aplicación de parches al sistema operativo y las actualizaciones de configuración en los terminales de los dispositivos de hardware, que son necesarias para mejorar la disponibilidad y ofrecer nuevas funciones.

Estos eventos de mantenimiento se programan con 14 días de antelación y, por lo general, se producen durante un período de cuatro horas en las horas de poco tráfico en la ubicación de Direct Connect donde se encuentra el punto final del dispositivo. Por lo general, las actividades de mantenimiento se completan antes de que venza el período completo de cuatro horas y recibirás una notificación cuando termines el trabajo. En raras ocasiones, cuando circunstancias imprevistas obliguen a ampliar el período de mantenimiento, te enviaremos una notificación por separado con la estimación de finalización revisada.

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

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

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

Además:

- Reciba notificaciones en su sistema de monitoreo o venta de entradas integrándolo con AWS Health. Para realizar la integración AWS Health, consulta Monitorizar eventos AWS Health con Amazon EventBridge en la Guía del AWS Health usuario.
- Consulte los programas de mantenimiento planificados en su AWS Health Dashboard.

En raras circunstancias, un evento de mantenimiento planificado no puede ocurrir según lo programado. Si esto ocurriera, enviaremos una notificación de cancelación y reprogramaremos el evento en el futuro siguiendo el mismo proceso descrito anteriormente.

Mantenimiento de emergencia de Direct Connect

Los eventos de mantenimiento de emergencia se inician de forma crítica para evitar eventos inminentes que afecten al servicio o resolver problemas que ya hayan provocado una interrupción de la conectividad. En estos casos, es necesario tomar medidas inmediatas para restaurar el punto final afectado a un estado saludable.

Si bien nos esforzamos por avisar con antelación siempre que es posible, algunas situaciones pueden requerir que el mantenimiento comience de inmediato. Recibirás notificaciones cuando el mantenimiento de emergencia esté programado o en marcha y, de nuevo, cuando se complete.

Estos eventos suelen producirse durante un período de dos horas en la ubicación de Direct Connect en la que se encuentra el punto final del dispositivo. Las actividades de mantenimiento suelen completarse dentro de este período. En los casos en que circunstancias imprevistas exijan ampliar el período de mantenimiento, como la sustitución del hardware, enviaremos una notificación por separado con la estimación de finalización revisada.

Mantenimiento por parte de terceros

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

Preparación de eventos de mantenimiento

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

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

Durante un evento de mantenimiento planificado, Direct Connect drena el tráfico hacia y desde el punto final de conexión que se está realizando el mantenimiento y obliga al tráfico a utilizar

las conexiones redundantes. Esto permite un redireccionamiento del tráfico de red más fluido sin necesidad de intervención manual si no se ha configurado la máxima resiliencia. Como alternativa, puede optar por controlar el redireccionamiento del tráfico entre conexiones redundantes durante los períodos de mantenimiento mediante el uso de las comunidades de Border Gateway Protocol (BGP) preferidas a nivel local. Para obtener más información sobre las comunidades BGP, consulte. Routing policies and BGP communities

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

Validación de resiliencia

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

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

Solicitudes de aplazamiento o cancelación de eventos de mantenimiento

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

Seguridad MAC en AWS Direct Connect

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

En el siguiente diagrama, la AWS Direct Connect conexión cruzada debe estar conectada a una interfaz MACsec compatible en el dispositivo periférico del cliente. MACsec over Direct Connect proporciona cifrado de capa 2 para el point-to-point tráfico entre el dispositivo perimetral Direct Connect y el dispositivo perimetral del cliente. Este cifrado se produce después de intercambiar y verificar las claves de seguridad entre las interfaces de ambos extremos de la conexión cruzada.

> **Note**
>
> MACsec proporciona point-to-point seguridad en los enlaces Ethernet; por lo tanto, no proporciona end-to-end cifrado en varios segmentos secuenciales de Ethernet u otros segmentos de red.

MACsec conceptos

Los siguientes son los conceptos clave para MACsec:

- Seguridad MAC (MACsec): 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

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

  El modo de cifrado se puede configurar durante la configuración de la conexión y se puede modificar más adelante. De forma predeterminada, las nuevas conexiones MACsec habilitadas se configuran en el modo «should_encrypt» para evitar posibles problemas de conectividad durante la configuración inicial.

MACsec rotación de teclas

- Rotación CNN/CAK (manual)

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

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

- Rotación automática de la clave de asociación segura (SAK)

  El SAK, que se deriva del CKN/CAK par activo, se somete a una rotación automática en función de lo siguiente:

  - intervalos de tiempo
  - volumen de tráfico cifrado
  - MACsec establecimiento de sesión

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

Conexiones compatibles

MACsec está disponible en conexiones específicas de Direct Connect y grupos de agregación de enlaces:

MACsec Conexiones compatibles

- Conexiones dedicadas de
- LAGs
- Interconexiones entre socios

> **Note**
>
> Las conexiones alojadas MACsec son compatibles si el AWS Direct Connect socio las implementa en sus interconexiones.

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

Conexiones dedicadas de

Lo siguiente le ayudará a familiarizarse con MACsec las conexiones AWS Direct Connect dedicadas. No hay cargos adicionales por su uso MACsec. Los pasos para configurar MACsec una conexión dedicada se encuentran enComience con MACsec una conexión dedicada.

Las operaciones de interconexión de los socios siguen los mismos procedimientos que las conexiones dedicadas. Cuando ejecute comandos de CLI o SDK para las interconexiones de los socios, las respuestas incluirán información MACsec relacionada cuando corresponda.

MACsec requisitos previos para las conexiones dedicadas

Tenga en cuenta los siguientes requisitos para MACsec las conexiones dedicadas:

- MACsec es 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 las conexiones de 10 Gbps, GCM-AES-256 y GCM-AES-XPN-256.
  - Para conexiones de 100 Gbps y 400 Gbps, -256. GCM-AES-XPN
- Solo se admiten claves de 256 bits MACsec .
- Se requiere la numeración extendida de paquetes (XPN) para las conexiones de 100 Gbps y 400 Gbps. Para conexiones de 10 Gbps, Direct Connect admite GCM-AES-256 y -256. GCM-AES-XPN Las conexiones de alta velocidad, como las dedicadas de 100 Gbps y 400 Gbps, pueden agotar rápidamente el espacio original de numeración MACsec 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 necesario y debe estar activado. No se puede ajustar esta configuración.
- No se admite el IEEE 802.1Q (punto q/VLAN) tag offset/dot 1) para mover una etiqueta de VLAN fuera de q-in-clear una carga útil cifrada.

Además, debe realizar las siguientes tareas antes de configurar MACsec una conexión dedicada.

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

  Puede crear el par con una herramienta estándar abierta. El par debe cumplir los requisitos especificados de the section called “Configure el enrutador en las instalaciones”.
- Asegúrese de 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.

LAGs

Los siguientes requisitos le ayudarán a familiarizarse con los grupos MACsec de agregación de enlaces de Direct Connect (LAGs):

- LAGs debe estar compuesto por conexiones dedicadas MACsec compatibles con el cifrado MACsec
- Todas las conexiones dentro de un LAG deben tener el mismo ancho de banda y ser compatibles MACsec
- MACsec la configuración se aplica de manera uniforme en todas las conexiones del LAG
- Permite la creación de LAG y se MACsec puede hacer simultáneamente

Interconexiones entre socios

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

Roles vinculados a servicios

AWS Direct Connect utiliza funciones vinculadas al AWS Identity and Access Management servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM al que se vincula directamente. AWS Direct Connect Los roles vinculados al servicio están predefinidos AWS Direct Connect e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre. Un rol vinculado a un servicio facilita la configuración AWS Direct Connect , ya que no es necesario añadir manualmente los permisos necesarios. AWS Direct Connect define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Direct Connect puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM. Para obtener más información, consulte the section called “Roles vinculados a servicios”.

MACsec consideraciones clave previamente compartidas CKN/CAK

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

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

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

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

Comience a usarlo MACsec en una AWS Direct Connect conexión dedicada

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

Paso 1: Cree una conexión

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

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

Si utilizas varias conexiones como redundancia, puedes crear un LAG que lo admita MACsec. Para obtener más información, consulte MACsec consideraciones y Crear un grupo de agregación de enlaces (LAG).

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

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

- Asocie un MACsec CKN/CAK a una conexión
- Asocie un MACsec CKN/CAK a un LAG

Paso 4: Configurar su enrutador en las instalaciones

Actualice su router local con la MACsec clave 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 de .

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

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

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

- 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 su red y una de las AWS Direct Connect ubicaciones.

Existen dos tipos de conexiones:

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

Temas

- AWS Direct Connect Conexiones dedicadas
- AWS Direct Connect Conexiones alojadas
- Eliminar una AWS Direct Connect conexión
- Actualizar una AWS Direct Connect conexión
- Ver los detalles AWS Direct Connect de la conexión

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 Socios de APN que trabajan con 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. Puede crear una conexión independiente o puede crear una conexión para asociarla a un LAG en su cuenta. Si asocia una conexión a un LAG, se crea con la misma velocidad del puerto y ubicación especificados en el LAG.

Después de solicitar la conexión, podrá descargar una Carta de autorización y asignación de instalación de conexión (LOA-CFA) o recibirá un correo electrónico en el que se le solicitará más información. Si recibe una solicitud para obtener más información, deberá responder en un plazo de 7 días o se eliminará la conexión. La LOA-CFA es la autorización para AWS conectarse y su proveedor de red la necesita para solicitarle una conexión cruzada. Si no tiene equipo en la 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:

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

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

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

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

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

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

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

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

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

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

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

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

eliminarla usted mismo. Para obtener más información, consulte Eliminar una AWS Direct Connect conexión.

Temas

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

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. 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, 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 Siguiente.

6. En la página Configurar conexiones, proporcione los siguientes detalles.

   a. En la lista desplegable de Ancho de banda, elija el ancho de banda necesario para la conexión. Este valor puede oscilar entre 1 Gbps y 400 Gbps.

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

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

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

      MACsec solo está disponible en conexiones dedicadas.

   e. (Opcional) Seleccione Añadir etiqueta para añadir key/value pares y así poder identificar mejor esta conexión.

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

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

7. Elija Siguiente.

8. En la página Revisar y crear, verifique la conexión. En esta página también se muestran los costos estimados del uso del puerto y los cargos adicionales por transferencia de datos.

9. Seleccione Crear.

10. Descargue su Carta de autorización y asignación de instalaciones de conexión (LOA-CFA). Para obtener más información, consulte the section called “Carta de autorización y asignación de instalación de conexión (LOA-CFA)”.

Utilice uno de los siguientes comandos.

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

Crea 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. Abra 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 Añadir etiqueta para añadir key/value pares que ayuden a identificar aún más esta conexión.

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

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

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

Para obtener más información, consulte Conexiones dedicadas y alojadas.

Descarga el AWS Direct Connect LOA-CFA

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

Para descargar el documento LOA-CFA

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

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

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

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

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

Asocie un MACsec CKN/CAK a una conexión AWS Direct Connect

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

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

Para asociar una MACsec clave a una conexión

1. Abre la 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 CAK/CKN par] Elija el par de claves y, a continuación, haga lo siguiente:

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

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

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

- associate-mac-sec-key (AWS CLI)
- AssociateMacSecKey(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, la línea de comandos o la 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 clave mediante la línea de comandos o la 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

En el caso de las conexiones alojadas, los valores posibles son 50 Mbps, 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps, 500 Mbps, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps y 25 Gbps. Tenga en cuenta que solo los 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 únicamente se encuentran disponibles en ubicaciones de Direct Connect con velocidades de puerto disponibles de 100 Gbps.

Tenga en cuenta lo siguiente:

- Las velocidades de los puertos de conexión solo las puede cambiar su socio de AWS Direct Connect. Consulte con su socio de AWS Direct Connect para ver si admiten la actualización o la degradación de una conexión existente. Si su socio admite la actualización o degradación de su conexión, ya no tendrá que eliminar y volver a crear una conexión para actualizar o reducir el ancho de banda de una conexión alojada existente.
- 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 reduce 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
- Ver los detalles de la conexión de

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

Acepte una conexión 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, la línea de comandos o la API.

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 la API

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

Eliminar una AWS Direct Connect conexión

Puede eliminar una conexión siempre y cuando no tenga interfaces virtuales adjuntas. Si eliminas la conexión, se detendrán todos los cargos por hora de puerto de esta conexión, pero es posible que continúes incurriendo en cargos por conexiones cruzadas o por circuitos de red (ver más abajo). 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 la LOA de la conexión que contiene la información de las diferentes cuentas para disponer de la información relevante sobre los circuitos que se desconectan. Para conocer los pasos a fin de descargar la LOA de conexión, consulte Carta de autorización y asignación de instalación de conexión (LOA-CFA).

Al eliminar una conexión, AWS indicará al proveedor de colocación que desconecte el dispositivo de red del router Direct Connect quitando el cable de conexión cruzada de fibra óptica del panel de conexiones correspondiente. AWS Sin embargo, es posible que el proveedor de servicios de coubicación o de circuitos aún cobre cargos por conexión cruzada o por circuito de red, ya que es posible que el cable de conexión cruzada permanezca conectado al dispositivo de red. Estos cargos por la conexión cruzada son ajenos a Direct Connect, y se deben anular con el proveedor de servicios de coubicación o de circuitos a partir de la información que figura en la LOA.

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

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

Para eliminar una conexión

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

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

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

Actualizar una AWS Direct Connect conexión

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

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

> **Note**
>
> MACsec solo 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 la API

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

Ver los detalles AWS Direct Connect de la conexión

Puede ver el estado actual de la conexión mediante la AWS Direct Connect consola, la línea de comandos o la API. También puede ver el ID de conexión (por ejemplo, `dxcon-12nikabc`) y comprobar que coincide con el ID de conexión que aparece en el documento LOA-CFA que ha recibido o descargado.

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

Para ver los detalles de una conexión

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel izquierdo, elija Connections (Conexiones).

3. Seleccione una conexión y, a continuación, elija Ver detalles.

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

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

Solicitud de conexiones cruzadas en AWS Direct Connect ubicaciones

Una vez que haya descargado la Carta de autorización y Asignación de instalaciones de conexión (LOA-CFA), debe completar la conexión de red cruzada, también conocida como conexión cruzada. Si ya tiene el equipo ubicado en una AWS Direct Connect ubicación, póngase en contacto con el proveedor correspondiente para completar la conexión cruzada. Para obtener instrucciones específicas sobre cada proveedor, consulte las tablas que aparecen a continuación. Los socios y la información de contacto aparecen organizados por regiones. Para conocer los precios específicos de conexión cruzada, deberá ponerse en contacto directamente con el socio de Direct Connect. Una vez establecida la conexión cruzada, puede crear las interfaces virtuales mediante la AWS Direct Connect consola.

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

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

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

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

Opciones de conectividad

Es posible que las opciones disponibles para establecer conexión con una ubicación de Direct Connect varíen según el socio y la región de AWS . Puede trabajar con uno de los socios de la red de AWS socios (APN), que le proporcionará una o más de las siguientes opciones de conectividad:

- Si tiene recursos desplegados en la misma center/colocation instalación de datos que la ubicación de Direct Connect, la instalación puede proporcionar una conexión cruzada entre el AWS Direct Connect equipo y sus recursos. Para ello, primero debe proporcionar la LOA-CFA a la instalación. Para obtener más información, consulte Carta de autorización y asignación de instalación de conexión (LOA-CFA). A continuación aparece un ejemplo de esta opción de conectividad de Direct Connect:

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

- Amplíe la conexión de Direct Connect a nivel 3 (nivel de red) desde la ubicación de Direct Connect hasta la suya. Para ello, trabaje con los socios de Direct Connect. Para esta opción de conectividad, el socio de Direct Connect proporciona un router dentro de la ubicación de

Direct Connect que forma una sesión de Border Gateway Protocol (BGP) con el AWS equipo. A continuación, el socio de Direct Connect estableció otro BGP con usted; por ejemplo, esto podría realizarse mediante conmutación de etiquetas multiprotocolo (MPLS). A continuación aparece un ejemplo de esta opción de conectividad Direct Connect.

Este de EE. UU. (Ohio)

Ubicación	Cómo solicitar una conexión
Cologix, Columbus COL2	Póngase en contacto con Cologix en sales@cologix.com.
Cologix MIN3, Minneapolis	Póngase en contacto con Cologix en sales@cologix.com.
CyrusOne West III, Houston	Envíe una solicitud mediante el formulario de contacto con el cliente.
Equinix CH2, Chicago	Póngase en contacto con Equinix en awsdealreg@equinix.com.
QTS, Chicago	Póngase en contacto con QTS en @qtsdatacenters .com. AConnect
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 32 km, 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 Realty IAD38, 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.
Equinix MI1, Miami	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix NY5, Seacaucus	Póngase en contacto con Equinix en awsdealreg@equinix.com.
KIO Networks, Querétaro, México QRO1	Contacte a KIO Networks”.
Markley, One Summer Street, Boston	Para los clientes actuales, cree una solicitud a través del portal de clientes. Para nuevas consultas, póngase en contacto con sales@markleygroup.com.
Centros de datos de Netrality, 2ª planta MMR, Filadelfia	Póngase en contacto con los Centros de datos de Netrality en support@netrality.com.

Ubicación	Cómo solicitar una conexión
QTS, Atlanta ATL1	Póngase en contacto con QTS en AConnect@qtsdatacenters.com.

Oeste de EE. UU. (Norte de California)

Ubicación	Cómo solicitar una conexión
CoreSite, LA1, Los Ángeles	Realice un pedido a través del Portal de CoreSite Clientes. Una vez rellenado el formulario, revise el pedido y, a continuación, apruébelo en el sitio web.
CoreSite SV2, Milpitas	Realice un pedido a través del portal de 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 en el 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.
Equinix LA3, 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.
PhoenixNAP, Phoenix	Póngase en contacto con phoenixNAP Provisioning en provisioning@phoenixnap.com.

Oeste de EE. UU. (Oregón)

Ubicación	Cómo solicitar una conexión
CoreSite DE1, Denver	Realice un pedido a través del Portal 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.
Equinix SE2, Seattle	Póngase en contacto con Equinix en support@equinix.com.
Pittock Block, Portland	Envíe las solicitudes por correo electrónico a crossconnect@pittock.com o llame por teléfono al +1 503 226 6777.
Switch SUPERNAP 8, Las Vegas	Póngase en contacto con Switch SUPERNAP en orders@supernap.com.
TierPoint Seattle	Póngase 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).

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

Asia-Pacífico (Yakarta)

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

Asia-Pacífico (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.
DC2STT Delhi, Delhi	Póngase en contacto con STT en caso de consulta. AWSDX@sttelemediagdc .in.
STT GDC Pvt. Ltd. VSB, Chennai	Póngase en contacto con STT si tiene alguna consulta. AWSDX@sttelemediagdc .in.

Ubicación	Cómo solicitar una conexión
STT Hyderabad, Hyderabad DC1	Póngase en contacto con STT en caso de consulta. AWSDX@sttelemediagdc .in.

Asia-Pacífico (Seúl)

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

Asia-Pacífico (Singapur)

Ubicación	Cómo solicitar una conexión
Equinix HK1, Tsuen Wan N.T., RAE de Hong Kong	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix SG2, Singapur	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Global Switch, Singapur	Póngase en contacto con Global Switch en salessingapore@globalswitch.com.
GPX, Mumbai	Póngase en contacto con GPX (Equinix) en awsdealreg@equinix.com.
iAdvantage Mega-i, Hong Kong	Póngase en contacto con iAdvantage en cs@iadvantage.net o haga un pedido con el iAdvantage Cabling Order e-Form (formulario electrónico de solicitud de cableado de iAdvantage).

Ubicación	Cómo solicitar una conexión
Menara AIMS, Kuala Lumpur	Los clientes de AIMS existentes pueden solicitar una orden X-Connect en el portal del servicio de atención al cliente al completar el formulario de solicitud de orden de trabajo de ingeniería. Póngase en contacto con service.delivery@aims.com.my si hay problemas para enviar la solicitud.
Centro de datos TCC, Bangkok	Póngase en contacto con TCC Technology Co., Ltd en gateway.ne@tcc-technology.com.

Asia-Pacífico (Sídney)

Ubicación	Cómo solicitar una conexión
CDC Hume 2, Canberra	Inicie sesión en el portal de clientes de CDC.
Datacom DH6, Auckland	Contacte a Datacom a través de Datacom Orbit –Auckland.
Equinix ME2, Melbourne	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix SY3, Sídney	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Global Switch, Sídney	Póngase en contacto con Global Switch en salessydney@globalswitch.com.
NEXTDC C1, Canberra	Póngase en contacto con NEXTDC en nxtops@nextdc.com.
NEXTDC M1, Melbourne	Póngase en contacto con NEXTDC en nxtops@nextdc.com.
NEXTDC P1, Perth	Póngase en contacto con NEXTDC en nxtops@nextdc.com.
NEXTDC S2, Sídney	Póngase en contacto con NEXTDC en nxtops@nextdc.com.

Asia-Pacífico (Tokio)

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

Canadá (centro)

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

China (Pekín)

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

China (Ningxia)

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

Europa (Fráncfort)

Ubicación	Cómo solicitar una conexión
CE Colo, Praga, República Checa	Póngase en contacto con CE Colo en info@cecolo.com.
DigiPlex Ulven, Oslo, Noruega	Póngase en contacto con nosotros DigiPlex en helpme@digiplex.com.
Equinix AM3, Ámsterdam, Países Bajos	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix FR5, Frankfurt	Póngase en contacto con Equinix en awsdealreg@equinix.com.

Ubicación	Cómo solicitar una conexión
Equinix HE6, Helsinki	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix MU1, Múnich	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix WA1, Varsovia	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Interxion AMS7, Ámsterdam	Póngase en contacto con Interxion en customer.services@interxion.com.
Interxion CPH2, Copenhague	Póngase en contacto con Interxion en customer.services@interxion.com.
Interxion FRA6, Fráncfort	Póngase en contacto con Interxion en customer.services@interxion.com.
Interxion MAD2, Madrid	Póngase en contacto con Interxion en customer.services@interxion.com.
Interxion VIE2, Viena	Póngase en contacto con Interxion en customer.services@interxion.com.
Interxion ZUR1, Zúrich	Póngase en contacto con Interxion en customer.services@interxion.com.
IPB, Berlín	Póngase en contacto con IPB en kontakt@ipb.de.
Equinix ITConic MD2, Madrid	Póngase en contacto con Equinix en awsdealreg@equinix.com.

Europa (Irlanda)

Ubicación	Cómo solicitar una conexión
Digital Realty (Reino Unido), Docklands	Póngase en contacto con Digital Realty (Reino Unido) en amazon.orders@digitalrealty.com.
Eircom Clonshaugh	Contacte a Eircom a través de datacentre@eirevo.ie.

Ubicación	Cómo solicitar una conexión
Equinix DX1, Dublín	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix LD5, Londres (Slough)	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Interxion, Dublín DUB2	Póngase en contacto con Interxion en customer.services@interxion.com.
Interxion MRS1, Marsella	Póngase en contacto con Interxion en customer.services@interxion.com.

Europa (Milán)

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

Europa (Londres)

Ubicación	Cómo solicitar una conexión
Digital Realty (Reino Unido), Docklands	Póngase en contacto con Digital Realty (Reino Unido) en amazon.orders@digitalrealty.com.
Equinix LD5, Londres (Slough)	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix, 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
Equinix PA3, París	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Interxion PAR7, París	Póngase en contacto con Interxion en customer.services@interxion.com.
Telehouse Voltaire, París	Contacte a Telehouse Paris Voltaire a través de la página Contáctenos.

Europa (Estocolmo)

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

Europa (Zúrich)

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

Israel (Tel Aviv)

Ubicación	Cómo solicitar una conexión
MedOne, Haifa	Póngase en contacto con nosotros MedOne en support@Medone.co.il

Ubicación	Cómo solicitar una conexión
EdgeConnex, Herzliya	Póngase en contacto con nosotros en info@edgeconnecx.com EdgeConnect

Medio Oriente (Baréin)

Ubicación	Cómo solicitar una conexión
AWS DC53Baréin, 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 DC52Baréin, Manama	Para realizar la conexión, puede colaborar con uno de nuestros socios proveedores de red de la ubicación para establecer la conectividad. Luego, entregará una carta de autorización (LOA) del proveedor de la red a AWS través del AWS Support Center. AWS completa la conexión cruzada en esta ubicación.

Medio Oriente (EAU)

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

América del Sur (São Paulo)

Ubicación	Cómo solicitar una conexión
Cirion BNARAGMS, Buenos Aires	Contacte Cirion a través de cloud.connect@ciriontechnologies.com.
Equinix RJ2, Río de Janeiro	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Equinix SP4, São Paulo	Póngase en contacto con Equinix en awsdealreg@equinix.com.
Tivit	Póngase en contacto con Tivit en aws@tivit.com.br.

AWS GovCloud (Este de EE. UU.)

No puede solicitar conexiones en esta región.

AWS GovCloud (Estados Unidos-Oeste)

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

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

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

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

- Los rangos de direcciones IP a los que accedas a AWS través de tus propias direcciones IP (BYOIP) no se incluyen en el `.json` archivo, pero AWS aun así anuncian estas direcciones BYOIP a través de una interfaz virtual pública.
- AWS no vuelve a anunciar los prefijos de los clientes que se recibieron a través de las interfaces virtuales públicas de Direct Connect en redes externas a. AWS Los prefijos anunciados en una interfaz virtual pública estarán visibles para todos los clientes. AWS

> **Note**
>
> Le recomendamos que utilice un filtro de firewall (basado en la source/destination dirección de los paquetes) para controlar el tráfico que entra y sale de algunos prefijos.

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

SiteLink

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

SiteLink es una función opcional de Direct Connect para interfaces virtuales privadas 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.
> - SiteLink no funciona si un router local anuncia la misma ruta AWS en varias interfaces virtuales.

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

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

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

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

SiteLink admite un tamaño máximo de MTU de trama gigante de 8500 o 9001, según el tipo de interfaz virtual. Para obtener más información, consulte MTUs para interfaces virtuales privadas o interfaces virtuales de tránsito.

Requisitos previos de las interfaces virtuales

Antes de crear una interfaz virtual, haga lo siguiente:

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

Para crear una interfaz virtual, necesita la siguiente información:

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

Recurso	Información necesaria
	Note • No puede usar el mismo ASN para la puerta de enlace del cliente y la puerta de enlace gateway/Direct Connect virtual en la interfaz virtual. • Puede usar el mismo ASN de la pasarela de cliente para varias interfaces virtuales. • Varias interfaces virtuales pueden tener el mismo ASN de puerta de enlace virtual/puerta de enlace de Direct Connect y ASN de puerta de enlace de cliente siempre que formen parte de diferentes conexiones de Direct Connect. Por ejemplo: Puerta de enlace virtual (ASN 64.496) <---Interfaz virtual 1 (conexión Direct Connect 1) ---> Puerta de enlace de cliente (ASN 64.511) Puerta de enlace virtual (ASN 64.496) <---Interfaz virtual 2 (conexión Direct Connect 2) ---> Puerta de enlace de cliente (ASN 64.511)
VLAN	Una etiqueta de red de área local virtual (VLAN) única que aún no se encuentra en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de AWS Direct Connect . Si tiene una conexión alojada, su socio le proporcionará este valor. AWS Direct Connect No puede modificar el valor después de haber creado la interfaz virtual.

Recurso	Información necesaria

Direcciones IP de mismo nivel	Una interfaz virtual puede admitir una sesión de interconexión BGP para IPv4 cada sesión o una de ellas (doble pila). IPv6 No utilices Elastic IPs (EIPs) ni traigas tus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias sesiones de BGP para la misma familia de enrutamiento IP en la misma interfaz virtual. Los rangos de las direcciones IP que se asignan a cada extremo de la interfaz virtual para la sesión de intercambio de tráfico del BGP.
	
	• IPv4:
	  • (Solo interfaz virtual pública) Debe especificar IPv4 direcciones públicas únicas de su propiedad.
	  Note
	  • El emparejamiento IPs para las interfaces virtuales privadas y de tránsito puede realizarse desde cualquier rango de IP válido. Esto también puede incluir direcciones IP públicas propiedad del cliente, siempre que solo se utilicen para crear la sesión de emparejamiento de BGP y no se anuncien a través de la interfaz virtual ni se utilicen para la NAT.
	  • No podemos garantizar que podamos atender todas las solicitudes de direcciones públicas proporcionadas. AWS IPv4
	  El valor puede ser uno de los siguientes:
	  • Un CIDR propiedad del cliente IPv4
	  Puede ser cualquier tipo de máscara pública IPs (propiedad del cliente o proporcionada por él AWS), pero se debe usar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del router. AWS Por ejemplo, si asigna un `/31` rango, por ejemplo, podría usarlo

Recurso	Información necesaria
	`203.0.113.0` para su IP homóloga y `203.0.113.1` para la AWS IP homóloga. `203.0.113.0/31` O bien, si asignas un `/24` rango, por ejemplo`198.51.100.0/24` , puedes usarlo `198.51.100.10` para tu IP homóloga y `198.51.100.20` para la IP AWS homóloga. • Un rango de IP propiedad de su AWS Direct Connect socio o ISP, junto con una autorización LOA-CFA. • Y AWS proporcionó un CIDR 1/31. Ponte en contacto con AWS Support para solicitar un IPv4 CIDR público (y proporciona un caso de uso en tu solicitud) • (Solo interfaz virtual privada) Amazon puede generar IPv4 direcciones privadas para usted. Si especifica la suya propia, asegúrese de especificar 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` • IPv6: Amazon te asigna automáticamente un CIDR de IPv6 /125. No puede especificar sus propias direcciones homólogas. IPv6
Familia de direcciones	Si la sesión de emparejamiento de BGP finalizará o. IPv4 IPv6

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

Recurso	Información necesaria

(Solo para la interfaz virtual pública) Prefijos que desea anunciar	IPv4 Rutas públicas o IPv6 rutas para anunciar a través de BGP. Debe comunicar al menos un prefijo a través del BGP, hasta un máximo de 1 000 prefijos.
	• IPv4: El IPv4 CIDR puede superponerse con otro IPv4 CIDR público que se haya anunciado que AWS Direct Connect se utilice cuando se dé alguna de las siguientes condiciones:
	  • CIDRs Son de diferentes regiones. AWS Asegúrese de aplicar etiquetas de comunidad del BGP a los prefijos públicos.
	  • Utiliza AS_PATH cuando tiene un ASN público en una configuración. active/passive
	  Para obtener más información, consulte Políticas de enrutamiento y comunidades de BGP.
	• A través de una interfaz virtual pública de Direct Connect, puede especificar cualquier longitud de prefijo de /1 a /32 IPv4 y de /1 a /64 para. IPv6
	• Puede agregar prefijos adicionales a una interfaz virtual pública existente y anunciarlos si se pone en contacto con AWS Asistencia. En su caso de soporte, proporcione una lista de los prefijos de CIDR adicionales que desee agregar a la interfaz virtual pública y anunciar.

Recurso	Información necesaria
(Solo interfaces virtuales privadas y de tránsito) Tramas gigantes	La unidad máxima de transmisión (MTU) de los paquetes superada. AWS Direct Connect El valor predeterminado es 1500. El establecimiento de la MTU de una interfaz virtual en 8500 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Se admiten tramas gigantes de hasta 8500 de MTU para Direct Connect. Las rutas estáticas y las rutas propagadas configuradas en la tabla de rutas de Transit Gateway admitirán tramas gigantes, incluso desde EC2 instancias con entradas de la tabla de rutas estáticas de VPC al 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 redes privadas VIFs y de tránsito VIFs, la cuenta se aplica a la interfaz virtual y al destino de la puerta de enlace gateway/Direct Connect privada virtual.
- En el caso de las cuentas públicas VIFs, la cuenta se utiliza para la facturación de la interfaz virtual. El uso de transferencia de datos salientes (DTO) se calcula en beneficio del propietario del recurso según la velocidad de transferencia de AWS Direct Connect datos.

> **Note**
>
> Los prefijos de 31 bits se admiten en todos los tipos de interfaz virtual de Direct Connect. Consulte la RFC 3021: Uso de prefijos de 31 bits en los enlaces para obtener más información. IPv4 Point-to-Point

MTUs para 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 + etiqueta VLAN de 4 bytes + bytes para el datagrama IP + 4 bytes FCS) en la capa de enlace.

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

Una vez que habilite tramas gigantes para su interfaz virtual privada o de tránsito, solo podrá asociarla con una conexión o LAG que sea compatible con tramas gigantes. Las tramas gigantes se admiten en una interfaz virtual privada asociada a una puerta de enlace privada virtual o de Direct Connect, o en una interfaz virtual de tránsito asociada a una puerta de enlace de Direct Connect. Si tiene dos interfaces virtuales privadas que anuncian la misma ruta pero utilizan valores de MTU diferentes, o si tiene una Site-to-Site VPN que anuncia la misma ruta, se utilizan 1500 MTU.

> **Important**
>
> Las tramas gigantes solo se aplicarán a las rutas propagadas AWS Direct Connect y a las rutas estáticas a través de puertas de enlace de tránsito. Las tramas gigantes de las puertas de enlace de tránsito solo admiten 8500 bytes.
> Si una EC2 instancia no admite tramas gigantes, descarta las tramas jumbo de Direct Connect. Todos los tipos de EC2 instancias admiten tramas gigantes, excepto las C1 CC1, T1 y M1. Para obtener más información, consulte la Unidad máxima de transmisión de red (MTU) para tu 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 conocer los pasos que se deben seguir para configurar la MTU de una interfaz virtual privada, consulte Establecer las MTU de una interfaz virtual privada.

AWS Direct Connect interfaces virtuales

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

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

Consulte la siguiente información para crear una interfaz virtual:

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

Requisitos previos

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

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

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

La unidad de transmisión máxima (MTU) de una conexión de red es el tamaño, en bytes, del mayor paquete permitido que se puede transferir a través de la conexión. La MTU de una interfaz virtual privada puede ser 1500 o 9001 (tramas gigantes). La MTU de una interfaz virtual de tránsito puede

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

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

Crear una interfaz virtual AWS Direct Connect pública

Cuando creas una interfaz virtual pública, podemos tardar hasta 72 horas laborables en revisar y aprobar tu solicitud.

Aprovisionamiento de una interfaz virtual pública

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 Public (Pública).
5. En Public virtual interface settings (Configuración de la interfaz virtual pública), haga lo siguiente:
   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.
   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.
   c. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

d. Para BGP ASN, introduzca el número de sistema autónomo (ASN) del protocolo Border Gateway del router homólogo local para la nueva interfaz virtual.

   Los valores válidos son 1-2.147.483.647.

   > **Note**
   >
   > Al establecer una sesión de emparejamiento de BGP a AWS través de una interfaz virtual pública, utilice el 7224 como ASN para establecer la sesión de BGP de forma paralela. AWS El ASN del router o dispositivo de puerta de enlace del cliente debe ser diferente al de ese ASN.

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

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

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

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

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

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

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

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

      > **Important**
      >
      > Puede agregar prefijos adicionales a una interfaz virtual pública existente y anunciarlos si se pone en contacto con AWS Asistencia. En su caso de soporte,

proporcione una lista de los prefijos de CIDR adicionales que desee agregar a la interfaz virtual pública y anunciar.

d. (Opcional) Añada o elimine una etiqueta.

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

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

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

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

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

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

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

La unidad de transmisión máxima (MTU) de una conexión de red es el tamaño, en bytes, del mayor paquete permitido que se puede transferir a través de la conexión. La MTU de una interfaz virtual privada puede ser 1500 o 9001 (tramas gigantes). La MTU de una interfaz virtual de tránsito puede ser 1500 o 8500 (tramas gigantes). Puede especificar la MTU al crear la interfaz o actualizarla tras crearla. El establecimiento de la MTU de una interfaz virtual en 8500 (tramas gigantes) o 9001

(tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la consola de AWS Direct Connect y busque Jumbo Frame Capable (Con capacidad de tramas gigantes) en la pestaña Summary (Resumen).

Para aprovisionar una interfaz virtual privada a una VPC

1. Abra la AWS Direct Connectconsola en la versión 2/home. https://console.aws.amazon.com/directconnect/
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En 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 Puerta de enlace de Direct Connect, seleccione la puerta de enlace de Direct Connect.
   e. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).
   f. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

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

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

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

- Para el router peer ip de Amazon, introduce la dirección IPv4 CIDR a la que se va a enviar el tráfico. AWS

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

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

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

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

d. (Opcional) Añada o elimine una etiqueta.

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

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

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

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

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

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

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

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

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

1. Abra la AWS Direct Connectconsola en https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Virtual Interfaces.
3. Elija Create virtual interface (Crear interfaz virtual).
4. En Virtual interface type (Tipo de interfaz virtual) en Type (Tipo), elija Transit (Tránsito).
5. En Transit virtual interface settings (Configuración de la interfaz virtual de tránsito), haga lo siguiente:
   a. En Virtual interface name (Nombre de la interfaz virtual), escriba un nombre para la interfaz virtual.
   b. En Connection (Conexión), elija la conexión de Direct Connect que desea utilizar para esta interfaz.
   c. Como propietario de la interfaz virtual, elija Mi AWS cuenta si la interfaz virtual es para su AWS cuenta.
   d. En Puerta de enlace de Direct Connect, seleccione la puerta de enlace de Direct Connect.
   e. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).
   f. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

Los valores válidos son 1 a 2147483647.

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

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

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

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

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

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

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

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

d. (Opcional) Añada o elimine una etiqueta.

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

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

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

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

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

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

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

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

- describe-direct-connect-gateway-archivos 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

Para descargar el archivo de configuración del router

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 manualmente MACsec, utilice la siguiente tabla como guía.

Parámetro	Descripción
Longitud del CKN	Se trata de una cadena de 64 caracteres hexadecimales (0–9, A–E). Utilice la longitud completa para maximizar la compatibilidad multiplat aforma.
Longitud de la CAK	Se trata de una cadena de 64 caracteres hexadecimales (0–9, A–E). Utilice la longitud completa para maximizar la compatibilidad multiplat aforma.
Algoritmo criptográfico	AES_256_CMAC
Conjunto de cifrado de SAK	• Para conexiones de 100 Gbps: GCM_AES_XPN_256 • Para conexiones de 10 Gbps: GCM_AES_XPN_256 o GCM_AES _256
Conjunto de cifrado de claves	16

Parámetro	Descripción
Desplazamiento de confidencialidad	0
Indicador de ICV	No
Tiempo de cambio de clave de SAK	Sustitución de PN>

Interfaces AWS Direct Connect virtuales alojadas

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

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

Para crear una interfaz virtual, necesita la siguiente información:

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

Recurso	Información necesaria
virtual privada) Conexión	sesión del BGP se hereda de la puerta de enlace privada virtual. Al crear una puerta de enlace privada virtual, puede especificar su propio ASN privado. De lo contrario, Amazon proporciona un ASN predeterminado. Para obtener información, consulte Crear una puerta de enlace privada virtual en la Guía del usuario de Amazon VPC. Para conectarse a una VPC a través de una puerta de enlace de Direct Connect, se necesita la puerta de enlace de Direct Connect. Para obtener más información, consulte Puertas de enlace de Direct Connect.
VLAN	Una etiqueta de red de área local virtual (VLAN) única que aún no se encuentra en uso en su conexión. El valor debe estar entre 1 y 4094 y debe cumplir con el estándar Ethernet 802.1Q. Esta etiqueta es necesaria para cualquier tráfico que atraviese la conexión de 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 interconexión BGP para IPv4 cada sesión o una de ellas (doble pila). IPv6 No utilices Elastic IPs (EIPs) ni traigas tus propias direcciones IP (BYOIP) del Amazon Pool para crear una interfaz virtual pública. No puede crear varias sesiones de BGP para la misma familia de enrutamiento IP en la misma interfaz virtual. Los rangos de las direcciones IP que se asignan a cada extremo de la interfaz virtual para la sesión de intercambio de tráfico del BGP.
	
	• IPv4:
	  • (Solo interfaz virtual pública) Debe especificar IPv4 direcciones públicas únicas de su propiedad. El valor puede ser uno de los siguientes:
	  • Un CIDR propiedad del cliente IPv4
	
	  Puede ser cualquier tipo de máscara pública IPs (propiedad del cliente o proporcionada por él AWS), pero se debe usar la misma máscara de subred tanto para la IP homóloga como para la IP homóloga del router. AWS Por ejemplo, si asigna un `/31` rango, por ejemplo, podría usarlo `203.0.113.0` para su IP homóloga y `203.0.113.1` para la AWS IP homóloga. `203.0.113.0/31` O bien, si asignas un `/24` rango, por ejemplo`198.51.100.0/24` , puedes usarlo `198.51.100.10` para tu IP homóloga y `198.51.100.20` para la IP AWS homóloga.
	  • Un rango de IP propiedad de su AWS Direct Connect socio o ISP, junto con una autorización LOA-CFA
	  • Un AWS CIDR /31 proporcionado. Ponte en contacto con AWS Support para solicitar un IPv4 CIDR público (y proporciona un caso de uso en tu solicitud)
	
	  Note
	  No podemos garantizar que podamos tramitar todas las solicitudes AWS de direcciones públicas IPv4 proporcionadas.
	
	  • (Solo interfaz virtual privada) Amazon puede generar IPv4 direcciones privadas para usted. Si especifica la suya propia, asegúrese de especific ar privada únicamente CIDRs para la interfaz de su router y la interfaz

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

Recurso	Información necesaria

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

(Solo interface s virtuales privadas y de tránsito) Tramas gigantes	La unidad máxima de transmisión (MTU) de los paquetes superada. AWS Direct Connect El valor predeterminado es 1500. El establecimiento de la MTU de una interfaz virtual en 9001 (tramas gigantes) puede provocar una actualización de la conexión física subyacente si no se actualizó para admitir tramas gigantes. Al actualizar la conexión se interrumpe la conectividad de red para todas las interfaces virtuales asociadas con la conexión durante un máximo de 30 segundos. Las tramas gigantes solo se aplican a las rutas propagadas desde. AWS Direct Connect Si agrega rutas estáticas a una tabla de enrutamiento que apuntan a una puerta de enlace privada virtual, el tráfico enrutado a través de las rutas estáticas se envía utilizando 1500 MTU. Para comprobar si una conexión o interfaz virtual admite tramas gigantes, selecciónela en la AWS Direct Connect consola y busque Jumbo Frame Capable 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. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

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

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

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

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

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

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

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

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

c. (Opcional) Añada o elimine una etiqueta.

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

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

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

7. Una vez que el propietario de la otra cuenta de AWS haya aceptado la interfaz virtual alojada, podrá descargar el archivo de configuración. Para obtener más información, consulte Descargar el archivo de configuración del enrutador de .

Para crear una interfaz virtual privada alojada mediante la línea de comandos o la 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. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).

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

   Los valores válidos son 1-2.147.483.647.

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

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

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

- Para el router peer ip de Amazon, introduce la dirección IPv4 CIDR a la que se va a enviar el tráfico. AWS

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

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

   Si no ingresa un valor, luego generamos una clave de BGP.
9. (Opcional) Añada o elimine una etiqueta.

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

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

   [Eliminar una etiqueta] Junto a la etiqueta, elija Remove tag (Quitar etiqueta).
10. Elija Create virtual interface (Crear interfaz virtual).
11. Una vez que el propietario de la otra cuenta de AWS haya aceptado la interfaz virtual alojada, podrá descargar el archivo de configuración. Para obtener más información, consulte Descargar el archivo de configuración del enrutador de .

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

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

Cree una interfaz virtual de tránsito AWS Direct Connect alojada

Para crear una interfaz virtual de tránsito alojada

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Elija Create virtual interface (Crear interfaz virtual).
8. Después de que la interfaz virtual alojada sea aceptada por el propietario de la otra cuenta de AWS , podrá descargar el archivo de configuración del enrutador para el dispositivo. Para obtener más información, consulte Descargar el archivo de configuración del enrutador de .

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

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

Ver detalles de la interfaz AWS Direct Connect virtual

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

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

Para ver los detalles de una interfaz virtual

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

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

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

Agregar un par BGP a una interfaz AWS Direct Connect virtual

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

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

No se admite el BGP multiprotocolo. IPv4 y 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 de mismo nivel.

Para añadir un BGP de mismo nivel

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 Add peering (Añadir intercambio).
5. (Interfaz virtual privada) Para agregar pares de IPv4 BGP, haga lo siguiente:
   - Elija IPv4.
   - Para especificar estas direcciones IP usted mismo, en Your router peer ip, introduzca la dirección IPv4 CIDR de destino a la que Amazon debe enviar el tráfico. Para el router peer ip de Amazon, introduce la dirección IPv4 CIDR a la que se va a enviar el tráfico. AWS
6. (Interfaz virtual pública) Para agregar pares de IPv4 BGP, haga lo siguiente:
   - Para la IP del mismo nivel de su router, introduzca la dirección de destino del IPv4 CIDR a la que se debe enviar el tráfico.
   - En el caso de la IP homóloga del router Amazon, introduce la dirección IPv4 CIDR a la que se va a enviar el tráfico. AWS

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

7. (Interfaz virtual privada o pública) Para agregar pares de IPv6 BGP, elija. IPv6 Las IPv6 direcciones homólogas se asignan automáticamente desde el conjunto de IPv6 direcciones de Amazon; no puedes especificar IPv6 direcciones personalizadas.
8. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

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

   Los valores válidos son 1-2.147.483.647.

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

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

- create-bgp-peer (AWS CLI)
- Crear BGPPeer (API)AWS Direct Connect

Eliminar un par BGP de interfaz AWS Direct Connect virtual

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

Para eliminar un BGP de mismo nivel

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 interfaz virtual y, a continuación, elija View details (Ver detalles).
4. En Peerings (Intercambios), seleccione el intercambio que desea eliminar y, a continuación, elija Delete (Eliminar).
5. En el cuadro de diálogo Remove peering from virtual interface (Eliminar un intercambio de tráfico de la interfaz virtual), elija Delete (Eliminar).

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

- delete-bgp-peer (AWS CLI)
- Eliminar BGPPeer (API)AWS Direct Connect

Establecer la MTU de una interfaz virtual AWS Direct Connect privada

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

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

Para establecer la MTU de una interfaz virtual privada

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 interfaz virtual y, a continuación, elija Edit (Editar).
4. En Jumbo MTU (tamaño de MTU 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 establecer la MTU de una interfaz virtual privada alojada mediante la línea de comandos o la API

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

Agregar o quitar etiquetas de interfaz AWS Direct Connect virtual

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

Para añadir o eliminar una etiqueta de interfaz virtual

1. Abre 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 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, la línea de comandos o la API.

Eliminación de 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 la API

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

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 puerta de enlace privada virtual o de Direct Connect. En una interfaz virtual de tránsito, debe tener una puerta de enlace de Direct Connect o una puerta de enlace de tránsito existente.

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

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

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

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

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

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

- confirm-public-virtual-interface (AWS CLI)

- ConfirmPublicVirtualInterface(AWS Direct Connect API)

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

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

Migrar una interfaz AWS Direct Connect virtual

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

- Migrar una interfaz virtual existente asociada con una conexión a otro LAG.
- Migrar una interfaz virtual existente asociada con un LAG existente a un LAG nuevo.
- Migrar una interfaz virtual existente asociada con una conexión a otra conexión.

> **Note**
>
> - Puede migrar una interfaz virtual a una conexión nueva dentro de la misma región, pero no puede migrarla de una región a otra. Al migrar o asociar una interfaz virtual existente a una conexión nueva, los parámetros de configuración asociados con esas interfaces virtuales son los mismos. Para solucionar este problema, puede preparar la configuración en la conexión y, a continuación, actualizar la configuración de BGP.
> - No puede migrar una VIF de una conexión alojada a otra conexión alojada. Las VLAN IDs son únicas; por lo tanto, migrar un VIF de esta manera significaría que VLANs no coinciden. Es necesario eliminar la conexión o la VIF y, a continuación, volver a crearla mediante una VLAN que sea igual para la conexión y la VIF.

> **Important**
>
> La interfaz virtual estará inactiva durante un periodo breve. Le recomendamos que realice este procedimiento durante un periodo de mantenimiento.

Para migrar una interfaz virtual

1. Abra la AWS Direct Connectconsola en la v2/home. https://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 Connection (Conexión), seleccione el LAG o la conexión.
5. Elija Edit virtual interface (Editar interfaz virtual).

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

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

AWS Direct Connect 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. LAGs agiliza la configuración porque la configuración del LAG se aplica a todas las conexiones del grupo.

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

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

Puede crear un LAG desde las conexiones existentes o puede aprovisionar nuevas conexiones. Una vez que haya creado el LAG, puede asociar las conexiones existentes (ya sea de forma independiente como parte de otro LAG) al LAG.

Se aplican las siguientes reglas:

- Todas las conexiones deben ser conexiones dedicadas y tener una velocidad de puerto de 1 Gbps, 10 Gbps, 100 Gbps o 400 Gbps.
- Todas las conexiones del LAG deben utilizar el mismo ancho de banda.
- Puede tener un máximo de dos conexiones de 100 Gbps o 400 Gbps, o cuatro conexiones con una velocidad de puerto inferior a 100 G en un LAG. Cada conexión del LAG cuenta para el límite de conexión global de la región.
- Todas las conexiones del LAG deben terminar en el mismo AWS Direct Connect punto final.
- LAGs son compatibles con todos los tipos de interfaces virtuales: públicas, privadas y de tránsito.

Al crear un LAG, 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 instalación de conexión (LOA-CFA).

Todos LAGs tienen un atributo que determina el número mínimo de conexiones en el LAG que deben estar operativas para que el propio LAG esté operativo. De forma predeterminada, los nuevos LAGs tienen este atributo establecido en 0. Puede actualizar el LAG para especificar un valor diferente, pero si lo hace, el LAG completo dejará de funcionar si el número de conexiones operativas es inferior a este umbral. Este atributo se puede utilizar para evitar la utilización excesiva de las otras conexiones.

Todas las conexiones de un LAG deben funcionar en modo Active/Activo.

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

Temas

- MACsec consideraciones para AWS Direct Connect

- Crear un LAG en un AWS Direct Connect punto final
- Ver los detalles del LAG en un AWS Direct Connect punto final
- Actualizar un LAG en un AWS Direct Connect punto final
- Asociar una conexión a un LAG en un AWS Direct Connect punto final
- Desasociar una conexión de un LAG en un AWS Direct Connect punto final
- Asocie un MACsec CKN/CAK a un LAG de punto AWS Direct Connect final
- Eliminar la asociación entre una clave MACsec secreta y un LAG de AWS Direct Connect punto final
- Eliminar un LAG de AWS Direct Connect punto final

MACsec consideraciones para AWS Direct Connect

Tenga en cuenta lo siguiente cuando desee configurar MACsec enLAGs:

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

Crear un LAG en un AWS Direct Connect punto final

Puede crear un LAG aprovisionando nuevas conexiones o añadiendo conexiones existentes.

No puede crear un LAG con conexiones nuevas si esto hace que supere el límite de conexiones global de la región.

Para crear un LAG a partir de las 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 puede migrar una conexión desde un LAG existente si el hecho de eliminar la conexión provoca que el número mínimo de conexiones operativas del LAG caiga por debajo del umbral establecido.

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

Creación de un 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. Seleccione Create LAG (Crear LAG).
4. En Lag creation type (Tipo de creación de LAG), elija Request new connections (Solicitar conexiones nuevas) y proporcione la información siguiente:
   - LAG Name (Nombre del LAG): un nombre para el LAG.
   - Location (Ubicación): la ubicación del LAG.
   - Port speed (Velocidad del puerto): la velocidad del puerto para las conexiones.
   - Number of new connections (Número de conexiones nuevas): el número de conexiones nuevas que se van a crear. Puede tener un máximo de cuatro conexiones cuando la velocidad del puerto es de 1G o 10G; o dos cuando la velocidad del puerto es de 100 Gbps o 400 Gbps.
   - (Opcional) Configure la seguridad MAC (MACsec) para la conexión. En Configuración adicional, selecciona Solicitar un puerto MACsec compatible.

     MACsec solo 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. Seleccione Create LAG (Crear LAG).

Para crear un LAG desde 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. Seleccione Create LAG (Crear LAG).
4. En Lag creation type (Tipo de creación de LAG), elija Use existing connections (Usar conexiones existentes) y proporcione la información siguiente:
   - LAG Name (Nombre del LAG): un nombre para el LAG.
   - Conexión existente: la conexión de Direct Connect que se va a utilizar para el LAG.
   - (Opcional) Número de conexiones nuevas: el número de conexiones nuevas que se van a crear. Puede tener un máximo de cuatro conexiones cuando la velocidad del puerto es de 1G o 10G; o de dos cuando la velocidad del puerto es de 100 Gbps o 400 Gbps.
   - Minimum links (Mínimo de enlaces): el número mínimo de conexiones que deben estar operativas para que el LAG funcione. Si no especifica un valor, se asignará el valor predeterminado (0).
5. (Opcional) Añada o elimine una etiqueta.

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

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

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

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

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

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

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

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

Una vez que crea un LAG, puede asociar o desasociar conexiones. Para obtener más información, consulte Asociar una conexión a un LAG y Desasociar una conexión de un LAG.

Ver los detalles del LAG en un AWS Direct Connect punto final

Después de crear un LAG, puede ver sus detalles mediante la AWS Direct Connect consola, la línea de comandos o la API.

Para ver la información de los LAG

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija LAGs.
3. Seleccione el LAG y elija View details (Ver detalles).
4. Puede ver información sobre el LAG, incluido su ID y el AWS Direct Connect punto final en el que terminan las conexiones.

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

- describe-lags (AWS CLI)
- DescribeLags(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 o la API:

- El nombre del LAG.
- El valor del número mínimo de conexiones que deben estar operativas para que el LAG funcione.
- El modo de MACsec cifrado del LAG.

MACsec solo está disponible en conexiones dedicadas.

AWS asigna este valor a cada conexión que forma parte del LAG.

Los valores válidos son:

- `should_encrypt`
- `must_encrypt`

  Al establecer el modo de cifrado en este valor, las conexiones se desactivan cuando el cifrado se encuentra inactivo.
- `no_encrypt`

- Las etiquetas.

> **Note**
>
> Si ajusta el umbral del número mínimo de conexiones operativas, asegúrese de que el nuevo valor no provoque que el LAG caiga por debajo del umbral y deje de funcionar.

Actualización de 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 el LAG y, a continuación, elija Editar.
4. Modifique el LAG.

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

   [Ajustar el número mínimo de conexiones] En Mínimo de enlaces, ingrese el número mínimo de conexiones operativas.

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

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

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

5. Elija Edit LAG (Editar LAG).

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

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

Asociar una conexión a un LAG en un AWS Direct Connect punto final

Puede asociar una conexión existente a un LAG mediante la AWS Direct Connect consola, la línea de comandos o la API. La conexión puede ser independiente o puede ser parte de otro LAG. La conexión debe estar en el mismo AWS dispositivo y debe usar el mismo ancho de banda que el LAG. Si la conexión ya está asociada a otro LAG, no puede volver a asociarla si el hecho de eliminar la conexión provoca que el número mínimo de conexiones operativas del LAG caiga por debajo del umbral establecido.

La asociación de una conexión con un nuevo LAG automáticamente vuelve a asociar sus interfaces virtuales al LAG.

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

Asociación de una conexión a 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 el LAG y, a continuación, elija Ver detalles.
4. En Connections (Conexiones), elija Associate connection (Asociar conexión).
5. En Connection (Conexión), elija la conexión de Direct Connect que se va a utilizar para el LAG.

6. Elija Associate Connection (Asociar conexión).

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

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

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

Convierte una conexión en autónoma desasociándola de un LAG mediante la AWS Direct Connect consola, la línea de comandos o la API. No puede desasociar una conexión si al hacerlo provoca que el número mínimo de conexiones operativas del LAG caiga por debajo del umbral establecido.

Desasociar una conexión de un LAG no anula automáticamente las interfaces virtuales.

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

Desasociar una conexión de un LAG

1. Abre 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 el LAG y, a continuación, elija Ver detalles.
4. En Connections (Conexiones), seleccione la conexión en la lista de conexiones disponibles y elija Disassociate (Desasociar).
5. En el cuadro de diálogo de confirmación, elija Desasociar.

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

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

Asocie un MACsec CKN/CAK a un LAG de punto AWS Direct Connect final

Tras crear el LAG compatible MACsec, puede asociar un CKN/CAK a la conexión mediante la AWS Direct Connect consola, la línea de comandos o la API.

> **Note**
>
> No puede modificar una clave MACsec secreta después de asociarla a un LAG. Si necesita modificar la clave, desasocie la clave de la conexión y, a continuación, asocie una clave nueva a la conexión. Para obtener información sobre cómo quitar una asociación, consulte the section called “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 el LAG y elija View details (Ver detalles).
4. Elija Asociar clave.
5. Introduzca la clave. MACsec

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

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

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

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

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

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

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

Para eliminar una asociación entre un LAG y una MACsec clave

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 el LAG y elija View details (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 un LAG y una MACsec clave mediante la línea de comandos o la API

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

Eliminar un LAG de AWS Direct Connect punto final

Si ya no lo necesita LAGs, puede eliminarlos. No puede eliminar un LAG si tiene interfaces virtuales asociadas. Primero debe eliminar las interfaces virtuales o asociarlas a otro LAG u otra conexión. Eliminar un LAG no elimina las conexiones del LAG; debe eliminar las conexiones usted mismo. Para obtener más información, consulte Eliminar una conexión.

Puede eliminar un LAG mediante la AWS Direct Connect consola, la línea de comandos o la API.

Eliminación de 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 y LAGs, a continuación, elija Eliminar.

4. En el cuadro de diálogo de confirmación, elija Eliminar.

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

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

AWS Direct Connect pasarelas

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

- Puertas de enlace de Direct Connect

  Con una puerta de enlace Direct Connect, puedes asociar la puerta de enlace Direct Connect a una puerta de enlace de tránsito con varias VPCs, una puerta de enlace privada virtual o, si usas AWS Cloud WAN, a una red principal de Cloud WAN.
- Asociaciones de la puerta de enlace 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.
- asociaciones de redes principales de WAN en la nube

  Utilice una puerta de enlace de Direct Connect para asociar una puerta de enlace de Direct Connect a una red AWS Network Manager principal.
- Interacciones de prefijos permitidos

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

Temas

- AWS Direct Connect pasarelas
- AWS Direct Connect asociaciones de pasarelas privadas virtuales
- AWS Direct Connect pasarelas y asociaciones de pasarelas de tránsito
- AWS Direct Connect asociaciones de redes principales de Gateway y AWS Cloud WAN
- Interacciones de prefijos permitidas para las puertas de enlace AWS Direct Connect

AWS Direct Connect pasarelas

Utilice la AWS Direct Connect puerta de enlace para conectar su VPCs. Asocia una AWS Direct Connect puerta de enlace a cualquiera de las siguientes opciones:

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

También puede utilizar una puerta de enlace privada virtual para ampliar su zona local. Esta configuración permite que la VPC asociada con la zona local se conecte a una puerta de enlace de Direct Connect. La puerta de enlace de Direct Connect se conecta a una ubicación de Direct Connect en una región. El centro de datos en las instalaciones tiene una conexión de Direct Connect con la ubicación de Direct Connect. Para obtener más información, consulte Acceso a las zonas locales mediante una puerta de enlace de Direct Connect en la Guía del usuario de Amazon VPC.

Una puerta de enlace de Direct Connect es un recurso disponible en todo el mundo. Puede conectarse a cualquier región del mundo mediante una puerta de enlace de Direct Connect. Esto incluye AWS GovCloud (US), pero no incluye, las regiones de AWS China. Una puerta de enlace Direct Connect es un componente virtual de Direct Connect diseñado para actuar como un conjunto distribuido de reflectores de ruta BGP. Como funciona fuera de la ruta del tráfico de datos, evita la creación de un único punto de falla o la introducción de dependencias específicas. Regiones de AWS La alta disponibilidad está intrínsecamente integrada en su diseño, lo que elimina la necesidad de múltiples puertas de enlace Direct Connect.

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 puerta de enlace de Direct Connect no permite que las asociaciones de puerta de enlace que se encuentran en la misma puerta de enlace de Direct Connect se envíen tráfico entre sí (por ejemplo, una puerta de enlace privada virtual a otra puerta de enlace privada virtual). Una excepción a esta regla, implementada en noviembre de 2021, es cuando se anuncia una superred en dos o más VPCs, 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-to-VPC comunicación dentro de una puerta de enlace de Direct Connect, haga lo siguiente:

1. Configure grupos de seguridad en las instancias y otros recursos de la VPC para bloquear el tráfico entre ellas y VPCs utilícelos también como parte del grupo de seguridad predeterminado de la VPC.
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 VPC que desee conectar a la red local, en lugar de utilizar la misma puerta de enlace de Direct Connect para varias. VPCs Por ejemplo, en lugar de utilizar una sola puerta de enlace de Direct Connect para el desarrollo y la producción VPCs, utilice puertas de enlace de Direct Connect independientes para cada una de ellas VPCs.

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 enrutamiento a los adjuntos de la VPC que tengan configurada la opción de agujero negro.

Temas

- Escenarios
- Crear una AWS Direct Connect puerta de enlace
- Migre de una puerta de enlace privada virtual a una AWS Direct Connect puerta de enlace
- Eliminar una puerta de enlace de AWS Direct Connect

Escenarios

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

Caso: asociaciones de puerta de enlace privada virtual

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

Caso: asociaciones de puerta de enlace privada virtual entre cuentas

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

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

Caso: asociaciones de puerta de enlace de tránsito

El siguiente diagrama 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 puerta de enlace de tránsito que tiene asociaciones de VPC.
- Una puerta de enlace de Direct Connect.
- Una asociación entre la puerta de enlace de Direct Connect y la puerta de enlace de tránsito.
- Una interfaz virtual de tránsito vinculada a la puerta de enlace de Direct Connect.

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

- 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 puertas de enlace de tránsito, consulte Trabajo con puertas de enlace de tránsito en la Guía de puertas de enlace de tránsito de Amazon VPC.

Caso: asociaciones de puerta de enlace de tránsito entre cuentas

Considere este escenario en el que el propietario de una puerta de enlace de Direct Connect es la cuenta Z. La cuenta A posee la puerta de enlace de tránsito y desea utilizar la puerta de enlace de Direct Connect. La cuenta Z acepta las propuestas de asociación y puede actualizar de forma opcional los prefijos permitidos de la puerta de enlace de tránsito de la cuenta A. 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 enrutamiento a los clientes, ya que la cuenta Z es la propietaria de la puerta de enlace.

Crear una AWS Direct Connect puerta de enlace

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

Para crear una puerta de enlace 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 Puertas de enlace de Direct Connect.
3. Elija Crear puerta de enlace de Direct Connect.
4. Especifique la información siguiente y elija Crear puerta de enlace de Direct Connect.
   - Nombre: escriba un nombre que ayude a identificar la puerta de enlace de Direct Connect.
   - Amazon side ASN (ASN del lado de Amazon): especifique el ASN del lado de Amazon de la sesión de BGP. El ASN debe estar comprendido entre 64 512 y 65 534 o entre 4 200 000 000 y 4 294 967 294.

> **Note**
>
> Si quieres crear una puerta de enlace Direct Connect para usarla con una red principal de AWS Cloud WAN. La ASN no debe estar en el mismo rango que la ASN de la red principal.

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

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

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

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

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

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

Para migrar a una puerta de enlace de Direct Connect

1. Cree una puerta de enlace de Direct Connect.

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

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

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

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

Eliminar una puerta de enlace de AWS Direct Connect

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

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

Para eliminar una puerta de enlace de Direct Connect

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

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

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

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. Asocia una puerta de enlace de Direct Connect con la puerta de enlace privada virtual de la VPC. A continuación, crea una interfaz virtual privada para la AWS Direct Connect conexión a la puerta de enlace Direct Connect. Puede adjuntar varias interfaces virtuales privadas a la puerta de enlace 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 de forma incorrecta.
- Existen límites para la creación y el uso de puertas de enlace de Direct Connect. Para obtener más información, consulte Cuotas de Direct Connect.
- No puede adjuntar una puerta de enlace de Direct Connect en una puerta de enlace privada virtual cuando la puerta de enlace de Direct Connect ya se encuentra asociada a una puerta de enlace de tránsito.
- El elemento VPCs al que se conecta a través de una puerta de enlace de Direct Connect no puede tener bloques CIDR superpuestos. Si agrega un bloque IPv4 CIDR a una VPC asociada a una puerta de enlace de Direct Connect, asegúrese de que el bloque CIDR no se superponga con un bloque CIDR existente de ninguna otra VPC asociada. Para obtener más información, consulte Añadir bloques IPv4 CIDR a una VPC en la Guía del usuario de Amazon VPC.
- No se puede crear una interfaz virtual pública a una puerta de enlace de Direct Connect.
- Una puerta de enlace de Direct Connect solo admite la comunicación entre interfaces virtuales privadas adjuntas y puertas de enlace privadas virtuales asociadas; puede habilitar una puerta de enlace privada virtual a otra puerta de enlace privada. No se admiten los siguientes flujos de tráfico:
  - Comunicación directa entre las VPCs que están asociadas a una única puerta de enlace Direct Connect. Esto incluye el tráfico desde una VPC a otra mediante un enganche mediante una red en las instalaciones a través de una única puerta de enlace de Direct Connect.
  - Comunicación directa entre las interfaces virtuales que están asociadas a la puerta de enlace única de Direct Connect.
  - Comunicación directa entre las interfaces virtuales asociadas a una puerta de enlace única de Direct Connect y una conexión de VPN en una puerta de enlace privada virtual que está asociada con la misma puerta de enlace de Direct Connect.

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

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

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

Temas

- Cree una puerta de enlace privada AWS Direct Connect virtual
- Asociar o desasociar puertas de AWS Direct Connect enlace privadas virtuales
- Cree una interfaz virtual privada para la AWS Direct Connect puerta de enlace
- Asocie una puerta de enlace privada AWS Direct Connect virtual entre cuentas

Cree una puerta de enlace privada AWS Direct Connect virtual

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

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

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

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

1. Abra la AWS Direct Connectconsola en la versión 2/home. https://console.aws.amazon.com/directconnect/
2. En el panel de navegación, elija Puertas de enlace privadas virtuales y, a continuación, elija Crear una puerta de enlace privada virtual.
3. (Opcional) Escriba un nombre para la puerta de enlace privada virtual. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
4. Para ASN, deje la selección predeterminada para utilizar el ASN de Amazon predeterminado. De lo contrario, elija Custom ASN (ASN personalizado) y escriba un valor. Para un ASN de 16 bits ASN, el valor debe estar dentro del rango de 64 512 a 65 534. Para un ASN de 32 bits ASN, el valor debe estar dentro del rango de 4 200 000 000 a 4 294 967 294.
5. Elija Crear puerta de enlace privada virtual.
6. Seleccione la puerta de enlace privada virtual que ha creado y, a continuación, elija Acciones, Asociar a la VPC.
7. Seleccione la VPC en la lista y elija Yes, Attach.

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

- CreateVpnGateway(API de Amazon EC2 Query)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (AWS Tools for Windows PowerShell)

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

- AttachVpnGateway(API de Amazon EC2 Query)
- 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, la línea de comandos o la API. El propietario de la cuenta de la puerta de enlace privada virtual realiza estas operaciones.

Para asociar una puerta de enlace privada virtual

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

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

Para desasociar una puerta de enlace privada virtual

1. 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, seleccione la puerta de enlace de Direct Connect.
3. Elija Ver detalles.
4. Elija Asociaciones de puerta de enlace y, a continuación, seleccione la puerta de enlace privada virtual.
5. Elija Desasociar.

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

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

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

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

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

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

Para aprovisionar una interfaz virtual privada en una puerta de enlace 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 Puerta de enlace de Direct Connect, seleccione la puerta de enlace de Direct Connect.
   e. En VLAN, escriba el número de ID de la red de área local virtual (VLAN).
   f. En ASN del BGP, ingrese el número de sistema autónomo para protocolo de puerta de enlace fronteriza del enrutador de mismo nivel en las instalaciones de la nueva interfaz virtual.

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

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

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

- Para el router peer ip de Amazon, introduce la dirección IPv4 CIDR a la que se va a enviar el tráfico. AWS

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

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

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

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

d. (Opcional) Añada o elimine una etiqueta.

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

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

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

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

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 de .

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

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

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

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

Asocie una puerta de enlace privada AWS Direct Connect virtual entre cuentas

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

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

Prefijos permitidos

Al asociar una puerta de enlace privada virtual a una puerta de enlace de Direct Connect, debe especificar una lista de prefijos de Amazon VPC que se deben anunciar a la puerta de enlace de Direct Connect. La lista de prefijos actúa como un filtro que permite anunciar lo mismo CIDRs o uno menor CIDRs en la puerta de enlace de Direct Connect. En Prefijos permitidos, debe definir un rango

que coincida o que sea más amplio que el CIDR de la VPC porque aprovisionamos CIDR de VPC completos en la puerta de enlace privada virtual.

Por ejemplo, supongamos que el CIDR de la VPC es 10.0.0.0/16. Puede definir Allowed prefixes (Prefijos permitidos) en 10.0.0.0/16 (el valor del CIDR de la VPC) o en 10.0.0.0/15 (un valor que es más amplio que el del CIDR de la VPC).

Los prefijos de red interior de interfaz virtual anunciados a través de Direct Connect se propagan únicamente a las puertas de enlace de tránsito entre regiones, no dentro de la misma región. Para obtener más información sobre cómo interactúan los prefijos permitidos con las puertas de enlace privadas virtuales y las puertas de enlace de tránsito, consulte Interacciones de prefijos permitidos.

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 puertas de enlace de Direct Connect. Para obtener más información, consulte Cuotas de Direct Connect.
- Una puerta de enlace de Direct Connect admite la comunicación entre las interfaces virtuales de tránsito vinculadas y las puertas de enlace de tránsito asociadas.
- Si te conectas a varias pasarelas de tránsito que se encuentran en diferentes regiones, usa una única ASNs para cada pasarela de tránsito.
- Cualquier dirección de point-to-point conectividad que utilice un `/30` rango, por ejemplo`192.168.0.0/30`, no se propaga a una puerta de enlace de tránsito.

Asociación de una puerta de enlace de tránsito entre cuentas

Puede asociar una puerta de enlace 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 puerta de enlace de Direct Connect puede anular cualquiera de los prefijos solicitados en la propuesta de asociación.

Prefijos permitidos

En el caso de una asociación de puerta de enlace de tránsito, aprovisione la lista de prefijos permitidos de la puerta de enlace de Direct Connect. La lista se 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 asignación CIDRs. Los prefijos de la lista de prefijos permitidos de la puerta de enlace de Direct Connect se originan en la puerta de enlace de Direct Connect y se publican en la red local. Para obtener más información sobre cómo los prefijos permitidos interactúan con las puertas de enlace de tránsito y las puertas de enlace privadas virtuales, consulte Interacciones de prefijos permitidos.

Temas

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

Asocie o desasocie una puerta de enlace de tránsito mediante la AWS Direct Connect consola, la línea de comandos o la 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 Puertas de enlace de Direct Connect y, a continuación, seleccione la puerta de enlace de Direct Connect.
3. Elija Ver detalles.
4. Elija Asociaciones de puerta de enlace y, a continuación, elija Asociar puerta de enlace.
5. En Puertas de enlace, elija la puerta de enlace de tránsito que desee asociar.
6. En Prefijos permitidos, ingrese los prefijos (separados por una coma o en una línea nueva) que la puerta de enlace de Direct Connect anuncia en el centro de datos en las instalaciones. Para obtener más información sobre los prefijos permitidos, consulte Interacciones de prefijos permitidos.
7. Elija Asociar puerta de enlace

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

Desasociación de una puerta de enlace de tránsito

1. 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, seleccione la puerta de enlace de Direct Connect.
3. Elija Ver detalles.
4. Elija Asociaciones de puerta de enlace y, a continuación, seleccione la puerta de enlace de tránsito.
5. Elija Desasociar.

Actualización de los prefijos permitidos para una puerta de enlace de tránsito

Puede agregar o eliminar prefijos permitidos en la puerta de enlace de tránsito.

1. 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 para la que desee modificar los prefijos permitidos y, a continuación, elija Editar.
5. En Prefijos permitidos, ingrese los prefijos que la puerta de enlace de Direct Connect anuncia en el centro de datos en las instalaciones. En el caso de varios prefijos, separe cada prefijo con una coma o coloque cada prefijo en una línea nueva. Los prefijos que añada deben coincidir con los de Amazon CIDRs VPC 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. Esto puede tardar varios minutos o más tiempo en completarse.

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

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

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

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

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

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

A fin de actualizar los prefijos permitidos para una puerta de enlace de tránsito mediante la línea de comando o API

- update-direct-connect-gateway-asociación ()AWS CLI

- UpdateDirectConnectGatewayAssociation(AWS Direct Connect API)

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

Para conectar tu AWS Direct Connect conexión a la pasarela de tránsito, debes crear una interfaz de tránsito para tu conexión. Especifique la puerta de enlace de Direct Connect a la que se va a conectar. Puedes usar la AWS Direct Connect consola, la línea de comandos o la API.

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

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

1. 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 Puerta de enlace de Direct Connect, seleccione la puerta de enlace de Direct Connect.

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

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

   Los valores válidos son 1 a 2147483647.

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

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

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

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

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

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

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

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

d. (Opcional) Añada o elimine una etiqueta.

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

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

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

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

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

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

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

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

- describe-direct-connect-gateway-archivos 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 tránsito debe estar conectada a una VPC o VPN de tu AWS cuenta. El propietario de la puerta de enlace de Direct Connect debe compartir el ID de la puerta de enlace de Direct Connect y

el ID de su cuenta de AWS . Después de crear la propuesta, el propietario de la puerta de enlace 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, la línea de comandos o la API.

Para crear una propuesta de asociación

1. Abre 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 Asociaciones de puerta de enlace de Direct Connect y, a continuación, elija Asociar puerta de enlace de Direct Connect.
5. En Association account type (Tipo de cuenta para la asociación), en Account owner (Propietario de la cuenta), elija Another account (Otra cuenta).
6. En Propietario de la puerta de enlace de Direct Connect, ingrese el ID de la cuenta a la que pertenece la puerta de enlace de Direct Connect.
7. En Association settings (Configuración de la asociación), haga lo siguiente:
   a. En ID de la puerta de enlace de Direct Connect), escriba el ID de la puerta de enlace de Direct Connect.
   b. En Propietario de la interfaz virtual, ingrese el ID de la cuenta a la que pertenece la interfaz virtual para la asociación.
   c. (Opcional) Para especificar una lista de los prefijos que se permitirán desde la puerta de enlace de tránsito, agregue los prefijos a Prefijos permitidos utilizando comas a fin de separarlos o introduciéndolos en diferentes líneas.
8. Elija Asociar puerta de enlace de Direct Connect.

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

- create-direct-connect-gateway- propuesta de asociación ()AWS CLI
- CreateDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

Aceptar o rechazar una propuesta de pasarela de tránsito y AWS Direct Connect asociación

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

Para aceptar una propuesta de asociación

1. Abre 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 Direct Connect.
3. Seleccione la puerta de enlace de Direct Connect que tiene propuestas pendientes y, a continuación, elija Ver detalles.
4. En la pestaña Pending proposals (Propuestas pendientes), seleccione la propuesta y, a continuación, elija Accept proposal (Aceptar propuesta).
5. (Opcional) Para especificar una lista de los prefijos que se permitirán desde la puerta de enlace de tránsito, agregue los prefijos a Prefijos permitidos utilizando comas para separarlos o introduciéndolos en diferentes líneas.
6. Elija Accept proposal (Aceptar propuesta).

Para rechazar una propuesta de asociación

1. 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.
3. Seleccione la puerta de enlace de Direct Connect que tiene propuestas pendientes y, a continuación, elija Ver detalles.
4. En la pestaña Propuestas pendientes, seleccione la puerta de enlace de tránsito y, a continuación, elija Rechazar propuesta.
5. En el cuadro de diálogo Reject proposal (Rechazar propuesta), escriba Delete y, a continuación, elija Reject proposal (Rechazar propuesta).

Para ver las propuestas de asociación mediante la línea de comandos o la API

- describe-direct-connect-gateway-propuestas de asociación ()AWS CLI
- DescribeDirectConnectGatewayAssociationProposals(API)AWS Direct Connect

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

- accept-direct-connect-gateway-asociación-propuesta ()AWS CLI
- AcceptDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

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

- delete-direct-connect-gateway-asociación-propuesta ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

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, la línea de comandos o la API. Para actualizar los prefijos permitidos para una pasarela de tránsito y una asociación de Direct Connect mediante la AWS Direct Connect consola,

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

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

- update-direct-connect-gateway-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 puerta de enlace tránsito de la puerta de enlace de Direct Connect. Para obtener más información, consulte Crear una propuesta de asociación de puerta de enlace de tránsito.

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

Para eliminar una propuesta de asociación

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/v2/home.
2. En el panel de navegación, elija Puertas de enlace de tránsito y, a continuación, seleccione la puerta de enlace de tránsito.
3. Elija Ver detalles.
4. Elija Asociaciones pendientes de la puerta de enlace, seleccione la asociación y, a continuación, elija Eliminar asociación.
5. En el cuadro de diálogo Delete association proposal (Eliminar propuesta de asociación), escriba Delete y, a continuación, elija Delete (Eliminar).

Para eliminar una propuesta de asociación pendiente mediante la línea de comandos o la API

- delete-direct-connect-gateway- propuesta de asociación ()AWS CLI
- DeleteDirectConnectGatewayAssociationProposal(API)AWS Direct Connect

AWS Direct Connect asociaciones de redes principales de Gateway y AWS Cloud WAN

Asocia una AWS Direct Connect puerta de enlace a una red principal de AWS Cloud WAN mediante un tipo de adjunto Direct Connect en Cloud WAN. Esta asociación directa enruta el tráfico entre las ubicaciones de borde seleccionadas de la red principal y las conexiones de Direct Connect mediante la ruta más corta disponible.

El tipo de adjunto de puerta de enlace Direct Connect admite BGP (protocolo Border Gateway) para la propagación automática de la información de enrutamiento entre la red principal y las ubicaciones locales. El accesorio Direct Connect también es compatible con las funciones estándar de Cloud WAN, como la administración central basada en políticas, la automatización de los archivos adjuntos basada en etiquetas y la segmentación para configuraciones de seguridad avanzadas.

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

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

Temas

- Requisitos previos
- Consideraciones
- Asociaciones de pasarelas Direct Connect a una red central de Cloud WAN
- Verificar la asociación de una AWS Direct Connect puerta de enlace a una red central de AWS Cloud WAN

Requisitos previos

La asociación de una puerta de enlace Direct Connect con una red principal de Cloud WAN requiere lo siguiente:

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

Consideraciones

Se aplican los siguientes límites a las asociaciones de pasarelas de Direct Connect con una red principal de Cloud WAN:

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

- Es posible que Cloud WAN no admita tipos de adjuntos específicos si se utiliza el tipo de adjunto Direct Connect para el transporte. Para obtener más información sobre los adjuntos de la puerta de enlace Direct Connect a una red principal de Cloud WAN, consulta los adjuntos de la puerta de enlace Direct Connect en AWS Cloud WAN en la Guía del usuario de AWS Cloud WAN.
- CloudWatch Network Monitor admite métricas de latencia y pérdida de paquetes cuando se usa con un tipo de adjunto de puerta de enlace Cloud WAN Direct Connect. No se admite la función Network Health Indicator. Para obtener más información, consulte Uso del monitor Amazon CloudWatch de red en la Guía del Amazon CloudWatch usuario.

Asociaciones de pasarelas Direct Connect a una red central de Cloud WAN

La asociación de una puerta de enlace Direct Connect a una red principal de AWS Cloud WAN se realiza mediante la consola de AWS Cloud WAN o la línea de comandos de Cloud WAN APIs .

Para asociar una puerta de enlace Direct Connect existente a una red principal de Cloud WAN, crea un nuevo adjunto de Direct Connect en la consola de Cloud WAN. Una vez creado el adjunto de Direct Connect, se establece la asociación. De forma predeterminada, al crear la asociación, puede elegir la opción predeterminada para incluir todas las ubicaciones de borde de la red principal en el segmento de red principal elegido. Como alternativa, puede especificar ubicaciones de borde individuales.

Para obtener más información sobre los adjuntos de la puerta de enlace Direct Connect a una red principal de Cloud WAN, consulta los adjuntos de la puerta de enlace Direct Connect en AWS Cloud WAN en la Guía del usuario de AWS Cloud WAN.

Verificar la asociación de una AWS Direct Connect puerta de enlace a una red central de AWS Cloud WAN

Puedes verificar la asociación de una puerta de enlace de Direct Connect a una red principal de Cloud WAN mediante la consola Direct Connect, la API de Direct Connect o la línea de comandos.

Para verificar la asociación de una puerta de enlace Direct Connect a una red principal de Cloud WAN mediante la consola

1. Abre la AWS Direct Connectconsola en la https://console.aws.amazon.com/directconnect/versión2/home.
2. Elija las puertas de enlace Direct Connect en el panel de navegación.
3. Elija el adjunto de la puerta de enlace Direct Connect cuya asociación desee ver.

4. Seleccione la pestaña de Asociaciones de puerta de enlace.
   - La columna ID muestra el ID de la red principal a la que está asociada la puerta de enlace Direct Connect.
   - La columna Estado aparece asociada.
   - La columna Tipo de asociación muestra Cloud WAN Core Network.

Para verificar la asociación de una puerta de enlace Direct Connect a una red principal de Cloud WAN mediante la línea de comandos o la API

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

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

Aprenda cómo interactúan los prefijos permitidos con las puertas de enlace de tránsito y las puertas de enlace privadas virtuales. Para obtener más información, consulte Routing policies and BGP communities.

Asociaciones de la puerta de enlace privada virtual

La lista de prefijos (IPv4 y IPv6) 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 el mismo rango, o en uno más amplio, que el bloque CIDR de VPC.

> **Note**
>
> La lista de permitidos solo funciona como un filtro y solo el CIDR de VPC asociado se anunciará en la puerta de enlace de cliente.

Piense en una situación en la que tiene una VPC con el CIDR 10.0.0.0/16 adjunta a una puerta de enlace privada virtual.

- Cuando la lista de prefijos permitidos se establece en 22.0.0.0/24, no recibe ninguna ruta porque 22.0.0.0/24 es diferente o más amplia que 10.0.0.0/16.

- Cuando la lista de prefijos permitidos se establece en 10.0.0.0/24, no recibe ninguna ruta porque 10.0.0.0/24 es diferente o más amplia que 10.0.0.0/16.
- Cuando la lista de prefijos permitidos se establece en 10.0.0.0/15, no recibe 10.0.0.0/16 porque la dirección IP es más amplia que 10.0.0.0/16.

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

Asociaciones de la 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 asignación CIDRs. Los prefijos permitidos funcionan de forma diferente en función del tipo de puerta de enlace:

- En el caso de las asociaciones de puerta de enlace de tránsito, solo se anunciarán en las instalaciones los prefijos permitidos ingresados. Se mostrarán como originarios del ASN de la puerta de enlace de Direct Connect.
- En el caso de las 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 que tiene una VPC con un CIDR 10.0.0.0/16 asociado a una puerta de enlace de tránsito.

- Cuando la lista de prefijos permitidos se establece en 22.0.0.0/24, recibe 22.0.0.0/24 a través de BGP en su interfaz virtual de tránsito. No recibe 10.0.0.0/16 porque aprovisionamos directamente los prefijos que se encuentran en la lista de prefijos permitidos.
- Cuando la lista de prefijos permitidos se establece en 10.0.0.0/24, recibe 10.0.0.0/24 a través de BGP en su interfaz virtual de tránsito. No recibe 10.0.0.0/16 porque aprovisionamos directamente los prefijos que se encuentran en la lista de prefijos permitidos.
- Cuando la lista de prefijos permitidos se establece en 10.0.0.0/8, recibe 10.0.0.0/8 a través de BGP en su interfaz virtual de tránsito.

No se permiten las superposiciones de prefijos permitidos cuando hay varias puertas de enlace de tránsito asociadas a una puerta de enlace de Direct Connect. Por ejemplo, si tiene una puerta de enlace de tránsito con una lista de prefijos permitidos que incluye 10.1.0.0/16 y una segunda puerta de enlace de tránsito con una lista de prefijos permitidos que incluye 10.2.0.0/16 y 0.0.0.0/0, no puede establecer las asociaciones de la segunda puerta de enlace de tránsito en 0.0.0.0/0. 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 puede retrasar o eliminar solo el tráfico que utiliza ese prefijo.

Ejemplo: Prefijos permitidos en una configuración de puerta de enlace de tránsito

Considere la configuración en la que hay instancias en dos 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 en 65030. Para obtener más información, consulte Cree una puerta de enlace de Direct Connect.
- Interfaz virtual de tránsito: establezca la VLAN en 899 y el ASN homólogo del router del cliente en 65020. Para obtener más información, consulte Cree una interfaz virtual de tránsito en la puerta de enlace de Direct Connect.
- Asociación de la puerta de enlace Direct Connect con la puerta de enlace de tránsito: establezca los prefijos permitidos en 10.0.0.0/8.

  Este bloque CIDR abarca ambos bloques CIDR de VPC (10.0.0.0/16 y 10.2.0.0/16). Para obtener más información, consulte Asociar una puerta de enlace de tránsito a Direct Connect o desasociarla de este..

- Ruta de VPC: para enrutar el tráfico desde la VPC 10.2.0.0/16, cree una ruta en la tabla de enrutamiento de la VPC con un destino de 0.0.0.0/0 y el ID de la puerta de enlace de tránsito como destino. Esto permite que el tráfico de la VPC llegue a la puerta de enlace Direct Connect. Para obtener más información sobre el enrutamiento a una puerta de enlace de tránsito, consulte Enrutamiento de una puerta de enlace de tránsito en la Guía del usuario de Amazon VPC.

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, el AWS CLI AWS Tools for Windows PowerShell, el o un AWS SDK. Cuando se utilizan estas herramientas para administrar etiquetas, es preciso especificar el nombre de recurso de Amazon (ARN) del recurso. Para obtener más información sobre ARNs, 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
Connections	Sí	Sí	Sí	Sí
Interfaces virtuales	Sí	Sí	Sí	No
Grupos de agregación de enlaces (LAG)	Sí	Sí	Sí	Sí
Interconexiones	Sí	Sí	Sí	Sí
Puertas de enlace de Direct Connect	Sí	Sí	Sí	No

Restricciones de las etiquetas

Las siguientes reglas y restricciones se aplican a las etiquetas:

- Número máximo de etiquetas por recurso: 50
- Longitud máxima de la clave: 128 caracteres Unicode
- Longitud máxima del valor: 265 caracteres Unicode

- Las claves y los valores de las etiquetas distinguen entre mayúsculas y minúsculas.
- El `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 Administración de facturación y costos de AWS usuario.

Uso de etiquetas mediante la CLI o la API

Utilice lo siguiente para añadir, actualizar, listar y eliminar las etiquetas de los recursos.

Tarea	API	CLI
Agregar o sobrescribir una o varias etiquetas.	TagResource	tag-resource
Eliminar una o varias etiquetas .	UntagResource	untag-resource
Describir una o varias etiquetas.	DescribeTags	describe-tags

Ejemplos

Utilice el comando tag-resource para etiquetar la conexión `dxcon-11aa22bb`.

```
aws directconnect tag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tags "key=Purpose,value=Production"
```

Utilice el comando describe-tags para describir las etiquetas `dxcon-11aa22bb` de la conexión.

```
aws directconnect describe-tags --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb
```

Utilice el comando untag-resource para eliminar una etiqueta de la conexión `dxcon-11aa22bb`.

```
aws directconnect untag-resource --resource-arn arn:aws:directconnect:us-
east-1:123456789012:dxcon/dxcon-11aa22bb --tag-keys Purpose
```

Seguridad en AWS Direct Connect

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

La seguridad es una responsabilidad compartida entre usted AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad aplicables AWS Direct Connect, consulte los AWS servicios incluidos en el ámbito de aplicación por programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza 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
- Identity and Access Management para Direct Connect
- Inicio de sesión y supervisión AWS Direct Connect
- Validación de conformidad para AWS Direct Connect
- Resiliencia en AWS Direct Connect
- Seguridad de la infraestructura en AWS Direct Connect

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. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulta las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulta la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS .

Con fines de protección de datos, 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:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Cómo trabajar con CloudTrail senderos en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulta Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con AWS Direct Connect o Servicios de AWS

utiliza la consola, la API o. AWS CLI AWS SDKs Cualquier dato que ingrese en etiquetas o campos de texto de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Para obtener más información sobre la protección de datos, consulte la entrada de blog relativa al modelo de responsabilidad compartida de AWS y GDPR en el blog de seguridad de AWS .

Temas

- Privacidad del tráfico entre redes en AWS Direct Connect
- Cifrado en tránsito AWS Direct Connect

Privacidad del tráfico entre redes en AWS Direct Connect

Tráfico entre el servicio y las aplicaciones y clientes locales

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 a VPCs. Para obtener más información, consulte Asociaciones de la puerta de enlace 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 para VPCs. Para obtener más información, consulte Asociaciones de la puerta de enlace privada virtual y Asociaciones de la puerta de enlace de tránsito.

Cifrado en tránsito AWS Direct Connect

AWS Direct Connect no cifra el tráfico que está en tránsito de forma predeterminada. Para cifrar los datos en tránsito que los atraviesan AWS Direct Connect, debe utilizar las opciones de cifrado de

tránsito de ese servicio. Para obtener más información sobre el cifrado del tráfico de EC2 instancias, consulta Encryption in Transit en la Guía del EC2 usuario de Amazon.

Con AWS Direct Connect y AWS Site-to-Site VPN, puede combinar una o más conexiones de red AWS Direct Connect dedicadas con la VPN de Amazon VPC. Esta combinación proporciona una conexión privada IPsec cifrada que también reduce los costes de la red, aumenta el rendimiento del ancho de banda y proporciona una experiencia de red más uniforme que las conexiones VPN basadas en Internet. Para obtener más información, consulte Opciones de conectividad de Amazon VPC-to-Amazon VPC.

MAC Security (MACsec) es un estándar IEEE 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 Seguridad MAC (MACsec).

Identity and Access Management para Direct Connect

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

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- Funcionamiento de Direct Connect con IAM
- Ejemplos de políticas basadas en identidades de Direct Connect
- Funciones vinculadas al servicio para AWS Direct Connect
- AWS políticas gestionadas para AWS Direct Connect
- Solución de problemas de identidad y acceso de Direct Connect

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 ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Direct Connect, consulte Solución de problemas de identidad y acceso de Direct Connect.

Administrador de servicio: si está a cargo de los recursos de Direct Connect de su empresa, es probable que tenga acceso completo a Direct Connect. Su trabajo consiste en determinar a qué características y recursos de Direct Connect deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestionador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Direct Connect, consulte Funcionamiento de Direct Connect con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera obtener más detalles sobre cómo escribir políticas para administrar el acceso a Direct Connect. Para consultar ejemplos de las políticas basadas en identidades de Direct Connect que puede utilizar en IAM, consulte Ejemplos de políticas basadas en identidades de Direct Connect.

Autenticación con identidades

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

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAM Identity 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, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accedes AWS mediante la federación, estás asumiendo un rol de forma indirecta.

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

Si accede AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre la firma de solicitudes, consulte AWS Signature Versión 4 para solicitudes API en la Guía del usuario de IAM.

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

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste para crear la cuenta. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

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

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web AWS Directory Service, el directorio del Centro de Identidad o cualquier usuario al que acceda Servicios de AWS mediante las credenciales proporcionadas a través de una fuente de identidad. Cuando las identidades federadas acceden Cuentas de AWS, asumen funciones y las funciones proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puede crear usuarios y grupos en el Centro de identidades de IAM o puede conectarse y sincronizarse con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus Cuentas de AWS aplicaciones. Para obtener más información, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center .

Usuarios y grupos de IAM

Un usuario de IAM es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes 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 los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad dentro de usted Cuenta de AWS que tiene permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una persona determinada. Para asumir temporalmente un rol de IAM en el AWS Management Console, puede cambiar de un rol de usuario a uno de IAM (consola). Puedes asumir un rol llamando a una operación de AWS API AWS CLI o usando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

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

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles de federación, consulte Crear un rol para un proveedor de identidad de terceros (federación) en la Guía de usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunas Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- 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 usuario o un rol de IAM para realizar acciones en AWS ellas, se te considera principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. El FAS utiliza los permisos del principal que llama Servicio de AWS y los solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio

desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

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

- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un rol de IAM para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y realizan AWS CLI solicitudes a la AWS API. Esto es preferible a almacenar las claves de acceso en 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 Usar un rol de IAM para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del usuario de IAM.

Administración de acceso mediante políticas

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

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

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

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción

`iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de la API AWS Management Console AWS CLI, la o la AWS API.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

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

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

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

Listas de control de acceso () 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. ACLs son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3 y Amazon VPC son ejemplos de servicios compatibles. AWS WAF ACLs Para obtener más información ACLs, 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 característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCPs): SCPs son políticas de JSON que especifican los permisos máximos para una organización o unidad organizativa (OU). AWS Organizations AWS Organizations es un servicio para agrupar y 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. El SCP limita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre Organizations SCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son políticas de JSON que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las políticas de IAM asociadas a cada recurso que poseas. El RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades, incluidos los permisos Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyo RCPs, consulte Políticas de control de recursos (RCPs) 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 más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

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

Funcionamiento de Direct Connect con IAM

Antes de utilizar IAM para administrar el acceso a Direct Connect, conozca qué características de IAM se pueden utilizar con Direct Connect.

Características de IAM que puede utilizar con Direct Connect

Característica de IAM	Compatibilidad de Direct Connect
Políticas basadas en identidades	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política (específicas del servicio)	Sí
ACLs	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	Sí

Característica de IAM	Compatibilidad de Direct Connect
Roles vinculados al servicio	No

Para obtener una visión general de cómo funcionan Direct Connect y otros AWS servicios con la mayoría de las funciones de IAM, consulte AWS los servicios que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidades de Direct Connect

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociada. Para obtener más información sobre los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades de Direct Connect

Para ver ejemplos de políticas basadas en identidades de Direct Connect, consulte Ejemplos de políticas basadas en identidades de Direct Connect.

Políticas basadas en recursos en Direct Connect

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal

en una política en función de recursos. Los directores pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

Para habilitar el acceso entre cuentas, puede especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso son diferentes Cuentas de AWS, el administrador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política basada en recursos concede acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Cross account resource access in IAM en la Guía del usuario de IAM.

Acciones de políticas de Direct Connect

Compatibilidad con las acciones de políticas: sí

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

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

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

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

Las acciones de políticas de Direct Connect utilizan el siguiente prefijo antes de la acción:

```
Direct Connect
```

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

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

```
        ]
```

Recursos de políticas de Direct Connect

Compatibilidad con los recursos de políticas: sí

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

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes 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, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Para ver una lista de los tipos de recursos de Direct Connect y sus respectivos tipos ARNs, consulte Recursos definidos por Direct Connect en la referencia de la AWS Direct Connect API. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por Direct Connect.

Para ver ejemplos de políticas basadas en identidades de Direct Connect, consulte Ejemplos de políticas basadas en identidades de Direct Connect.

Para ver ejemplos de políticas basadas en recursos de Direct Connect, consulte Ejemplos de políticas basadas en identidades de Direct Connect que utilizan condiciones basadas en etiquetas.

Claves de condición de políticas de Direct Connect

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

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

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones

condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

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

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

Para ver una lista de claves de condición de Direct Connect, consulte Claves de condición de Direct Connect en la Referencia de la API de AWS Direct Connect . Para saber con qué acciones y recursos se puede utilizar una clave de condición, consulte Acciones, recursos y claves de condición para Direct Connect en la Referencia de autorización de servicio.

Para ver ejemplos de políticas basadas en identidades de Direct Connect, consulte Ejemplos de políticas basadas en identidades de Direct Connect.

ACLs en Direct Connect

Soportes ACLs: No

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

ABAC con Direct Connect

Compatibilidad con ABAC (etiquetas en las políticas): parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar

etiquetas a las entidades de IAM (usuarios o roles) y a muchos AWS recursos. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

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

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

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

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

Uso de credenciales temporales con Direct Connect

Compatibilidad con credenciales temporales: sí

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

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

Puedes crear credenciales temporales manualmente mediante la AWS CLI API o. AWS A continuación, puede utilizar esas credenciales temporales para acceder AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de utilizar claves de acceso a largo plazo. Para 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 usuario o un rol de IAM 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. FAS utiliza los permisos del principal que llama y los que solicita Servicio de AWS para realizar solicitudes a los servicios descendentes. Servicio de AWS Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio de Direct Connect

Compatibilidad con roles de servicio: sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de Direct Connect. Edite los roles de servicio solo cuando Direct Connect proporcione orientación para hacerlo.

Roles vinculados a servicios para Direct Connect

Compatibilidad con roles vinculados al servicio: no

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

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol

vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidades de Direct Connect

De forma predeterminada, los usuarios y los roles no tienen permiso para crear ni modificar los recursos de Direct Connect. Tampoco pueden realizar tareas mediante la AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS la API. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

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

Para obtener más información sobre las acciones y los tipos de recursos definidos por Direct Connect, incluido el ARNs formato de cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición de Direct Connect en la Referencia de autorización del servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Acciones, recursos y condiciones de Direct Connect
- Uso de la consola de Direct Connect
- 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. Con el fin de obtener más información, consulta las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

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

Acciones, recursos y condiciones de Direct Connect

Con las políticas basadas en identidades de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Direct Connect admite acciones, claves de condiciones y recursos específicos. Para obtener información sobre todos los elementos que utiliza en una política JSON, consulte Referencia de los elementos de las políticas JSON de IAM en la Guía del usuario de IAM.

Acciones

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

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Las acciones políticas suelen tener el mismo nombre que la operación de AWS API asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

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

Las acciones de políticas de Direct Connect utilizan el siguiente prefijo antes de la acción: `directconnect:`. Por ejemplo, para conceder permiso a alguien para ejecutar una EC2 instancia de Amazon con la operación de la EC2 `DescribeVpnGateways` API de Amazon, debes incluir la `ec2:DescribeVpnGateways` acción en su política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`. Direct Connect define su propio conjunto de acciones que describen las tareas que se pueden realizar con este servicio.

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

JSON

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

```
                "ec2:DescribeVpnGateways"
            ],
            "Resource": "*"
        }
    ]
}
```

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

JSON

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

Para ver una lista de las acciones de Direct Connect, consulte Acciones definidas por Direct Connect en la Guía del usuario de IAM.

Recursos

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

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes 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, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Direct Connect utiliza lo siguiente ARNs:

Recurso de conexión directa ARNs

Tipo de recurso	ARN
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`
dx-vif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`

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

Por ejemplo, para especificar la interfaz `dxcon-11aa22bb` en su instrucción, utilice el siguiente ARN:

```
"Resource": "arn:aws:directconnect:us-east-1:123456789012:dxcon/dxcon-11aa22bb
```

Para especificar todas las interfaces virtuales que pertenecen a una cuenta específica, utilice el carácter comodín (*):

```
"Resource": "arn:aws:directconnect:*:*:dxvif/*"
```

Algunas acciones de Direct Connect, como las empleadas para la creación de recursos, no se pueden llevar a cabo en un recurso específico. En dichos casos, debe utilizar el carácter comodín (*).

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

Para ver una lista de los tipos de recursos de Direct Connect y sus tipos ARNs, consulte los tipos de recursos definidos por AWS Direct Connect en la Guía del usuario de IAM. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por Direct Connect.

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

En el siguiente ejemplo, ninguna de las opciones especificadas `Effect` tendrá éxito si se `DescribeConnections` invoca la acción sin que se `connectionId` apruebe la solicitud.

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

```
]
```

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

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

Claves de condición

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

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

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

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

Direct Connect define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del usuario de IAM.

Puede utilizar claves de condición con el recurso de etiqueta. Para obtener más información, consulte Ejemplo: restricción del acceso a una región específica.

Para ver una lista de claves de condición de Direct Connect, consulte Claves de condición de Direct Connect en la Guía del usuario de IAM. Para obtener información sobre las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por Direct Connect.

Uso de la consola de Direct Connect

Para acceder a la consola de Direct Connect, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Direct Connect de su AWS cuenta. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

Para garantizar que esas entidades puedan seguir utilizando la consola de Direct Connect, adjunte también la siguiente política AWS administrada a las entidades. Para obtener más información, consulte Agregar de permisos a un usuario en la Guía del usuario de IAM.

```
directconnect
```

No es necesario conceder permisos mínimos de consola a los usuarios que solo realizan llamadas a la API AWS CLI o a la AWS API. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

Permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la API AWS CLI o AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Acceso de solo lectura a AWS Direct Connect

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

JSON

```
{
    "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.

JSON

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

Ejemplos de políticas basadas en identidades de Direct Connect que utilizan condiciones basadas en etiquetas

Puede controlar el acceso a los recursos y las solicitudes mediante condiciones de clave de etiqueta. También puede utilizar una condición en su política de IAM para controlar si se pueden utilizar claves de etiqueta específicas en un recurso o en una solicitud.

Para obtener información sobre el uso de etiquetas con políticas de IAM, consulte Control del acceso con etiquetas en la Guía del usuario de IAM.

Asociación de interfaces virtuales de Direct Connect basada en etiquetas

En el ejemplo siguiente se muestra cómo puede crear una política que permita asociar una interfaz virtual solo si la etiqueta contiene la clave de entorno y los valores preprod o production.

JSON

```
 {
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "directconnect:AssociateVirtualInterface"
    ],
    "Resource": "arn:aws:directconnect:*:*:dxvif/*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/environment": [
          "preprod",
          "production"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "directconnect:DescribeVirtualInterfaces",
    "Resource": "*"
  }
]
}
```

Control del acceso a solicitudes basado en etiquetas

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

JSON

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Action": "directconnect:TagResource",
        "Resource": "arn:aws:directconnect:*:*:dxvif/*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/environment": [
                    "preprod",
                    "production"
                ]
            },
            "ForAllValues:StringEquals": {"aws:TagKeys": "environment"}
        }
    }
}
```

Control de claves de etiqueta

Puede utilizar una condición en sus políticas de IAM para controlar si se pueden utilizar claves de etiqueta específicas en un recurso o en una solicitud.

En el ejemplo siguiente se muestra cómo puede crear una política que le permita etiquetar recursos, pero solo con la clave de etiqueta environment.

JSON

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
```

```
        "Action": "directconnect:TagResource",
        "Resource": "*",
        "Condition": {
          "ForAllValues:StringEquals": {
            "aws:TagKeys": [
              "environment"
            ]
          }
        }
      }
    }
```

Funciones vinculadas al servicio para AWS Direct Connect

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

Un rol vinculado a un servicio facilita la configuración AWS Direct Connect , ya que no es necesario añadir manualmente los permisos necesarios. AWS Direct Connect define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo AWS Direct Connect puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

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 acerca de otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a un servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de rol vinculados al servicio para AWS Direct Connect

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

El rol vinculado al servicio `AWSServiceRoleForDirectConnect` depende de los siguientes servicios para asumir el rol:

- `directconnect.amazonaws.com`

El rol vinculado al servicio `AWSServiceRoleForDirectConnect` utiliza la política administrada `AWSDirectConnectServiceRolePolicy`.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para que el rol vinculado al servicio `AWSServiceRoleForDirectConnect` se cree correctamente, la identidad de IAM con la que se utiliza AWS Direct Connect debe tener los permisos necesarios. Para conceder los permisos necesarios, asocie la siguiente política a la identidad de IAM.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "iam:CreateServiceLinkedRole",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "directconnect.amazonaws.com"
                }
            },
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": "iam:GetRole",
            "Effect": "Allow",
            "Resource": "*"
       }
    ]
}
```

Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Crear un rol vinculado a un servicio para 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 que se almacenan en tu nombre AWS Secrets Manager en la API o en la AWS Management Console API AWS CLI. AWS

> **Important**
>
> Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Para obtener más información, consulte Un nuevo rol ha aparecido en mi cuenta de IAM.

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

También puede utilizar la consola de IAM para crear un rol vinculado al servicio con el caso de uso de AWS Direct Connect. En la API AWS CLI o en la AWS API, cree un rol vinculado al servicio con el nombre del servicio. `directconnect.amazonaws.com` Para obtener más información, consulte Crear un rol vinculado a un servicio en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Edición de un rol vinculado a un servicio para 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 mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar un rol vinculado a un servicio para 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. La AWS Management Console AWS CLI, la API o la AWS

API AWS Direct Connect limpian los recursos y eliminan automáticamente la función vinculada al servicio.

También puede utilizar la consola de IAM para eliminar el rol vinculado al servicio. Para ello, primero debe eliminar de forma manual los recursos del rol vinculado al servicio y luego podrá eliminarlo.

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

Para eliminar 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 y LAGs. 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 a servicios mediante IAM

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

Regiones compatibles para los roles vinculados al servicio AWS Direct Connect

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

AWS políticas gestionadas para AWS Direct Connect

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

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

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

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

AWS política gestionada: AWSDirect ConnectFullAccess

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

Para ver los permisos de esta política, consulte AWSDirectConnectFullAccess en la AWS Management Console.

AWS política gestionada: AWSDirect ConnectReadOnlyAccess

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

Para ver los permisos de esta política, consulte AWSDirectConnectReadOnlyAccess en la AWS Management Console.

AWS política gestionada: AWSDirect ConnectServiceRolePolicy

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

Para ver los permisos de esta política, consulte AWSDirectConnectServiceRolePolicy en la AWS Management Console.

AWS Direct Connect actualizaciones de las políticas gestionadas AWS

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

Cambio	Descripción	Fecha
AWSDirectConnectServiceRolePolicy: política nueva	Para respaldar la seguridad de MAC, se AWSServiceRoleForDirectConnectagregó la función vinculada al servicio.	31 de marzo de 2021
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

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Direct Connect e IAM.

Temas

- No tengo autorización para realizar una acción en Direct Connect
- No estoy autorizado a realizar tareas como: PassRole
- Quiero permitir que personas ajenas a mí accedan Cuenta de AWS a mis recursos de Direct Connect

No tengo autorización para realizar una acción en Direct Connect

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `directconnect:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 directconnect:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `directconnect:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su AWS administrador. El gestionador 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.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Direct Connect. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador. AWS El gestionador 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 obtener más información, consulte lo siguiente:

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

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 tema de Amazon SNS. CloudWatch las alarmas no invocan acciones simplemente porque se encuentran en un estado determinado; el estado debe haber cambiado y se ha mantenido durante un número específico de períodos. Para obtener 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 los archivos de registro no hayan cambiado después de la entrega por CloudTrail. Para obtener más información, consulte

Registra las llamadas a la AWS Direct Connect API mediante AWS CloudTrail y Cómo trabajar con archivos de CloudTrail registro en la Guía del AWS CloudTrail usuario.

Para obtener más información, consulte Supervisar 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 de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

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

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde la perspectiva del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos

de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulta la Referencia de controles de Security Hub.

- Amazon GuardDuty: Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como el PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en AWS Direct Connect

La infraestructura 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, puedes 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 usar una 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 dedicadas para alcanzar su objetivo de 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 llamadas a la API 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. Nosotros recomendamos TLS 1.3. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Puede realizar estas operaciones de API 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 de Amazon Virtual Private Cloud (Amazon VPC). VPCs En efecto, esto aísla el acceso a la red a un AWS Direct Connect recurso determinado únicamente de la VPC específica de la red. AWS Por ejemplo, consulte the section called “Ejemplos de políticas basadas en identidades de Direct Connect”.

Seguridad del protocolo de puerta de enlace fronteriza (BGP)

La Internet depende en gran medida del BGP para enrutar la información entre los sistemas de red. El enrutamiento del BGP a veces puede ser susceptible a ataques maliciosos o al secuestro del BGP. Para saber cómo AWS proteger su red de forma más segura contra el secuestro de BGP, consulte Cómo AWS se ayuda a proteger el enrutamiento de Internet.

Utilice la AWS Direct Connect 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 Asignación de instalaciones de conexión (LOA-CFA) o aprovisionar una interfaz virtual pública o privada.

Antes de comenzar, asegúrese de que ha instalado y configurado la AWS CLI. Para obtener más información, consulte la Guía del usuario de AWS Command Line Interface.

Contenido

- Paso 1: Cree una conexión
- Paso 2: Descargar el documento LOA-CFA
- Paso 3: Crear una interfaz virtual y obtener la configuración del enrutador

Paso 1: Cree 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. Necesitará el ID para obtener el documento LOA-CFA en el siguiente paso.

```
aws directconnect create-connection --location Example location --bandwidth 1Gbps
 --connection-name "Connection to AWS"
```

```
{
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-EXAMPLE",
    "connectionState": "requested",
    "bandwidth": "1Gbps",
    "location": "Example location",
    "connectionName": "Connection to AWS",
    "region": "sa-east-1"
}
```

Paso 2: Descargar el documento LOA-CFA

Una vez que haya solicitado la conexión, podrá obtener el documento LOA-CFA mediante el comando `describe-loa`. El resultado aparece codificado en base64. Debe extraer el contenido relevante de la LOA, decodificarlo y generar un archivo PDF.

Para obtener el documento LOA-CFA a través de Linux o macOS

En este ejemplo, la última parte del comando decodifica el contenido mediante la utilidad base64 y envía el resultado a un archivo PDF.

```
aws directconnect describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent|base64 --decode > myLoaCfa.pdf
```

Para obtener el documento LOA-CFA mediante Windows

En este ejemplo, el resultado se extrae a un archivo denominado myLoaCfa .base64. El segundo comando utiliza la utilidad `certutil` para decodificar el archivo y enviar el resultado a un archivo PDF.

```
aws directconneawsct describe-loa --connection-id dxcon-fg31dyv6 --output text --query
 loaContent > myLoaCfa.base64
```

```
certutil -decode myLoaCfa.base64 myLoaCfa.pdf
```

Una vez que haya descargado el documento LOA-CFA, envíeselo a su proveedor de red o de coubicación.

Paso 3: Crear una interfaz virtual y obtener la configuración del enrutador

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 conectarla a la VPC. O bien, puede crear una interfaz virtual pública para conectarse a AWS servicios que no estén en una VPC. Puede crear una interfaz virtual que soporte nuestro IPv4 IPv6 tráfico.

Antes de comenzar, asegúrese de que ha leído todos los requisitos previos que detallan en the section called “Requisitos previos de las interfaces virtuales”.

Al crear una interfaz virtual mediante 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 de .

Creación de una interfaz virtual privada

1. Obtenga el ID de la puerta de enlace privada virtual (vgw-xxxxxxxx) adjunta a la VPC. Necesita el ID para crear la interfaz virtual en el siguiente paso.

   ```
   aws ec2 describe-vpn-gateways
   ```

   ```
   {
       "VpnGateways": [
           {
               "State": "available",
               "Tags": [
                   {
                       "Value": "DX_VGW",
   ```

```
                    "Key": "Name"
                }
            ],
            "Type": "ipsec.1",
            "VpnGatewayId": "vgw-ebaa27db",
            "VpcAttachments": [
                {
                    "State": "attached",
                    "VpcId": "vpc-24f33d4d"
                }
            ]
        }
    ]
}
```

2. Cree una interfaz virtual privada. Debe especificar un nombre, un ID de VLAN y un número de sistema autónomo (ASN) de BGP.

   Para IPv4 el tráfico, necesita IPv4 direcciones privadas para cada extremo de la sesión de interconexión de BGP. 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 peering de BGP; Amazon te asigna las direcciones. IPv6

3. Para ver la información de configuración del router en formato XML, describa la interfaz virtual que ha creado. Utilice el parámetro `--query` para extraer la información `customerRouterConfig` y el parámetro `--output` para organizar el texto en líneas delimitadas por tabulaciones.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-ffhhk74f
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-ffhhk74f">
  <vlan>101</vlan>
  <customer_address>192.168.1.2/30</customer_address>
  <amazon_address>192.168.1.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>private</connection_type>
```

```
</logical_connection>
```

Creación de una interfaz virtual pública

1. Para crear una interfaz virtual pública, debe especificar un nombre, un ID de VLAN y un número de sistema autónomo (ASN) de BGP.

   En cuanto al IPv4 tráfico, también debe especificar IPv4 las direcciones públicas para cada extremo de la sesión de interconexión de BGP y las IPv4 rutas públicas que anunciará a través de BGP. En el siguiente ejemplo, se crea una interfaz virtual pública para el tráfico. IPv4

```
aws directconnect create-public-virtual-interface --
connection-id dxcon-fg31dyv6 --new-public-virtual-interface
 virtualInterfaceName=PublicVirtualInterface,vlan=2000,asn=65000,amazonAddress=203.0.113.1/
{cidr=203.0.113.4/30}]
```

```
{
    "virtualInterfaceState": "verifying",
    "asn": 65000,
    "vlan": 2000,
    "customerAddress": "203.0.113.2/30",
    "ownerAccount": "123456789012",
    "connectionId": "dxcon-fg31dyv6",
    "addressFamily": "ipv4",
    "virtualGatewayId": "",
    "virtualInterfaceId": "dxvif-fgh0hcrk",
    "authKey": "asdf34example",
    "routeFilterPrefixes": [
        {
            "cidr": "203.0.113.0/30"
        },
        {
            "cidr": "203.0.113.4/30"
        }
    ],
    "location": "Example location",
    "bgpPeers": [
        {
            "bgpStatus": "down",
            "customerAddress": "203.0.113.2/30",
            "addressFamily": "ipv4",
```

```
            "authKey": "asdf34example",
            "bgpPeerState": "verifying",
            "amazonAddress": "203.0.113.1/30",
            "asn": 65000
        }
    ],
    "customerRouterConfig": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>\n<logical_connection id=\"dxvif-fgh0hcrk\">\n  <vlan>2000</
vlan>\n  <customer_address>203.0.113.2/30</customer_address>\n
 <amazon_address>203.0.113.1/30</amazon_address>\n  <bgp_asn>65000</bgp_asn>
\n  <bgp_auth_key>asdf34example</bgp_auth_key>\n  <amazon_bgp_asn>7224</
amazon_bgp_asn>\n  <connection_type>public</connection_type>\n</logical_connection>
\n",
    "amazonAddress": "203.0.113.1/30",
    "virtualInterfaceType": "public",
    "virtualInterfaceName": "PublicVirtualInterface"
}
```

Para crear una interfaz virtual pública que admita IPv6 el tráfico, puede especificar IPv6 las rutas que anunciará a través de BGP. No puedes especificar IPv6 direcciones para la sesión de intercambio de pares; 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 formato XML, describa la interfaz virtual que ha creado. Utilice el parámetro `--query` para extraer la información `customerRouterConfig` y el parámetro `--output` para organizar el texto en líneas delimitadas por tabulaciones.

```
aws directconnect describe-virtual-interfaces --virtual-interface-id dxvif-fgh0hcrk
 --query virtualInterfaces[*].customerRouterConfig --output text
```

```
<?xml version="1.0" encoding="UTF-8"?>
<logical_connection id="dxvif-fgh0hcrk">
  <vlan>2000</vlan>
  <customer_address>203.0.113.2/30</customer_address>
```

```
  <amazon_address>203.0.113.1/30</amazon_address>
  <bgp_asn>65000</bgp_asn>
  <bgp_auth_key>asdf34example</bgp_auth_key>
  <amazon_bgp_asn>7224</amazon_bgp_asn>
  <connection_type>public</connection_type>
</logical_connection>
```

Registra las llamadas a la AWS Direct Connect API mediante 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 las llamadas a la API AWS Direct Connect como eventos. Las llamadas capturadas incluyen llamadas desde la AWS Direct Connect consola y llamadas en código a las operaciones de la AWS Direct Connect API. 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 las notificaciones de Amazon SNS 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 referencia de la AWS Direct Connect API. Por ejemplo, las llamadas a las `CreatePrivateVirtualInterface` acciones `CreateConnection` y las acciones 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 le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales root o AWS Identity and Access Management (de usuario de IAM).
- 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 elemento `userIdentity` de CloudTrail.

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 llamadas a la API pública, 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 fundamental a la hora de mantener la fiabilidad, 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 un error multipunto en caso de que se produzca. Sin embargo, antes de comenzar a supervisar Direct Connect, conviene crear un plan de supervisión que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la supervisión?
- ¿Qué recursos deben monitorizarse?
- ¿Con qué frecuencia debe monitorizar estos recursos?
- ¿Qué herramientas de monitorización puede utilizar?
- ¿Quién se encarga de realizar las tareas de monitorización?
- ¿Quién debería recibir una notificación cuando surjan problemas?

El siguiente paso consiste en establecer un punto de referencia del rendimiento de Direct Connect normal en el entorno. Para ello se mide el rendimiento en distintos momentos y bajo distintas condiciones de carga. A medida que supervise Direct Connect, almacene datos de supervisión históricos. De este modo, puede compararlos con los datos de rendimiento actuales, identificar patrones de rendimiento normal y anomalías en el rendimiento, así como desarrollar métodos para la resolución de problemas.

Para establecer un punto de referencia, conviene supervisar el uso, el estado y la condición de las conexiones físicas de Direct Connect.

Contenido

- Herramientas de supervisión
- Monitoriza con Amazon CloudWatch

Herramientas de supervisión

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 supervisión automatizadas

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

- Amazon CloudWatch Alarms: observa una única métrica durante un período de tiempo que especifiques. Realiza una o varias acciones según el valor de la métrica con respecto a un umbral dado durante varios períodos de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS. CloudWatch las alarmas no invocan acciones simplemente porque se encuentran en un estado determinado; el estado debe haber cambiado y se ha mantenido durante un número específico de períodos. Para obtener información sobre las métricas y dimensiones disponibles, consulte 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 los archivos de registro no hayan cambiado después de la entrega por CloudTrail. Para obtener más información, consulte Registro de llamadas a la API de y Trabajar con archivos de CloudTrail registro en la Guía del AWS CloudTrail usuario.

Herramientas de supervisión 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 recogidas 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
- Ver AWS Direct Connect CloudWatch métricas
- Crea CloudWatch alarmas de Amazon para monitorear AWS Direct Connect las conexiones

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 desde conexiones dedicadas de Diect Connect.

Métrica	Descripción
`ConnectionState`	El estado de la conexión.1 indica activa y 0 indica inactiva.

Métrica	Descripción
	Esta métrica está disponible para conexiones dedicadas y alojadas. **Note** Esta métrica también se encuentra disponibl e en las cuentas de propietario de la interfaz virtual alojada, al igual que en las cuentas de propietario de la conexión. Unidades: no se devuelven unidades para esta métrica.
`ConnectionBpsEgress`	La velocidad de bits de los datos salientes desde el AWS lado de la conexión. El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especific ado (5 minutos de forma predeterminada y 1 minuto como mínimo). Puede cambiar el valor acumulado predeterminado. Es posible que esta métrica no esté disponible para una nueva conexión o cuando se reinicie un dispositi vo. La métrica se inicia cuando la conexión se utiliza para enviar o recibir tráfico. Unidades: bits por segundo

Métrica	Descripción
`ConnectionBpsIngress`	La velocidad de bits de los datos entrantes al AWS lado de la conexión. Es posible que esta métrica no esté disponible para una nueva conexión o cuando se reinicie un dispositivo. La métrica se inicia cuando la conexión se utiliza para enviar o recibir tráfico. Unidades: bits por segundo
`ConnectionPpsEgress`	` La velocidad de paquetes de los datos salientes desde el AWS lado de la conexión. El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especificado (5 minutos de forma predeterminada y 1 minuto como mínimo). Puede cambiar el valor acumulado predeterminado. Es posible que esta métrica no esté disponible para una nueva conexión o cuando se reinicie un dispositivo. La métrica se inicia cuando la conexión se utiliza para enviar o recibir tráfico. Unidades: paquetes por segundo

Métrica	Descripción
`ConnectionPpsIngress`	La velocidad de paquetes de datos entrantes al AWS lado de la conexión. El número registrado es el valor acumulado (promedio) durante el periodo de tiempo especific ado (5 minutos de forma predeterminada y 1 minuto como mínimo). Puede cambiar el valor acumulado predeterminado. Es posible que esta métrica no esté disponible para una nueva conexión o cuando se reinicie un dispositi vo. La métrica se inicia cuando la conexión se utiliza para enviar o recibir tráfico. Unidades: paquetes por segundo
`ConnectionCRCErrorCount`	Este recuento ya no está en uso. En su lugar, use `ConnectionErrorCount` .

Métrica	Descripción
`ConnectionErrorCount`	El recuento total de errores de todos los tipos de errores de nivel de MAC en el dispositivo de AWS . El total incluye errores de comprobación de redundancia cíclica (CRC). Esta métrica es el recuento de errores que se han producido desde el último punto de datos registrado. Cuando hay errores en la interfaz, la métrica muestra valores distintos de cero. Para obtener el recuento total de todos los errores del intervalo seleccionado en CloudWatch, por ejemplo, 5 minutos, aplique la estadística de «suma». 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 esta métrica se aplica a un LAG, 1 indica que todas las conexiones del LAG se encuentran cifradas up. 0 indica que al menos una conexión LAG se encuentra cifrada down.

AWS Direct Connect métricas de la interfaz virtual

Las siguientes métricas están disponibles en las interfaces AWS Direct Connect virtuales.

Métrica	Descripción
`VirtualInterfaceBpsEgress`	La velocidad de bits de los datos salientes desde el AWS lateral de la interfaz virtual. 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 para la conexión de Direct Connect y la interfaz virtual. Esta dimensión filtra los datos por conexión.
`OpticalLaneNumber`	Esta dimensión filtra los datos de `ConnectionLightLevelTx` y `ConnectionLightLevelRx`, y los filtra por el número de carril óptico de la conexión de Direct Connect.

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

Temas

- Ver 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**
>
> Al supervisar Direct Connect Through CloudWatch, puede solicitar métricas en intervalos de 1 minuto. Sin embargo, la frecuencia de actualización real está controlada por CloudWatch. Como CloudWatch controla el intervalo, Direct Connect no siempre puede garantizar intervalos inferiores a cinco minutos.

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

Para ver las métricas mediante la CloudWatch consola

Las métricas se agrupan en primer lugar por el espacio de nombres de servicio y, a continuación, por las diversas combinaciones de dimensiones dentro de cada espacio de nombres. Para obtener más información sobre cómo Amazon CloudWatch ver las métricas de Direct Connect, incluida la adición de funciones matemáticas o consultas prediseñadas, consulte Uso de Amazon CloudWatch métricas en la Guía del CloudWatch usuario de Amazon.

1. Abra la CloudWatch consola en. https://console.aws.amazon.com/cloudwatch/

2. En el panel de navegación, elija Metrics (Métricas) y, a continuación, All metrics (Todas las métricas).
3. En la sección de Métricas, elija DX.
4. Elija un ConnectionIdnombre de métrica y, a continuación, elija una de las siguientes opciones para definir mejor la métrica:
   - Agregar a la búsqueda: agrega esta métrica a los resultados de la búsqueda.
   - Solo buscar esta: solo busca esta métrica.
   - Eliminar del gráfico: elimina esta métrica del gráfico.
   - Solo graficar esta métrica: solo grafica esta métrica.
   - Graficar todos los resultados de la búsqueda: grafica todas las métricas.
   - Graficar con una consulta de SQL: abre Información de métricas: generador de consultas, que le permite elegir lo que desea graficar mediante la creación de una consulta de SQL. Para obtener más información sobre el uso de Metric Insights, consulta Consulta tus métricas con CloudWatch Metrics Insights en la Guía del CloudWatch usuario de Amazon.

Para ver las métricas mediante la AWS Direct Connect consola

1. 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

Puede crear una CloudWatch alarma que envíe un mensaje de Amazon SNS cuando la alarma cambie de estado. Una alarma vigila una métrica determinada durante el periodo especificado. Envía

una notificación a un tema de Amazon SNS en función del valor de la métrica con respecto a un umbral determinado durante varios periodos de tiempo.

Por ejemplo, puede crear una alarma que monitorice el estado de una conexión de AWS Direct Connect . Envía una notificación cuando el estado de conexión esté inactivo durante cinco periodos consecutivos de un minuto. Para obtener más información sobre lo que debe saber para crear una alarma y obtener más información sobre cómo crear una alarma, consulte Uso de Amazon CloudWatch Alarms en la Guía del CloudWatch usuario de Amazon.

Para crear una CloudWatch alarma.

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Alarms (Alarmas) y, a continuación, elija All Alarms (Todas las alarmas).
3. Seleccione Crear alarma.
4. Elija Seleccionar métrica y, a continuación, elija DX.
5. Elija la métrica de Métricas de conexión.
6. Seleccione la AWS Direct Connect conexión y, a continuación, elija la métrica Seleccionar métrica.
7. En la página Especificar la métrica y las condiciones, configure los parámetros de la alarma. Para obtener información más específica sobre las métricas y las condiciones, consulte Uso de Amazon CloudWatch Alarms en la Guía del CloudWatch usuario de Amazon.
8. 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 con AWS Direct Connect.

Componente	Cuota	Comentarios
Interfaces virtuales públicas o privadas por conexión AWS Direct Connect dedicada	50	Este límite no se puede aumentar.
Interfaces virtuales de tránsito por conexión AWS Direct Connect dedicada. Las interfaces virtuales de Transit se pueden usar para conectarse a una red central de Transit Gateway o WAN AWS en la nube. Para obtener más informaci ón, consulte Puertas de enlace.	4	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Interfaces virtuales públicas o privadas por conexión AWS Direct Connect dedicada e interfaces virtuales de tránsito por conexión AWS Direct Connect dedicada	51	Cuando se lanzó la AWS Direct Connect compatibilidad con Amazon VPC Transit Gateways, se añadió una cuota de una (1) interfaz virtual de tránsito a la cuota de 50 interfaces virtuales públicas o privadas por conexión dedicada. El número de interfaces virtuales de tránsito permitido ahora es de cuatro (4) y se tiene en cuenta para el máximo de 51 interface s virtuales por conexión dedicada. Este límite no se puede aumentar.
Interfaces virtuales privadas, públicas o de tránsito por AWS Direct Connect conexión alojada	1	Este límite no se puede aumentar.
AWS Direct Connect Conexiones activas por ubicación de Direct Connect por región y cuenta	10	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador

Componente	Cuota	Comentarios
		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 50 interfaces virtuales públicas o privadas por LAG. El número de interface s virtuales de tránsito permitido ahora es de cuatro (4) y se tiene en cuenta para el máximo de 51 interfaces virtuales por LAG. Este límite no se puede aumentar.
Rutas por sesión de Border Gateway Protocol (BGP) en una interfaz virtual privada o en una interfaz virtual de tránsito desde una instalación local a otra. AWS Si anuncia más de 100 rutas para cada sesión de BGP IPv4 y IPv6 durante ella, la sesión de BGP pasará a un estado inactivo con la sesión de BGP INACTIVA.	100 cada una para y IPv4 IPv6	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Rutas por sesión de protocolo de puerta de enlace fronteriza (BGP) en una interfaz virtual pública	1 000	Este límite no se puede aumentar.

Componente	Cuota	Comentarios
Conexiones dedicadas por grupo de agregación de enlace (LAG)	4 cuando la velocidad del puerto es inferior a 100 G 2 cuando la velocidad del puerto es de 100 G	
Enlaza grupos de agregación (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 puerta de enlace AWS Direct Connect	20	Este límite no se puede aumentar.
Pasarelas de tránsito por puerta de enlace AWS Direct Connect	6	Este límite no se puede aumentar.

Componente	Cuota	Comentarios
Número máximo de prefijos de ruta anunciados desde una puerta de enlace Direct Connect de la red central WAN de AWS Cloud conectada a una instalación local. **Note** Todas las interfaces virtuales de tránsito conectadas a esa puerta de enlace de Direct Connect recibirán todos los prefijos de ruta anunciados por la red principal.	5 000	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Interfaces virtuales (privadas o de tránsito) por puerta de enlace AWS Direct Connect	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 combinados para y IPv4 IPv6	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Número de interfaces virtuales por puerta de enlace privada virtual	No hay límite.	
Número de puertas de enlace de Direct Connect asociadas a una puerta de enlace de tránsito	20	Este límite no se puede aumentar.

Componente	Cuota	Comentarios
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: 1000BASE-LX (1310 nm), 10 GBASE-LR (1310 nm), 100 Gbps: 100 GBASE- y 400 Gbps: 400 GBASE-. LR4 LR4

Cuotas del BGP

Las siguientes son cuotas del BGP. Los temporizadores del BGP negocian hasta el valor más bajo entre los enrutadores. Los intervalos de la BFD los define el dispositivo más lento.

- Temporizador de retención predeterminado: 90 segundos
- Temporizador de retención mínimo: 3 segundos

  No se admite un valor de retención de 0.
- Temporizador de keepalive predeterminado: 30 segundos
- Temporizador de keepalive mínimo: 1 segundo
- Temporizador de reinicio fluido: 120 segundos

  Le recomendamos que no configure el reinicio fluido y la BFD de forma simultánea.
- Intervalo mínimo de detección de usuarios reales de la BFD: 300 ms
- Multiplicador mínimo de la BFD: 3

Consideraciones sobre el equilibrio de carga

Si desea utilizar el equilibrio de carga con varios puertos públicos, todos deben estar en la misma región. VIFs VIFs

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)
- Solución de problemas de capa 2 (enlace de datos)
- Solución de problemas de capa 3/4 (red/transporte)
- Solución de problemas de direccionamiento

Solución de problemas de capa 1 (físicos)

Si tú o tu proveedor de red tienen dificultades para establecer la conectividad física con un AWS Direct Connect dispositivo, sigue estos pasos para solucionar el problema.

1. Con la ayuda del proveedor de coubicación, compruebe que la conexión cruzada se ha completado. Pídale a él o a su proveedor de red que le faciliten una notificación de finalización de conexión cruzada y compare los puertos con los que aparecen en el documento LOA-CFA.
2. Compruebe que su router o el router del proveedor está encendido y que los puertos están activados.
3. Asegúrese de que los enrutadores utilicen el transceptor óptico correcto. La negociación automática del puerto debe estar deshabilitada si tiene una conexión con una velocidad de puerto superior a 1 Gbps. Sin embargo, según el punto final de AWS Direct Connect que dé servicio a su conexión, es posible que sea necesario activar o desactivar la negociación automática para las conexiones de 1 Gbps. Si es necesario deshabilitar la negociación automática para sus conexiones, la velocidad del puerto y el modo dúplex completo se deben configurar de forma manual. Si la interfaz virtual permanece inactiva, consulte Solución de problemas de capa 2 (enlace de datos). Según el punto final de Direct Connect que dé servicio a las terminaciones de la conexión, es posible que sea necesario habilitar o deshabilitar la negociación automática en consecuencia.
4. Compruebe que el router está recibiendo una señal óptica aceptable a través de la conexión cruzada.
5. Intente voltear (o girar) las hebras de fibra de transmisión/recepción.

6. Consulta las CloudWatch estadísticas de Amazon para AWS Direct Connect. Puede verificar las lecturas ópticas de Tx/Rx del AWS Direct Connect dispositivo (tanto de 1 Gbps como de 10 Gbps), el recuento de errores físicos y el estado operativo. Para obtener más información, consulta Monitoring with Amazon CloudWatch.
7. Póngase en contacto con el proveedor de coubicación y solicite un informe escrito para la señal óptica de transmisión/recepción a través de la conexión cruzada.
8. Si los pasos anteriores no resuelven los problemas de conectividad física, póngase en contacto con AWS Support y facilite la notificación de finalización de la conexión cruzada y el informe de la señal óptica que le ha proporcionado el proveedor de coubicación.

El siguiente diagrama contiene los pasos para diagnosticar problemas con la conexión física.

Cannot establish physical Direct Connect connection
Is cross connect complete?
No
Request completion notice from provider
Yes
Do ports on completion notice match LOA-CFA?
No
Contact provider
Yes
Is router on and ports activated?
No
Enable device and ports
Yes
Is router receiving optimal signal?
No
Check CW connection metrics
Flip Tx/Rx fiber strands
Still not working
Request optical signal report from provider
Contact Support
Yes
Done

Solución de problemas de capa 2 (enlace de datos)

Si la conexión AWS Direct Connect física está activa pero la interfaz virtual no funciona, siga los siguientes pasos para solucionar el problema.

1. Si no puede hacer ping a la dirección IP de mismo nivel de Amazon, compruebe que la dirección IP de mismo nivel está configurada correctamente y en la VLAN correcta. Asegúrese de que la dirección IP esté configurada en la subinterfaz de VLAN y no en la interfaz física (por ejemplo, GigabitEthernet 0/0.123 en lugar de 0/0). GigabitEthernet
2. Compruebe si el router tiene una entrada de dirección MAC desde el AWS punto final en la tabla de protocolos de resolución de direcciones (ARP).
3. Asegúrese de que los dispositivos intermedios entre los distintos puntos de enlace tienen habilitadas las redes troncales VLAN para la etiqueta de VLAN 802.1Q. El ARP no se puede establecer de forma AWS paralela hasta que AWS reciba el tráfico etiquetado.
4. Borre la caché de su tabla de ARP o de la del proveedor.
5. Si los pasos anteriores no establecen el ARP o sigues sin poder hacer ping a la IP del mismo nivel de Amazon, ponte en contacto con AWS Support.

El siguiente diagrama contiene los pasos para diagnosticar problemas con el enlace de datos.

Si la sesión de BGP sigue sin establecerse después de verificar estos pasos, consulte Solución de problemas de capa 3/4 (red/transporte). Si la sesión de BGP se ha establecido pero experimenta problemas de direccionamiento, consulte Solución de problemas de direccionamiento.

Solución de problemas de capa 3/4 (red/transporte)

Imagina una situación en la que tu conexión AWS Direct Connect física esté activa y puedas hacer ping a la dirección IP del mismo nivel de Amazon. Si la interfaz virtual está activa y la sesión de intercambio de tráfico BGP no se puede establecer, siga estos pasos para solucionar el problema:

1. Asegúrese de que el número de sistema autónomo (ASN) local de BGP y el ASN de Amazon están configurados correctamente.

2. Asegúrese de que el par IPs de ambos lados de la sesión de emparejamiento de BGP esté configurado 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 hay reglas de ACL ni de firewall que estén bloqueando el puerto TCP 179 ni ningún otro puerto TCP efímero con numeración alta. BGP necesita estos puertos para establecer una conexión TCP entre las direcciones IP de mismo nivel.
6. Compruebe si hay errores o mensajes de advertencia en los logs de BGP.
7. Si los pasos anteriores no establecen la sesión de peering de BGP, póngase en contacto con Support AWS.

El siguiente diagrama contiene los pasos para diagnosticar problemas con la sesión de intercambio de tráfico BGP.

Si la sesión de intercambio de tráfico BGP se ha establecido, pero experimenta problemas de direccionamiento, consulte Solución de problemas de direccionamiento.

Solución de problemas de direccionamiento

Imagine una situación en la que la interfaz virtual está activa y ha establecido una sesión de intercambio de tráfico BGP. Si no puede dirigir el tráfico a través de la interfaz virtual, siga estos pasos para solucionar el problema:

1. Asegúrese de que comunica una ruta para el prefijo de red local en la sesión de BGP. En una interfaz virtual privada, este puede ser un prefijo de red público o privado. En una interfaz virtual pública, este debe ser el prefijo de red direccionable públicamente.
2. En el caso de una interfaz virtual privada, asegúrese de que los grupos de seguridad y la red de VPC ACLs permitan el tráfico entrante y saliente para el prefijo de red local. Para obtener más información, consulte Grupos de seguridad y redes ACLs en la Guía del usuario de Amazon VPC.
3. En una interfaz virtual privada, asegúrese de que las tablas de enrutamiento de la VPC tienen prefijos que apuntan a la puerta de enlace privada virtual a la que está conectada la interfaz virtual privada. Por ejemplo, si quiere que todo el tráfico se dirija a su red local de forma predeterminada, puede agregar la ruta predeterminada (0.0.0.0/0 o ::/0) con la puerta de enlace privada virtual como destino en las tablas de enrutamiento de la VPC.
   - También puede habilitar la propagación de rutas para actualizar automáticamente sus tablas de ruteo en función de los anuncios de ruta dinámicos de BGP. Puede tener hasta 100 rutas propagadas por tabla de rutas. Este límite no se puede aumentar. Para obtener más información, consulte Habilitación y deshabilitación de la propagación de ruta en la Guía del usuario de Amazon VPC.
4. Si los pasos anteriores no resuelven sus problemas de enrutamiento, póngase en contacto con AWS 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. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

Cambio	Descripción	Fecha
Crear una asociación entre la puerta de enlace Direct Connect y una red AWS Network Manager principal	Ahora puede crear una asociación de puerta de enlace Direct Connect directamente entre Direct Connect y una red principal de AWS Cloud WAN.	25 de noviembre de 2024
Support para 400G	Se actualizaron los temas para incluir la compatibilidad con las conexiones de 400 G.	18 de julio de 2024
Se agregó un límite de SiteLink prefijos	Se agregó un prefijo límite para SiteLink al tema de cuotas y límites.	15 de junio de 2023
Support para SiteLink	Puede crear una interfaz virtual privada que permita la conectividad entre dos puntos de presencia de Direct Connect (PoPs) en la misma AWS región.	1 de diciembre de 2021
Support MAC Security	Puede utilizar AWS Direct Connect conexiones compatibl es MACsec con el cifrado de los datos desde el centro de datos corporativo hasta la AWS Direct Connect ubicación .	31 de marzo de 2021

Support para 100G	Temas actualizados para incluir la compatibilidad con conexiones dedicadas de 100 G.	12 de febrero de 2021
Nueva ubicación en Italia	Tema actualizado para incluir la ubicación nueva en Italia.	22 de enero de 2021
Nueva ubicación en Israel	Tema actualizado para incluir la ubicación nueva en Israel.	7 de julio de 2020
Soporte para pruebas de conmutación por error del kit de herramientas de resiliencia	Utilice la función de pruebas de conmutación por error del Resiliency Toolkit para probar la resiliencia de sus conexione s.	3 de junio de 2020
CloudWatch Soporte métrico VIF	Puede monitorear AWS Direct Connect las conexiones físicas y las interfaces virtuales mediante CloudWatch.	11 de mayo de 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 dedicadas para lograr su objetivo de SLA.	7 de octubre de 2019
Soporte regional adicional para Support for AWS Transit Gateway across accounts	Soporte regional adicional para AWS Transit Gateway todas las cuentas.	30 de septiembre de 2019

AWS Direct Connect soporte 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 la puerta de enlace de tránsito VPCs o VPNs 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.	27 de marzo de 2019
Soporte para marcos Jumbo	Puede enviar marcos gigantes (9001 MTU). AWS Direct Connect	11 de octubre de 2018
Comunidades BGP de preferencia local	Puede utilizar las etiquetas de comunidad de BGP de preferencia local para lograr el equilibrio entre el balanceo de carga y las preferencias de ruta del tráfico entrante a la red.	6 de febrero de 2018
AWS Direct Connect puerta de enlace	Puede usar una puerta de enlace Direct Connect para conectar su AWS Direct Connect conexión VPCs en regiones remotas.	1 de noviembre de 2017
CloudWatch Métricas de Amazon	Puedes ver CloudWatch las métricas de tus AWS Direct Connect conexiones.	29 de junio de 2017

Enlaza grupos de agregación	Puede crear un grupo de agregación de enlaces (LAG) para agregar varias AWS Direct Connect conexiones.	13 de febrero de 2017
IPv6 soporte	Su interfaz virtual ahora puede admitir una sesión de IPv6 emparejamiento BGP.	1 de diciembre de 2016
Compatibilidad del etiquetado	Ahora puede etiquetar sus recursos. AWS Direct Connect	4 de noviembre de 2016
LOA-CFA de autoservicio	Ahora puede descargar su carta de autorización y la asignación de la instalación de conexión (LOA-CFA) mediante la consola o la API. AWS Direct Connect	22 de junio de 2016
Nueva ubicación en Silicon Valley	Tema actualizado para incluir la ubicación nueva en Silicon Valley en la región Oeste de EE. UU. (Norte de California).	3 de junio de 2016
Nueva ubicación en Ámsterdam	Tema actualizado para incluir la ubicación nueva en Ámsterdam en la región Europa (Fráncfort).	19 de mayo de 2016
Nuevas ubicaciones en Portland, Oregón y Singapur	Tema actualizado para incluir las ubicaciones nuevas en Portland, Oregón y Singapur en las regiones Oeste de EE. UU. (Oregón) y Asia-Pacífico (Singapur).	27 de abril de 2016

Nueva ubicación en Sao Paulo, Brasil	Tema actualizado para incluir la ubicación nueva en São Paulo en la región América del Sur (São Paulo).	9 de diciembre de 2015
Nuevas ubicaciones en Dallas, Londres, Silicon Valley y Bombay	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 de noviembre de 2015
Nueva ubicación en la región de China (Pekín)	Temas actualizados para incluir la ubicación nueva en Pekín en la región China (Pekín).	14 de abril de 2015
Nueva sucursal de Las Vegas en la región del oeste de EE. UU. (Oregón)	Se actualizaron los temas para incluir la incorporación de la nueva sucursal de Las AWS Direct Connect Vegas en la región de EE. UU. Oeste (Oregón).	10 de noviembre de 2014
Nueva región de la 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 de octubre de 2014

Nuevas ubicaciones en la región de 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 de julio de 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.	4 de abril de 2014
Support para acceder a AWS regiones remotas	Nuevo tema añadido que explica cómo puede acceder a los recursos públicos de una región remota.	19 de diciembre de 2013
Support para conexiones alojadas	Temas actualizados para incluir la compatibilidad con conexiones alojadas.	22 de octubre de 2013
Nueva ubicación en la región de la 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 de junio de 2013
Nueva sucursal de Seattle en la región del oeste de EE. UU. (Oregón)	Se actualizaron los temas para incluir la incorporación de una nueva AWS Direct Connect ubicación en Seattle, que presta servicios a la región de EE. UU. Oeste (Oregón).	8 de mayo de 2013

Support para usar IAM con AWS Direct Connect	Se ha añadido un tema sobre su uso AWS Identity and Access Management con AWS Direct Connect.	21 de diciembre de 2012
Nueva región de 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 de diciembre de 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 ubicaciones que prestan servicio a las regiones de EE. UU. Este (Virginia del Norte) y Sudamérica (São Paulo).	13 de agosto de 2012

Support para las regiones de la 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 Californi a), UE (Irlanda), Asia Pacífico (Singapur) y Asia Pacífico (Tokio).	10 de enero de 2012
Support for the US West (Northern California) Region	Temas actualizados para la región EE. UU. Oeste (Norte de California).	8 de septiembre de 2011
Versión pública	La primera versión de AWS Direct Connect.	3 de agosto de 2011

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.