
Amazon Virtual Private Cloud

Guía del usuario



Amazon Virtual Private Cloud: Guía del usuario

Copyright © 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 comerciales 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 Amazon VPC?	1
Conceptos de Amazon VPC	1
Acceder a Amazon VPC	2
Precios de Amazon VPC	2
Cómo funciona Amazon VPC	3
VPC y subredes	3
VPC predeterminadas y no predeterminadas	3
Direccionamiento IP	4
Comparar IPv4 e IPv6	4
Direcciones IPv4 privadas	5
Direcciones IPv4 públicas	5
Direcciones IPv6	6
Utilizar sus propias direcciones IP	7
Tablas de ruteo	7
Acceder a Internet	7
Acceder a una red corporativa o doméstica	8
Conectar VPC y redes	8
AWSConsideraciones sobre la red global privada de	8
Introducción	10
Requisitos previos	10
Paso 1: Crear una VPC	10
Paso 2: ver información de las VPC	12
Paso 3: Lanzar una instancia en su VPC	13
Paso 4: Conectar a la instancia de E2 en la subred pública	13
Paso 5: eliminar	13
Pasos siguientes	14
Nubes virtuales privadas	15
Conceptos básicos sobre VPC	15
Ajuste de tamaño de la VPC	16
Ajuste de tamaño de VPC para IPv4	16
Administración de bloques de CIDR de IPv4 para una VPC	17
Ajuste de tamaño de VPC para IPv6	20
Trabajar con VPC	21
Creación de una VPC	21
Vea las VPC	25
Asociar un bloque de CIDR de una dirección IP secundaria con la VPC	25
Asociar un bloque de CIDR IPv6 a su VPC	26
Desasociar un bloque de CIDR IPv4 de su VPC	26
Desasociar un bloque de CIDR IPv6 de la VPC	27
Eliminar su VPC	27
VPC predeterminadas	28
Componentes de VPC predeterminados	29
Subredes predeterminadas	31
Consultar la VPC y las subredes predeterminadas	31
Crear una VPC predeterminada	32
Crear una subred predeterminada	33
Eliminar las subredes predeterminadas y la VPC predeterminada	34
Conjuntos de opciones de DHCP	34
¿Qué es DHCP?	34
¿Qué son los conjuntos de opciones?	35
Trabajar con los conjuntos de opciones de DHCP	37
Atributos DNS	42
Servidor DNS de Amazon	42
Nombre de host DNS	43

Atributos de DNS en su VPC	43
Cuotas de DNS	45
Consultar los nombres de host DNS de su instancia EC2	45
Ver y actualizar los atributos de DNS de su VPC	46
Zonas alojadas privadas	47
Compartir la VPC	47
Requisitos previos para las VPC compartidas	48
Compartir una subred	48
Dejar de compartir una subred compartida	49
Identificar al propietario de una subred compartida	50
Permisos para las subredes compartidas	50
Facturar y medir para el propietario y los participantes	51
Limitaciones	51
Ejemplo de uso compartido de subredes	52
Ampliar una VPC a otra zona	52
Ampliar los recursos de VPC a Local Zones	53
Ampliar los recursos de VPC a las zonas de Wavelength	56
Subredes en AWS Outposts	58
Subredes	60
Conceptos básicos sobre subredes	60
Tipos de subred	60
Configuración de subredes	61
Diagrama de la subred	61
Tamaño de subred	62
Ajuste de tamaño de subredes para direcciones IPv6	63
Enrutar la subred	63
Seguridad de la subred	64
Trabajar con subredes	64
Crear una subred en la VPC	64
Ver las subredes	65
Asociar un bloque de CIDR IPv6 a su subred	66
Desasociar un bloque de CIDR IPv6 de la subred	66
Modificar el atributo de direcciones IPv4 públicas de su subred	66
Modificar el atributo de direcciones IPv6 de su subred	67
Eliminar una subred	67
Información general de la API y de los comandos	67
Reservas de CIDR de subred	68
Trabaje con reservas de CIDR de subred mediante la consola	69
Trabajar con reservas de CIDR de subred mediante la AWS CLI	69
Listas de prefijos	70
Conceptos y reglas de las listas de prefijos	70
Administración de identidades y accesos para listas de prefijos	71
Trabajar con listas de prefijos administradas por el cliente	72
Trabajar con listas de prefijos administradas por AWS	77
Trabajar con listas de prefijos compartidas	78
Tablas de ruteo	81
Conceptos de las tablas de enrutamiento	81
Tablas de enrutamiento de subred	82
Tablas de ruteo de gateway	86
Prioridad de la ruta	88
Cuotas de la tabla de enrutamiento	90
Opciones de enrutamiento de ejemplo	90
Trabajar con tablas de ruteo	99
Enrutamiento de Middlebox	106
ACL de red	120
Conceptos básicos de la ACL de red	120
Reglas de ACL de red	121

ACL de red predeterminada	121
ACL de red personalizada	123
ACL de red personalizadas y otros servicios de AWS	133
Puertos efímeros	133
Detección de la MTU de la ruta	133
Trabajar con ACL de red	134
Ejemplo: controlar el acceso a las instancias de una subred	138
Reglas recomendadas para casos de uso del asistente de la VPC	140
Conectar la VPC	141
Gateways de Internet	142
Habilitar el acceso a Internet	142
Acceso a Internet desde una subred de la VPC	144
Información general de la API y de los comandos	148
Direcciones IP elásticas	149
Gateways de Internet de solo salida	153
Conceptos básicos de las gateways de Internet de solo salida	153
Trabajar con gateways de Internet de solo salida	154
Información general de la API y de la CLI	156
Dispositivos NAT	156
Gateways NAT	157
Instancias NAT	184
Comparación de los dispositivos NAT	192
AWS Transit Gateway	194
AWS Virtual Private Network	194
Interconexiones de VPC	195
Ejemplos sobre el uso del emparejamiento de VPC y AWS PrivateLink	196
Supervisión	197
Logs de flujo de VPC	197
Conceptos básicos de logs de flujo	198
Registros de log de flujo	200
Ejemplos de registros de log de flujo	205
Limitaciones de los logs de flujo	210
Precios de registros de flujo	210
Publicar en CloudWatch Logs	211
Publicar en Amazon S3	216
Trabajar con registros de flujo	222
Realizar consultas mediante Athena	226
Solucionar problemas	229
Seguridad	232
Protección de los datos	232
Privacidad del tráfico entre redes	233
Cifrado en tránsito	235
Seguridad de la infraestructura	235
Aislamiento de red	235
Controlar el tráfico de red	236
Identity and Access Management	237
Público	237
Autenticarse con identidades	237
Administrar el acceso con políticas	239
Cómo funciona Amazon VPC con IAM	241
Ejemplos de políticas	245
Solucionar problemas	252
AWSPolíticas administradas por	254
Grupos de seguridad	255
Conceptos básicos de los grupos de seguridad	256
Grupos de seguridad predeterminados para las VPC	256
Reglas del grupo de seguridad	257

Trabajar con grupos de seguridad	259
Trabajar con reglas de grupos de seguridad	261
Administrar de manera centralizada los grupos de seguridad de VPC mediante AWS Firewall Manager	264
Resiliencia	265
Validación de la conformidad	265
Configuración y análisis de vulnerabilidades	266
Prácticas recomendadas	266
Recursos adicionales	267
Tutorials	268
Tutoriales sobre el uso de la AWS CLI	268
Subredes y VPC habilitada para IPv4	268
Subredes y VPC de doble pila	273
VPC con IPv6 habilitado y subredes con solo IPv6	282
Tutoriales sobre el uso de AWS Management Console	291
Crear VPC con el asistente	291
Migrar VPC existentes de IPv4 a IPv6	360
Uso con otros servicios	375
AWS PrivateLink	375
AWS Network Firewall	376
DNS Firewall de Route 53 Resolver	377
Cuotas	378
VPC y subredes	378
DNS	378
Direcciones IP elásticas (IPv4)	378
Gateways	379
Listas de prefijos administradas por el cliente	379
ACL de red	380
Interfaces de red	380
Tablas de ruteo	381
Grupos de seguridad	381
Interconexiones de VPC	382
Puntos de conexión de la VPC	382
Uso compartido de VPC	383
Limitación controlada de API de Amazon EC2	383
Recursos de cuotas adicionales	383
Historial de revisión	385

¿Qué es Amazon VPC?

Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es muy similar a la red tradicional que usaría en su propio centro de datos, pero con los beneficios que supone utilizar la infraestructura escalable de AWS.

Conceptos de Amazon VPC

Amazon VPC es la capa de red para Amazon EC2. Si es nuevo en Amazon EC2, consulte [¿Qué es Amazon EC2?](#) en la Guía del usuario de Amazon EC2 para instancias de Linux para obtener una breve información general.

A continuación se enumeran los conceptos clave de las VPC:

- Nube virtual privada (VPC): una red virtual dedicada a su cuenta de AWS.
- Subred: un intervalo de direcciones IP en la VPC.
- Bloque de CIDR: enrutamiento entre dominios sin clase. Metodología de asignación de direcciones de protocolo de Internet y agregación de rutas. Para obtener más información, consulte [Enrutamiento entre dominios sin clase](#) en Wikipedia.
- Tabla de enrutamiento: un conjunto de reglas, denominadas rutas, que se utilizan para determinar dónde se dirige el tráfico de red.
- Conjuntos de opciones de DHCP: información de configuración (como nombre de dominio y servidor de nombres de dominio) pasada a instancias de EC2 cuando se lanzan en subredes de VPC.
- Gateway de Internet: una gateway que asocia a la VPC para habilitar la comunicación entre los recursos de la VPC e Internet.
- Puertas de enlace de Internet de solo salida: un tipo de puerta de enlace de Internet que permite a una instancia de EC2 en una subred acceder a Internet, pero impide que los recursos de Internet inicien la comunicación con la instancia.
- Punto de enlace de la VPC: le permite conectar de manera privada la VPC a los servicios admitidos de AWS y a los servicios del punto de enlace de la VPC habilitados por PrivateLink, sin necesidad de contar con una puerta de enlace de Internet, un dispositivo NAT, una conexión de VPN ni una conexión de AWS Direct Connect. Las instancias de su VPC no necesitan direcciones IP públicas para comunicarse con los recursos del servicio.
- Puerta de enlace NAT: un servicio administrado por AWS que permite que las instancias de EC2 en las subredes privadas se conecten a Internet, a otras VPC o a las redes en las instalaciones.
- Instancia NAT: una instancia de EC2 en una subred pública que permite que las instancias en las subredes privadas se conecten a Internet, a otras VPC o a las redes en las instalaciones.
- Puertas de enlace de operador: para las subredes de las zonas de Wavelength, este tipo de puerta de enlace permite el tráfico entrante desde una red de operador de telecomunicaciones en una ubicación específica y el tráfico saliente a una red de operador de telecomunicaciones e Internet.
- Listas de prefijos: un conjunto de bloques de CIDR que se pueden utilizar para configurar grupos de seguridad de VPC, tablas de enrutamiento de VPC y tablas de enrutamiento de AWS Transit Gateway, y se pueden compartir con otras cuentas de AWS mediante Resource Access Manager (RAM).
- Los grupos de seguridad funcionan como un firewall virtual para controlar el tráfico entrante y saliente de un recurso de AWS, como una instancia de EC2. Cada VPC incluye un grupo de seguridad predeterminado y puede crear grupos de seguridad adicionales. El grupo de seguridad solo se puede utilizar en la VPC para la que se creó.
- ACL de red: una capa de seguridad opcional para la VPC que actúa como firewall a fin de controlar el tráfico dentro y fuera de las subredes.

Acceder a Amazon VPC

Puede crear, acceder y administrar las VPC con cualquiera de las siguientes interfaces:

- AWS Management Console — proporciona una interfaz web que puede utilizar para acceder a sus VPC.
- AWS Command Line Interface (AWS CLI): proporciona comandos para numerosos servicios de AWS, incluido Amazon VPC, y es compatible con Windows, Mac y Linux. Para obtener más información, consulte [AWS Command Line Interface](#).
- AWS SDK: proporcionan API específicas de cada lenguaje y se encargan de muchos de los detalles de conexión, tales como, el cálculo de firmas, el control de reintentos de solicitudes y el control de errores. Para obtener más información, consulte [AWS SDK](#).
- API de consulta: proporciona acciones de API de nivel bajo a las que se llama mediante solicitudes HTTPS. La API de consulta es la forma más directa de acceder a Amazon VPC, pero requiere que la aplicación controle niveles de detalle de bajo nivel, como la generación de hash para firmar la solicitud y el control de errores. Para obtener más información, consulte las [Amazon VPC actions](#) (Acciones de Amazon VPC) en la Referencia de la API de Amazon EC2.

Precios de Amazon VPC

No hay cargo adicional por usar la VPC. Se aplican cargos por algunos componentes de VPC, como las gateways NAT, Reachability Analyzer y la replicación de tráfico. Para obtener más información, consulte [Precios de Amazon VPC](#).

Cómo funciona Amazon VPC

Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido. Esta red virtual es muy similar a la red tradicional que usaría en su propio centro de datos, pero con los beneficios que supone utilizar la infraestructura escalable de AWS.

Conceptos

- [VPC y subredes \(p. 3\)](#)
- [VPC predeterminadas y no predeterminadas \(p. 3\)](#)
- [Direccionamiento IP \(p. 4\)](#)
- [Tablas de ruteo \(p. 7\)](#)
- [Acceder a Internet \(p. 7\)](#)
- [Acceder a una red corporativa o doméstica \(p. 8\)](#)
- [Conectar VPC y redes \(p. 8\)](#)
- [AWSConsideraciones sobre la red global privada de \(p. 8\)](#)

VPC y subredes

Una nube virtual privada (VPC) es una red virtual dedicada para su cuenta de AWS. Esta infraestructura en la nube está aislada lógicamente de otras redes virtuales de la nube de AWS. Puede lanzar recursos de AWS, como instancias de Amazon EC2, en la VPC. Puede especificar un intervalo de direcciones IP para la VPC, añadir subredes, asociar grupos de seguridad y configurar tablas de ruteo.

Una subred es un rango de direcciones IP en su VPC. Puede lanzar recursos de AWS en una subred especificada. Utilice una subred pública para los recursos que deben conectarse a Internet y una subred privada para los recursos que no dispondrán de conexión a Internet.

Para proteger los recursos de AWS de cada subred, puede utilizar varias capas de seguridad, como grupos de seguridad y listas de control de acceso a la red (ACL).

Opcionalmente, puede asociar un bloque de CIDR IPv6 a la VPC y asignar direcciones IPv6 a las instancias de la VPC.

Más información

- [Conceptos básicos sobre VPC \(p. 15\)](#)
- [Conceptos básicos sobre subredes \(p. 60\)](#)
- [Privacidad del tráfico entre redes en Amazon VPC \(p. 233\)](#)
- [Direccionamiento IP \(p. 4\)](#)

VPC predeterminadas y no predeterminadas

Si su cuenta se creó después del 04-12-2013, incluirá una VPC predeterminada que tiene una subred predeterminada en cada zona de disponibilidad. Las VPC predeterminadas ofrecen los beneficios de las características avanzadas de EC2-VPC y están listas para el uso. Si tiene una VPC predeterminada y no especifica una subred al lanzar una instancia, la instancia se lanzará en la VPC predeterminada. No hace falta tener conocimientos sobre Amazon VPC para lanzar instancias en la VPC predeterminada.

También puede crear su propia VPC y configurarla según sea necesario. Estas VPC se conocen como VPC no predeterminadas. Las subredes creadas en la VPC no predeterminada y las subredes adicionales que cree en su VPC predeterminada se denominan subredes no predeterminadas.

Más información

- [VPC predeterminadas \(p. 28\)](#)
- [Introducción a Amazon VPC \(p. 10\)](#)

Direccionamiento IP

Las direcciones IP permiten que los recursos de la VPC se comuniquen entre sí y con otros recursos a través de Internet.

Al crear una VPC, debe asignarle un bloque de CIDR de IPv4 (un rango de direcciones IPv4 privadas), un bloque de CIDR de IPv6 o ambos (doble pila). No es posible obtener acceso a las direcciones IPv4 privadas a través de Internet. Las direcciones IPv6 son únicas a escala mundial y se pueden configurar para que sigan siendo privadas o accesibles en Internet.

La VPC puede funcionar en modo de pila doble. Esto significa que los recursos se pueden comunicar mediante IPv4, IPv6 o tanto IPv4 como IPv6. Las direcciones IPv4 e IPv6 son independientes entre sí; debe agregar rutas y reglas de grupo de seguridad de forma individual para IPv4 e IPv6.

Contenido

- [Comparar IPv4 e IPv6 \(p. 4\)](#)
- [Direcciones IPv4 privadas \(p. 5\)](#)
- [Direcciones IPv4 públicas \(p. 5\)](#)
- [Direcciones IPv6 \(p. 6\)](#)
- [Utilizar sus propias direcciones IP \(p. 7\)](#)

Comparar IPv4 e IPv6

En la tabla siguiente se resumen las diferencias entre IPv4 e IPv6 en Amazon EC2 y Amazon VPC.

Característica	IPv4	IPv6
Formato	Consta de 32 bits, con 4 grupos de hasta 3 dígitos decimales	Consta de 128 bits, con 8 grupos de hasta 4 dígitos hexadecimales
Tamaño de la VPC	De /16 a /28	Fijo de /56
Tamaño de la subred	De /16 a /28	Fijo de /64
Selección de direcciones	Puede elegir el bloque de CIDR IPv4 para la VPC o puede asignar un bloque de CIDR desde Amazon VPC IP Address Manager (IPAM). Para obtener más información acerca de Amazon VPC, consulte ¿Qué es IPAM? en la Guía del usuario de IPAM de Amazon VPC.	Puede traer su propio bloque de CIDR IPv6 a AWS para la VPC, elegir un bloque de CIDR IPv6 proporcionado por Amazon o asignar un bloque de CIDR de Amazon VPC IP Address Manager (IPAM). Para obtener más información acerca de Amazon VPC, consulte ¿Qué es IPAM? en la Guía del usuario de IPAM de Amazon VPC.
Direcciones IP elásticas	Soportado	No admitido
Gateways NAT	Soportado	No admitido

Característica	IPv4	IPv6
Puntos de conexión de la VPC	Soportado	No admitido
Instancias EC2	Compatible con todos los tipos de instancias	Compatible con todas las instancias de generación actual y con las instancias C3, R3 e I2.
AMI	Compatible con todas las AMI	Compatible con AMI configuradas para DHCPv6
Nombres DNS	Las instancias reciben nombres de DNS basados en IPBN o RBN proporcionado por Amazon. El nombre de DNS se resuelve en los registros de DNS seleccionados para la instancia.	Las instancias reciben nombres de DNS basado en IPBN o RBN proporcionado por Amazon. El nombre de DNS se resuelve en los registros de DNS seleccionados para la instancia.

Direcciones IPv4 privadas

Las direcciones IPv4 privadas (también denominadas direcciones IP privadas en este tema) no están disponibles a través de Internet y puede utilizarse para la comunicación entre las instancias de su VPC. Al lanzar una instancia en una VPC, se asigna una dirección IP privada principal del rango de direcciones IPv4 de la subred a la interfaz de red predeterminada (eth0) de la instancia. A cada instancia se le asigna también un nombre de host DNS privado (interno) que se resuelve en la dirección IP privada de la instancia. El nombre de host puede ser de dos tipos: basado en recursos o basado en IP. Para obtener más información, consulte [Nombres de instancias EC2](#). Si no especifica ninguna dirección IP privada principal, se seleccionará una dirección IP disponible en el rango de la subred. Para obtener más información sobre las interfaces de red, consulte [Interfaces de red elástica](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Es posible asignar direcciones IP privadas adicionales, conocidas como direcciones IP privadas secundarias, a las instancias en ejecución en la VPC. A diferencia de la dirección IP privada principal, es posible volver a asignar una dirección IP privada secundaria de una interfaz de red a otra. La dirección IP privada permanecerá asociada a la interfaz de red al detener y reiniciar la instancia. Asimismo, se liberará cuando se termine la instancia. Para obtener más información acerca de las direcciones IP principales y secundarias, consulte [Varias direcciones IP](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Las direcciones IP privadas son las direcciones IP que se encuentran en el rango del CIDR IPv4 de la VPC. La mayoría de los rangos de direcciones IP de la VPC se engloban en los rangos de direcciones IP privadas (no direccionables públicamente) especificados en RFC 1918. Sin embargo, puede utilizar los bloques de CIDR direccionables públicamente para su VPC. Independientemente del rango de direcciones IP de su VPC, no se admite el acceso directo a Internet desde el bloque de CIDR de su VPC, incluido el bloque de CIDR públicamente direccionable. Por ello, debe configurar el acceso a Internet a través de una gateway como, por ejemplo, una gateway de Internet, una gateway privada virtual, una conexión de AWS Site-to-Site VPN o AWS Direct Connect.

Direcciones IPv4 públicas

Todas las subredes tienen un atributo que determina si una interfaz de red creada en la subred recibe automáticamente una dirección IPv4 pública (también denominada dirección IP pública en este tema). Por lo tanto, al lanzar una instancia en una subred con este atributo habilitado, se asigna una dirección IP pública a la interfaz de red principal (eth0) que se crea para la instancia. La dirección IP pública se asigna a la dirección IP privada principal mediante conversión de direcciones de red (NAT).

Para controlar si su instancia recibe una dirección IP pública, haga lo siguiente:

- Modifique el atributo de direcciones IP públicas de su subred. Para obtener más información, consulte [Modificar el atributo de direcciones IPv4 públicas de su subred \(p. 66\)](#).
- Habilite o deshabilite la característica de direcciones IP públicas durante el lanzamiento de la instancia. Esta acción anulará el atributo de direcciones IP públicas de su subred.

La dirección IP pública se asigna desde el grupo de direcciones IP públicas de Amazon. Por lo tanto, no se asocia a su cuenta. Cuando se desasocia una dirección IP pública de su instancia, esta se libera de nuevo al grupo y deja de estar disponible para su utilización. Por lo tanto, no es posible asociar o desasociar manualmente las direcciones IP públicas. En su lugar, en determinados casos, se libera la dirección IP pública desde su instancia, o bien se asigna una dirección nueva. Para obtener más información, consulte [Direcciones IP públicas](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Si necesita asignar una dirección IP pública persistente a su cuenta con la posibilidad de asignarla o eliminarla de las instancias según sus necesidades, utilice una dirección IP elástica. Para obtener más información, consulte [Asociar direcciones IP elásticas con recursos en la VPC \(p. 149\)](#).

Si su VPC está habilitada para ofrecer compatibilidad con los nombres de host DNS, cada instancia que reciba una dirección IP pública o una dirección IP elástica también recibirá un nombre de host DNS público. El nombre de host DNS público se resuelve en la dirección IP pública de la instancia fuera de la red de la instancia y en una dirección IP privada de la instancia desde dentro de la red de la instancia. Para obtener más información, consulte [Atributos DNS para la VPC \(p. 42\)](#).

Direcciones IPv6

Es posible asociar de manera opcional un bloque de CIDR IPv6 a su VPC y sus subredes. Para obtener más información, consulte [Asociar un bloque de CIDR IPv6 a su subred \(p. 66\)](#).

Su instancia de la VPC recibirá una dirección IPv6 si se asocia un bloque de CIDR IPv6 a su VPC y su subred y si se cumple alguna de las condiciones siguientes:

- La subred está configurada para asignar automáticamente una dirección IPv6 a la interfaz de red principal de una instancia durante el lanzamiento.
- Al asignar manualmente una dirección IPv6 a su instancia durante el lanzamiento.
- Al asignar una dirección IPv6 a su instancia tras el lanzamiento.
- Al asignar una dirección IPv6 a una interfaz de red de la misma subred y al adjuntar la interfaz de red a su instancia tras el lanzamiento.

Cuando su instancia recibe una dirección IPv6 durante el lanzamiento, la dirección se asocia a la interfaz de red principal (eth0) de la instancia. Es posible desasociar la dirección IPv6 de la interfaz de red principal. No se admite la utilización de nombres de host de DNS IPv6 con su instancia.

Tenga en cuenta que la dirección IPv6 persiste al detener e iniciar la instancia. Asimismo, se libera al terminar la instancia. No puede volver a asignar una dirección IPv6 mientras esté asignada a otra interfaz de red, primero debe anular la asignación.

Puede asignar direcciones IPv6 adicionales a su instancia. Para ello, asígnelas a una interfaz de red adjunta a su instancia. El número de direcciones IPv6 que puede asignar a una interfaz de red, así como el número de interfaces de red que puede adjuntar a una instancia varía según el tipo de instancia. Para obtener más información, consulte [Direcciones IP por interfaz de red por tipo de instancia](#) en la Guía del usuario de Amazon EC2.

Las direcciones de IPv6 son únicas a nivel global y se pueden configurar para que sigan siendo privadas o para que estén disponibles en Internet. Es posible controlar si las instancias están disponibles a través de sus direcciones IPv6 controlando el direccionamiento de su subred, o bien utilizando un grupo de

seguridad y reglas de ACL de red. Para obtener más información, consulte [Privacidad del tráfico entre redes en Amazon VPC](#) (p. 233).

Para obtener más información acerca de los rangos de direcciones IPv6 reservados, consulte [IANA IPv6 Special-Purpose Address Registry](#) y [RFC4291](#).

Utilizar sus propias direcciones IP

Puede traer parte o todo su rango de direcciones IPv4 públicas o su rango de direcciones IPv6 a su cuenta de AWS. Sigue siendo el propietario del rango de direcciones, pero AWS lo anuncia en Internet de forma predeterminada. Una vez que traiga su gama de direcciones a AWS, aparecerá en su cuenta como un grupo de direcciones. Puede crear una dirección IP elástica desde el grupo de direcciones IPv4 y asociar un bloque CIDR IPv6 de su grupo de direcciones IPv6 a una VPC.

Para obtener más información, consulte [Traer sus propias direcciones IP \(BYOIP\)](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Tablas de ruteo

Las tablas de enrutamiento contienen conjuntos de reglas, denominadas rutas, que se utilizan para determinar dónde se dirige el tráfico de red de su VPC. Puede asociar de forma explícita una subred con una tabla de ruteo particular. De lo contrario, la subred se asocia de forma implícita con la tabla de ruteo principal.

Cada ruta de una tabla de ruteo especifica el rango de direcciones IP al que desea que vaya el tráfico (el destino) y la gateway, la interfaz de red o la conexión a través de la cual enviar el tráfico (el destino).

Más información

- [Configurar tablas de enrutamiento](#) (p. 81)

Acceder a Internet

Es posible controlar el modo en que las instancias lanzadas en la VPC tienen acceso a los recursos externos a la VPC.

Una VPC predeterminada incluye una puerta de enlace de Internet y las subredes predeterminadas son subredes públicas. Las instancias que se lanzan en subredes predeterminadas tienen dirección IPv4 privada y dirección IPv4 pública. Dichas instancias pueden comunicarse con Internet a través del gateway de Internet. Una gateway de Internet permite que las instancias se conecten a Internet a través del borde de la red de Amazon EC2.

De forma predeterminada, las instancias que se lanzan en subredes no predeterminadas disponen de dirección IPv4 privada; sin embargo, no disponen de dirección IPv4 pública a no ser que asigne específicamente una en el lanzamiento o que modifique el atributo de dirección IP pública de la subred. Dichas instancias pueden comunicarse entre sí, pero no pueden tener acceso a Internet.

Puede habilitar el acceso a Internet para una instancia que se haya lanzado en una subred no predeterminada. Para ello, adjunte un gateway de Internet a su VPC (siempre que su VPC no sea una VPC predeterminada) y asocie una dirección IP elástica a la instancia.

De manera alternativa, para permitir que una instancia de su VPC inicie conexiones salientes a Internet y bloquear las conexiones entrantes no solicitadas, puede utilizar un dispositivo de conversión de direcciones de red (NAT). El dispositivo NAT asigna varias direcciones IPv4 privadas a una única dirección IPv4 pública. Puede configurar los dispositivos NAT con una dirección IP elástica y conectarlos a Internet a través de puertas de enlace de Internet. Esto permite conectar una instancia de una subred privada a

Internet a través del dispositivo NAT, direccionando el tráfico desde la instancia a la puerta de enlace de Internet y las respuestas a la instancia.

Si asocia un bloque de CIDR IPv6 a su VPC y asigna direcciones IPv6 a sus instancias, las instancias pueden conectarse a Internet a través de IPv6 a través de una gateway de Internet. De manera alternativa, las instancias podrán iniciar conexiones salientes a Internet mediante IPv6 a través de un gateway de Internet de solo salida. Puesto que el tráfico IPv6 está aislado del tráfico IPv4, las tablas de ruteo deben incluir rutas separadas para el tráfico IPv6.

Más información

- [Conexión a Internet mediante una puerta de enlace de Internet \(p. 142\)](#)
- [Habilitar el tráfico IPv6 saliente mediante una puerta de enlace de Internet de solo salida \(p. 153\)](#)
- [Conexión a Internet u otras redes mediante dispositivos NAT \(p. 156\)](#)

Acceder a una red corporativa o doméstica

De manera opcional, puede conectar su VPC a su propio centro de datos corporativo utilizando una conexión de AWS Site-to-Site VPN de IPsec y, de este modo, convertir la nube de AWS en una ampliación de su centro de datos.

Una conexión VPN de sitio a sitio consta de dos túneles de VPN entre una puerta de enlace privada virtual o una puerta de enlace de tránsito en el lado de AWS y un dispositivo de puerta de enlace de cliente ubicado en su centro de datos. El dispositivo de gateway de cliente es un dispositivo físico o dispositivo de software que configure en su lado de la conexión de VPN de sitio a sitio.

Más información

- [AWS Site-to-Site VPN Guía del usuario de](#)
- [Transit Gateways \(Gateways de tránsito\)](#)

Conectar VPC y redes

Puede crear una interconexión de VPC entre dos VPC que permite direccionar el tráfico entre ellas de forma privada. Las instancias de ambas VPC se pueden comunicar entre sí siempre que se encuentren en la misma red.

También puede crear una gateway de tránsito y utilizarla para interconectar las VPC y las redes locales. La gateway de tránsito actúa como un enrutador virtual regional para el tráfico que fluye entre sus asociaciones, que puede incluir VPC, conexiones de VPN, gateways de AWS Direct Connect e interconexiones de gateways de tránsito.

Más información

- [Guía de interconexión de VPC](#)
- [Transit Gateways \(Gateways de tránsito\)](#)

AWS Consideraciones sobre la red global privada de

AWS proporciona una red global privada de alto rendimiento y baja latencia que ofrece un entorno seguro de informática en la nube para satisfacer sus necesidades de redes. AWS Las regiones están conectadas

a múltiples proveedores de servicios de Internet (ISP), así como a una red troncal global privada, lo que proporciona un mejor rendimiento de la red para el tráfico entre regiones enviado por los clientes.

Tenga en cuenta las siguientes consideraciones:

- El tráfico que circula en una zona de disponibilidad, o entre las zonas de disponibilidad de todas las regiones, se transfiere a través de la red global privada de AWS.
- El tráfico que circula entre las regiones siempre se dirige a través de la red global privada de AWS, salvo en las regiones de China.

Existen diversos factores que pueden causar la pérdida de paquetes de red, incluyendo las colisiones de flujos de red, los errores de nivel inferior (capa 2) y otros errores de red. Creamos y utilizamos nuestras redes para minimizar la pérdida de paquetes. Nos encargamos de medir las tasas de pérdida de paquetes (PLR) en toda la red troncal que conecta las regiones de AWS. Operamos la red troncal para obtener un valor de p99 de la tasa PLR por hora inferior al 0,0001 %.

Introducción a Amazon VPC

Para comenzar a usar Amazon VPC, puede crear una VPC con dos subredes. Cuando se haya creado la VPC y las subredes, podrá lanzar una instancia de EC2 en la subred y conectarse a ella. Después de conectarse correctamente a la instancia, terminará la instancia y eliminará la VPC y las subredes. Para saber más acerca del proceso estándar de creación de VPC y para obtener información completa sobre cada una de las opciones, consulte [Creación de una VPC \(p. 21\)](#).

Note

En este ejercicio, creará una VPC y dos subredes. Dentro de una de las subredes lanzará una instancia de EC2 bajo demanda. La creación de una VPC y de subredes es gratuita, pero existen cargos por el uso de datos asociados a las instancias de EC2. Para obtener más información, consulte [Precios de Amazon EC2 bajo demanda](#).

Contenido

- [Requisitos previos \(p. 10\)](#)
- [Paso 1: Crear una VPC \(p. 10\)](#)
- [Paso 2: ver información de las VPC \(p. 12\)](#)
- [Paso 3: Lanzar una instancia en su VPC \(p. 13\)](#)
- [Paso 4: Conectar a la instancia de E2 en la subred pública \(p. 13\)](#)
- [Paso 5: eliminar \(p. 13\)](#)
- [Pasos siguientes \(p. 14\)](#)

Requisitos previos

Si es la primera vez que usa AWS, debe registrarse en Amazon Web Services (AWS) antes de comenzar a usar Amazon VPC. Al registrarse, su cuenta de AWS se registra de forma automática en todos los servicios de AWS, incluido Amazon VPC.

Si todavía no ha creado una cuenta de AWS, diríjase a <https://aws.amazon.com/> y elija create a free account (crear una cuenta gratuita).

Para obtener más información acerca de los permisos de IAM necesarios para trabajar con Amazon VPC, consulte [Identity and Access Management para Amazon VPC \(p. 237\)](#) y [Ejemplos de políticas de Amazon VPC \(p. 245\)](#).

Paso 1: Crear una VPC

En este paso, se crea una VPC, subredes, zonas de disponibilidad, puertas de enlace NAT y puntos de conexión de la VPC.

Para crear una VPC, subredes y otros recursos de la VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.

2. En el panel de navegación, elija Your VPCs, Create VPC.
3. En Resources to create (Recursos a crear), elija VPC, subnets, etc. (VPC, subredes, etc.).
4. Modifique las opciones según sea necesario:
 - Name tag auto-generation: (Generación automática de etiquetas de nombre): elija una etiqueta de nombre que se aplicará a los recursos que cree. La etiqueta se puede generar automáticamente para el usuario o el usuario puede definir el valor. El valor definido se utilizará para generar la etiqueta Nombre en todos los recursos como "nombre-recurso". Por ejemplo, si ingresa "Preproducción", cada subred será etiquetada con una etiqueta de nombre "Preproducción-subred". Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizar etiquetas para buscar y filtrar los recursos o hacer un seguimiento de los costos de AWS.
 - IPv4 CIDR block (Bloque de CIDR IPv4): elija un CIDR IPv4 para la VPC. Esta opción es obligatoria.
 - IPv6 CIDR block (Bloque de CIDR IPv6): no deje seleccionado ningún bloque de CIDR IPv6 para este ejercicio.
 - Tenancy (Tenencia): elija Default (Predeterminado) para este ejercicio a fin de garantizar que las instancias de EC2 lanzadas en esta VPC utilicen el atributo de tenencia de la instancia de EC2 especificado al lanzarla. Para obtener más información, consulte [. Creación de una VPC \(p. 21\)](#).
 - Availability Zones (AZs) (Zonas de Disponibilidad [AZs]): elija 1 para este ejercicio. Una zona de disponibilidad es uno o más centros de datos discretos con alimentación, redes y conectividad redundantes en una región de AWS. Las zonas de disponibilidad le dan la capacidad de operar aplicaciones de producción y bases de datos de mayor disponibilidad, tolerancia a errores y escalabilidad de lo que sería posible desde un único centro de datos. Si particiona las aplicaciones que se ejecutan en subredes a través de zonas de disponibilidad, estará mejor aislado y protegido de incidencias relacionadas con cortes de energía, rayos, tornados, terremotos, etc.
 - Customize AZs (Personalizar zonas de disponibilidad): deje seleccionadas las opciones predeterminadas para este ejercicio.
 - Number of public subnets (Número de subredes públicas): elija 1 para este ejercicio. Una subred "pública" es una subred que como entrada de la tabla de enrutamiento apunta a una puerta de enlace de Internet. Esto permite que las instancias de EC2 que se ejecutan en la subred sean de acceso público a través de Internet.
 - Customize public subnets CIDR blocks (Personalice los bloques CIDR de las subredes públicas): deje seleccionadas las opciones predeterminadas para este ejercicio. Para obtener más información, consulte [. Creación de una VPC \(p. 21\)](#).
 - Number of private subnets (Número de subredes privadas): elija 1 para este ejercicio. La subred "privada" es una subred que no dispone de una entrada a la tabla de enrutamiento que apunte a una puerta de enlace de Internet. Utilice subredes privadas para asegurar los recursos del backend que no necesitan un acceso público a través de Internet.
 - Customize private subnets CIDR blocks (Personalizar los bloques de CIDR de las subredes privadas): deje seleccionadas las opciones predeterminadas para este ejercicio. Para obtener más información, consulte [. Creación de una VPC \(p. 21\)](#).
 - NAT gateways (Puertas de enlace NAT): elija None (Ninguna) para este ejercicio. Una puerta de enlace NAT es un servicio administrado por AWS que permite a las instancias de EC2 en subredes privadas enviar tráfico saliente a Internet. En cambio, los recursos de Internet no pueden establecer una conexión con las instancias. Tenga en cuenta que existe un costo asociado a las puertas de enlace NAT. Para obtener más información, consulte [. Gateways NAT \(p. 157\)](#).
 - VPC endpoints (Puntos de conexión de la VPC): elija None (Ninguno) para este ejercicio. Un punto de conexión de VPC le permite conectar de forma privada la VPC a servicios de AWS compatibles como Amazon S3. Los puntos de conexión de la VPC le permiten crear una VPC aislada y cerrada de la Internet pública. El uso de puntos de enlace de gateway no supone ningún cargo adicional. Esto puede ayudar a evitar los costos asociados con las puertas de enlace NAT.
 - DNS options (Opciones de DNS): selecciona ambas opciones de resolución de nombres de dominio para las instancias de EC2 lanzadas en esta VPC.

- Enable DNS hostnames (Habilitar nombres de host DNS): permite aprovisionar nombres de host para las direcciones IPv4 públicas de las instancias de EC2.
 - Enable DNS resolution (Habilitar resolución DNS): permite aprovisionar nombres de host para las direcciones IPv4 públicas de las instancias de EC2 y habilita la resolución de nombres de dominio de los nombres de host.
5. En el panel Preview (Vista preliminar), puede ver la VPC, la subred, las tablas de enrutamiento y las conexiones de red que se crearán. Una conexión de red -igw representa una puerta de enlace de Internet que se creará. También se agregará una entrada de enrutamiento que apunte a la puerta de enlace de Internet en la tabla de enrutamiento asociada a la subred pública.
 6. Seleccione Create VPC.

Paso 2: ver información de las VPC

Una vez creada la VPC, podrá ver información acerca de la subred, la gateway de Internet y las tablas de enrutamiento.

Para ver la información de sus VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs (Sus VPC). Anote el nombre y el ID de la VPC que creó (consulte las columnas Name y VPC ID). Utilizará esta información más adelante para identificar los componentes asociados a su VPC.
3. En el panel de navegación, elija Subnets. La consola muestra las subredes públicas y privadas creadas. Puede identificar la subred por su nombre mediante la columna Name, o bien puede utilizar la información de VPC que obtuvo en el paso anterior y consultar la columna VPC.
4. En el panel de navegación, elija Internet Gateways (Puertas de enlace de Internet). Encontrará la gateway de Internet asociada con su VPC consultando la columna VPC, que muestra el ID y el nombre de la VPC (si corresponde).
5. En el panel de navegación, elija Route Tables (Tablas de enrutamiento). La VPC tiene asociadas dos nuevas tablas de enrutamiento personalizadas.
 - Seleccione la tabla de enrutamiento que contenga la palabra private(privado) en el nombre y, a continuación, elija la pestaña Routes (Enrutamiento) para mostrar la información de enrutamiento en el panel de detalles. La primera fila de la tabla se corresponde con la ruta local, que permite que las instancias en la VPC se comuniquen. Esta ruta está presente en todas las tablas de ruteo y, por lo tanto, no se puede quitar.
 - Seleccione la tabla de enrutamiento que contenga la palabra public(público) en el nombre y, a continuación, elija la pestaña Routes (Enrutamiento) para mostrar la información de enrutamiento en el panel de detalles. La segunda fila muestra la entrada de la puerta de enlace de Internet para habilitar el flujo de tráfico con destino a Internet (0.0.0.0/0) desde la subred a la puerta de enlace de Internet.
6. Seleccione la tabla de ruteo principal. La tabla de enrutamiento principal solo tiene una ruta local.

Note

Cada VPC que se crea obtiene una tabla de enrutamiento predeterminada (llamada tabla de enrutamiento principal) además de una tabla de enrutamiento personalizada para cada subred. La tabla de enrutamiento principal controla el direccionamiento de todas las subredes que no están explícitamente asociadas a ninguna otra tabla de enrutamiento. Puede identificar la tabla de enrutamiento principal por el valor que tiene en la columna Principal al visualizar sus Tablas de enrutamiento. Si el valor de esa columna es Yes (Sí), la tabla de enrutamiento es una tabla de enrutamiento principal. Si el valor es No, la tabla de enrutamiento es una tabla de enrutamiento personalizada.

Paso 3: Lanzar una instancia en su VPC

Siga los pasos indicados en [Lanzamiento de una instancia](#) en la Guía del usuario de instancias de Linux de Amazon EC2.

Important

Al crear la instancia de EC2, asegúrese de lo siguiente:

- Al abrir la consola de EC2, asegúrese de utilizar la misma región de AWS en la que creó la VPC.
- Al configurar la instancia de EC2 para lanzarla en una VPC, elija la VPC y la subred pública que creó en el paso anterior.
- Al configurar la instancia de EC2 para que se inicie en la subred pública, asegúrese de que la opción Auto-assign Public IP (Asignación automática de IP pública) esté establecida en Enable (Habilitar). De forma predeterminada, una instancia en una VPC independiente no tiene asignada una dirección IPv4 pública, por lo que debemos asignar una dirección IPv4 pública para poder conectarnos a nuestra instancia en la subred a través de Internet.
- El asistente de lanzamiento de EC2 crea una regla de grupo de seguridad que permite a todas las direcciones IP (0.0.0.0/0) acceder a la instancia mediante SSH o RDP. Esto es aceptable para este ejercicio, pero constituye una práctica peligrosa en entornos de producción. En entornos de producción, se autorizaría el acceso a la instancia únicamente a una dirección IP o a un rango de direcciones IP específico.

Paso 4: Conectar a la instancia de E2 en la subred pública

Se puede acceder a la instancia de EC2 en la subred pública desde Internet. Es posible conectarse a la instancia desde la red doméstica mediante SSH o a través del Escritorio remoto.

- Para obtener más información acerca de cómo conectarse a una instancia de Linux en la subred pública, consulte [Conexión a una instancia de Linux](#) en la Guía del usuario de instancias de Linux de Amazon EC2.
- Para obtener más información acerca de cómo conectarse a una instancia de Windows en la subred pública, consulte este artículo sobre las [conexiones a instancias de Windows](#) en la Guía del usuario de instancias de Windows de Amazon EC2.

Paso 5: eliminar

Puede elegir seguir utilizando su instancia en su VPC o si no necesita la instancia puede terminarla y liberar su dirección IP elástica para evitar que se apliquen gastos adicionales. También puede eliminar la VPC. Tenga en cuenta que no se le cobrará por las VPC y los componentes de VPC creados en este ejercicio (como, por ejemplo, las subredes y las tablas de enrutamiento).

Antes de poder eliminar una VPC, debe finalizar las instancias que se estén ejecutando en esta. A continuación, puede eliminar la VPC y sus componentes mediante la consola de VPC.

Para terminar la instancia y eliminar la VPC

1. Para terminar la instancia de EC2, siga los pasos indicados en [Terminar una instancia](#) en la Guía del usuario de instancias de Linux de Amazon EC2.

2. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
3. En el panel de navegación, elija Your VPCs (Sus VPC).
4. Seleccione la VPC; elija Actions y luego elija Delete VPC.
5. Confirme la eliminación y elija Delete (Eliminar).

Pasos siguientes

Después de crear una VPC no predeterminada, es posible que desee hacer lo siguiente:

- Agregue subredes a la VPC. Para obtener más información, consulte . [Crear una subred en la VPC \(p. 64\)](#).
- Habilite la compatibilidad con IPv6 para la VPC y las subredes. Para obtener más información, consulte . [Asociar un bloque de CIDR IPv6 a su subred \(p. 66\)](#).
- Habilite instancias de una subred privada para acceder a Internet. Para obtener más información, consulte . [Conexión a Internet u otras redes mediante dispositivos NAT \(p. 156\)](#).

Nubes virtuales privadas (VPC)

Una nube virtual privada (VPC) es una red virtual dedicada para su cuenta de AWS. Esta infraestructura en la nube está aislada lógicamente de otras redes virtuales de la nube de AWS. Puede lanzar recursos de AWS, como instancias de Amazon EC2, en la VPC.

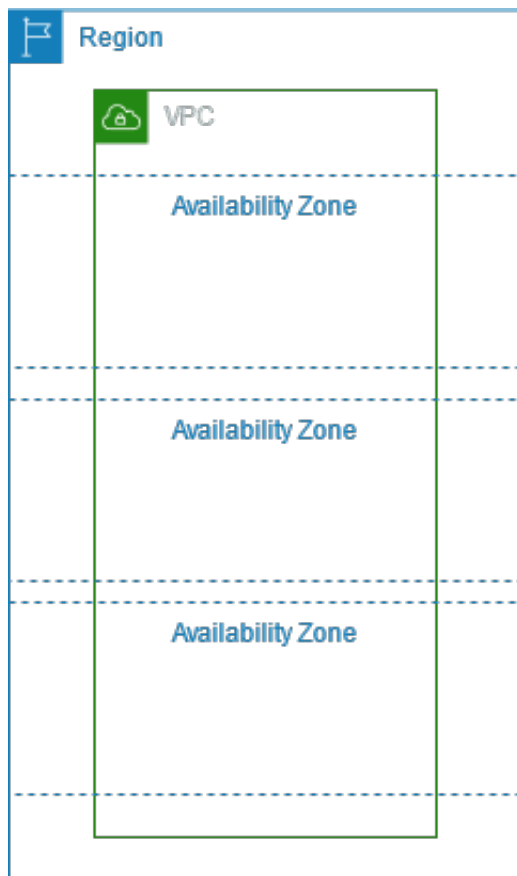
Contenido

- [Conceptos básicos sobre VPC \(p. 15\)](#)
- [Ajuste de tamaño de la VPC \(p. 16\)](#)
- [Trabajar con VPC \(p. 21\)](#)
- [VPC predeterminadas \(p. 28\)](#)
- [Conjuntos de opciones de DHCP en Amazon VPC \(p. 34\)](#)
- [Atributos DNS para la VPC \(p. 42\)](#)
- [Compartir la VPC con otras cuentas \(p. 47\)](#)
- [Ampliar una VPC a una zona local, una zona Wavelength o Outpost \(p. 52\)](#)

Conceptos básicos sobre VPC

Al crear una VPC, debe especificar un rango de direcciones IPv4 para la VPC como bloque de enrutamiento entre dominios sin clases (CIDR). Por ejemplo 10.0.0.0/16. Se trata del bloque de CIDR principal de la VPC. Para obtener más información acerca de la notación CIDR, consulte [RFC 4632](#).

Una VPC abarca todas las zonas de disponibilidad de la región. En el siguiente diagrama se muestra una VPC nueva. Después de crear la VPC, podrá añadir una o varias subredes en cada zona de disponibilidad. Para obtener más información, consulte [Subredes \(p. 60\)](#).



Ajuste de tamaño de la VPC

Amazon VPC admite el direccionamiento IPv4 e IPv6. Una VPC debe tener un bloque de CIDR IPv4. De forma opcional, puede asociar un bloque de CIDR IPv6 con su VPC.

Para obtener más información sobre el direccionamiento de IP, consulte [Direccionamiento IP](#) (p. 4).

Contenido

- [Ajuste de tamaño de VPC para IPv4](#) (p. 16)
- [Administración de bloques de CIDR de IPv4 para una VPC](#) (p. 17)
- [Ajuste de tamaño de VPC para IPv6](#) (p. 20)

Ajuste de tamaño de VPC para IPv4

Cuando crea una VPC, debe especificar un bloque de CIDR IPv4 para la VPC. El tamaño de bloque permitido oscila entre la máscara de subred /16 (65 536 direcciones IP) y /28 (16 direcciones IP). Una vez que haya creado su VPC, puede asociar bloques de CIDR secundarios con ella. Para obtener más información, consulte [Administración de bloques de CIDR de IPv4 para una VPC](#) (p. 17).

Al crear una VPC, se recomienda especificar un bloque de CIDR de los intervalos de direcciones IPv4 privadas como se especifica en [RFC 1918](#):

Intervalo RFC 1918	Ejemplo de bloque de CIDR
10.0.0.0 - 10.255.255.255 (prefijo 10/8)	Su VPC debe ser /16 o inferior, por ejemplo, 10.0.0.0/16.
172.16.0.0 - 172.31.255.255 (prefijo 172.16/12)	Su VPC debe ser /16 o inferior, por ejemplo, 172.31.0.0/16.
192.168.0.0 - 192.168.255.255 (prefijo 192.168/16)	Su VPC puede ser más pequeña, por ejemplo, 192.168.0.0/20.

Puede crear una VPC con un bloque de CIDR direccionable públicamente externo a los rangos de direcciones IPv4 privadas especificados en RFC 1918; sin embargo, para esta documentación, las direcciones IP privadas son aquellas direcciones IPv4 que se encuentran en el rango de CIDR de su VPC.

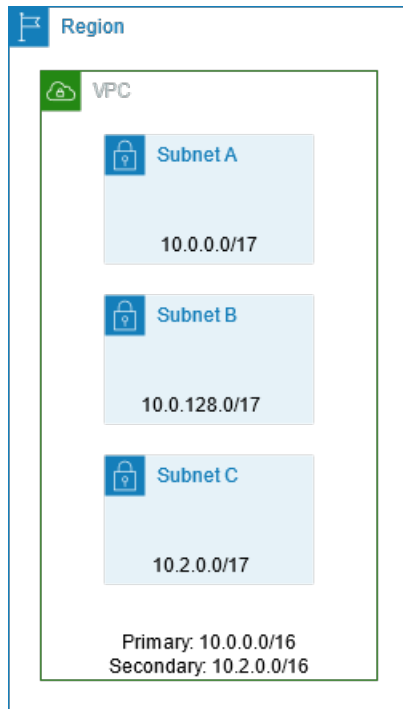
Si va a crear una VPC para usarla con otro servicio de AWS, consulte la documentación de dicho servicio para comprobar si hay requisitos específicos para el rango de direcciones IP o los componentes de red.

Si crea una VPC mediante una herramienta de la línea de comandos o la API de Amazon EC2, el bloque de CIDR se modifica automáticamente a su forma canónica. Por ejemplo, si especifica 100.68.0.18/18 para el bloque de CIDR, creamos un bloque de CIDR de 100.68.0.0/18.

Administración de bloques de CIDR de IPv4 para una VPC

Puede asociar bloques de CIDR IPv4 secundarios con su VPC. Al asociar un bloque de CIDR con su VPC, se agrega una ruta automáticamente a sus tables de ruteo de VPC para habilitar el direccionamiento en la VPC (el destino es el bloque de CIDR y el objetivo es `local`).

En el siguiente ejemplo, la VPC tiene un bloque de CIDR principal y otro secundario. Los bloques de CIDR de la subred A y la subred B provienen del bloque de CIDR principal de la VPC. El bloque de CIDR de la subred C proviene del bloque de CIDR secundario de la VPC.



En la siguiente tabla de enrutamiento se muestran las rutas locales de la VPC.

Destino	Objetivo
10.0.0.0/16	Local
10.2.0.0/16	Local

Para añadir un bloque de CIDR a su VPC, se aplican las siguientes reglas:

- El tamaño de bloque permitido oscila entre la máscara de subred /28 y /16.
- El bloque de CIDR no se debe solapar con otro bloque de CIDR existente que esté asociado con la VPC.
- Los rangos de las direcciones IPv4 que puede usar están sujetos a ciertas restricciones. Para obtener más información, consulte [Restricciones de asociación de bloques de CIDR IPv4 \(p. 19\)](#).
- No es posible aumentar o reducir el tamaño de un bloque de CIDR existente.
- Hay una cuota en el número de bloques de CIDR que se pueden asociar con una VPC y el número de rutas que se pueden agregar a una tabla de ruteo. No puede asociar un bloque de CIDR si el resultado supera las cuotas. Para obtener más información, consulte [Cuotas de Amazon VPC \(p. 378\)](#).
- El bloque de CIDR no debe ser igual o mayor que el rango de CIDR de destino en una ruta en cualquiera de las tablas de ruteo de VPC. Por ejemplo, en una VPC en la que el bloque de CIDR es 10.2.0.0/16, tiene una ruta existente en una tabla de enrutamiento con un destino de 10.0.0.0/24 para una gateway privada virtual. Desea asociar un bloque de CIDR en el rango 10.0.0.0/16. Debido a la ruta existente, no puede asociar un bloque de CIDR de 10.0.0.0/24 o mayor. No obstante, puede asociar un bloque de CIDR secundario de 10.0.0.0/25 o menor.
- Si ha habilitado la VPC para ClassicLink, puede asociar bloques de CIDR de los rangos 10.0.0.0/16 y 10.1.0.0/16, pero no puede asociar ningún otro bloque de CIDR del rango 10.0.0.0/8.
- Se aplican las siguientes reglas al agregar bloques de CIDR IPv4 a una VPC de forma parte de una interconexión de VPC:

- Si la interconexión de VPC es `active`, puede agregar bloques de CIDR a una VPC siempre que no se solapen con un bloque de CIDR de la VPC del mismo nivel.
- Si la interconexión de VPC es `pending-acceptance`, el propietario de la VPC del solicitante no puede agregar ningún bloque de CIDR a la VPC, independientemente de si se solapa con el bloque de CIDR de la VPC del aceptador. El propietario de la VPC del aceptador debe aceptar la interconexión o el propietario de la VPC del solicitante debe eliminar la solicitud de interconexión de VPC, agregar el bloque de CIDR y, a continuación, solicitar una nueva interconexión de VPC.
- Si la interconexión de VPC es `pending-acceptance`, el propietario de la VPC del aceptador puede agregar bloques de CIDR a la VPC. Si un bloque de CIDR secundario se solapa con un bloque de CIDR de la VPC del solicitante, se produce un error en la interconexión de VPC y no se puede aceptar.
- Si utiliza AWS Direct Connect para conectar con varias VPC a través de una gateway de Direct Connect, las VPC asociadas a la gateway no deben tener bloques de CIDR solapados. Si añade un bloque de CIDR a una de las VPC asociadas a la gateway de Direct Connect, asegúrese de que el nuevo bloque de CIDR no se solape con un bloque de CIDR existente de cualquier otra VPC asociada. Para obtener más información, consulte [gateways de Direct Connect](#) en la Guía del usuario de AWS Direct Connect.
- Cuando añade o elimina un bloque de CIDR, este puede pasar por varios estados: `associating` | `associated` | `disassociating` | `disassociated` | `failing` | `failed`. El bloque de CIDR está listo para usar cuando se encuentra en el estado `associated`.

Puede desvincular un bloque de CIDR que haya asociado con la VPC; sin embargo, no puede desvincular el bloque de CIDR con el que haya creado originalmente la VPC (el bloque de CIDR principal). Para visualizar el CIDR principal de la VPC en la consola de Amazon VPC, elija Your VPCs (Sus VPC), seleccione la casilla de verificación para su VPC y elija la pestaña CIDRs. Para ver el CIDR principal mediante la AWS CLI, utilice el comando [describe-vpcs](#) de la siguiente manera. El CIDR principal se devuelve en el de nivel superior `CidrBlock` element.

```
aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d --query Vpcs[*].CidrBlock
```

A continuación, se muestra un ejemplo del resultado.

```
[  
  "10.0.0.0/16",  
]
```

Restricciones de asociación de bloques de CIDR IPv4

En la siguiente tabla se proporciona información general de las asociaciones de bloques de CIDR permitidas y restringidas, que dependen del rango de direcciones IPv4 en el que se encuentre el bloque de CIDR principal de la VPC.

Rango de direcciones IP del bloque de CIDR principal	Asociaciones restringidas	Asociaciones permitidas
10.0.0.0/8	<p>Bloques de CIDR de otros rangos RFC 1918* (172.16.0.0/12 y 192.168.0.0/16).</p> <p>Si su bloque de CIDR principal es del rango 10.0.0.0/15 (de 10.0.0.0 a 10.1.255.255), no puede agregar un</p>	<p>Cualquier otro bloque de CIDR del rango 10.0.0.0/8 que no esté restringido.</p> <p>Cualquier bloque de IPv4 direccionable públicamente (no RFC 1918), o un bloque de CIDR del rango 100.64.0.0/10.</p>

Rango de direcciones IP del bloque de CIDR principal	Asociaciones restringidas	Asociaciones permitidas
	<p>bloque de CIDR del rango 10.0.0.0/16 (de 10.0.0.0 a 10.0.255.255).</p> <p>Bloques de CIDR del rango 198.19.0.0/16.</p>	
172.16.0.0/12	<p>Bloques de CIDR de otros rangos RFC 1918* (10.0.0.0/8 y 192.168.0.0/16).</p> <p>Bloques de CIDR del rango 172.31.0.0/16.</p> <p>Bloques de CIDR del rango 198.19.0.0/16.</p>	<p>Cualquier otro bloque de CIDR del rango 172.16.0.0/12 que no esté restringido.</p> <p>Cualquier bloque de IPv4 direccionable públicamente (no RFC 1918), o un bloque de CIDR del rango 100.64.0.0/10.</p>
192.168.0.0/16	<p>Bloques de CIDR de otros rangos RFC 1918* (10.0.0.0/8 y 172.16.0.0/12).</p> <p>Bloques de CIDR del rango 198.19.0.0/16.</p>	<p>Cualquier otro bloque de CIDR del rango 192.168.0.0/16.</p> <p>Cualquier bloque de IPv4 direccionable públicamente (no RFC 1918), o un bloque de CIDR del rango 100.64.0.0/10.</p>
198.19.0.0/16	Bloques de CIDR de los rangos RFC 1918*.	Cualquier bloque de IPv4 direccionable públicamente (no RFC 1918), o un bloque de CIDR del rango 100.64.0.0/10.
Bloque de CIDR direccionable públicamente (no RFC 1918), o un bloque de CIDR del rango 100.64.0.0/10	<p>Bloques de CIDR de los rangos RFC 1918*.</p> <p>Bloques de CIDR del rango 198.19.0.0/16.</p>	Cualquier otro bloque de CIDR IPv4 direccionable públicamente (no RFC 1918), o un bloque de CIDR del rango 100.64.0.0/10.

*Los rangos de RFC 1918 son los rangos de direcciones IPv4 privadas que se especifican en [RFC 1918](#).

Ajuste de tamaño de VPC para IPv6

Es posible asociar un único bloque de CIDR IPv6 a una VPC existente de su cuenta o al crear una nueva VPC. El bloque de CIDR es una longitud de prefijo determinada de /56. Puede solicitar un bloque de CIDR IPv6 del grupo de direcciones IPv6 de Amazon.

Si ha asociado un bloque de CIDR IPv6 a su VPC, podrá asociar un bloque de CIDR IPv6 a una subred existente en su VPC, o bien podrá crear una nueva subred. Para obtener más información, consulte [the section called "Ajuste de tamaño de subredes para direcciones IPv6" \(p. 63\)](#).

Por ejemplo, puede crear una VPC y especificar que desea asociar un bloque de CIDR IPv6 proporcionado por Amazon a la VPC. Amazon asigna el siguiente bloque de CIDR IPv6 a su VPC: 2001:db8:1234:1a00::/56. No puede elegir el intervalo de direcciones IP usted mismo. Puede crear una subred y asociar un bloque de CIDR IPv6 desde este rango. Por ejemplo, 2001:db8:1234:1a00::/64.

Puede desasociar un bloque de CIDR IPv6 de una VPC. Tras anular la asociación de un bloque de CIDR IPv6 de una VPC, no podrá esperar recibir el mismo CIDR si vuelve a asociar un bloque de CIDR IPv6 a su VPC más adelante.

Trabajar con VPC

Utilice los siguientes procedimientos para crear y configurar nubes virtuales privadas (VPC). Antes de que pueda lanzar recursos en la VPC, debe crear subredes.

De manera alternativa, puede crear una VPC y sus subredes, puertas de enlace y tablas de enrutamiento en un solo paso. Para obtener más información, consulte [the section called “Crear VPC con el asistente” \(p. 291\)](#).

Tareas

- [Creación de una VPC \(p. 21\)](#)
- [Vea las VPC \(p. 25\)](#)
- [Asociar un bloque de CIDR de una dirección IP secundaria con la VPC \(p. 25\)](#)
- [Asociar un bloque de CIDR IPv6 a su VPC \(p. 26\)](#)
- [Desasociar un bloque de CIDR IPv4 de su VPC \(p. 26\)](#)
- [Desasociar un bloque de CIDR IPv6 de la VPC \(p. 27\)](#)
- [Eliminar su VPC \(p. 27\)](#)

Creación de una VPC

Siga los pasos de esta sección para crear una VPC. Al crear una VPC, tiene dos opciones:

- Solo VPC: crea solo una VPC sin ningún recurso adicional como subredes o puertas de enlace NAT dentro de la VPC.
- VPC, subredes, etc.: crea una VPC, subredes, puerta de enlace NAT y puntos de conexión de la VPC.

Siga los pasos de cualquiera de las dos secciones siguientes en función de la opción que se adapte a sus necesidades.

Crear una solo VPC

Siga los pasos de esta sección para crear solo una VPC sin recursos adicionales.

Para crear una solo VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs, Create VPC.
3. En Resources to create (Recursos a crear), elija VPC only (Solo VPC).
4. Especifique los siguientes detalles de VPC según sea necesario.
 - Name tag: indique, de manera opcional, un nombre para su VPC. Esta acción creará una etiqueta con una clave de Name y el valor que especifique.
 - Bloque de CIDR de IPv4: especifique un bloque de CIDR de IPv4 (o un rango de direcciones IP) para la VPC. Elija una de las siguientes opciones:
 - Entrada manual de CIDR de IPv4: introduzca manualmente un CIDR de IPv4. El bloque de CIDR debe ser de un tamaño de entre /16 y /28. Se recomienda especificar un bloque de CIDR de los

rangos de direcciones IP privadas (no direccionables públicamente) tal como se especifica en [RFC 1918](#). Por ejemplo, 10.0.0.0/16 o 192.168.0.0/16.

Note

Puede especificar un rango de direcciones IPv4 enrutables públicamente. Sin embargo, actualmente no admitimos el acceso directo a Internet desde bloques de CIDR enrutables públicamente en una VPC. Las instancias de Windows no se podrán iniciar correctamente si se lanzan en una VPC con rangos que oscilan desde 224.0.0.0 a 255.255.255.255 (rangos de direcciones IP de clase D y clase E).

- Bloque de CIDR de IPv4 con asignación de IPAM: si hay un grupo de direcciones IPv4 de IP Address Manager (IPAM) de Amazon VPC disponible en esta región, puede obtener un CIDR de un grupo de IPAM. Si selecciona un grupo de IPAM, el tamaño del CIDR está limitado por las reglas de asignación del grupo de IPAM (mínimo permitido, máximo permitido y predeterminado). Para obtener más información acerca de Amazon VPC, consulte [¿Qué es IPAM?](#) en la Guía del usuario de IPAM de Amazon VPC.
- Bloque de CIDR IPv6: de forma opcional, puede asociar un bloque de CIDR IPv6 con su VPC. Elija una de las siguientes opciones y, a continuación, elija Select CIDR (Seleccionar CIDR):
 - No IPv6 CIDR block (Sin bloque de CIDR IPv6): no se aprovisionará ningún CIDR IPv6 para esta VPC.
 - Bloque de CIDR de IPv6 con asignación de IPAM: si hay un grupo de direcciones IPv6 de IP Address Manager (IPAM) de Amazon VPC disponible en esta región, puede obtener un CIDR de un grupo de IPAM. Si selecciona un grupo de IPAM, el tamaño del CIDR está limitado por las reglas de asignación del grupo de IPAM (mínimo permitido, máximo permitido y predeterminado). Para obtener más información acerca de Amazon VPC, consulte [¿Qué es IPAM?](#) en la Guía del usuario de IPAM de Amazon VPC.
 - Amazon-provided IPv6 CIDR block (Bloque de CIDR IPv6 proporcionado por Amazon): solicita un bloque de CIDR IPv6 de un grupo de direcciones IPv6 de Amazon. En Network Border Group (Grupo de borde de red), seleccione el grupo desde el que AWS anuncia las direcciones IP. Amazon proporciona un tamaño de bloque de CIDR de IPv6 fijo de /56. No es posible configurar el tamaño del CIDR de IPv6 que proporciona Amazon.
 - IPv6 CIDR owned by me (CIDR IPv6 de mi propiedad: [BYOIP](#)) asigna un bloque de CIDR IPv6 de su grupo de direcciones IPv6. En Pool (Grupo), elija el grupo de direcciones IPv6 desde el que desea asignar el bloque de CIDR IPv6.
- Tenancy (Tenencia): elija la opción de tenencia para esta VPC.
 - Seleccione Default (Predeterminado) para garantizar que las instancias de EC2 lanzadas en esta VPC utilicen el atributo de tenencia de la instancia de EC2 especificado al lanzarla.
 - Seleccione Dedicated (Dedicado) para garantizar que las instancias de EC2 lanzadas en esta VPC se ejecuten en instancias de tenencia dedicada, independientemente del atributo de tenencia especificado al lanzarlas.

Para obtener más información acerca de la tenencia, consulte [Configuración de la tenencia de instancia con una configuración de lanzamiento](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

Note

Si su AWS Outposts necesita una conectividad privada, debe seleccionar Default (Predeterminada). Para obtener más información sobre AWS Outposts, consulte [¿Qué es AWS Outposts?](#) en la Guía del usuario de AWS Outposts.

- Etiquetas: agrega etiquetas opcionales a la VPC. Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizar etiquetas para buscar y filtrar los recursos o hacer un seguimiento de los costos de AWS.

5. Seleccione Create VPC.

También puede utilizar una herramienta de la línea de comandos.

Para crear una VPC con una herramienta de la línea de comandos

- [create-vpc](#) (AWS CLI)
- [New-EC2Vpc](#) (AWS Tools for Windows PowerShell)

Para describir una VPC con una herramienta de la línea de comandos

- [describe-vpcs](#) (AWS CLI)
- [Get-EC2Vpc](#) (AWS Tools for Windows PowerShell)

Para obtener más información acerca de las direcciones IP, consulte [Direccionamiento IP](#) (p. 4).

Cuando haya creado la VPC, podrá crear las subredes. Para obtener más información, consulte [Crear una subred en la VPC](#) (p. 64).

Crear una VPC, subredes y otros recursos de la VPC

En este paso, se crea una VPC, subredes, zonas de disponibilidad, puertas de enlace NAT y puntos de conexión de la VPC.

Para crear una VPC, subredes y otros recursos de la VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs, Create VPC.
3. En Resources to create (Recursos a crear), elija VPC, subnets, etc. (VPC, subredes, etc.).
4. Modifique las opciones según sea necesario:
 - Name tag auto-generation: (Generación automática de etiquetas de nombre): elija la etiqueta de nombre que se aplicará a los recursos que cree. La etiqueta se puede generar automáticamente para el usuario o el usuario puede definir el valor. El valor definido se utilizará para generar la etiqueta Nombre en todos los recursos como "nombre-recurso". Por ejemplo, si ingresa "Preproducción", cada subred será etiquetada con una etiqueta de nombre "Preproducción-subred". Para obtener más información acerca de las etiquetas, consulte [Etiquetas](#).
 - IPv4 CIDR block (Bloque de CIDR IPv4): elija un CIDR IPv4 para la VPC. Esta opción es obligatoria.
 - IPv6 CIDR block (Bloque de CIDR IPv6): elija un CIDR IPv6 para la VPC.
 - Tenancy (Tenencia): elija la opción de tenencia para esta VPC.
 - Seleccione Default (Predeterminado) para garantizar que las instancias de EC2 lanzadas en esta VPC utilicen el atributo de tenencia de la instancia de EC2 especificado al lanzarla.
 - Seleccione Dedicated (Dedicado) para garantizar que las instancias de EC2 lanzadas en esta VPC se ejecuten en instancias de tenencia dedicada, independientemente del atributo de tenencia especificado al lanzarlas.

Para obtener más información acerca de la tenencia, consulte [Configuración de la tenencia de instancia con una configuración de lanzamiento](#) en la Guía del usuario de Amazon EC2 Auto Scaling.

Note

Si su AWS Outposts necesita una conectividad privada, debe seleccionar Default (Predeterminada). Para obtener más información sobre AWS Outposts, consulte [¿Qué es AWS Outposts?](#) en la Guía del usuario de AWS Outposts.

- Availability Zones (AZs) (Zonas de disponibilidad [AZ]): elija el número de zonas de disponibilidad (AZ) en las que desea crear subredes. Una zona de disponibilidad es uno o más centros de datos

discretos con alimentación, redes y conectividad redundantes en una región de AWS. Las zonas de disponibilidad le dan la capacidad de operar aplicaciones de producción y bases de datos de mayor disponibilidad, tolerancia a errores y escalabilidad de lo que sería posible desde un único centro de datos. Si particiona las aplicaciones que se ejecutan en subredes a través de zonas de disponibilidad, estará mejor aislado y protegido de incidencias relacionadas con cortes de energía, rayos, tornados, terremotos, etc.

- **Customize AZs (Personalizar las zonas de disponibilidad):** elija en qué zonas de disponibilidad se crearán las subredes.
- **Number of public subnets (Número de subredes públicas):** elija el número de subredes que desea que se consideren subredes “públicas”. Una subred “pública” es una subred que como entrada de la tabla de enrutamiento apunta a una puerta de enlace de Internet. Esto permite que las instancias de EC2 que se ejecutan en la subred sean de acceso público a través de Internet.
- **Customize public subnets CIDR blocks (Personalizar los bloques de CIDR de las subredes públicas):** elija los bloques de CIDR para las subredes “públicas”.
- **Number of private subnets (Número de subredes privadas):** elija el número de subredes que desea que se consideren subredes “privadas”. La subred “privada” es una subred que no dispone de una entrada a la tabla de enrutamiento que apunte a una puerta de enlace de Internet. Utilice subredes privadas para asegurar los recursos del backend que no necesitan un acceso público a través de Internet.
- **Customize private subnets CIDR blocks (Personalizar los bloques de CIDR de las subredes privadas):** elija los bloques de CIDR para las subredes “privadas”.
- **NAT gateways (Puertas de enlace NAT):** elija el número de zonas de disponibilidad en las que crear puertas de enlace de traducción de direcciones de red (NAT). Una puerta de enlace NAT es un servicio administrado por AWS que permite a las instancias de EC2 en subredes privadas enviar tráfico saliente a Internet. En cambio, los recursos de Internet no pueden establecer una conexión con las instancias. Tenga en cuenta que existe un costo asociado a las puertas de enlace NAT. Para obtener más información, consulte [. Gateways NAT \(p. 157\)](#).
- **VPC endpoints (Puntos de conexión de VPC):** un punto de conexión de VPC le permite conectar de forma privada la VPC a servicios de AWS compatibles como Amazon S3. Los puntos de conexión de la VPC le permiten crear una VPC aislada y cerrada de la Internet pública. El uso de puntos de enlace de gateway no supone ningún cargo adicional. Esto puede ayudar a evitar los costos asociados con las puertas de enlace NAT.
- **DNS options (Opciones de DNS):** elija las opciones de resolución de nombres de dominio para las instancias de EC2 lanzadas en esta VPC.
 - **Enable DNS hostnames (Habilitar nombres de host DNS):** permite aprovisionar nombres de host para las direcciones IPv4 públicas de las instancias de EC2.
 - **Enable DNS resolution (Habilitar resolución DNS):** permite aprovisionar nombres de host para las direcciones IPv4 públicas de las instancias de EC2 y habilita la resolución de nombres de dominio de los nombres de host.

Note

Si desea aprovisionar nombres de host DNS IPv4 públicos para las instancias de EC2 lanzadas en las subredes que está creando, debe habilitar tanto **Enable DNS hostnames (Habilitar nombres de host DNS)** como **Enable DNS resolution (Habilitar resolución DNS)** en la VPC. Si habilita únicamente la opción **Enable DNS hostnames (Habilitar nombres de host DNS)**, el nombre de host DNS IPv4 público no se aprovisiona.

5. En el panel **Preview (Vista preliminar)**, puede ver la VPC planificada, la subred, las tablas de enrutamiento y las interfaces de red que se crearán.
6. Seleccione **Create VPC**.

Vea las VPC

Utilice los siguientes pasos para ver los detalles de las VPC.

Para ver los detalles de la VPC mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija VPC.
3. Seleccione la VPC y, a continuación, elija View Details (Ver detalles).

Para describir una VPC con una herramienta de la línea de comandos

- [describe-vpcs](#) (AWS CLI)
- [Get-EC2Vpc](#) (AWS Tools for Windows PowerShell)

Para ver todas las VPC en las regiones

Abra la consola de Amazon EC2 Global View en <https://console.aws.amazon.com/ec2globalview/home>.

Para obtener más información acerca del uso de Amazon EC2 Global View, consulte [Enumerar y filtrar recursos mediante Amazon EC2 Global View](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Asociar un bloque de CIDR de una dirección IP secundaria con la VPC

Puede agregar bloques de CIDR a la VPC. No se olvide consultar las [restricciones \(p. 17\)](#) aplicables.

Después de haber asociado un bloque de CIDR, el estado cambia a `associating`. El bloque de CIDR está listo para usar cuando se encuentra en el estado `associated`.

En la Amazon Virtual Private Cloud Console, se proporciona el estado de la solicitud en la parte superior de la página.

Para agregar un bloque de CIDR a su VPC con la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs (Sus VPC).
3. Seleccione la VPC y elija Actions (Acciones), Edit CIDRs (Editar CIDR).
4. Elija la opción Add new IPv4 CIDR (Agregar nuevo CIDR IPv4) o Add new IPv6 CIDR (Agregar nuevo CIDR IPv6).
5. Para obtener información completa sobre cuáles son las opciones de CIDR, consulte [Creación de una VPC \(p. 21\)](#).
6. Seleccione la opción Close.

Para agregar un bloque de CIDR con una herramienta de la línea de comandos

- [associate-vpc-cidr-block](#) (AWS CLI)
- [Register-EC2VpcCidrBlock](#) (AWS Tools for Windows PowerShell)

Puede crear subredes después de haber agregado los bloques de CIDR que necesite. Para obtener más información, consulte [Crear una subred en la VPC \(p. 64\)](#).

Asociar un bloque de CIDR IPv6 a su VPC

Es posible asociar un bloque de CIDR IPv6 a cualquier VPC existente. La VPC no puede tener ningún bloque de CIDR IPv6 asociado.

Para asociar un bloque de CIDR IPv6 a una VPC con la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs (Sus VPC).
3. Seleccione la VPC y elija Actions (Acciones), Edit CIDRs (Editar CIDR).
4. Elija Add IPv6 CIDR (Agregar CIDR de IPv6).
5. Para IPv6 CIDR block (Bloque de CIDR de IPv6), realice una de las siguientes operaciones:
 - Elija Amazon-provided IPv6 CIDR block (Bloque de CIDR de IPv6 proporcionado por Amazon) para solicitar un bloque de CIDR de IPv6 del grupo de Amazon de direcciones IPv6. En Network border group (Grupo de bordes de red), seleccione el grupo desde el cuál AWS anuncia las direcciones IP.
 - Elija IPv6 CIDR owned by me (CIDR de IPv6 de mi propiedad) para asignar un bloque de CIDR de IPv6 del grupo de direcciones IPv6. En Pool (Grupo), elija el grupo de direcciones IPv6 desde el que desea asignar el bloque de CIDR IPv6.
6. Seleccione Select CIDR (Seleccionar CIDR).
7. Seleccione la opción Close.

Para asociar un bloque de CIDR IPv6 a una VPC con una herramienta de la línea de comandos

- [associate-vpc-cidr-block](#) (AWS CLI)
- [Register-EC2VpcCidrBlock](#) (AWS Tools for Windows PowerShell)

Desasociar un bloque de CIDR IPv4 de su VPC

Si su VPC tiene varios bloques de CIDR IPv4 asociados a ella, puede desvincular un bloque de CIDR IPv4 de la VPC. No se puede desvincular el bloque de CIDR IPv4 principal. Solo se puede desvincular un bloque de CIDR completo, es decir, no se puede desvincular un subconjunto de un bloque de CIDR o un rango fusionado de bloques de CIDR. Primero debe eliminar todas las subredes del bloque de CIDR.

Para eliminar un bloque de CIDR de una VPC con la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs.
3. Seleccione la VPC y elija Actions, Edit CIDRs.
4. En VPC IPv4 CIDRs, elija el botón de eliminación (una cruz) correspondiente al bloque de CIDR que se eliminará.
5. Seleccione la opción Close.

También puede utilizar una herramienta de la línea de comandos.

Para eliminar un bloque de CIDR IPv4 de una VPC con una herramienta de la línea de comandos

- [disassociate-vpc-cidr-block](#) (AWS CLI)
- [Unregister-EC2VpcCidrBlock](#) (AWS Tools for Windows PowerShell)

Desasociar un bloque de CIDR IPv6 de la VPC

Si ya no desea que la VPC admita IPv6 pero desea seguir utilizando la VPC para crear y comunicarse con recursos IPv4, puede desasociar el bloque de CIDR IPv6.

Para anular la asociación de un bloque de CIDR IPv6, primero deberá anular la asignación de las direcciones IPv6 asignadas a las instancias de su subred.

Para desvincular un bloque de CIDR IPv6 de una VPC con la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs.
3. Seleccione su VPC, elija Actions, Edit CIDRs.
4. Elimine el bloque de CIDR IPv6 seleccionando el icono con forma de equis.
5. Seleccione la opción Close.

Note

La anulación de la asociación de un bloque de CIDR IPv6 no elimina automáticamente las reglas del grupo de seguridad, las reglas de ACL de red ni las rutas de las tablas de ruteo configuradas para las redes IPv6. Por lo tanto, deberá modificar o eliminar manualmente dichas reglas o rutas.

También puede utilizar una herramienta de la línea de comandos.

Para desvincular un bloque de CIDR IPv6 de una VPC con una herramienta de la línea de comandos

- [disassociate-vpc-cidr-block](#) (AWS CLI)
- [Unregister-EC2VpcCidrBlock](#) (AWS Tools for Windows PowerShell)

Eliminar su VPC

Para eliminar una VPC mediante la consola de VPC, primero debe terminar o eliminar los siguientes componentes:

- Todas las instancias de la VPC: para obtener información acerca de cómo terminar una instancia, consulte [Terminar la instancia](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
- Interconexiones de VPC
- Puntos de enlace de interfaz
- Gateways NAT

Cuando elimina una VPC mediante la consola de VPC, también eliminamos automáticamente los siguientes componentes de VPC:

- Subredes
- Grupos de seguridad
- ACL de red
- Tablas de ruteo
- Puntos de enlace de gateway
- Puertos de enlace a internet
- Gateways de Internet de solo salida
- Opciones de DHCP

Si tiene una conexión de AWS Site-to-Site VPN, no es necesario eliminarla ni eliminar los demás componentes relacionados con la VPN (como, por ejemplo, la gateway de cliente y la gateway privada virtual). Si tiene pensado utilizar la gateway de cliente con otra VPC, se recomienda conservar la conexión de Site-to-Site VPN y las gateway. De lo contrario, debe volver a configurar el dispositivo de gateway de cliente después de crear una nueva conexión de Site-to-Site VPN.

Para eliminar su VPC con la consola

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Termine todas las instancias de la VPC. Para obtener más información, consulte [Terminar la instancia](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
3. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
4. En el panel de navegación, elija Your VPCs.
5. Seleccione la VPC que desea eliminar y elija Actions, Delete VPC.
6. Si tiene una conexión de Site-to-Site VPN, seleccione la opción para eliminarla, de lo contrario, déjela sin seleccionar. Elija Delete VPC (Eliminar VPC).

También puede utilizar una herramienta de la línea de comandos. Cuando elimina una VPC mediante la línea de comandos, primero debe terminar todas las instancias y eliminar o desconectar todos los recursos asociados, incluidas las subredes, los grupos de seguridad personalizados, las ACL de red personalizadas, las tablas de enrutamiento personalizadas, las interconexiones con VPC, los puntos de enlace, la gateway de NAT, la gateway de Internet y la gateway de Internet de solo salida.

Para eliminar una VPC con la línea de comandos

- [delete-vpc](#) (AWS CLI)
- [Remove-EC2Vpc](#) (AWS Tools for Windows PowerShell)

VPC predeterminadas

Si ha creado su cuenta de AWS después del 04/12/2013, dispone de una VPC predeterminada en cada región de AWS. Una VPC predeterminada incluye una subred pública en cada zona de disponibilidad, una puerta de enlace de Internet y la configuración para habilitar la resolución DNS. Por lo tanto, puede comenzar a lanzar inmediatamente instancias de Amazon EC2 en la VPC predeterminada. También puede utilizar servicios como Elastic Load Balancing, Amazon RDS y Amazon EMR en la VPC predeterminada.

Una VPC predeterminada resulta adecuada para comenzar rápidamente y para lanzar instancias públicas, como un blog o un sitio web simple. Puede modificar los componentes de la VPC predeterminada según sea necesario. Si lo prefiere, puede crear VPC que se adapten a sus necesidades específicas. Por ejemplo, mediante el rango de bloques de CIDR y los tamaños de subred preferidos.

También puede agregar subredes no predeterminadas a la VPC predeterminada. El proceso es el mismo que para agregar una subred a una VPC no predeterminada. Para obtener más información, consulte [the section called "Crear una subred en la VPC" \(p. 64\)](#).

Contenido

- [Componentes de VPC predeterminados \(p. 29\)](#)
- [Subredes predeterminadas \(p. 31\)](#)
- [Consultar la VPC y las subredes predeterminadas \(p. 31\)](#)
- [Crear una VPC predeterminada \(p. 32\)](#)
- [Crear una subred predeterminada \(p. 33\)](#)
- [Eliminar las subredes predeterminadas y la VPC predeterminada \(p. 34\)](#)

Componentes de VPC predeterminados

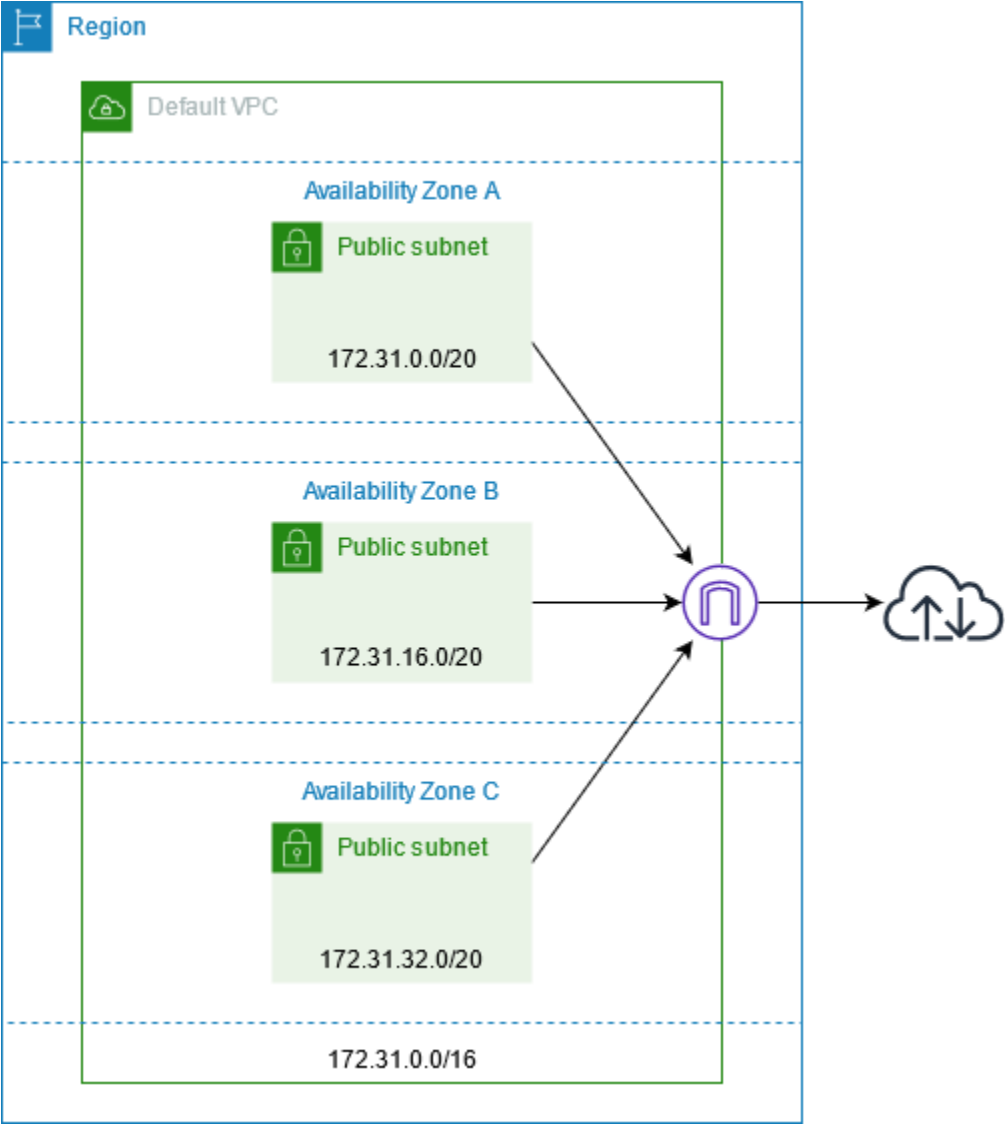
Al crear una VPC predeterminada, hacemos lo siguiente para configurarla para usted:

- Crear una VPC con un bloque de CIDR de IPv4 de tamaño /16 (172.31.0.0/16). Esto proporciona hasta 65 536 direcciones IPv4 privadas.
- Crear una subred predeterminada de tamaño /20 en cada zona de disponibilidad. Proporciona hasta 4096 direcciones por subred, de las cuales unas cuantas están reservadas para nuestro uso.
- Crear un [puerto de enlace a Internet \(p. 142\)](#) y conectarlo con su VPC predeterminada.
- Agregar una ruta en la tabla de enrutamiento que apunte todo el tráfico (0.0.0.0/0) a la gateway de Internet.
- Crear un grupo de seguridad predeterminado y asociarlo a su VPC predeterminada.
- Crear una lista de control de acceso (ACL) de red predeterminada y asociarla a su VPC predeterminada.
- Asociar las opciones de DHCP predeterminadas configuradas para su cuenta de AWS con su VPC predeterminada.

Note

Amazon crea los recursos anteriores en su nombre. Las políticas de IAM no se aplican a estas acciones porque usted no lleva a cabo estas acciones. Por ejemplo, si tiene una política de IAM que deniega la capacidad de llamar a `CreateInternetGateway` y, a continuación, llama a `CreateDefaultVpc`, se sigue creando la gateway de Internet en la VPC predeterminada.

El siguiente gráfico muestra los componentes clave que configuramos para una VPC predeterminada.



En la tabla siguiente se muestran las rutas de la tabla de enrutamiento principal de la VPC predeterminada.

Destino	Objetivo
172.31.0.0/16	local
0.0.0.0/0	<i>internet_gateway_id</i>

Puede usar una VPC predeterminada como lo haría con otras VPC:

- Agregue subredes no predeterminadas adicionales.
- Modifique la tabla de ruteo principal.
- Agregue tablas de ruteo adicionales.
- Asocie grupos de seguridad adicionales.
- Actualice las reglas del grupo de seguridad predeterminado.

- Agregue conexiones de AWS Site-to-Site VPN.
- Agregue más bloques de CIDR IPv4.
- Acceda a las VPC en una región remota mediante una gateway de Direct Connect. Para obtener información acerca de las opciones de puerta de enlace de Direct Connect, consulte [Puertas de enlace de Direct Connect](#) en la Guía del usuario de AWS Direct Connect.

Puede utilizar una subred predeterminada al igual que usaría cualquier otra subred; agregue tablas de ruteo personalizadas y establezca ACL de red. También puede especificar una subred predeterminada específica al lanzar una instancia EC2.

De forma opcional, puede asociar un bloque de CIDR IPv6 con su VPC predeterminada. Para obtener más información, [Trabajar con VPC \(p. 21\)](#).

Subredes predeterminadas

De forma predeterminada, las subredes predeterminadas son subredes públicas, ya que la tabla de ruteo principal envía al puerto de enlace a Internet el tráfico de la subred que está destinado a Internet. Puede convertir una subred predeterminada en una subred privada eliminando la ruta del destino 0.0.0.0/0 al puerto de enlace a Internet. Sin embargo, si hace esto, ninguna instancia EC2 que se esté ejecutando en esa subred podrá obtener acceso a Internet.

Las instancias que lance en una subred predeterminada reciben direcciones IPv4 públicas y una dirección IPv4 privada, y nombres de host DNS públicos y privados. Las instancias que lance en una subred que no sea predeterminada en una VPC predeterminada no reciben una dirección IPv4 pública ni un nombre de host DNS. Puede cambiar el comportamiento predeterminado de asignación de direcciones IP públicas de su subred. Para obtener más información, consulte [Modificar el atributo de direcciones IPv4 públicas de su subred \(p. 66\)](#).

De vez en cuando, puede que AWS añada una nueva zona de disponibilidad a una región. En la mayoría de los casos, crearemos automáticamente una nueva subred predeterminada en esta zona de disponibilidad para su VPC predeterminada en unos pocos días. Sin embargo, si ha hecho alguna modificación en su VPC predeterminada, no agregaremos una subred predeterminada nueva. Si una zona de disponibilidad no tienen una subred predeterminada, puede crearla. Para obtener más información, consulte [Crear una subred predeterminada \(p. 33\)](#).

Consultar la VPC y las subredes predeterminadas

Puede consultar la VPC y las subredes predeterminadas con la consola de Amazon VPC o la línea de comandos.

Para ver la VPC y las subredes predeterminadas con la consola de

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs.
3. En la columna Default VPC, busque el valor Yes. Anote el ID de la VPC predeterminada.
4. En el panel de navegación, elija Subnets.
5. En la barra de búsqueda, escriba el ID de la VPC predeterminada. Las subredes devueltas son las que se encuentran en su VPC predeterminada.
6. Para comprobar qué subredes son las predeterminadas, busque el valor Yes en la columna Default Subnet.

Para describir la VPC predeterminada con la línea de comandos

- Utilice [describe-vpcs](#) (AWS CLI)

- Utilice [Get-EC2Vpc](#) (AWS Tools for Windows PowerShell)

Use los comandos con el filtro `isDefault` y establezca el valor de filtro en `true`.

Para describir las subredes predeterminadas con la línea de comandos

- Utilice [describe-subnets](#) (AWS CLI)
- Utilice [Get-EC2Subnet](#) (AWS Tools for Windows PowerShell)

Use los comandos con el filtro `vpc-id` y establezca el valor de filtro en el ID de la VPC predeterminada. En el resultado, el campo `DefaultForAz` se establece en `true` para las subredes predeterminadas.

Crear una VPC predeterminada

Si elimina la VPC predeterminada, puede crear otra. No puede restaurar una VPC predeterminada anterior que haya eliminado y no puede marcar una VPC no predeterminada existente como predeterminada. Si su cuenta admite EC2-Classic, no puede usar estos procedimientos para crear una VPC predeterminada en una región que admite EC2-Classic.

Al crear una VPC predeterminada, se crea con los [componentes \(p. 29\)](#) estándar de una VPC predeterminada, incluida una subred predeterminada en cada zona de disponibilidad. No puede especificar sus propios componentes. Es posible que los bloques de CIDR de subred de la nueva VPC predeterminada no se mapeen a las mismas zonas de disponibilidad que la VPC predeterminada anterior. Por ejemplo, si la subred con el bloque de CIDR `172.31.0.0/20` se creó en `us-east-2a` en la VPC predeterminada anterior, se puede crear en `us-east-2b` en la nueva VPC predeterminada.

Si ya tiene una VPC predeterminada en la región, no puede crear otra.

Para crear una VPC predeterminada con la consola de

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija **Your VPCs**.
3. Elija **Actions, Create Default VPC**.
4. Seleccione **Create (Crear)**. Cierre la pantalla de confirmación.

Para crear una VPC predeterminada con la línea de comandos

Puede utilizar el comando [create-default-vpc](#) de la AWS CLI. Este comando no tiene parámetros de entrada.

```
aws ec2 create-default-vpc
```

A continuación, se muestra un ejemplo del resultado.

```
{
  "Vpc": {
    "VpcId": "vpc-3f139646",
    "InstanceTenancy": "default",
    "Tags": [],
    "Ipv6CidrBlockAssociationSet": [],
    "State": "pending",
    "DhcpOptionsId": "dopt-61079b07",
    "CidrBlock": "172.31.0.0/16",
```

```
    "IsDefault": true  
  }  
}
```

Como alternativa, puede utilizar el comando [New-EC2DefaultVpc](#) herramientas para Windows PowerShell o la acción [CreateDefaultVpc](#) de la API de Amazon EC2.

Crear una subred predeterminada

Si una zona de disponibilidad no tienen una subred predeterminada, puede crearla. Por ejemplo, puede ser conveniente crear una subred predeterminada después de haber eliminado una anterior, o cuando AWS ha agregado una nueva zona de disponibilidad y no ha creado automáticamente una subred predeterminada para esa zona en su VPC predeterminada.

Cuando se crea una subred predeterminada, su tamaño es de un bloque de CIDR IPv4 de tamaño /20 en el espacio contiguo disponible más cercano de la VPC predeterminada. Se aplican las siguientes reglas:

- No puede especificar otro bloque de CIDR.
- No es posible restaurar una subred predeterminada previamente eliminada.
- Solo puede tener una subred predeterminada por zona de disponibilidad.
- No es posible crear una subred predeterminada en una VPC que no sea predeterminada.

Si el espacio de direcciones de la VPC predeterminada no basta para crear un bloque de CIDR de tamaño /20, la solicitud fracasa. Si necesita agregar más espacio de direcciones, puede [agregar un bloque de CIDR IPv4 a su VPC](#) (p. 17).

Si ha asociado un bloque de CIDR IPv6 a su VPC predeterminada, la nueva subred predeterminada no recibirá automáticamente un bloque e CIDR IPv6. Sin embargo, puede asociarle un bloque de CIDR IPv6 después de haberla creado. Para obtener más información, consulte [Asociar un bloque de CIDR IPv6 a su subred](#) (p. 66).

No es posible crear una subred predeterminada con la AWS Management Console.

Para crear una subred predeterminada mediante la AWS CLI

Use el comando [create-default-subnet](#) de la AWS CLI y especifique la zona de disponibilidad en la que se debe crear la subred.

```
aws ec2 create-default-subnet --availability-zone us-east-2a
```

A continuación, se muestra un ejemplo del resultado.

```
{  
  "Subnet": {  
    "AvailabilityZone": "us-east-2a",  
    "Tags": [],  
    "AvailableIpAddressCount": 4091,  
    "DefaultForAz": true,  
    "Ipv6CidrBlockAssociationSet": [],  
    "VpcId": "vpc-1a2b3c4d",  
    "State": "available",  
    "MapPublicIpOnLaunch": true,  
    "SubnetId": "subnet-1122aabb",  
    "CidrBlock": "172.31.32.0/20",  
    "AssignIpv6AddressOnCreation": false  
  }  
}
```

```
}
```

Para obtener más información acerca de cómo configurar la AWS CLI, consulte la [Guía del usuario de AWS Command Line Interface](#).

También puede utilizar el comando `New-EC2DefaultSubnet` de herramientas para Windows PowerShell o la acción `CreateDefaultSubnet` de la API de Amazon EC2.

Eliminar las subredes predeterminadas y la VPC predeterminada

Puede eliminar una subred predeterminada o una VPC predeterminada de la misma forma que puede eliminar cualquier otra subred o VPC. Para obtener más información, consulte [Trabajar con VPC \(p. 21\)](#). Sin embargo, si elimina sus subredes predeterminadas o su VPC predeterminada, debe especificar explícitamente una subred en otra VPC en la que lance la instancia, ya que no se pueden lanzar instancias en EC2-Classic. Si no tiene otra VPC, debe crear una VPC y una subred que no sean predeterminadas. Para obtener más información, consulte [Creación de una VPC \(p. 21\)](#).

Si elimina la VPC predeterminada, puede crear otra. Para obtener más información, consulte [Crear una VPC predeterminada \(p. 32\)](#).

Si elimina una subred predeterminada, puede crear otra. Para obtener más información, consulte [Crear una subred predeterminada \(p. 33\)](#). Para asegurarse de que su nueva subred predeterminada se comporta según lo esperado, modifique el atributo de la subred para que asigne las direcciones IP públicas a instancias lanzadas en esa subred. Para obtener más información, consulte [Modificar el atributo de direcciones IPv4 públicas de su subred \(p. 66\)](#). Solo puede tener una subred predeterminada por zona de disponibilidad. No es posible crear una subred predeterminada en una VPC que no sea predeterminada.

Conjuntos de opciones de DHCP en Amazon VPC

En esta sección se explica cómo los dispositivos de red de la VPC utilizan el Protocolo de configuración dinámica de host (DHCP), los parámetros de comunicación de red almacenados en los conjuntos de opciones de DHCP y cómo personalizar los conjuntos de opciones utilizados por los dispositivos de su VPC.

Contenido

- [¿Qué es DHCP? \(p. 34\)](#)
- [¿Qué son los conjuntos de opciones? \(p. 35\)](#)
- [Trabajar con los conjuntos de opciones de DHCP \(p. 37\)](#)

¿Qué es DHCP?

Cada dispositivo de una red TCP/IP requiere una dirección IP para comunicarse con los demás dispositivos de la red. En el pasado, se asignaban manualmente las direcciones IP a cada dispositivo de la red. En la actualidad, los servidores de Protocolo de configuración dinámica de host (DHCP) asignan las direcciones IP de forma dinámica. Para obtener más información sobre la interacción entre un cliente DHCP y un servidor, consulte [Protocolo de configuración dinámica de host: operación](#).

El servidor DHCP es responsable de arrendar direcciones IP a clientes DHCP y proporcionar información de red adicional que los clientes necesitan para comunicarse a través de la red, como el nombre del servidor DNS de la red, la dirección IP del enrutador y la máscara de subred.

En la nube de AWS, las instancias de EC2 que se ejecutan en subredes de VPC pueden recuperar el arrendamiento de direcciones IP y la información de red adicional según sea necesario desde un servidor DHCP de AWS IPv4 o IPv6.

Note

Si tiene una configuración de VPC que requiere que sus aplicaciones realicen solicitudes directas al servidor DHCP de Amazon, es posible que el servidor proporcione o no la información de configuración de red adicional que podría estar esperando. Presenta las siguientes limitaciones:

- Una instancia de EC2 de una subred de doble pila solo puede recuperar su dirección IPv6 del servidor DHCP IPv6. No puede recuperar ninguna configuración de red adicional del servidor DHCP IPv6, como los nombres de servidor DNS o los nombres de dominio.
- Una instancia de EC2 de una subred exclusiva para IPv6 puede recuperar su dirección IPv6 del servidor DHCP IPv6 e información adicional de configuración de red, como nombres de servidor DNS y nombres de dominio.

Siguientes pasos

- [¿Qué son los conjuntos de opciones? \(p. 35\)](#)
- [Trabajar con los conjuntos de opciones de DHCP \(p. 37\)](#)

¿Qué son los conjuntos de opciones?

Un conjunto de opciones de DHCP es un grupo de configuraciones de red que utilizan las instancias de EC2 de la VPC para comunicarse a través de la red virtual. Cada VPC dispone de un conjunto de opciones de DHCP predeterminado, pero puede crear un conjunto de opciones de DHCP personalizado si, por ejemplo, desea que las instancias de la VPC utilicen un servidor DNS de terceros para la resolución de nombres de dominio en lugar del servidor DNS de Amazon. También puede desasociar todos los conjuntos de opciones de la VPC si desea desactivar por completo la resolución de nombres de dominio.

Contenido

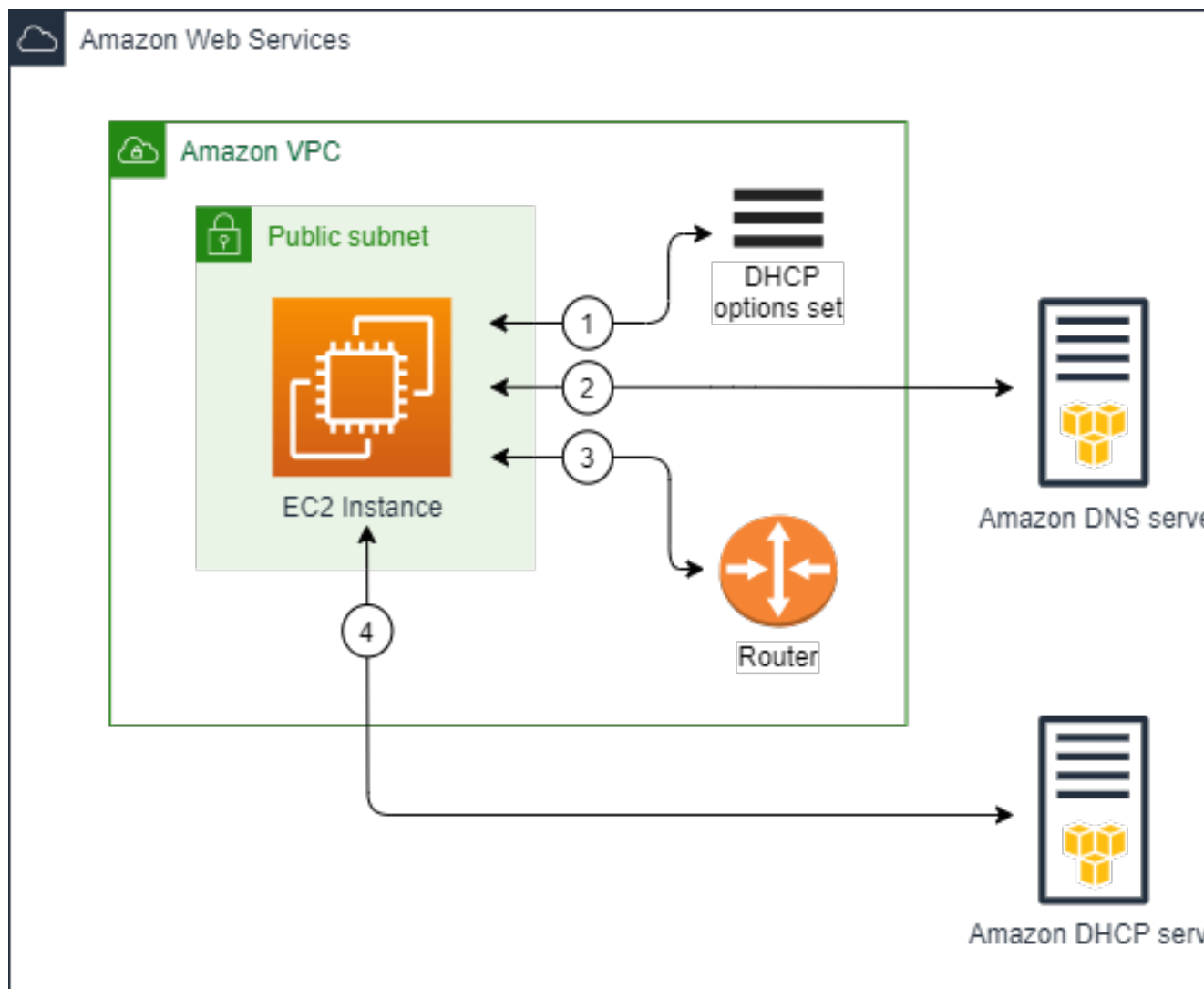
- [¿Qué hay en el conjunto de opciones predeterminado? \(p. 35\)](#)
- [¿Qué contiene un conjunto de opciones personalizado? \(p. 36\)](#)

¿Qué hay en el conjunto de opciones predeterminado?

Cada VPC dispone de un conjunto de opciones predeterminado que contiene las siguientes configuraciones de red:

- DNS server (Servidor DNS): los servidores de nombres DNS que las interfaces de red utilizarán para la resolución de nombres de dominio.
- Domain name (Nombre de dominio): el nombre de dominio que las instancias de EC2 de la VPC utilizarán en sus nombres de host privados.

Si utiliza el conjunto de opciones predeterminado, las instancias lanzadas en la VPC utilizan las configuraciones de red almacenadas en el conjunto de opciones predeterminado (1) para llegar al servidor DNS de Amazon (2) y conectarse a otros dispositivos de la red a través del enrutador de la VPC (3). Sin embargo, las instancias pueden interactuar con el servidor DHCP de Amazon en cualquier momento para obtener la concesión de su dirección IP y sus configuraciones de red adicionales (4).



Siguientes pasos

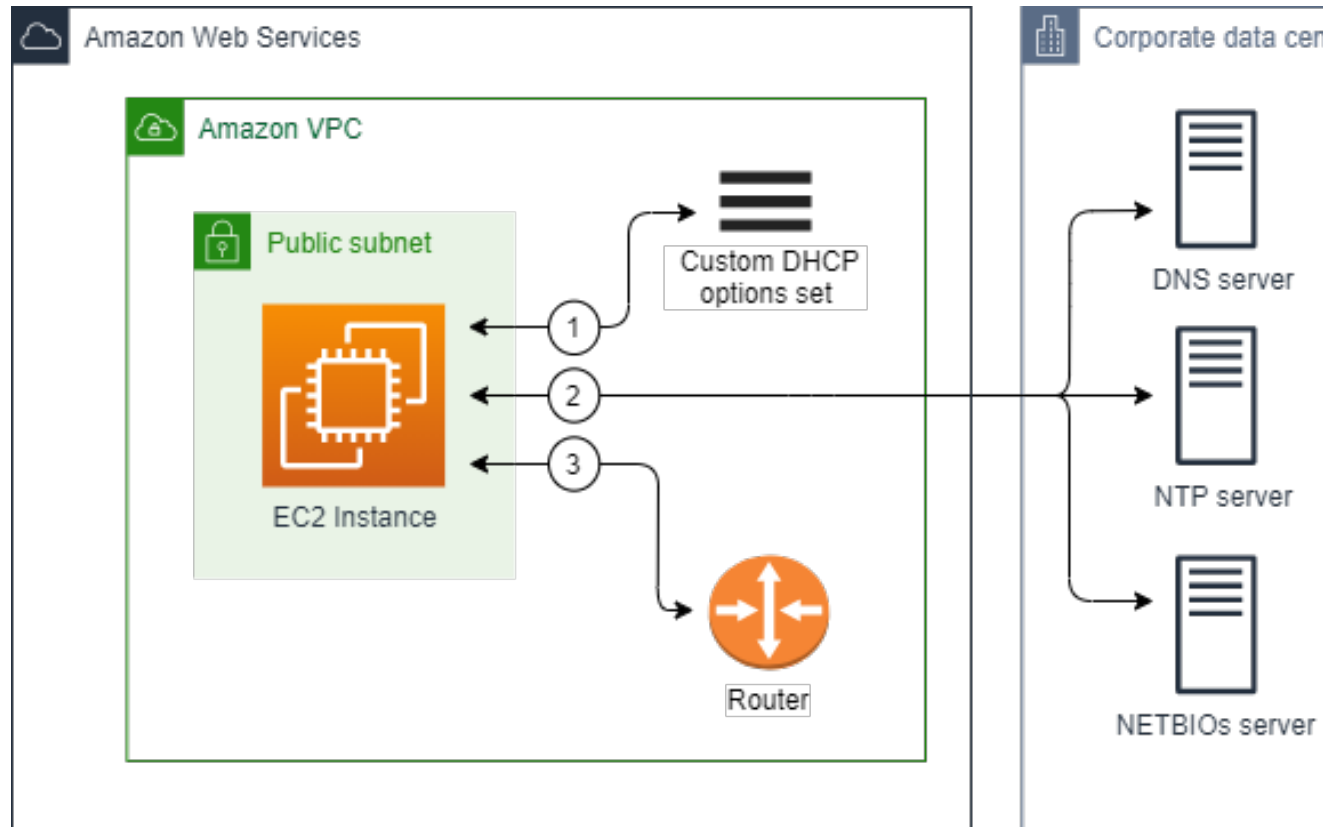
- [Ver el conjunto de opciones predeterminadas \(p. 38\)](#)
- [Modificar el conjunto de opciones asociado a una VPC \(p. 40\)](#)

¿Qué contiene un conjunto de opciones personalizado?

Puede crear su propio conjunto de opciones de DHCP en Amazon VPC. Esto le permite configurar las siguientes configuraciones de red adicionales:

- **NTP servers (Servidores NTP)**: los servidores NTP que proporcionan el tiempo a las instancias de la red.
- **NetBIOS name servers (Servidores de nombres NetBIOS)**: para las instancias Windows EC2, el nombre de computadora NetBIOS es un nombre descriptivo asignado a la instancia para identificarla en la red. Un servidor de nombres NetBIOS mantiene una lista de asignaciones entre los nombres de computadoras NetBIOS y las direcciones de red de las redes que utilizan NetBIOS como servicio de nombres.
- **NetBIOS node type (Tipo de nodo NetBIOS)**: para las instancias de EC2 de Windows, el método que utilizan las instancias para resolver nombres NetBIOS en direcciones IP.

Si utiliza un conjunto de opciones personalizado, las instancias lanzadas en la VPC utilizan las configuraciones de red en el conjunto de opciones de DHCP personalizado (1) para interactuar con los servidores DNS, NTP y NetBIOS que no son de Amazon (2) y conectarse a otros dispositivos de la red a través del enrutador de la VPC (3).



Siguientes pasos

- [Crear un conjunto de opciones de DHCP \(p. 38\)](#)
- [Modificar el conjunto de opciones asociado a una VPC \(p. 40\)](#)

Trabajar con los conjuntos de opciones de DHCP

Esta sección muestra cómo visualizar y trabajar con los conjuntos de opciones de DHCP.

Las instancias de EC2 lanzadas en subredes de VPC utilizan automáticamente las opciones de DHCP predeterminadas a menos que cree un nuevo conjunto de opciones de DHCP o desasocie el conjunto de opciones predeterminadas de la VPC. Un conjunto de opciones de DHCP personalizadas le permite personalizar la VPC con su propio servidor DNS, nombre de dominio y mucho más. La desvinculación del conjunto de opciones predeterminadas de la VPC le permite desactivar la resolución de nombres de dominio en la VPC.

Contenido

- [Ver el conjunto de opciones predeterminadas \(p. 38\)](#)
- [Crear un conjunto de opciones de DHCP \(p. 38\)](#)
- [Modificar el conjunto de opciones asociado a una VPC \(p. 40\)](#)
- [Eliminar un conjunto de opciones de DHCP \(p. 41\)](#)

Ver el conjunto de opciones predeterminadas

Para ver las opciones de DHCP predeterminadas

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija DHCP Options Sets.
3. Elija el conjunto de opciones disponibles.
4. Ver las configuraciones en el conjunto de opciones predeterminadas:
 - Domain name servers (Servidores de nombres de dominio): se trata de los servidores DNS que se utilizarán para resolver la dirección IP del host. En el conjunto de opciones predeterminadas, el único valor es AmazonProvidedDNS. Para obtener más información acerca de este servidor, consulte [Servidor DNS de Amazon](#) (p. 42).
 - Domain name (Nombre de dominio): se trata del nombre de dominio que se adjuntará a las direcciones IPv4 públicas de las instancias de EC2 lanzadas en la VPC.

En el conjunto de opciones predeterminadas, para las VPC de la región de AWS `us-east-1`, el valor es `ec2.internal`. Para las VPC de otras regiones, el valor es `region.compute.internal` (por ejemplo, `ap-northeast-1.compute.internal`).

- NTP servers (Servidores NTP): los servidores NTP que proporcionan el tiempo a la red. En el conjunto de opciones predeterminadas, no existe ningún valor para los servidores NTP. El conjunto de opciones de DHCP predeterminadas no incluye un servidor NTP porque las instancias de EC2 utilizan de forma predeterminada el servicio Amazon Time Sync para recuperar la hora.
- NetBIOS name servers (Servidores de nombres NetBIOS): para las instancias Windows EC2, el nombre de computadora NetBIOS es un nombre descriptivo asignado a la instancia para identificarla en la red. El servidor de nombres NetBIOS mantiene una lista de asignaciones entre los nombres de computadoras NetBIOS y las direcciones de red de las redes que utilizan NetBIOS como servicio de nombres. En el conjunto de opciones predeterminadas, no existe ningún valor para los servidores de nombres NetBIOS.
- NetBIOS node type (Tipo de nodo NetBIOS): para las instancias de EC2 de Windows, este es el método que utilizan las instancias para resolver nombres NetBIOS en direcciones IP. En el conjunto de opciones predeterminadas, no existe ningún valor para el tipo de nodo NetBIOS.

Describe uno o varios conjuntos de opciones de DHCP utilizando la AWS CLI o la API

Para obtener más información acerca de las interfaces de la línea de comandos, junto con una lista de API disponibles, consulte [Acceder a Amazon VPC](#) (p. 2).

- [describe-dhcp-options](#) (AWS CLI)
- [Get-EC2DhcpOption](#) (AWS Tools for Windows PowerShell)

Crear un conjunto de opciones de DHCP

Un conjunto de opciones de DHCP personalizadas le permite personalizar la VPC con su propio servidor DNS, nombre de dominio y mucho más.

De forma predeterminada, AWS asigna a todas las instancias de VPC no predeterminadas un nombre de host que no se puede resolver (por ejemplo, `ip-10-0-0-202`). Es posible asignar su propio nombre de dominio a sus instancias y a sus propios servidores DNS. Para ello, debe especificar un conjunto personalizado de opciones de DHCP para utilizarlas con la VPC.

Puede crear tantos conjuntos de opciones de DHCP adicionales como desee. Sin embargo, solo podrá asociar una VPC a un conjunto de opciones de DHCP a la vez.

Para crear un conjunto de opciones de DHCP

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija DHCP Options Sets.
3. Luego, Create DHCP options set (Crear conjunto de opciones de DHCP).
4. O bien, en el caso de Tag settings (configuración de etiquetas), ingrese un nombre para el conjunto de opciones de DHCP. De esta manera, se crea una etiqueta Name para el conjunto de opciones de DHCP.
5. En el caso de DHCP options (Opciones de DHCP), proporcione los parámetros de configuración que necesita.

Important

Si la VPC tiene una gateway de Internet, asegúrese de especificar su propio servidor DNS o el servidor DNS de Amazon (AmazonProvidedDNS) para el valor Domain name servers (Servidores de nombres de dominio). De lo contrario, las instancias que necesiten comunicarse con internet no tendrán acceso al DNS.

Note

Aunque todos los ajustes son opcionales, no se puede crear un conjunto de opciones sin definir al menos un ajuste.

- Domain name servers (Servidores de nombres de dominio) (optional): se trata de los servidores DNS que se utilizarán para resolver la dirección IP de un host a partir del nombre del mismo.

Ingrese AmazonProvidedDNS o servidores de nombres de dominio personalizados. Utilizar ambas cosas puede provocar un comportamiento inesperado. Puede ingresar las direcciones IP de hasta cuatro servidores de nombres de dominio IPv4 (o hasta tres servidores de nombre de dominio IPv4 y AmazonProvidedDNS) y cuatro servidores de nombres de dominio IPv6 separados por comas. Si bien puede especificar hasta ocho servidores de nombres de dominio, es posible que algunos sistemas operativos impongan límites más bajos. Para obtener más información acerca del servidor DNS de Amazon, consulte [Servidor DNS de Amazon \(p. 42\)](#).

- Domain name (Nombre de dominio) (optional): se trata del nombre de dominio que se adjuntará a las direcciones IPv4 públicas de las instancias de EC2 lanzadas en la VPC.

Si no utiliza AmazonProvidedDNS, los servidores de nombres de dominio personalizados deben resolver el nombre de host según corresponda. Si utiliza una zona alojada privada de Amazon Route 53, puede usar AmazonProvidedDNS. Para obtener más información, consulte [Atributos DNS para la VPC \(p. 42\)](#).

Algunos sistemas operativos Linux aceptan el uso de varios nombres de dominio separados por espacios. Sin embargo, otros sistemas operativos Linux y Windows tratan el valor como un dominio único, lo que da lugar a un comportamiento inesperado. Si el conjunto de opciones de DHCP está asociado a una VPC que contiene instancias en las que no se ejecutan los mismos sistemas operativos, especifique solo un nombre de dominio.

- NTP servers (Servidores NTP) (optional): los servidores NTP que proporcionan el tiempo a la red.

Ingrese las direcciones IP de hasta ocho servidores de protocolo de tiempo de red (NTP) (cuatro direcciones IPv4 y cuatro direcciones IPv6).

Puede especificar el servicio de sincronización de tiempo de Amazon en la dirección IPv4 169.254.169.123 o la dirección IPv6 fd00::ec2::123. Solo se puede acceder a la dirección IPv6 en [Instancias EC2 integradas en el sistema Nitro](#).

Para obtener más información acerca de la opción de servidores NTP, consulte [RFC 2132](#). Para obtener más información acerca de Amazon Time Sync Service, consulte [Configurar la hora para una instancia](#) en la Guía del usuario de instancias de Linux de Amazon EC2.

- NetBIOS name servers (Servidores de nombres NetBIOS) (opcional): ingrese las direcciones IP de hasta cuatro servidores de nombres NetBIOS.

Para las instancias Windows EC2, el nombre de computadora NetBIOS es un nombre descriptivo asignado a la instancia para identificarla en la red. El servidor de nombres NetBIOS mantiene una lista de asignaciones entre los nombres de computadoras NetBIOS y las direcciones de red de las redes que utilizan NetBIOS como servicio de nombres.

- NetBIOS node type (Tipo de nodo NetBIOS): para las instancias de EC2 de Windows, este es el método que utilizan las instancias para resolver nombres NetBIOS en direcciones IP. En el conjunto de opciones predeterminadas, no existe ningún valor para el tipo de nodo NetBIOS.

Las opciones de tipo de nodo de NetBIOS son 1, 2, 4 u 8. Le recomendamos que especifique 2 (punto a punto o nodo-P). Actualmente no se admiten la difusión ni la multidifusión. Para obtener más información sobre estos tipos de nodos, consulte la sección 8.7 de [RFC 2132](#) y la sección 10 de [RFC1001](#).

6. Agregar Etiquetas.
7. Luego, Create DHCP options set (Crear conjunto de opciones de DHCP).
8. Anote el ID del nuevo conjunto de opciones de DHCP (dopt-xxxxxxx). Necesitará este ID en el siguiente paso.
9. Configurar la VPC para utilizar el nuevo conjunto de opciones. Para obtener más información, consulte [Modificar el conjunto de opciones asociado a una VPC \(p. 40\)](#).

Los conjuntos de opciones de DHCP no se pueden modificar una vez creados. Si necesita que la VPC utilice un conjunto diferente de opciones de DHCP, debe crear un nuevo conjunto de opciones y, a continuación, asociarlo a la VPC. También se puede especificar que la VPC utilice el conjunto de opciones predeterminadas o que no utilice opciones de DHCP.

Cree un conjunto de opciones de DHCP para la VPC utilizando la AWS CLI o la API

Para obtener más información acerca de las interfaces de la línea de comandos, junto con una lista de API disponibles, consulte [Acceder a Amazon VPC \(p. 2\)](#).

- [create-dhcp-options](#) (AWS CLI)
- [New-EC2DhcpOption](#) (AWS Tools for Windows PowerShell)

Modificar el conjunto de opciones asociado a una VPC

Siga los pasos de esta sección para modificar el conjunto de opciones de DHCP que utiliza la VPC. Puede asignar un nuevo conjunto de opciones de DHCP a la VPC o puede desasociar un conjunto de opciones de DHCP de la VPC. Es posible que desee desasociar cualquier conjunto de opciones para desactivar la resolución de nombres de dominio en la VPC.

Note

- En el siguiente procedimiento, se da por sentado que ya ha creado el conjunto de opciones de DHCP. De lo contrario, cree el conjunto de opciones tal y como se describe en la sección anterior.
- Si asocia un nuevo conjunto de opciones de DHCP con la VPC, las instancias existentes y todas las nuevas que lance en dicha VPC utilizan las nuevas opciones. No es necesario reiniciar ni volver a lanzar las instancias. Los cambios en las instancias se aplican de forma automática en unas pocas horas, en función de la frecuencia con la que renueva la concesión de DHCP. Si lo desea, puede renovar de forma explícita la concesión a través del sistema operativo de la instancia.

- Puede tener varios conjuntos de opciones de DHCP, aunque solo podrá asociar un conjunto de opciones de DHCP a una VPC a la vez. Si elimina una VPC, también se desasocia de la VPC el conjunto de opciones de DHCP que está asociado a la VPC.

Para cambiar el conjunto de opciones de DHCP asociado a una VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs (Sus VPC).
3. Seleccione la casilla de verificación de la VPC y, a continuación, elija Actions (Acciones), Edit DHCP Options Set (Editar conjunto de opciones de DHCP).
4. En DHCP options set (Conjunto de opciones de DHCP), elija un nuevo conjunto de opciones de DHCP o elija No DHCP options set (Sin conjunto de opciones de DHCP) para no utilizar las opciones de DHCP en la VPC.
5. Elija Save changes.

Asociación a la VPC especificada de un conjunto de opciones de DHCP o de ninguna opción de DHCP utilizando la AWS CLI o la API

Para obtener más información acerca de las interfaces de la línea de comandos, junto con una lista de API disponibles, consulte [Acceder a Amazon VPC \(p. 2\)](#).

- [associate-dhcp-options](#) (AWS CLI)
- [Register-EC2DhcpOption](#) (AWS Tools for Windows PowerShell)

Eliminar un conjunto de opciones de DHCP

Cuando ya no necesite el conjunto de opciones de DHCP, utilice el siguiente procedimiento para eliminarlo. Asegúrese de cambiar las VPC que utilizan estas opciones a otro conjunto de opciones o a ningún conjunto de opciones antes de eliminar dicho conjunto de opciones. Para obtener más información, consulte [the section called “Modificar el conjunto de opciones asociado a una VPC” \(p. 40\)](#).

Para eliminar un conjunto de opciones de DHCP

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija DHCP Options Sets.
3. Seleccione el botón de opción para el conjunto de opciones de DHCP y, a continuación, elija Actions, (Acciones), Delete DHCP options set (Eliminar conjunto de opciones DHCP).
4. Cuando se le solicite su confirmación, ingrese delete (eliminar) y, luego, elija Delete DHCP options set (Eliminar conjunto de opciones de DHCP).

Eliminar un conjunto de opciones de DHCP utilizando la AWS CLI o la API

Para obtener más información acerca de las interfaces de la línea de comandos, junto con una lista de API disponibles, consulte [Acceder a Amazon VPC \(p. 2\)](#).

- [delete-dhcp-options](#) (AWS CLI)
- [Remove-EC2DhcpOption](#) (AWS Tools for Windows PowerShell)

Atributos DNS para la VPC

El sistema de nombres de dominio (DNS) es un estándar mediante el cual los nombres utilizados en Internet se resuelven a sus direcciones IP correspondientes. Un nombre de host DNS es un nombre que denomina de forma única y absoluta a un equipo, y se compone de un nombre de host y de un nombre de dominio. Los servidores DNS resuelven los nombres de host DNS a sus direcciones IP correspondientes.

Las direcciones IPv4 públicas permiten la comunicación a través de Internet, mientras que las direcciones IPv4 privadas permiten la comunicación dentro de la red de la instancia. Para obtener más información, consulte [Direccionamiento IP](#) (p. 4).

Amazon proporciona un servidor DNS para ([the Amazon Route 53 Resolver](#) (p. 42)) la VPC. Para usar su propio servidor DNS, cree un nuevo conjunto de opciones de DHCP para la VPC. Para obtener más información, consulte [Conjuntos de opciones de DHCP en Amazon VPC](#) (p. 34).

Contenido

- [Servidor DNS de Amazon](#) (p. 42)
- [Nombre de host DNS](#) (p. 43)
- [Atributos de DNS en su VPC](#) (p. 43)
- [Cuotas de DNS](#) (p. 45)
- [Consultar los nombres de host DNS de su instancia EC2](#) (p. 45)
- [Ver y actualizar los atributos de DNS de su VPC](#) (p. 46)
- [Zonas alojadas privadas](#) (p. 47)

Servidor DNS de Amazon

Las opciones predeterminadas del DHCP establecidas para la VPC incluyen dos opciones:

- `domain-name-servers=AmazonProvidedDNS`
- `domain-name=domain-name-for-your-region`

AmazonProvidedDNS es un servidor de Amazon Route 53 Resolver, y esta opción habilita los DNS para las instancias que necesiten comunicarse a través de la puerta de enlace de Internet de la VPC. El servidor DNS no reside dentro de una subred específica o zona de disponibilidad en una VPC. La cadena AmazonProvidedDNS se asigna a un servidor DNS que se ejecuta en 169.254.169.253 (y la dirección IP reservada en la base del rango de red IPv4 de la VPC más dos) y fd00:ec2::253. Por ejemplo, el servidor DNS de la red 10.0.0.0/16 se encuentra en 10.0.0.2. En el caso de las VPC con varios bloques de CIDR IPv4, la dirección IP del servidor DNS se encuentra en el bloque de CIDR principal.

Al lanzar una instancia en una VPC, dicha instancia, se le proporciona una instancia con un nombre de anfitrión de DNS privado. También se le proporciona un nombre de anfitrión de DNS público si la instancia está configurada con una dirección IPv4 pública y los atributos DNS de la VPC están habilitados.

El formato del nombre de host DNS privado depende de cómo configure la instancia EC2 al lanzarla. Para obtener más información sobre los tipos de nombres de host DNS privados, consulte [Nombres de instancias EC2](#).

El servidor DNS de Amazon de la VPC se utiliza para resolver los nombres de dominio de DNS que especifique en una zona alojada privada en Route 53. Para obtener más información acerca de las zonas alojadas privadas, consulte [Funcionamiento de las zonas alojadas privadas](#) en la Guía para desarrolladores de Amazon Route 53.

Reglas y consideraciones

Cuando se utiliza el servidor de Amazon DNS, se aplican las siguientes reglas y consideraciones.

- No puede filtrar tráfico hacia o desde el servidor DNS de Amazon mediante ACL de red o grupos de seguridad.
- Los servicios que utilizan el marco de trabajo de Hadoop, por ejemplo, Amazon EMR, requieren que las instancias resuelvan sus propios nombres completos de dominio (FQDN). En estos casos, la resolución de DNS puede producir error si la opción `domain-name-servers` está establecida con un valor predeterminado. Para asegurarse de que la resolución de DNS se realiza correctamente, considere la posibilidad de añadir un programa de envío condicional que reenvíe las consultas del dominio `region-name.compute.internal` al servidor DNS de Amazon. Para obtener más información, consulte [Configuración de una VPC para alojar clústeres](#) en la Guía de administración de Amazon EMR.
- Windows Server 2008 no permite utilizar un servidor DNS que se encuentre en el rango de direcciones locales del vínculo (169.254.0.0/16).
- Amazon Route 53 Resolver sólo admite consultas DNS recursivas.

Nombre de host DNS

Cuando lanza una instancia, esta siempre recibe una dirección IPv4 privada y un nombre de anfitrión de DNS privado que corresponde dicha dirección IPv4 privada. Si la instancia tiene una dirección IPv4 pública, los atributos del DNS de la VPC determinan si recibe un nombre de anfitrión de DNS público correspondiente a la dirección IPv4 pública. Para obtener más información, consulte [Atributos de DNS en su VPC](#) (p. 43).

Con el servidor DNS proporcionado por Amazon habilitado, los nombres de anfitrión de DNS se asignan y resuelven de la siguiente manera.

Nombre de DNS de IP privada (solo IPv4)

El nombre de host DNS IPv4 basado en IPBN que se resuelve en la dirección IPv4 privada de la instancia. Puede utilizar el nombre de host DNS de IP privada (solo IPv4) para la comunicación entre instancias de la misma red, pero no podemos resolver el nombre de host DNS fuera de la red en la que se encuentra la instancia. Para obtener más información acerca de IPBN, consulte [Tipos de nombres de host de instancias EC2](#).

Nombre de DNS de recursos privados

El nombre de DNS basado en RBN que se puede resolver en los registros DNS A y AAAA seleccionados para esta instancia. Este nombre de host DNS está visible en los detalles de la instancia para las instancias de subredes de doble pila y solo IPv6. Para obtener más información sobre RBN, consulte [Tipos de nombres de host de instancias EC2](#).

DNS IPv4 público

Un nombre de host DNS IPv4 público (externo) tiene el formato `ec2-public-ipv4-address.compute-1.amazonaws.com` para la región `us-east-1` y el formato `ec2-public-ipv4-address.region.compute.amazonaws.com` para las demás regiones. El servidor DNS de Amazon resuelve un nombre de host DNS público en la dirección IPv4 pública de la instancia fuera de la red de la instancia y en la dirección IPv4 privada de la instancia desde dentro de la red de la instancia. Para obtener más información, consulte [Direcciones IPv4 públicas y nombres de host DNS externos](#) en la Guía del usuario de Amazon EC2 para instancias Linux.

Atributos de DNS en su VPC

Los siguientes atributos de la VPC determinan la compatibilidad del DNS proporcionada para la VPC. Si ambos atributos están habilitados, una instancia lanzada en la VPC recibe un nombre de anfitrión de DNS

público si se le asigna una dirección IPv4 pública o una dirección IP elástica al momento de la creación. Si habilita ambos atributos para una VPC que no los tenía previamente inhabilitados, las instancias ya iniciadas en esa VPC recibirán nombres de anfitrión de DNS público si tienen una dirección IPv4 pública o una dirección IP elástica.

Para verificar si los atributos están habilitados para la VPC, consulte [Ver y actualizar los atributos de DNS de su VPC \(p. 46\)](#).

Atributo	Descripción
<code>enableDnsHostnames</code>	<p>Determina si la VPC admite la asignación de nombres de anfitrión de DNS público a las instancias con direcciones IP públicas.</p> <p>Si ambos atributos de DNS son <code>true</code>, las instancias de la VPC obtienen nombres de anfitrión de DNS público.</p> <p>El valor predeterminado de este atributo es <code>false</code>, a menos que la VPC sea una VPC predeterminada o se haya creado mediante el asistente de consola de la VPC.</p>
<code>enableDnsSupport</code>	<p>Determina si la VPC admite la resolución de DNS a través del servidor DNS proporcionado por Amazon.</p> <p>Si este atributo es <code>true</code>, las consultas al servidor DNS proporcionado por Amazon se realizan de manera exitosa. Para obtener más información, consulte Servidor DNS de Amazon (p. 42).</p> <p>El valor predeterminado de este atributo es <code>true</code>, independientemente de cómo se cree la VPC.</p>

Reglas y consideraciones

Se aplican las siguientes reglas.

- Si los dos atributos están configurados con el valor `true`, se producirán las siguientes situaciones:
 - Las instancias con direcciones IP públicas obtienen los nombres de anfitrión de DNS público correspondientes.
 - El servidor Amazon Route 53 Resolver puede resolver los nombres de host de DNS privados proporcionados por Amazon.
- Si al menos uno de los atributos se establece en `false`, ocurriría lo siguiente:
 - Las instancias con direcciones IP públicas no obtienen los nombres de anfitrión de DNS público correspondientes.
 - El servidor Amazon Route 53 Resolver no puede resolver los nombres de host de DNS privados proporcionados por Amazon.
 - Las instancias reciben nombres de host DNS privados personalizados si hay un nombre de dominio personalizado en el [conjunto de opciones de DHCP \(p. 34\)](#). Si no está utilizando el servidor Amazon Route 53 Resolver, sus servidores de nombres de dominio personalizados deberán resolver el nombre de host según corresponda.
- Si utiliza nombres de dominio de DNS personalizados definidos en una zona alojada privada en Amazon Route 53 o utiliza un DNS privado con puntos de enlace de la VPC de interfaz (AWS PrivateLink), debe establecer los atributos `enableDnsHostnames` y `enableDnsSupport` en `true`.
- El Amazon Route 53 Resolver puede resolver nombres de host de DNS privados en direcciones IPv4 privadas para todos los espacios de direcciones, incluido aquél en el que el rango de direcciones IPv4 de la VPC queda fuera de los rangos de direcciones IPv4 privadas especificados por [RFC 1918](#). Sin

embargo, si creó la VPC antes de octubre de 2016, Amazon Route 53 Resolver no resuelve los nombres de host DNS privados si el intervalo de direcciones IPv4 de la VPC queda fuera de estos intervalos. Para habilitar esta compatibilidad, póngase en contacto con [AWS Support](#).

Cuotas de DNS

Cada instancia EC2 puede enviar 1024 paquetes por segundo por interfaz de red a Route 53 Resolver (en concreto, la dirección .2, como 10.0.0.2 y 169.254.169.253). Esta cuota no puede incrementarse. El número de consultas de DNS por segundo que Route 53 Resolver admite varía según el tipo de consulta, el tamaño de respuesta y el protocolo en uso. Para obtener más información y recomendaciones para una arquitectura de DNS escalable, consulte la guía técnica de AWS [Hybrid DNS with Active Directory](#) (DNS híbrido con Active Directory).

Si alcanza la cuota, Amazon Route 53 Resolver rechaza el tráfico. Algunas de las causas para alcanzar la cuota pueden ser un problema de limitación controlada de DNS o consultas de metadatos de instancia que utilizan la interfaz de red de Route 53 Resolver. Para obtener información sobre cómo resolver problemas de limitación de DNS de VPC, consulte [Cómo puedo determinar si mis consultas de DNS en el servidor DNS proporcionado por Amazon están fallando debido a la limitación de DNS de VPC](#). Para obtener instrucciones acerca de la recuperación de metadatos de instancia, consulte [Retrieve instance metadata](#) (Recuperar metadatos de instancia) en la Guía del usuario de Amazon EC2 para instancias Linux.

Consultar los nombres de host DNS de su instancia EC2

Puede consultar los nombres de host DNS para una instancia en ejecución o una interfaz de red utilizando la consola o la línea de comandos de Amazon EC2.

Los campos Public DNS (IPv4) (DNS público [IPv4]) y Private DNS (DNS privado) están disponibles cuando las opciones de DNS están habilitadas para la VPC asociada a la instancia. Para obtener más información, consulte [the section called “Atributos de DNS en su VPC” \(p. 43\)](#).

Instancia

Para ver los nombres de host DNS para una instancia utilizando la consola

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia de la lista.
4. En el panel de detalles, los campos Public DNS (IPv4) y Private DNS mostrarán los nombres de host DNS, si corresponde.

Para ver los nombres de host DNS para una instancia utilizando la línea de comandos

Puede utilizar uno de los siguientes comandos. Para obtener más información acerca de estas interfaces de línea de comandos, consulte [Acceder a Amazon VPC \(p. 2\)](#).

- [describe-instances](#) (AWS CLI)
- [Get-EC2Instance](#) (AWS Tools for Windows PowerShell)

Interfaz de red

Para ver el nombre de host DNS privado para una interfaz de red utilizando la consola

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione la interfaz de red de la lista.
4. En el panel de detalles, el campo Private DNS (IPv4) (DNS privado (IPv4)) mostrará el nombre de host DNS privado.

Para ver los nombres de host DNS para una interfaz de red utilizando la línea de comandos

Puede utilizar uno de los siguientes comandos. Para obtener más información acerca de estas interfaces de línea de comandos, consulte [Acceder a Amazon VPC \(p. 2\)](#).



- `describe-network-interfaces` (AWS CLI)
- `Get-EC2NetworkInterface` (AWS Tools for Windows PowerShell)

Ver y actualizar los atributos de DNS de su VPC

Puede consultar y actualizar los atributos de compatibilidad de DNS para la VPC mediante la consola de Amazon VPC.

Para describir y actualizar la compatibilidad de DNS para una VPC utilizando la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs (Sus VPC).
3. Seleccione la casilla de verificación de la VPC.
4. Revise la información de Details (Detalles). En este ejemplo, se habilitan tanto los DNS hostnames (Nombre de host DNS) como la DNS resolution (Resolución de DNS).

Details	CIDRs	Flow logs	Tags
Details			
VPC ID  vpc-e03dd489	State  Available	DNS hostnames Enabled	DNS resolution Enabled

5. Para actualizar estas configuraciones, elija Actions (Acciones) y Edit DNS Resolution (Editar nombres de host de DNS) o Edit DNS Hostnames (Editar nombres de host de DNS). Cuando se le pregunte, seleccione o desactive Enable (Habilitar) y luego seleccione y Save changes (Guarde los cambios).

Para describir la compatibilidad de DNS para una VPC utilizando la línea de comandos

Puede utilizar uno de los siguientes comandos. Para obtener más información acerca de estas interfaces de línea de comandos, consulte [Acceder a Amazon VPC \(p. 2\)](#).

- `describe-vpc-attribute` (AWS CLI)

- [Get-EC2VpcAttribute](#) (AWS Tools for Windows PowerShell)

Para actualizar la compatibilidad de DNS para una VPC utilizando la línea de comandos

Puede utilizar uno de los siguientes comandos. Para obtener más información acerca de estas interfaces de línea de comandos, consulte [Acceder a Amazon VPC \(p. 2\)](#).

- [modify-vpc-attribute](#) (AWS CLI)
- [Edit-EC2VpcAttribute](#) (AWS Tools for Windows PowerShell)

Zonas alojadas privadas

Para acceder a los recursos de la VPC mediante nombres de dominio de DNS personalizados, como `example.com`, en lugar de utilizar direcciones IPv4 privadas o nombres de alojamiento de DNS privados proporcionados por AWS, puede crear una zona alojada privada en Route 53. Una zona alojada privada es un contenedor que mantiene información acerca de cómo se desea dirigir el tráfico de un dominio y sus subdominios dentro de una o varias VPC sin tener que exponer sus recursos en Internet. A continuación, puede crear conjuntos de registros de recursos de Route 53, que determinan cómo responde Route 53 a las consultas para el dominio y los subdominios. Por ejemplo, si desea que las solicitudes del navegador se dirijan a un servidor web en su VPC, creará un registro A en su zona hospedada privada y especificará la dirección IP en ese servidor web. Para obtener más información acerca de la creación de una zona alojada privada, consulte [Uso de zonas alojadas privadas](#) en la Guía para desarrolladores de Amazon Route 53.

Para obtener acceso a recursos utilizando nombres de dominio DNS personalizados, debe estar conectado a una instancia en su VPC. Desde su instancia, puede comprobar que su recurso de la zona hospedada privada esté accesible desde su nombre DNS personalizado mediante el comando `ping`; por ejemplo, `ping mywebserver.example.com`. (Debe asegurarse de que las reglas del grupo de seguridad de su instancia permiten el tráfico ICMP entrante para que el comando `ping` funcione).

Puede obtener acceso a una zona hospedada privada desde una instancia de EC2-Classic vinculada a su VPC mediante ClassicLink, siempre que su VPC esté habilitada para la compatibilidad de DNS con ClassicLink. Para obtener más información, consulte [Habilitación de la compatibilidad de DNS para ClassicLink](#) en la Guía del usuario de Amazon EC2 para instancias de Linux. En caso contrario, las zonas hospedadas privadas no admitirán las relaciones transitivas fuera de la VPC; por ejemplo, no es posible obtener acceso a los recursos utilizando sus nombres DNS privados personalizados desde el otro lado de una conexión VPN. Para obtener más información, consulte [Limitaciones de ClassicLink](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Important

Si utiliza nombres de dominio DNS personalizados definidos en una zona alojada privada en Amazon Route 53, debe establecer los atributos `enableDnsHostnames` y `enableDnsSupport` como `true`.

Compartir la VPC con otras cuentas

El uso compartido de VPC permite que varias Cuentas de AWS creen sus recursos de aplicaciones, como instancias de Amazon EC2, bases de datos de Amazon Relational Database Service (RDS), clústeres de Amazon Redshift y funciones de AWS Lambda, en nubes virtuales privadas (VPC) compartidas y administradas de manera centralizada. En este modelo, la cuenta propietaria de la VPC (el propietario) comparte una o varias subredes con otras cuentas (los participantes) que pertenecen a la misma organización de AWS Organizations. Después de compartir una subred, los participantes pueden ver, crear, modificar y eliminar los recursos de su aplicación en las subredes compartidas con ellos. Los

participantes no pueden ver, modificar ni eliminar recursos que pertenezcan a otros participantes o al propietario de la VPC.

También puede compartir las VPC para aprovechar el enrutamiento implícito dentro de una VPC en las aplicaciones que requieran un alto grado de interconectividad y que estén dentro de los mismos límites de confianza. De este modo, se reduce el número de VPC que se crean y administran, al tiempo que se utilizan cuentas independientes para la facturación y el control de acceso. Puede simplificar las topologías de red interconectando las VPC de Amazon VPC compartidas mediante las características de conectividad, como AWS PrivateLink, transit gateways e interconexión de VPC. Para obtener más información sobre las ventajas de compartir las VPC, consulte [Uso compartido de VPC: un nuevo enfoque a la administración de varias cuentas y VPC](#).

Contenido

- [Requisitos previos para las VPC compartidas \(p. 48\)](#)
- [Compartir una subred \(p. 48\)](#)
- [Dejar de compartir una subred compartida \(p. 49\)](#)
- [Identificar al propietario de una subred compartida \(p. 50\)](#)
- [Permisos para las subredes compartidas \(p. 50\)](#)
- [Facturar y medir para el propietario y los participantes \(p. 51\)](#)
- [Limitaciones \(p. 51\)](#)
- [Ejemplo de compartir subredes públicas y subredes privadas. \(p. 52\)](#)

Requisitos previos para las VPC compartidas

Debe habilitar el uso compartido de recursos desde la cuenta de administración para la organización. Para obtener información acerca de cómo habilitar el uso compartido de recursos, consulte [Habilitar el uso compartido con AWS Organizations](#) en la Guía del usuario de AWS RAM.

Compartir una subred

Puede compartir subredes distintas de la predeterminada con otras cuentas en su organización. Para compartir subredes, primero debe crear un recurso compartido con las subredes que se vayan a compartir y las cuentas de AWS, las unidades organizativas o una organización completa con las que desee compartir las subredes. Para obtener más información acerca de la creación de un recurso compartido, consulte [Creación de un recurso compartido](#) en la Guía del usuario de AWS RAM.

Para compartir una subred con la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets.
3. Seleccione su subred y elija Actions (Acciones), Share subnet (Compartir subred).
4. Seleccione su recurso compartido y elija Share subnet (Compartir subred).

Para compartir una subred con la AWS CLI

Utilice los comandos [create-resource-share](#) y [associate-resource-share](#).

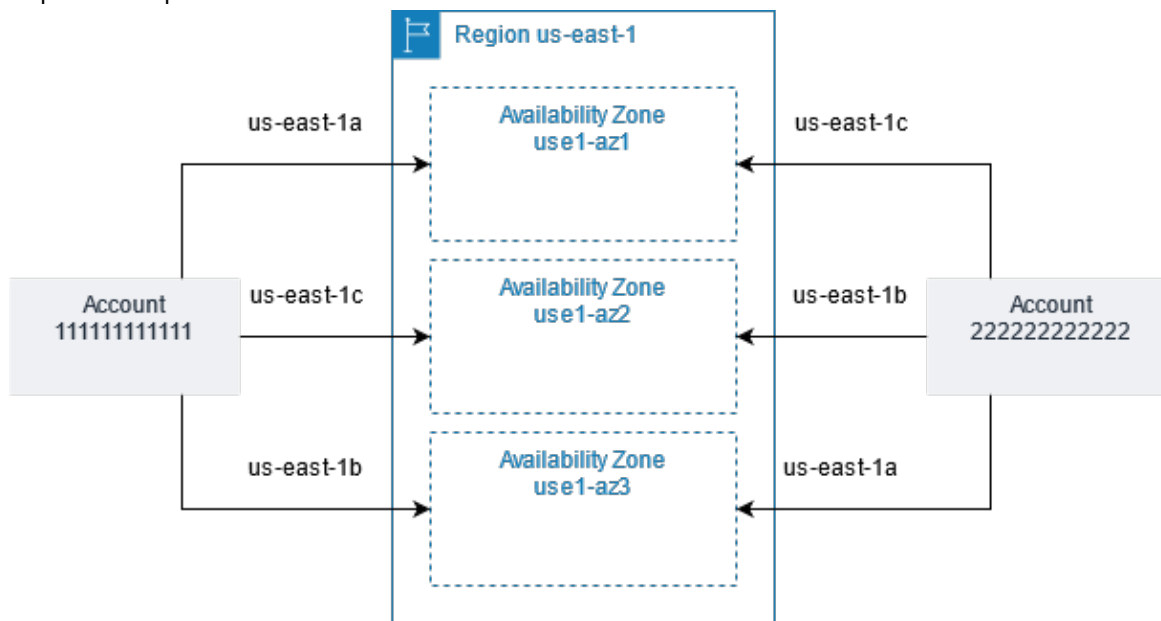
Asignar subredes en las zonas de disponibilidad

Para garantizar que los recursos se distribuyen por todas las zonas de disponibilidad de una región, asignamos zonas de disponibilidad de manera independiente a nombres de cada cuenta. Por ejemplo, es

posible que la zona de disponibilidad `us-east-1a` de su cuenta de AWS no se encuentre en la misma ubicación de `us-east-1a` que otra cuenta de AWS.

Para coordinar las zonas de disponibilidad entre cuentas para compartir VPC, debe usar un ID de AZ, que es un identificador único y constante de una zona de disponibilidad. Por ejemplo, `use1-az1` es el ID de AZ de una de las zonas de disponibilidad de la región `us-east-1`. Utilice los ID de AZ para determinar la ubicación de los recursos de una cuenta relativos a otra cuenta. Puede ver el ID de AZ de cada subred en la consola de Amazon VPC.

En el siguiente diagrama se ilustran dos cuentas con asignaciones diferentes de código de zona de disponibilidad para ID de AZ.



Dejar de compartir una subred compartida

El propietario puede dejar de compartir una subred compartida con los participantes en cualquier momento. Cuando el propietario deja de compartir una subred compartida, se aplican las siguientes reglas:

- Los recursos existentes de los participantes siguen ejecutándose en la subred que se ha dejado de compartir.
- Los participantes ya no pueden crear nuevos recursos en la subred que se ha dejado de compartir.
- Los participantes pueden modificar, describir y eliminar los recursos que están en la subred.
- Si los participantes siguen teniendo recursos en la subred que se ha dejado de compartir, el propietario no puede eliminar la subred compartida ni la VPC de la subred compartida. El propietario solo puede eliminar la subred compartida o la VPC de la subred compartida una vez que todos los participantes hayan eliminado todos los recursos de la subred no compartida.

Para dejar de compartir una subred con la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets.
3. Seleccione su subred y elija Actions (Acciones), Share subnet (Compartir subred).
4. Elija Actions (Acciones), Stop sharing (Dejar de compartir).

Para dejar de compartir una subred con la AWS CLI

Utilice el comando `disassociate-resource-share`.

Identificar al propietario de una subred compartida

Los participantes pueden consultar las subredes que se han compartido con ellos mediante la consola de Amazon VPC o la herramienta de línea de comandos.

Para identificar al propietario de una subred con la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets. La columna Owner (Propietario) muestra el propietario de la subred.

Para identificar al propietario de una subred con la AWS CLI

Utilice los comandos `describe-subnets` y `describe-vpcs`, que incluyen el ID del propietario en la salida.

Permisos para las subredes compartidas

Owner permissions (Permisos del propietario)

Los propietarios de la VPC son los responsables de crear, administrar y eliminar todos los recursos de la VPC, lo que incluye a las subredes, las tablas de enrutamiento, las ACL de red, las interconexiones, los puntos de enlace de gateway, los puntos de enlace de interfaz, los puntos de enlace de Amazon Route 53 Resolver, las puertas de enlace de Internet, las puertas de enlace NAT, las puertas de enlace virtuales privadas y las vinculaciones de transit gateway.

Los propietarios de la VPC no pueden modificar ni eliminar los recursos de los participantes, incluidos los grupos de seguridad que crean los participantes. Los propietarios de la VPC pueden ver los detalles de todas las interfaces de red y los grupos de seguridad que están asociados a los recursos de los participantes para solucionar problemas y realizar auditorías. Los propietarios de la VPC pueden crear suscripciones a nivel del log de flujo en la VPC, la subred o la interfaz de red para monitorizar el tráfico y solucionar problemas.

Permisos de los participantes

Los participantes que están en una VPC compartida son responsables de crear, administrar y eliminar los recursos, incluidas las instancias Amazon EC2, las bases de datos de Amazon RDS y los balanceadores de carga. Los participantes no pueden ver ni modificar los recursos que pertenezcan a otras cuentas participantes. Los participantes pueden ver los detalles de las tablas de ruteo y las ACL de red asociadas a las subredes compartidas con ellos. Sin embargo, no pueden modificar los recursos de nivel de VPC, incluidas las tablas de ruteo, las ACL de red y las subredes. Los participantes pueden hacer referencia a los grupos de seguridad que pertenecen a otros participantes o al propietario mediante el ID de grupo de seguridad. Los participantes solo pueden crear suscripciones de registro de flujo para las interfaces de las que son propietarios. Los participantes no pueden asociar directamente una de sus zonas alojadas privadas con la VPC compartida. Si el participante necesita controlar el comportamiento de una zona alojada privada asociada a la VPC, existen dos opciones:

- Los participantes pueden crear y compartir una zona alojada privada con el propietario de la VPC. Para obtener información acerca de cómo compartir una zona alojada privada, consulte [Asociación de una VPC de Amazon VPC y una zona alojada privada que creó con diferentes cuentas de AWS](#) en la Guía para desarrolladores de Amazon Route 53.

- El propietario de la VPC puede crear un rol de IAM entre cuentas que proporcione control sobre una zona alojada privada que el propietario ya ha asociado a la VPC. El propietario puede conceder a la cuenta participante los permisos necesarios para asumir el rol. Para obtener más información, consulte [Tutorial de IAM: delegación de acceso entre cuentas de AWS mediante roles de IAM](#) en la Guía del usuario de AWS Identity and Access Management. A continuación, la cuenta de participación puede asumir el rol y ejercer cualquier control sobre la zona alojada privada que el propietario haya delegado a través del permiso del rol.

Facturar y medir para el propietario y los participantes

En una VPC compartida, cada participante paga por los recursos de sus aplicaciones, incluidos las instancias de Amazon EC2, las bases de datos de Amazon Relational Database Service, los clústeres de Amazon Redshift y las funciones de AWS Lambda. Los participantes también pagan los gastos de la transferencia de datos asociados a la transferencia de datos entre zonas de disponibilidad, la transferencia de datos a través de interconexiones con VPC y la transferencia de datos a través de una gateway de AWS Direct Connect. Los propietarios de la VPC pagan los gastos por hora (si procede) y los cargos de procesamiento y por transferencia de datos a través de gateways NAT, gateways privadas virtuales, transit gateways, puntos de enlace de la VPC y AWS PrivateLink. La transferencia de datos dentro de la misma zona de disponibilidad (identificada de forma exclusiva mediante el AZ-ID) es gratuita independientemente de la propiedad de los recursos de comunicación.

Limitaciones

Se aplican las siguientes limitaciones al uso compartido de VPC:

- Los propietarios solo pueden compartir subredes con otras cuentas o unidades organizativas que estén en la misma organización de AWS Organizations.
- Los propietarios no pueden compartir subredes que estén en una VPC predeterminada.
- Los participantes no pueden lanzar recursos mediante grupos de seguridad que sean propiedad de otros participantes que comparten la VPC o del propietario de la VPC.
- Los participantes no pueden lanzar recursos mediante el grupo de seguridad predeterminado de la VPC porque pertenece al propietario.
- Los propietarios no pueden lanzar recursos mediante grupos de seguridad que sean propiedad de otros participantes.
- Cuando los participantes lanzan recursos en una subred compartida, deben asegurarse de adjuntar su grupo de seguridad al recurso y no contar con el grupo de seguridad predeterminado. Los participantes no pueden utilizar el grupo de seguridad predeterminado ya que pertenece al propietario de la VPC.
- Los participantes no pueden crear puntos de enlace de Route 53 Resolver en una VPC que no posean. Solo el propietario de la VPC puede crear recursos a nivel de la VPC, como puntos de enlace de entrada.
- Las etiquetas de VPC y las etiquetas de los recursos de la VPC compartida no se comparten con los participantes.
- Solo el propietario de una subred puede adjuntar una transit gateway a la subred compartida. Los participantes no pueden hacerlo.
- Los participantes pueden crear balanceadores de carga de aplicaciones y balanceadores de carga de red en una VPC compartida, pero no pueden registrar los destinos que se ejecutan en subredes que no se han compartido con ellos.
- Solo el propietario de una subred puede seleccionar una subred compartida al momento de crear un equilibrador de carga de puerta de enlace. Los participantes no pueden hacerlo.
- Las cuotas de servicio se aplican a cada cuenta.

Ejemplo de compartir subredes públicas y subredes privadas.

Considere un escenario en el que desea que una cuenta sea responsable de la infraestructura, incluidas las subredes, las tablas de ruteo, las gateways, los rangos de CIDR y otras cuentas que estén en la misma organización de AWS para utilizar las subredes. Un propietario de VPC (cuenta A) crea la infraestructura de direccionamiento, incluidas las VPC, las subredes, las tablas de ruteo, las gateways y las ACL de red. La cuenta D desea crear aplicaciones expuestas al público. Las cuentas B y C desean crear aplicaciones privadas que no necesiten conectarse a Internet y deben encontrarse en subredes privadas. La cuenta A puede usar AWS Resource Access Manager para crear un recurso compartido para las subredes y, a continuación, compartirlas. La cuenta A comparte la subred pública con la cuenta D y la subred privada con las cuentas B y C. Las cuentas B, C y D pueden crear recursos en las subredes. Cada cuenta solo puede ver las subredes que se comparten con ella, por ejemplo, la cuenta D solo puede ver la subred pública. Cada una de las cuentas puede controlar sus recursos, incluidas las instancias y los grupos de seguridad.

La cuenta A administra la infraestructura IP, incluidas las tablas de ruteo para las subredes públicas y las privadas. No se requiere configuración adicional para las subredes compartidas, por lo que las tablas de ruteo son las mismas que las de las subredes no compartidas.

La cuenta A (ID de cuenta 111111111111) comparte la subred pública con la cuenta D (444444444444). La cuenta D ve la siguiente subred y la columna Owner (Propietario) proporciona dos indicadores de que la subred es compartida.

- El ID de cuenta es el propietario de la VPC (1111111111111111) y es diferente del ID de la cuenta D (4444444444444444).
- La palabra "compartido" aparece junto al ID de la cuenta del propietario.

Create subnet

Actions

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	Route table	Default subnet	Owner
<input type="checkbox"/>		subnet-0bb1c79de301436ee	available	vpc-0ee975135d74bdcfe	10.0.0.0/24	251	rtb-0825a8caf09467ea8	No	111111111111 (S)

Ampliar una VPC a una zona local, una zona Wavelength o Outpost

Puede alojar recursos de VPC, como subredes, en varias ubicaciones de todo el mundo. Estas ubicaciones se componen de regiones, zonas de disponibilidad, Local Zones y zonas de Wavelength. Cada región es un área geográfica independiente.

- Las zonas de disponibilidad son varias ubicaciones aisladas dentro de cada región.
- Las Local Zones le permiten colocar recursos, como de cómputo y de almacenamiento, en varias ubicaciones más cercanas a los usuarios finales.
- AWS Outposts brinda servicios, infraestructura y modelos operativos nativos de AWS a prácticamente cualquier centro de datos, espacio de ubicación o instalación en las instalaciones.
- Las zonas de Wavelength permiten a los desarrolladores crear aplicaciones que ofrecen latencia extremadamente baja para dispositivos 5G y usuarios finales. Wavelength implementa servicios de computación y almacenamiento de AWS estándar al borde de redes 5G de operadores de telecomunicaciones.

AWS opera centros de datos con tecnología de vanguardia y alta disponibilidad. Aunque es infrecuente, puede suceder que se produzcan errores que afecten a la disponibilidad de las instancias que están en la misma ubicación. Si aloja todas las instancias en una misma ubicación y se produce un error en ella, ninguna de las instancias estaría disponible.

Para ayudarlo a determinar qué implementación es la mejor para usted, consulte [Preguntas frecuentes de AWS Wavelength](#).

Ampliar los recursos de VPC a Local Zones

Las AWS Local Zones le permiten colocar recursos más cerca de sus usuarios finales y conectarse sin problemas a la gama completa de servicios de la región de AWS a través de API y conjuntos de herramientas conocidos. Puede ampliar la región de VPC mediante la creación de una nueva subred que tenga una asignación de zona local. Cuando crea una subred en una Local Zone, extiende la VPC a esta Local Zone.

Para utilizar una Local Zone, debe seguir un proceso de tres pasos:

- En primer lugar, acceda a la Local Zone.
- A continuación, cree una subred en la zona local.
- Por último, lance los recursos seleccionados en la subred de la Local Zone para que las aplicaciones estén más cerca de los usuarios finales.

Un grupo de bordes de red es un conjunto exclusivo de zonas de disponibilidad o Local Zones desde donde AWS anuncia las direcciones IP públicas.

Cuando crea una VPC que tiene direcciones IPv6, puede elegir asignar un conjunto de direcciones IP públicas proporcionadas por Amazon a la VPC y también establecer un grupo de bordes de red para las direcciones que limitan las direcciones al grupo. Cuando establece un grupo de bordes de red, las direcciones IP no pueden moverse entre grupos de bordes de red. El grupo de bordes de red `us-west-2` contiene las cuatro zonas de disponibilidad EE.UU. Oeste (Oregón). El grupo de bordes de red `us-west-2-lax-1` contiene las Local Zones de Los Ángeles.

Las siguientes reglas se aplican a las Local Zones:

- Las subredes de la Local Zone siguen las mismas reglas de enrutamiento que las subredes de la zona de disponibilidad, incluidas las tablas de enrutamiento, los grupos de seguridad y las ACL de red.
- Puede asignar Local Zones a subredes mediante la Amazon Virtual Private Cloud Console, la AWS CLI o la API.
- Debe aprovisionar las direcciones IP públicas para utilizarlas en una zona local. Cuando asigna direcciones, puede especificar la ubicación desde la que se anuncia la dirección IP. Nos referimos a esto como un grupo de bordes de red, y puede establecer este parámetro para limitar las direcciones a esta ubicación. Cuando aprovisiona las direcciones IP, no puede moverlas entre la Local Zone y la región principal (por ejemplo, desde `us-west-2-lax-1a` hasta `us-west-2`).
- Puede solicitar las direcciones IP proporcionadas por IPv6 de Amazon y asociarlas con el grupo de bordes de red para una VPC nueva o existente.

Note

IPv6 solo se admite en las Local Zones de Los Ángeles.

- El tráfico de salida de Internet sale de una Local Zone de la Local Zone.

Para obtener más información acerca de cómo trabajar con las Local Zones en Linux, consulte [Local Zones](#) en la Guía del usuario de Amazon EC2 para instancias de Linux. Para obtener más información acerca de cómo trabajar con las Local Zones en Windows, consulte [Local Zones](#) en la Guía del usuario de

Amazon EC2 para instancias de Windows. Ambas guías contienen una lista de las Local Zones disponibles y los recursos que puede lanzar en cada Local Zone.

Consideraciones para las gateways de Internet

Tenga en cuenta la siguiente información cuando utilice puertas de enlace de Internet (en la región principal) en Local Zones:

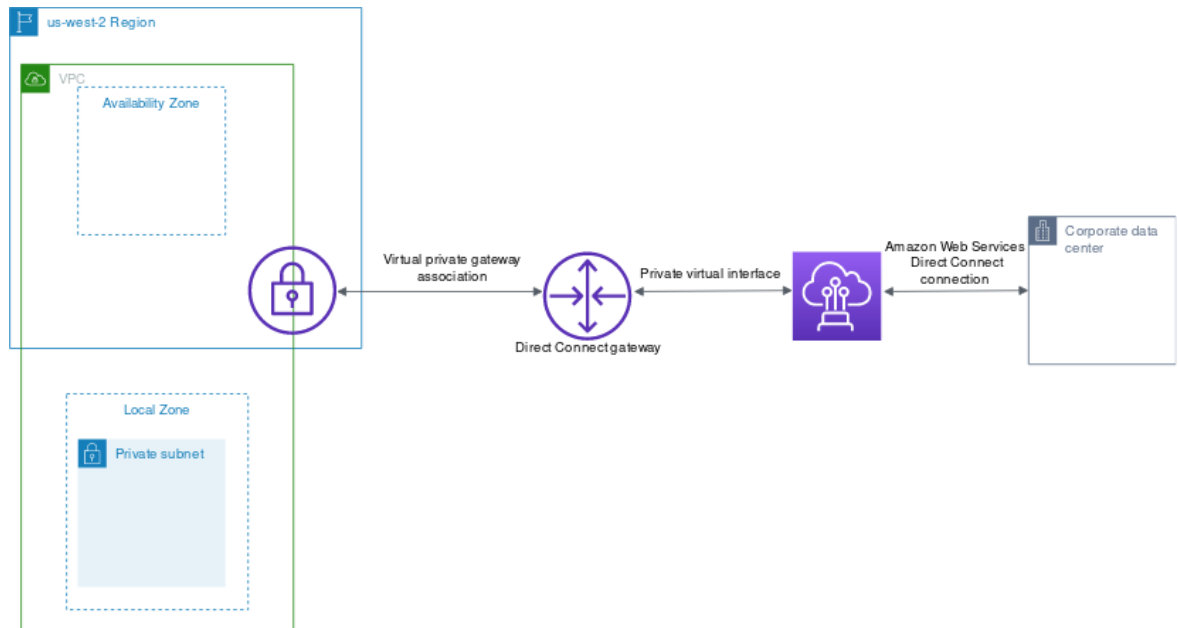
- Puede utilizar puertas de enlace de Internet en Local Zones con direcciones IP elásticas o direcciones IP públicas asignadas de forma automática por Amazon. Las direcciones IP elásticas que asocie deben incluir el grupo de bordes de red de la Local Zone. Para obtener más información, consulte [the section called “Direcciones IP elásticas”](#) (p. 149).

No se puede asociar una dirección IP elástica que esté establecida para la región.

- Las direcciones IP elásticas que se utilizan en las Local Zones tienen las mismas cuotas que las direcciones IP elásticas de una región. Para obtener más información, consulte [the section called “Direcciones IP elásticas \(IPv4\)”](#) (p. 378).
- Puede utilizar gateways de Internet en tablas de enrutamiento que estén asociadas a recursos de zona locales. Para obtener más información, consulte [the section called “Enrutar a una gateway de Internet”](#) (p. 90).

Acceder a Local Zones mediante una gateway de Direct Connect

Tenga en cuenta el escenario en el que desea que un centro de datos local acceda a los recursos que se encuentran en una zona local. Debe utilizar una gateway privada virtual para la VPC asociada con la Local Zone para conectarse a una gateway de Direct Connect. La gateway de Direct Connect se conecta a una ubicación de AWS Direct Connect de una región. El centro de datos en las instalaciones tiene una conexión de AWS Direct Connect con la ubicación de AWS Direct Connect.



Se deben configurar los siguientes recursos para esta configuración:

- Una gateway privada virtual para la VPC asociada con la subred de zona local. Puede consultar la VPC de la subred en la página de detalles de la subred de la Amazon Virtual Private Cloud Console o utilizar [describe-subnets](#).

Para obtener información acerca de cómo crear una gateway privada virtual, consulte [Crear una gateway de destino](#) en la Guía del usuario de AWS Site-to-Site VPN.

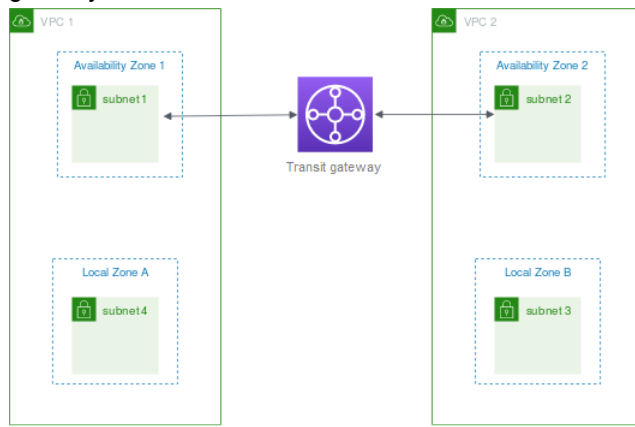
- Una conexión de Direct Connect. AWS recomienda utilizar una de las siguientes ubicaciones para obtener el mejor rendimiento de latencia en las Local Zones de Los Ángeles:
 - T5 en El Segundo, Los Ángeles, CA (AWS recomienda esta ubicación para obtener la latencia más baja en la Local Zone de Los Ángeles)
 - CoreSite LA1, Los Ángeles, CA
 - Equinix LA3, El Segundo, CA

Para obtener información acerca de cómo solicitar una conexión, consulte [Conexiones cruzadas](#) en la Guía del usuario de AWS Direct Connect.

- Una gateway de Direct Connect. Para obtener información acerca de cómo crear una gateway de Direct Connect, consulte [Crear una gateway de Direct Connect](#) en la Guía del usuario de AWS Direct Connect.
- Una asociación de gateway privada virtual para conectar la VPC a la gateway de Direct Connect. Para obtener información acerca de cómo crear una asociación de gateway privada virtual, consulte [Asociación y desasociación de gateways privadas virtuales](#) en la Guía del usuario de AWS Direct Connect.
- Una interfaz virtual privada en la conexión desde la ubicación de AWS Direct Connect hasta el centro de datos en las instalaciones. Para obtener información acerca de cómo crear una gateway de Direct Connect, consulte [Creación de una interfaz virtual privada para la gateway de Direct Connect](#) en la Guía del usuario de AWS Direct Connect.

Conectar las subredes de una zona local a una transit gateway

No se puede crear una conexión de transit gateway para una subred en una zona local. En el siguiente diagrama, se muestra cómo configurar la red para que las subredes de la zona local se conecten a una Transit Gateway mediante la zona de disponibilidad principal. Cree subredes en las Local Zones y subredes en las zonas de disponibilidad principales. Conecte las subredes de las zonas de disponibilidad principales a la Transit Gateway y, a continuación, cree una ruta en la tabla de enrutamiento para cada VPC que enruta el tráfico destinado al CIDR de la otra VPC a la interfaz de red para la conexión de transit gateway



Cree los siguientes recursos para este escenario:

- Una subred en cada zona de disponibilidad principal. Para obtener más información, consulte [the section called “Crear una subred en la VPC” \(p. 64\)](#).
- Una transit gateway. Para obtener más información, consulte [Creación de Transit Gateway](#) en Transit Gateways de Amazon VPC.

- Una conexión de transit gateway para cada VPC mediante la zona de disponibilidad principal. Para obtener más información, consulte [Creación de una conexión de transit gateway a VPC](#) en Transit Gateways de Amazon VPC.
- Una tabla de enrutamiento de la transit gateway asociada con la conexión de transit gateway. Para obtener más información, consulte [Tablas de enrutamiento de Transit Gateway](#) en Transit Gateways de Amazon VPC.
- Para cada VPC, una entrada en la tabla de enrutamiento de la VPC que tiene el otro CIDR de la VPC como destino, y el ID de la interfaz de red de la conexión de transit gateway como destino. A fin de buscar la interfaz de red para la conexión de transit gateway, busque en las descripciones de las interfaces de red el ID de la conexión de transit gateway. Para obtener más información, consulte [the section called “Enrutar para una transit gateway” \(p. 94\)](#).

A continuación, se muestra una tabla de enrutamiento de ejemplo para la VPC 1.

Destino	Objetivo
<i>CIDR de VPC</i>	<i>local</i>
<i>CIDR de VPC</i>	<i>vpc1-attachment-network-interface-id</i>

A continuación, se muestra una tabla de enrutamiento de ejemplo para la VPC 2.

Destino	Objetivo
<i>CIDR de VPC</i>	<i>local</i>
<i>CIDR de VPC</i>	<i>vpc2-attachment-network-interface-id</i>

A continuación se muestra un ejemplo de la tabla de enrutamiento de la transit gateway. Los bloques de CIDR de cada VPC se propagan a la tabla de enrutamiento de la transit gateway.

CIDR	Attachment	Tipo de ruta
<i>CIDR de VPC</i>	<i>Conexión de la VPC 1</i>	propagada
<i>CIDR de VPC</i>	<i>Conexión de la VPC 2</i>	propagada

Ampliar los recursos de VPC a las zonas de Wavelength

AWS Wavelength permite a los desarrolladores crear aplicaciones que ofrecen una latencia extremadamente baja para dispositivos móviles y usuarios finales. Wavelength implementa servicios de computación y almacenamiento de AWS estándar al borde de redes 5G de operadores de telecomunicaciones. Los desarrolladores pueden ampliar una Amazon Virtual Private Cloud (VPC) a una o varias zonas de Wavelength y, luego, utilizar recursos de AWS como instancias de Amazon Elastic Compute Cloud (EC2) para ejecutar aplicaciones que requieran una latencia ultrabaja y conectarse a servicios de AWS en la región.

Para utilizar una zona de Wavelength, primero debe optar por la zona. A continuación, cree una subred en la zona de Wavelength. Puede crear instancias Amazon EC2, volúmenes de Amazon EBS, subredes

de Amazon VPC y gateways de operador en zonas de Wavelength. Además, puede utilizar servicios que funcionen con EC2, EBS y VPC o se organicen con ellos, como Amazon EC2 Auto Scaling, los clústeres de Amazon EKS, los clústeres de Amazon ECS, Amazon EC2 Systems Manager, Amazon CloudWatch, AWS CloudTrail y AWS CloudFormation. Los servicios de Wavelength forman parte de una VPC que está conectada a través de una conexión de confianza y alto ancho de banda a una región de AWS para brindar un fácil acceso a servicios como Amazon DynamoDB y Amazon RDS.

Las siguientes reglas se aplican a las zonas de Wavelength:

- Una VPC se extiende a una zona de Wavelength al crear una subred en la VPC y asociarla a la zona de Wavelength.
- De forma predeterminada, cada subred que cree en una VPC que abarca una zona de Wavelength hereda la tabla de enrutamiento de VPC principal, incluida la ruta local.
- Cuando lanza una instancia EC2 en una subred en una zona de Wavelength, le asigna una dirección IP de operador. La gateway de operador utiliza la dirección para el tráfico desde la interfaz a Internet o dispositivos móviles. La gateway de operador utiliza NAT para traducir la dirección y, a continuación, envía el tráfico al destino. El tráfico de la red del operador de telecomunicaciones se dirige a través de la gateway de operador.
- Puede establecer el objetivo de una tabla de enrutamiento de VPC o de una tabla de enrutamiento de subred en una zona de Wavelength en una gateway de operador, que permite el tráfico entrante desde una red de operador en una ubicación específica y el tráfico saliente a la red de operador y a Internet. Para obtener más información acerca de las opciones de enrutamiento en una zona de Wavelength, consulte [Enrutamiento](#) en la Guía para desarrolladores de AWS Wavelength.
- Las subredes de las zonas de Wavelength tienen los mismos componentes de red que las subredes de las zonas de disponibilidad, incluidas direcciones IPv4, conjuntos de opciones DHCP y ACL de red.
- No se puede crear una conexión de transit gateway para una subred en una zona Wavelength. En su lugar, cree los datos adjuntos a través de una subred en la zona de disponibilidad principal y, a continuación, enrute el tráfico a los destinos deseados a través de la transit gateway. Consulte la siguiente sección para ver un ejemplo.

Consideraciones para varias zonas de Wavelength

Las instancias EC2 que se encuentren en dos zonas de Wavelength diferentes de la misma VPC no pueden comunicarse entre sí. Si necesita comunicación entre zonas de Wavelength, AWS recomienda utilizar varias VPC, una para cada zona de Wavelength. Puede utilizar una transit gateway para conectar las VPC. Esta configuración permite la comunicación entre instancias en las zonas de Wavelength.

El tráfico de una zona de Wavelength a otra se dirige a través de la región de AWS. Para obtener más información, consulte [AWS Transit Gateway](#).

En el siguiente diagrama se muestra cómo configurar la red para que las instancias de dos zonas de Wavelength diferentes puedan comunicarse. Tiene dos zonas de Wavelength (zona de Wavelength A y zona de Wavelength B). Debe crear los siguientes recursos para habilitar la comunicación:

- Para cada zona de Wavelength, una subred de una zona de disponibilidad que es la zona de disponibilidad principal de la zona de Wavelength. En el ejemplo, creará la subred 1 y la subred 2. Para obtener información sobre la creación de subredes, consulte [the section called "Crear una subred en la VPC" \(p. 64\)](#). Utilice [describe-availability-zones](#) para encontrar la zona principal.
- Una transit gateway. La transit gateway conecta las VPC. Para obtener información acerca de cómo crear una transit gateway, consulte [Crear una transit gateway](#) en la Guía de transit gateways de Amazon VPC.
- Para cada VPC, hay una conexión de VPC a la transit gateway en la zona de disponibilidad principal de la zona de Wavelength. Para obtener más información, consulte [Creación de una conexión de transit gateway a VPC](#) en Guía de Transit Gateways de Amazon VPC.

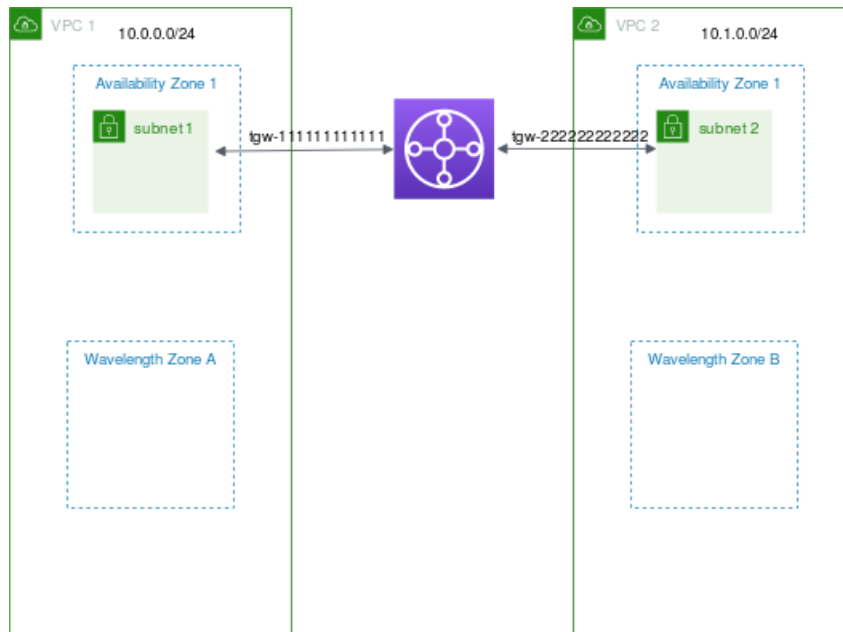
- Entradas para cada VPC en la tabla de enrutamiento de la transit gateway. Para obtener información acerca de cómo crear rutas de transit gateway, consulte [Tablas de enrutamiento de la transit gateway](#) en la Guía de transit gateway de Amazon VPC.
- Para cada VPC, una entrada en la tabla de enrutamiento de la VPC que tiene el otro CIDR de la VPC como destino y el ID de transit gateway como destino. Para obtener más información, consulte [the section called “Enrutar para una transit gateway” \(p. 94\)](#).

En el ejemplo, la tabla de enrutamiento para VPC 1 tiene la siguiente entrada:

Destino	Objetivo
10.1.0.0/24	tgw-2222222222222222

La tabla de enrutamiento para VPC 2 tiene la siguiente entrada:

Destino	Objetivo
10.0.0.0/24	tgw-2222222222222222



Subredes en AWS Outposts

AWS Outposts le ofrece las mismas herramientas, API, servicios e infraestructura de hardware de AWS para crear y ejecutar sus aplicaciones en las instalaciones y en la nube. AWS Outposts es ideal para cargas de trabajo que necesitan acceso de baja latencia a los sistemas o las aplicaciones en las instalaciones, así como para cargas de trabajo que necesitan almacenar y procesar datos de manera local. Para obtener más información acerca de AWS Outposts, consulte [AWS Outposts](#).

Amazon VPC abarca todas las zonas de disponibilidad de una región de AWS. Al conectar Outposts a la región principal, todas las VPC existentes y creadas recientemente en la cuenta abarcan todas las zonas de disponibilidad y cualquier ubicación de Outpost asociada de la región.

Las siguientes reglas se aplican a AWS Outposts:

- Las subredes deben residir en una ubicación de Outpost.
- Una gateway local gestiona la conectividad de red entre la VPC y las redes en las instalaciones. Para obtener información acerca de las gateways locales, consulte [Gateways locales](#) en la Guía del usuario de AWS Outposts.
- Si su cuenta está asociada a AWS Outposts, debe asignar la subred a un Outpost especificando el ARN del Outpost cuando cree la subred.
- De forma predeterminada, cada subred que crea en una VPC asociada a un Outpost hereda la tabla de ruteo de la VPC principal, incluida la ruta de la gateway local. También puede asociar explícitamente una tabla de ruteo personalizada a las subredes de la VPC y tener una gateway local como destino del siguiente salto para todo el tráfico que se tiene que enrutar en la red en las instalaciones.

Subredes para la VPC

Una subred es un rango de direcciones IP en su VPC. Puede lanzar recursos de AWS en una subred especificada. Utilice una subred pública para los recursos que deben conectarse a Internet y una subred privada para los recursos que no dispondrán de conexión a Internet.

Para proteger los recursos de AWS de cada subred, puede utilizar varias capas de seguridad, como grupos de seguridad y listas de control de acceso a la red (ACL).

Contenido

- [Conceptos básicos sobre subredes \(p. 60\)](#)
- [Tamaño de subred \(p. 62\)](#)
- [Enrutar la subred \(p. 63\)](#)
- [Seguridad de la subred \(p. 64\)](#)
- [Trabajar con subredes \(p. 64\)](#)
- [Utilizar reservas de CIDR de subred \(p. 68\)](#)
- [Agrupar bloques de CIDR mediante listas de prefijos \(p. 70\)](#)
- [Configurar tablas de enrutamiento \(p. 81\)](#)
- [Controlar el tráfico hacia las subredes utilizando las ACL de red \(p. 120\)](#)

Conceptos básicos sobre subredes

Una subred es un rango de direcciones IP en su VPC. Puede iniciar recursos de AWS, como las instancias EC2, en una subred específica. Al crear una subred, debe especificar el bloque de CIDR IPv4 de la subred, que es un subconjunto del bloque de CIDR de la VPC. Cada subred debe residir enteramente en una zona de disponibilidad y no puede abarcar otras zonas. Al lanzar instancias en distintas zonas de disponibilidad, puede proteger sus aplicaciones de los errores que se produzcan en una única zona.

De forma opcional, puede agregar subredes en una zona local, que es una implementación de la infraestructura de AWS que acerca los servicios de cómputo, almacenamiento, base de datos y otros servicios selectos a los usuarios finales. Una zona local permite que sus usuarios finales ejecuten aplicaciones que requieren latencias de milisegundos de un solo dígito. Para obtener más información, consulte [Local Zones](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Contenido

- [Tipos de subred \(p. 60\)](#)
- [Configuración de subredes \(p. 61\)](#)
- [Diagrama de la subred \(p. 61\)](#)

Tipos de subred

Cuando crea una subred, según las configuraciones establecidas para la VPC y las configuraciones que haya ajustado para la subred, tiene las siguientes opciones IPv4 e IPv6:

- Solo IPv4: la VPC está asociada a un CIDR de IPv4 o CIDR tanto de IPv4 como IPv6. Si los CIDR de subred que elige son rangos CIDR de IPv4, cualquier instancia EC2 lanzada dentro de la subred se comunicará solo a través de IPv4.
- Doble pila (IPv4 e IPv6): la VPC está asociada a un CIDR de IPv4 o varios CIDR de IPv4 e IPv6. Como resultado, cualquier subred que cree en la VPC puede ser subredes de doble pila. Cualquier instancia EC2 lanzada dentro de la subred se comunicará a través de la IP de la subred.
- Solo IPv6: la VPC está asociada a los CIDR tanto de IPv4 como de IPv6. Si selecciona la opción solo IPv6 al crear la subred, cualquier instancia EC2 lanzada dentro de la subred se comunicará solo a través de IPv6.

Según cómo configure la VPC, las subredes se pueden considerar públicas, privadas o solo de VPN:

- Subred pública: el tráfico IPv4 o IPv6 de la subred se dirige a una gateway de Internet o a una gateway de Internet solo de salida y puede llegar a la Internet pública. Para obtener más información, consulte [Conexión a Internet mediante una puerta de enlace de Internet \(p. 142\)](#).
- Subred privada: el tráfico IPv4 o IPv6 de la subred no se dirige a una gateway de Internet ni a una gateway de Internet solo de salida y no puede llegar a la Internet pública.
- Subred solo de VPN: la subred no tiene una ruta a la gateway de Internet, pero tiene el tráfico dirigido a una gateway privada virtual para la conexión de Site-to-Site VPN. Para obtener más información, consulte la [Guía del usuario de AWS Site-to-Site VPN](#).

Independientemente del tipo de subred, el intervalo de dirección IPv4 interno de la subred es siempre privado, es decir, no se anuncia el bloque de direcciones en Internet. Para obtener más información sobre direcciones IP privadas en las VPC, consulte [Direccionamiento IP \(p. 4\)](#).

Configuración de subredes

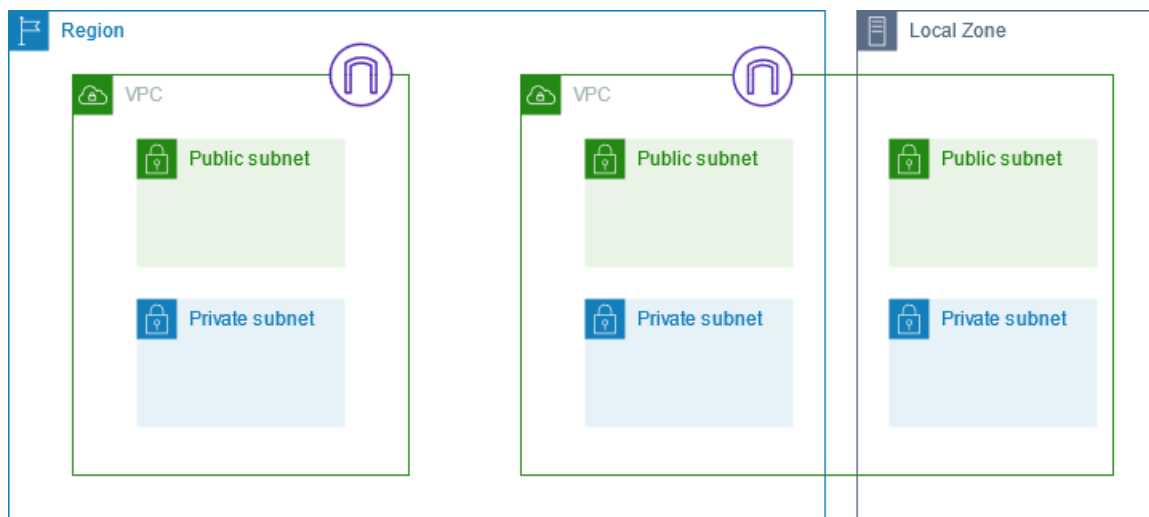
Todas las subredes tienen un atributo modificable que determina si se asigna a la interfaz de red creada en dicha subred una dirección IPv4 pública y, si procede, una dirección IPv6. Esto incluye la interfaz de red principal (eth0) que se crea para una instancia al lanzar una instancia en dicha subred. Independientemente del atributo de la subred, durante el lanzamiento podrá anular este parámetro para instancias específicas.

Cuando se haya creado una subred, podrá modificar la siguiente configuración para la subred.

- Configuración de IP de asignación automática: permite configurar los ajustes de IP de asignación automática a fin de solicitar automáticamente una dirección IPv4 o IPv6 pública para una nueva interfaz de red en esta subred.
- Configuración de nombre basado en recursos (RBN): permite especificar el tipo de nombre de host para las instancias EC2 de esta subred y configurar cómo se gestionan las consultas de registros DNS A y AAAA. Para obtener más información sobre esta configuración, consulte [Tipos de nombre de host de instancias de Amazon EC2](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Diagrama de la subred

El siguiente diagrama muestra dos VPC en una región. Cada VPC tiene subredes públicas y privadas y una puerta de enlace de Internet. La VPC de la derecha también abarca una zona local y tiene subredes en la zona local.



Tamaño de subred

El bloque de CIDR de una subred puede ser el mismo que el de la VPC (para una subred única de la VPC) o un subconjunto del mismo para la VPC (a fin de crear múltiples subredes en la VPC). El tamaño de bloque permitido oscila entre la máscara de subred /28 y /16. Si crea más de una subred en una VPC, los bloques de CIDR de las subredes no se pueden solapar.

Por ejemplo, si crea una VPC con un bloque de CIDR 10.0.0.0/24, esta admitirá 256 direcciones IP. Este bloque de CIDR se puede dividir en dos subredes con 128 direcciones IP cada una. Una subred utilizará el bloque de CIDR 10.0.0.0/25 (para el intervalo de direcciones 10.0.0.0 - 10.0.0.127) y la otra utilizará el bloque de CIDR 10.0.0.128/25 (para el intervalo de direcciones 10.0.0.128 - 10.0.0.255).

Existen herramientas en Internet que pueden servirle de ayuda para calcular y crear bloques de CIDR de subredes IPv4. Puede encontrar otras herramientas que se adapten a sus necesidades buscando términos como “calculadora de subred” o “calculadora de CIDR”. Además, su grupo de ingeniería de red podrá ayudarle a determinar los bloques de CIDR que debe especificar para las subredes.

Las cuatro primeras direcciones IP y la última dirección IP de cada bloque de CIDR de las subredes no se podrán utilizar y no se pueden asignar a un recurso, como una instancia de EC2. Por ejemplo, en una subred con el bloque de CIDR 10.0.0.0/24, estarán reservadas las cinco direcciones IP siguientes:

- 10.0.0.0: dirección de red.
- 10.0.0.1: reservada por AWS para el enrutador de la VPC.
- 10.0.0.2: reservada por AWS. La dirección IP del servidor DNS es la base del intervalo de red de la VPC más dos. En el caso de las VPC con varios bloques de CIDR, la dirección IP del servidor DNS se encuentra en el CIDR principal. También reservamos la base de cada intervalo de red más dos para todos los bloques de CIDR de la VPC. Para obtener más información, consulte [Servidor DNS de Amazon \(p. 42\)](#).
- 10.0.0.3: reservada por AWS para el uso futuro.
- 10.0.0.255: dirección de transmisión de red. Puesto que la difusión no se admite en las VPC, esta dirección queda reservada.

Si crea una subred mediante una herramienta de la línea de comandos o la API de Amazon EC2, el bloque de CIDR se modifica automáticamente a su forma canónica. Por ejemplo, si especifica 100.68.0.18/18 para el bloque de CIDR, creamos un bloque de CIDR de 100.68.0.0/18.

Ajuste de tamaño de subredes para direcciones IPv6

Si ha asociado un bloque de CIDR IPv6 a su VPC, podrá asociar un bloque de CIDR IPv6 a una subred existente en su VPC, o bien podrá crear una nueva subred. El bloque de CIDR IPv6 de una subred es una longitud de prefijo determinada de /64.

Hay herramientas disponibles en Internet para ayudarle a calcular y crear bloques de CIDR de subred IPv6; por ejemplo, [IPv6 Address Planner](#). Puede encontrar otras herramientas que se adapten a sus necesidades buscando términos como "calculadora de subred IPv6" o "calculadora de CIDR IPv6". Además, su grupo de ingeniería de red podrá ayudarle a determinar los bloques de CIDR IPv6 que debe especificar para las subredes.

Las cuatro primeras direcciones IPv6 y la última dirección IPv6 de cada bloque de CIDR de las subredes no se podrán utilizar y no se pueden asignar a una instancia de EC2. Por ejemplo, en una subred con el bloque de CIDR 2001:db8:1234:1a00/64, estarán reservadas las cinco direcciones IP siguientes:

- 2001:db8:1234:1a00::
- 2001:db8:1234:1a00::1
- 2001:db8:1234:1a00::2
- 2001:db8:1234:1a00::3
- 2001:db8:1234:1a00:ffff:ffff:ffff:ffff

Enrutar la subred

Cada subred debe estar asociada a una tabla de ruteo que, a su vez, especifica las rutas permitidas para el tráfico saliente de la subred. Cada subred que se crea se asocia automáticamente a la tabla de ruteo principal de la VPC. Es posible cambiar la asociación y el contenido de la tabla de ruteo principal. Para obtener más información, consulte [Configurar tablas de enrutamiento \(p. 81\)](#).

En el diagrama anterior, la tabla de ruteo asociada a la subred 1 direcciona todo el tráfico IPv4 (0.0.0.0/0) e IPv6 (:::/0) a un puerto de enlace a Internet (por ejemplo, igw-1a2b3c4d). Puesto que la instancia 1A tiene una dirección IP elástica IPv4 y una dirección IPv6, se puede acceder a ella desde Internet a través de IPv4 e IPv6.

(Solo IPv4) El acceso a la dirección IPv4 elástica o la dirección IPv4 pública asociada a su instancia se realiza a través del puerto de enlace a Internet de su VPC. El tráfico que pasa por la conexión de AWS Site-to-Site VPN entre su instancia y otra red atraviesa una gateway privada virtual y no la gateway de Internet; por lo tanto, no obtiene acceso a la dirección IPv4 elástica ni a la dirección IPv4 pública.

La instancia 2A no puede tener acceso a Internet, pero sí puede obtener acceso a otras instancias de la VPC. También puede permitir que una instancia de su VPC inicie conexiones salientes a Internet a través de IPv4 y bloquear las conexiones entrantes no deseadas procedentes de Internet mediante una instancia o una gateway de conversión de direcciones de red (NAT). Puesto que el número de direcciones IP elásticas que se puede asignar es limitado, se recomienda utilizar un dispositivo NAT si tiene más instancias que requieran dirección IP pública estática. Para obtener más información, consulte [Conexión a Internet u otras redes mediante dispositivos NAT \(p. 156\)](#). Para iniciar comunicaciones de solo salida a Internet mediante IPv6, puede utilizar un puerto de enlace a Internet de solo salida. Para obtener más información, consulte [Habilitar el tráfico IPv6 saliente mediante una puerta de enlace de Internet de solo salida \(p. 153\)](#).

La tabla de ruteo asociada a la subred 3 direcciona todo el tráfico IPv4 (0.0.0.0/0) a una gateway privada virtual (por ejemplo, vgw-1a2b3c4d). La instancia 3A puede acceder a los equipos de la red corporativa mediante la conexión de Site-to-Site VPN.

Seguridad de la subred

AWS proporciona dos características que puede utilizar para aumentar la seguridad de la VPC: los grupos de seguridad y las ACL de red. Los grupos de seguridad controlan el tráfico de entrada y salida de las instancias, mientras que las ACL de red controlan el tráfico de entrada y salida de las subredes. En la mayoría de los casos, los grupos de seguridad se ajustarán a sus necesidades. No obstante, puede usar también las ACL de red si desea agregar un nivel de seguridad adicional en la VPC. Para obtener más información, consulte [Privacidad del tráfico entre redes en Amazon VPC \(p. 233\)](#).

Por diseño, cada subred debe estar asociada a una ACL de red. Cada subred que se crea se asocia automáticamente a la ACL de red predeterminada de la VPC. Es posible cambiar la asociación y el contenido de la ACL de red predeterminada. Para obtener más información, consulte [Controlar el tráfico hacia las subredes utilizando las ACL de red \(p. 120\)](#).

Puede crear un log de flujo en su VPC o subred para capturar el flujo de tráfico entrante y saliente de las interfaces de red de su VPC o subred. También es posible crear un log de flujo en una interfaz de red individual. Para obtener más información, consulte [Registro del tráfico de IP con registros de flujo de la VPC \(p. 197\)](#).

Trabajar con subredes

Utilice los siguientes procedimientos para crear y configurar subredes para su nube virtual privada (VPC). Dependiendo de la conectividad que necesite, es posible que también deba agregar puertas de enlace y tablas de enrutamiento.

De manera alternativa, puede crear una VPC y sus subredes, puertas de enlace y tablas de enrutamiento en un solo paso. Para obtener más información, consulte [the section called “Crear VPC con el asistente” \(p. 291\)](#).

Tareas

- [Crear una subred en la VPC \(p. 64\)](#)
- [Ver las subredes \(p. 65\)](#)
- [Asociar un bloque de CIDR IPv6 a su subred \(p. 66\)](#)
- [Desasociar un bloque de CIDR IPv6 de la subred \(p. 66\)](#)
- [Modificar el atributo de direcciones IPv4 públicas de su subred \(p. 66\)](#)
- [Modificar el atributo de direcciones IPv6 de su subred \(p. 67\)](#)
- [Eliminar una subred \(p. 67\)](#)
- [Información general de la API y de los comandos \(p. 67\)](#)

Crear una subred en la VPC

Para agregar una nueva subred a su VPC, deberá especificar un bloque de CIDR IPv4 para la subred del rango de su VPC. Puede especificar la zona de disponibilidad en la que desea que se encuentre la subred. Puede tener varias subredes en la misma zona de disponibilidad.

Consideraciones

- También puede especificar un bloque de CIDR IPv6 para una subred si existe un bloque de CIDR IPv6 asociado a la VPC.
- Si crea una subred solo de IPv6, tenga en cuenta lo siguiente. Una instancia de EC2 lanzada en una subred de solo IPv6 recibe una dirección IPv6 pero no una dirección IPv4. Todas las instancias que lance en una subred de solo IPv6 deben ser [instancias integradas en el sistema Nitro](#).

- Para crear la subred en una zona local o en una zona Wavelength, debe habilitar la zona. Para obtener más información, consulte [Regiones y zonas](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Para añadir una subred a su VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets.
3. Elija Create subnet (Crear subred).
4. En VPC ID (ID de la VPC): elija la VPC para la subred.
5. (Opcional) En Subnet name (Nombre de la subred), ingrese un nombre para la subred. Esta acción creará una etiqueta con una clave de Name y el valor que especifique.
6. En Availability Zone (Zona de disponibilidad), puede elegir una zona para la subred o dejar la opción predeterminada No Preference (Sin preferencias) para que AWS elija una por usted.
7. Si la subred debe ser una subred de solo IPv6, elija IPv6-only (Solo IPv6). Esta opción está disponible solo si la VPC tiene un bloque de CIDR IPv6 asociado. Si elige esta opción, no podrá asociar un bloque de CIDR IPv4 a la subred.
8. En IPv4 CIDR block (Bloque de CIDR IPv4), ingrese el bloque de CIDR IPv4 de la subred. Por ejemplo, 10.0.1.0/24. Para obtener más información, consulte [Ajuste de tamaño de VPC para IPv4 \(p. 16\)](#). Si eligió IPv6-only (Solo IPv6), esta opción no está disponible.
9. En IPv6 CIDR block (bloque de CIDR IPv6), elija Custom IPv6 CIDR (CIDR IPv6 personalizado) y especifique el valor del par hexadecimal (por ejemplo, 00). Esta opción solo está disponible si la VPC tiene un bloque de CIDR IPv6 asociado.
10. Elija Create subnet (Crear subred).

Pasos siguientes

Cuando se haya creado la subred, podrá configurarla de la siguiente manera:

- Configurar el enrutamiento. A continuación, puede crear una tabla de enrutamiento personalizada y dirigir ese tráfico a una puerta de enlace asociada a la VPC, como una puerta de enlace de Internet. Para obtener más información, consulte [Configurar tablas de enrutamiento \(p. 81\)](#).
- Modificar el comportamiento del direccionamiento IP. Puede especificar si las instancias lanzadas en la subred reciben una dirección IPv4 pública, una dirección IPv6 o ambas. Para obtener más información, consulte [Configuración de subredes \(p. 61\)](#).
- Modificar la configuración del nombre basado en recursos (RBN). Para obtener más información, consulte [Tipos de nombres de host de instancias de Amazon EC2](#).
- Crear o modificar las ACL de la red. Para obtener más información, consulte [Controlar el tráfico hacia las subredes utilizando las ACL de red \(p. 120\)](#).
- Compartir la subred con otras cuentas. Para obtener más información, consulte [??? \(p. 48\)](#).

Ver las subredes

Utilice los pasos de la siguiente sección para ver los detalles de la subred.

Para ver las subredes en la región actual

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets.
3. Seleccione la casilla de verificación de la subred o elija el ID de la subred para abrir la página de detalles.

Para ver las subredes en las regiones

Abra la consola de Amazon EC2 Global View en <https://console.aws.amazon.com/ec2globalview/home>. Para obtener más información, consulte [Enumerar y filtrar recursos mediante Amazon EC2 Global View](#) en la Guía del usuario de instancias de Linux de Amazon EC2.

Asociar un bloque de CIDR IPv6 a su subred

Puede asociar un bloque de CIDR IPv6 a una subred existente de su VPC. La subred no puede tener ningún bloque de CIDR IPv6 asociado.

Para asociar un bloque de CIDR IPv6 a una subred

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets.
3. Seleccione su subred y elija Actions (Acciones), Edit IPv6 CIDRs (Editar CIDR IPv6).
4. Elija Add IPv6 CIDR. Especifique el par hexadecimal de la subred (por ejemplo, `00`).
5. Seleccione Save.

Desasociar un bloque de CIDR IPv6 de la subred

Si ya no desea que la subred admita IPv6 pero desea seguir utilizando la subred para crear y comunicarse con recursos IPv4, puede desasociar el bloque de CIDR IPv6.

Para anular la asociación de un bloque de CIDR IPv6, primero deberá anular la asignación de las direcciones IPv6 asignadas a las instancias de su subred.

Para desasociar un bloque de CIDR IPv6 de una subred

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets.
3. Seleccione la subred y elija Actions (Acciones), Edit IPv6 CIDRs (Editar CIDR IPv6).
4. Busque el bloque de CIDR IPv6 y elija Remove (Eliminar).
5. Seleccione Save.

Modificar el atributo de direcciones IPv4 públicas de su subred

De forma predeterminada, las subredes no predeterminadas tienen el atributo de direcciones IPv4 públicas configurado como `false`, mientras que las subredes predeterminadas tienen este atributo configurado como `true`. Las subredes no predeterminadas creadas por el asistente de instancias de lanzamiento de Amazon EC2 son una excepción, el asistente establece el atributo en `true`. Este atributo puede modificarse con la consola de Amazon VPC.

Para modificar el comportamiento de las direcciones IPv4 públicas de su subred

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets.
3. Seleccione su subred y elija Actions (Acciones), Edit subnet settings (Editar la configuración de subredes).

4. Si se activa la casilla de verificación Enable auto-assign public IPv4 address, se solicitará una dirección IPv4 pública para todas las instancias que se lancen en la subred seleccionada. Active o desactive la casilla de verificación según sea necesario y, a continuación, elija Save.

Modificar el atributo de direcciones IPv6 de su subred

De forma predeterminada, todas las subredes tienen el atributo de direcciones IPv6 configurado como `false`. Este atributo puede modificarse con la consola de Amazon VPC. Si habilita el atributo de direcciones IPv6 para su subred, las interfaces de red creadas en la subred recibirán una dirección IPv6 del rango de la subred. Las instancias lanzadas en la subred recibirán una dirección IPv6 en la interfaz de red principal.

Su subred debe tener asociado un bloque de CIDR IPv6.

Note

Si habilita la característica de direcciones IPv6 para la subred, la interfaz de red o la instancia solo reciben una dirección IPv6 si se crean con la versión 2016-11-15 o más reciente de la API de Amazon EC2. La consola de Amazon EC2 utiliza la versión de la API más reciente.

Para modificar el comportamiento de las direcciones IPv6 de su subred

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets.
3. Seleccione su subred y elija Actions (Acciones), Edit subnet settings (Editar la configuración de subredes).
4. Si se activa la casilla de verificación Enable auto-assign public IPv6 address, se solicitará una dirección IPv6 para todas las interfaces de red que se creen en la subred seleccionada. Active o desactive la casilla de verificación según sea necesario y, a continuación, elija Save.

Eliminar una subred

Si ya no necesita una subred, puede eliminarla. No se puede eliminar una subred si contiene alguna interfaz de red. Por ejemplo, debe terminar cualquier instancia en una subred antes de poder eliminarla.

Para eliminar una subred

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Termine todas las instancias de la subred. Para obtener más información, consulte [Terminar la instancia](#) en la Guía del usuario de EC2.
3. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
4. En el panel de navegación, elija Subnets.
5. Seleccione la subred y elija Actions (Acciones), Delete subnet (Eliminar subred).
6. Cuando se le pida confirmación, escriba **delete** y elija Delete (Eliminar).

Información general de la API y de los comandos

Puede realizar las tareas descritas en esta página utilizando la línea de comandos o una API. Para obtener más información acerca de las interfaces de la línea de comando, junto con una lista de las acciones de API disponibles, consulte [Acceder a Amazon VPC](#) (p. 2).

Agregado de una subred

- [create-subnet](#) (AWS CLI)
- [New-EC2Subnet](#) (AWS Tools for Windows PowerShell)

Describir las subredes

- [describe-subnets](#) (AWS CLI)
- [Get-EC2Subnet](#) (AWS Tools for Windows PowerShell)

Asociar un bloque de CIDR IPv6 a una subred

- [associate-subnet-cidr-block](#) (AWS CLI)
- [Register-EC2SubnetCidrBlock](#) (AWS Tools for Windows PowerShell)

Desasociar un bloque de CIDR IPv6 de una subred

- [disassociate-subnet-cidr-block](#) (AWS CLI)
- [Unregister-EC2SubnetCidrBlock](#) (AWS Tools for Windows PowerShell)

Eliminar una subred

- [delete-subnet](#) (AWS CLI)
- [Remove-EC2Subnet](#) (AWS Tools for Windows PowerShell)

Utilizar reservas de CIDR de subred

Una reserva de CIDR de subred es un rango de direcciones IPv4 o IPv6 de una subred. Cuando crea la reserva, debe especificar cómo va a utilizar el rango reservado. Están disponibles las siguientes opciones:

- Prefijo: puede asignar direcciones IP a las interfaces de red asociadas a una instancia. A fin de obtener más información, consulte [Asignación de prefijos a interfaces de red de Amazon EC2](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
- Explícito: AWS no se utilizan las direcciones IP. Las direcciones IP se asignan de forma manual a los recursos que se encuentran en la subred.

Las siguientes reglas aplican a las reservas de CIDR de subred:

- Puede reservar varios rangos de CIDR por subred. Los tipos de reserva para cada rango pueden ser ambos del mismo tipo (por ejemplo prefijo), o diferentes (por ejemplo, prefijo y explícito).
- Cuando se reservan varios rangos de CIDR dentro de la misma VPC, los rangos de CIDR no se superponen.
- Cuando reserva más de un rango en una subred para la Delegación de prefijos y esta está configurada para la asignación automática, elegimos de forma aleatoria una dirección IP para asignarla a la interfaz de red.
- Si se quita una reserva, las direcciones IP asignadas a los recursos no se modifican. Solo estarán disponibles las direcciones IP que no estén en uso.

Trabaje con reservas de CIDR de subred mediante la consola

Puede crear y administrar las reservas de CIDR de subred como se explica a continuación.

Para editar las reservas de CIDR de subred

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets.
3. Seleccione la subred.
4. Seleccione Actions (Acciones), luego, Edit CIDR reservations (Editar reservas de CIDR) y realice lo siguiente:
 - Para agregar una reserva de CIDR IPv4, elija IPv4, luego, Add IPv4 CIDR reservation (Agregar reserva de CIDR IPv4). Elija el tipo de reserva, ingrese el rango CIDR y elija Add (Agregar).
 - Para agregar una reserva de CIDR IPv6, elija IPv6 y, a continuación, Add IPv6 CIDR reservation (Agregar reserva de CIDR IPv6). Elija el tipo de reserva, ingrese el rango CIDR y elija Add (Agregar).
 - Para eliminar una reserva CIDR, elija Remove (Eliminar) al final de la entrada.

Trabajar con reservas de CIDR de subred mediante la AWS CLI

Puede utilizar la AWS CLI para crear y administrar reservas de CIDR de subred.

Tareas

- [Cómo crear una reserva de CIDR de subred \(p. 69\)](#)
- [Cómo visualizar las reservas de CIDR de subred \(p. 69\)](#)
- [Cómo eliminar una reserva de CIDR de subred \(p. 70\)](#)

Cómo crear una reserva de CIDR de subred

Puede usar [create-subnet-cidr-reservation](#) para crear una reserva de CIDR de subred.

```
aws ec2 create-subnet-cidr-reservation --subnet-id subnet-03c51e2eEXAMPLE --reservation-type prefix --cidr 2600:1f13:925:d240:3a1b::/80
```

A continuación, se muestra un ejemplo del resultado.

```
{
  "SubnetCidrReservation": {
    "SubnetCidrReservationId": "scr-044f977c4eEXAMPLE",
    "SubnetId": "subnet-03c51e2ef5EXAMPLE",
    "Cidr": "2600:1f13:925:d240:3a1b::/80",
    "ReservationType": "prefix",
    "OwnerId": "123456789012"
  }
}
```

Cómo visualizar las reservas de CIDR de subred

Puede usar [get-subnet-cidr-reservations](#) para ver los detalles de una reserva CIDR de subred.

```
aws ec2 get-subnet-cidr-reservations --subnet-id subnet-05eef9fb78EXAMPLE
```

Cómo eliminar una reserva de CIDR de subred

Puede usar [create-subnet-cidr-reservation](#) para eliminar una reserva de CIDR de subred.

```
aws ec2 delete-subnet-cidr-reservation --subnet-cidr-reservation-id scr-044f977c4eEXAMPLE
```

Agrupar bloques de CIDR mediante listas de prefijos

Una lista de prefijos es un conjunto de uno o más bloques CIDR. Puede utilizar listas de prefijos para facilitar la configuración y el mantenimiento de los grupos de seguridad y las tablas de enrutamiento. Puede crear una lista de prefijos a partir de las direcciones IP que utilice con frecuencia y hacer referencia a ellas como un conjunto en las reglas y rutas de los grupos de seguridad, en lugar de individualmente. Por ejemplo, puede consolidar reglas de grupos de seguridad con diferentes bloques de CIDR pero el mismo puerto y protocolo en una única regla que utilice una lista de prefijos. Si amplía su red y necesita permitir el tráfico desde otro bloque de CIDR, puede actualizar la lista de prefijos correspondiente y se actualizarán todos los grupos de seguridad que utilicen esa lista de prefijos.

Hay dos tipos de listas de prefijos:

- Listas de prefijos administradas por el cliente: conjuntos de rangos de direcciones IP definidas y administradas por usted. Puede compartir su lista de prefijos con otras cuentas de AWS, lo que permite que esas cuentas hagan referencia a la lista de prefijos en sus propios recursos.
- Listas de prefijos administradas por AWS: conjuntos de rangos de direcciones IP para los servicios de AWS. No puede crear, modificar, compartir ni eliminar una lista de prefijos administrada por AWS.

Contenido

- [Conceptos y reglas de las listas de prefijos \(p. 70\)](#)
- [Administración de identidades y accesos para listas de prefijos \(p. 71\)](#)
- [Trabajar con listas de prefijos administradas por el cliente \(p. 72\)](#)
- [Trabajar con listas de prefijos administradas por AWS \(p. 77\)](#)
- [Trabajar con listas de prefijos compartidas \(p. 78\)](#)

Conceptos y reglas de las listas de prefijos

Una lista de prefijos consta de entradas. Cada entrada consta de un bloque CIDR y, opcionalmente, de una descripción para el bloque CIDR.

Listas de prefijos administradas por el cliente

Las siguientes reglas se aplican a las listas de prefijos administradas por el cliente:

- Una lista de prefijos solo admite un único tipo de direccionamiento IP (IPv4 o IPv6). No puede combinar bloques CIDR IPv4 e IPv6 en una única lista de prefijos.
- Una lista de prefijos solo se aplica a la región donde la creó.

- Al crear una lista de prefijos, debe especificar el número máximo de entradas que puede admitir la lista de prefijos.
- Cuando se hace referencia a una lista de prefijos de un recurso, el número máximo de entradas de las listas de prefijos cuenta respecto de la cuota correspondiente al número de entradas del recurso. Por ejemplo, si crea una lista de prefijos con un máximo de 20 entradas y hace referencia a esa lista de prefijos en una regla de un grupo de seguridad, cuenta como 20 reglas de grupos de seguridad.
- Cuando hace referencia a una lista de prefijos en una tabla de ruteo, se aplican las reglas de prioridad de ruta. Para obtener más información, consulte [Listas de prefijos y prioridad de ruta \(p. 90\)](#).
- Puede modificar una lista de prefijos. Cuando agrega o elimina entradas, creamos una nueva versión de la lista de prefijos. Los recursos que hacen referencia al prefijo siempre usan la versión actual (la más reciente). Puede restaurar las entradas de una versión anterior de la lista de prefijos, que también crea a una nueva versión.
- Hay cuotas relacionadas con las listas de prefijos. Para obtener más información, consulte [Listas de prefijos administradas por el cliente \(p. 379\)](#).

AWSListas de prefijos administradas por

Las siguientes reglas se aplican a las listas de prefijos administradas por AWS:

- No puede crear, modificar, compartir ni eliminar una lista de prefijos administrada por AWS.
- Las diferentes listas de prefijos administradas por AWS tienen un peso diferente al utilizarlas. Para obtener más información, consulte [Peso de una lista de prefijos administrada por AWS \(p. 77\)](#).
- No se puede ver el número de la versión de una lista de prefijos administrada por AWS.

Administración de identidades y accesos para listas de prefijos

De forma predeterminada, los usuarios de IAM no tienen permiso para crear, consultar, modificar ni eliminar listas de prefijos. Puede crear una política de IAM que permita a los usuarios trabajar con listas de prefijos.

Para consultar una lista de acciones de Amazon VPC y las claves de recursos y condición que puede utilizar en una política de IAM, consulte [Acciones, recursos y claves de condición para Amazon EC2](#) en la Guía del usuario de IAM.

El siguiente ejemplo de política permite a los usuarios ver y trabajar con la lista de prefijos `pl-123456abcde123456` solamente. Los usuarios no pueden crear ni eliminar listas de prefijos.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:GetManagedPrefixListAssociations",
      "ec2:GetManagedPrefixListEntries",
      "ec2:ModifyManagedPrefixList",
      "ec2:RestoreManagedPrefixListVersion"
    ],
    "Resource": "arn:aws:ec2:region:account:prefix-list/pl-123456abcde123456"
  },
  {
    "Effect": "Allow",
    "Action": "ec2:DescribeManagedPrefixLists",
    "Resource": "*"
  }
]
```

```
} ]
```

Para obtener más información sobre el uso de IAM en Amazon VPC, consulte [Identity and Access Management para Amazon VPC](#) (p. 237).

Trabajar con listas de prefijos administradas por el cliente

Puede crear y administrar listas de prefijos administradas por el cliente. Puede ver listas de prefijos administradas por AWS.

Tareas

- [Crear una lista de prefijos](#) (p. 72)
- [Ver las listas de prefijos](#) (p. 73)
- [Ver las entradas de una lista de prefijos](#) (p. 73)
- [Ver las asociaciones \(referencias\) de su lista de prefijos](#) (p. 73)
- [Modifique una lista de prefijos](#) (p. 74)
- [Cambiar una lista de prefijos](#) (p. 74)
- [Restaurar una versión anterior de una lista de prefijos](#) (p. 75)
- [Eliminar una lista de prefijos](#) (p. 75)
- [Listas de prefijos de referencia en sus recursos de AWS](#) (p. 75)

Crear una lista de prefijos

Al crear una lista de prefijos, debe especificar el número máximo de entradas que puede admitir la lista de prefijos.

Limitación

No se puede agregar una lista de prefijos a una regla de grupo de seguridad si el número de reglas más el máximo de entradas de la lista de prefijos supera la cuota de reglas por grupo de seguridad de su cuenta.

Para crear una lista de prefijos mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Managed Prefix Lists (Listas de prefijos administradas).
3. Elija Create prefix list (Crear lista de prefijos).
4. En Prefix list name (Nombre de lista de prefijos), escriba un nombre para la lista de prefijos.
5. En Max entries (Entradas máximas), introduzca el número máximo de entradas para la lista de prefijos.
6. En Address family (Familia de direcciones), elija si la lista de prefijos admite entradas IPv4 o IPv6.
7. En Prefix list entries (Entradas de lista de prefijos), elija Add new entry (Agregar nueva entrada), e introduzca el bloque CIDR y una descripción para la entrada. Repita este paso para cada entrada.
8. (Opcional) En Tags (Etiquetas), agregue etiquetas a la lista de prefijos para ayudarle a identificarlas más adelante.
9. Elija Create prefix list (Crear lista de prefijos).

Para crear una lista de prefijos mediante la AWS CLI

Utilice el comando `create-managed-prefix-list`.

Ver las listas de prefijos

Puede ver sus listas de prefijos, las listas de prefijos que se comparten con usted y las listas de prefijos administradas por AWS.

Para ver listas de prefijos mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Managed Prefix Lists (Listas de prefijos administradas).
3. La columna Owner ID (ID del propietario) muestra el ID de la cuenta de AWS del propietario de la lista de prefijos. En las listas de prefijos administradas por AWS, el Owner ID (ID del propietario) es AWS.

Para ver listas de prefijos mediante la AWS CLI

Utilice el comando `describe-managed-prefix-lists`.

Ver las entradas de una lista de prefijos

Puede ver las entradas para sus listas de prefijos, las listas de prefijos que se comparten con usted y las listas de prefijos administradas por AWS.

Para ver las entradas de una lista de prefijos mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Managed Prefix Lists (Listas de prefijos administradas).
3. Seleccione la casilla de verificación de la lista de prefijos.
4. En el panel inferior, elija Entries (Entradas) para ver las entradas de la lista de prefijos.

Para ver las entradas de una lista de prefijos mediante la AWS CLI

Utilice el comando `get-managed-prefix-list-entries`.

Ver las asociaciones (referencias) de su lista de prefijos

Puede ver los ID y los propietarios de los recursos asociados a su lista de prefijos. Los recursos asociados son recursos que hacen referencia a la lista de prefijos en sus entradas o reglas.

Limitación

No se pueden ver los recursos asociados de una lista de prefijos administrada por AWS.

Para ver asociaciones de listas de prefijos mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Managed Prefix Lists (Listas de prefijos administradas).
3. Seleccione la casilla de verificación de la lista de prefijos.
4. En el panel inferior, elija Associations (Asociaciones) para ver los recursos que hacen referencia a la lista de prefijos.

Para ver asociaciones de listas de prefijos mediante la AWS CLI

Utilice el comando [get-managed-prefix-list-associations](#).

Modifique una lista de prefijos

Puede modificar el nombre de la lista de prefijos y añadir o eliminar entradas. Para modificar el número máximo de entradas, consulte [Cambiar una lista de prefijos \(p. 74\)](#).

Al actualizar las entradas de una lista de prefijos se crea una nueva versión de la lista de prefijos. Para actualizar el nombre o el número máximo de entradas de una lista de prefijos no se crea una nueva versión de la lista de prefijos.

Consideraciones

- No se puede modificar una lista de prefijos administrada por AWS.
- Cuando aumenta el número máximo de entradas en una lista de prefijos, se aplica el tamaño máximo aumentado a la cuota de entradas de los recursos que hacen referencia a la lista de prefijos. Si alguno de estos recursos no admite el tamaño máximo aumentado, se produce un error en la operación de modificación y se restaura el tamaño máximo anterior.

Para modificar una lista de prefijos mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Managed Prefix Lists (Listas de prefijos administradas).
3. Seleccione la casilla de verificación de la lista de prefijos y elija Actions (Acciones), Modify prefix list (Modificar lista de prefijos).
4. En Prefix list name (Nombre de la lista de prefijos), escriba un nuevo nombre para la lista de prefijos.
5. En Prefix list entries (Entradas de la lista de prefijos), elija Remove (Eliminar) para eliminar una entrada existente. Para añadir una nueva entrada, elija Add new entry (Añadir nueva entrada) e introduzca el bloque de CIDR y una descripción para la entrada.
6. Elija Save prefix list (Guardar lista de prefijos).

Para modificar una lista de prefijos mediante la AWS CLI

Utilice el comando [modify-managed-prefix-list](#).

Cambiar una lista de prefijos

Puede cambiar el tamaño de una lista de prefijos y modificar el número máximo de entradas en la lista de prefijos. El valor debe ser mayor o igual que el número de entradas de lista de prefijos. El nuevo valor debe ser mayor al valor actual.

Para cambiar una lista de prefijos mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Managed Prefix Lists (Listas de prefijos administradas).
3. Seleccione la casilla de verificación de la lista de prefijos y elija Actions (Acciones), Restore prefix list (Restaurar lista de prefijos).
4. Para New max entries (Nuevo máximo de entradas), introduzca un valor.
5. Elija Resize (Cambiar tamaño).

Para crear una lista de prefijos mediante la AWS CLI

Utilice el comando [modify-managed-prefix-list](#).

Restaurar una versión anterior de una lista de prefijos

Puede restaurar las entradas de una versión anterior de su lista de prefijos. De esta forma, se crea una versión nueva de la lista de prefijos.

Si ha disminuido el tamaño de la lista de prefijos, debe asegurarse de que la lista de prefijos es lo suficientemente grande como para contener las entradas de la versión anterior.

Para restaurar una versión anterior de una lista de prefijos mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Managed Prefix Lists (Listas de prefijos administradas).
3. Seleccione la casilla de verificación de la lista de prefijos y elija Actions (Acciones), Restore prefix list (Restaurar lista de prefijos).
4. Para Select prefix list version (Seleccione la versión de la lista de prefijos), elija una versión anterior. Las entradas de la versión seleccionada se muestran en Prefix list entries (Entradas de lista de prefijos).
5. Elija Restore prefix list (Restaurar lista de prefijos).

Para restaurar una versión anterior de una lista de prefijos mediante la AWS CLI

Utilice el comando [restore-managed-prefix-list-version](#).

Eliminar una lista de prefijos

Para eliminar una lista de prefijos, primero debe eliminar cualquier referencia a ella que haya en los recursos (como en las tablas de ruteo). Si ha compartido la lista de prefijos mediante AWS RAM, primero debe eliminar cualquier referencia que haya en los recursos propiedad del consumidor.

Limitación

No se puede eliminar una lista de prefijos administrada por AWS.

Para eliminar una lista de prefijos mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Managed Prefix Lists (Listas de prefijos administradas).
3. Seleccione la lista de prefijos y elija Actions (Acciones), Delete prefix list (Eliminar lista de prefijos).
4. En el cuadro de diálogo de confirmación, escriba `delete` y elija Delete (Eliminar).

Para eliminar una lista de prefijos mediante la AWS CLI

Utilice el comando [delete-managed-prefix-list](#).

Listas de prefijos de referencia en sus recursos de AWS

Puede hacer referencia a una lista de prefijos en los siguientes recursos de AWS.

Recursos

- [Grupos de seguridad de la VPC \(p. 76\)](#)
- [Tablas de enrutamiento de subred \(p. 76\)](#)

- [Tablas de enrutamiento de la transit gateway](#) (p. 76)

Grupos de seguridad de la VPC

Puede especificar una lista de prefijos como origen de una regla de entrada o como destino de una regla de salida. Para obtener más información acerca de los grupos de seguridad, consulte [Controlar el tráfico hacia los recursos mediante grupos de seguridad](#) (p. 255).

Para hacer referencia a una lista de prefijos en una regla de grupo de seguridad mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Seleccione el grupo de seguridad que desea actualizar.
4. Elija Actions (Acciones), Edit inbound rules (Editar reglas de entrada) o Actions (Acciones), Edit outbound rules (Editar reglas de salida).
5. Seleccione Add rule (Agregar regla). En Type (Tipo), seleccione el tipo de tráfico. En Source (Origen) (reglas de entrada) o Destination (Destino) (reglas de salida), elija el ID de la lista de prefijos.
6. Seleccione Save rules (Guardar reglas).

Para hacer referencia a una lista de prefijos en una regla de grupo de seguridad mediante la AWS CLI

Utilice los comandos [authorize-security-group-ingress](#) y [authorize-security-group-egress](#). Para el parámetro `--ip-permissions`, especifique el ID de la lista de prefijos mediante `PrefixListIds`.

Tablas de enrutamiento de subred

Puede especificar una lista de prefijos como destino de la entrada de la tabla de enrutamiento. No puede hacer referencia a una lista de prefijos en una tabla de ruteo de gateway. Para obtener más información acerca de las tablas de ruteo, consulte [Configurar tablas de enrutamiento](#) (p. 81).

Para hacer referencia a una lista de prefijos en una tabla de ruteo mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables (Tablas de ruteo) y, a continuación, seleccione la tabla de ruteo.
3. Elija Actions (Acciones), Edit routes (Editar rutas).
4. Para agregar una ruta, elija Add route (Añadir ruta).
5. En Destination (Destino), introduzca el ID de una lista de prefijos.
6. En Target (Objetivo), elija un objetivo.
7. Elija Save changes.

Para hacer referencia a una lista de prefijos en una tabla de ruteo mediante la AWS CLI

Utilice el comando [create-route](#) (AWS CLI). Utilice el parámetro `--destination-prefix-list-id` para especificar el ID de una lista de prefijos.

Tablas de enrutamiento de la transit gateway

Puede especificar una lista de prefijos como destino de una ruta. Para obtener más información, consulte [Referencias de listas de prefijos](#) en Transit gateways en Amazon VPC.

Trabajar con listas de prefijos administradas por AWS

Las listas de prefijos administradas por AWS son conjuntos de rangos de direcciones IP para los servicios de AWS.

Contenido

- [Utilizar una lista de prefijos administrada por AWS \(p. 77\)](#)
- [Peso de una lista de prefijos administrada por AWS \(p. 77\)](#)

Utilizar una lista de prefijos administrada por AWS

Las listas de prefijos administradas por AWS se crean y mantienen mediante AWS y pueden utilizarlas cualquier persona con una cuenta de AWS. No puede crear, modificar, compartir ni eliminar una lista de prefijos administrada por AWS.

Puede ver las listas de prefijos administradas por AWS y los ID de las listas de prefijos de las siguientes formas:

- Abra Managed Prefix Lists (Listas de prefijos administradas) en el panel de navegación de la consola de Amazon VPC.
- Utilice el comando [describe-managed-prefix-lists](#) de AWS CLI.
- Utilice la API [DescribeManagedPrefixLists](#).

Los siguientes listas de prefijos administradas por AWS están disponibles:

Nombre de una lista de prefijos	AWSServicio de
com.amazonaws.region.s3	Simple Storage Service (Amazon S3)
com.amazonaws.region.dynamodb	DynamoDB
com.amazonaws.global.cloudfront.origin-facing	Amazon CloudFront

Al igual que con las listas de prefijos administradas por el cliente, las listas de prefijos administradas por AWS pueden utilizarse con recursos de AWS tales como grupos de seguridad y tablas de enrutamiento. Para obtener más información, consulte [Listas de prefijos de referencia en sus recursos de AWS \(p. 75\)](#).

Peso de una lista de prefijos administrada por AWS

El peso de una lista de prefijos administrada por AWS hace referencia al número de entradas que adoptará una lista de prefijos de un recurso.

Nombre de una lista de prefijos	AWSServicio de	Weight
com.amazonaws.region.s3	Simple Storage Service (Amazon S3)	1
com.amazonaws.region.dynamodb	DynamoDB	1
com.amazonaws.global.cloudfront.origin-facing	Amazon CloudFront	55

El peso de una lista de prefijos administrada por Amazon CloudFront es única en cuanto a cómo afecta a las cuotas de Amazon VPC:

- Cuenta como 55 reglas en un grupo de seguridad. La [cuota predeterminada \(p. 381\)](#) es de 60 reglas, lo que deja espacio para solo 5 reglas adicionales en un grupo de seguridad. Puede [solicitar un aumento de la cuota](#).
- Cuenta como 55 rutas en una tabla de enrutamiento. La [cuota predeterminada \(p. 381\)](#) es de 50 rutas, así que debe [solicitar un aumento de la cuota](#) antes de poder agregar la lista de prefijos a una tabla de enrutamiento.

Para obtener más información, consulte [Utilizar la lista de prefijos administrados de CloudFront](#) en la Guía para desarrolladores de Amazon CloudFront.

Trabajar con listas de prefijos compartidas

Con AWS Resource Access Manager (AWS RAM), el propietario de una lista de prefijos puede compartir una lista de prefijos con:

- Cuentas específicas de AWS dentro o fuera de la organización en AWS Organizations
- Una unidad organizativa dentro de la organización en AWS Organizations
- Toda la organización en AWS Organizations

Los consumidores con los que se ha compartido una lista de prefijos pueden ver la lista de prefijos y sus entradas, y pueden hacer referencia a la lista de prefijos en sus recursos de AWS.

Para obtener más información acerca de AWS RAM, consulte la [Guía del usuario de AWS RAM](#).

Contenido

- [Requisitos previos para compartir listas de prefijos \(p. 78\)](#)
- [Compartir una lista de prefijos \(p. 78\)](#)
- [Identificar una lista de prefijos compartida \(p. 79\)](#)
- [Identificar referencias a una lista de prefijos compartida \(p. 79\)](#)
- [Dejar de compartir una lista de prefijos compartida \(p. 80\)](#)
- [Permisos de lista de prefijos compartida \(p. 80\)](#)
- [Facturación y medición \(p. 80\)](#)
- [Cuotas para AWS RAM \(p. 81\)](#)

Requisitos previos para compartir listas de prefijos

- Para compartir una lista de prefijos, debe ser su propietario. No puede compartir una lista de prefijos que se ha compartido con usted. No se puede compartir una lista de prefijos administrada por AWS.
- Para compartir una lista de prefijos con su organización o con una unidad organizativa en AWS Organizations, debe habilitar el uso compartido con AWS Organizations. Para obtener más información, consulte [Habilitar el uso compartido con AWS Organizations](#) en la Guía del usuario de AWS RAM.

Compartir una lista de prefijos

Para compartir una lista de prefijos, debe añadirla a un recurso compartido. Si no tiene un recurso compartido, primero debe crear uno mediante la [consola de AWS RAM](#).

Si forma parte de una organización en AWS Organizations y el uso compartido dentro de la organización está habilitado, los consumidores de la organización obtienen automáticamente acceso a la lista de prefijos compartida. De lo contrario, los consumidores reciben una invitación para unirse al recurso compartido y se les concede acceso a la lista de prefijos compartida después de aceptar la invitación.

Puede crear un recurso compartido y compartir una lista de prefijos de su propiedad mediante la consola de AWS RAM o la AWS CLI.

Para crear un recurso compartido y compartir una lista de prefijos mediante la consola de AWS RAM

Siga los pasos descritos en [Crear un recurso compartido](#) en la Guía del usuario de AWS RAM. En Select resource type (Seleccionar tipo de recurso), elija Prefix Lists (Listas de prefijos) y, a continuación, active la casilla de verificación de la lista de prefijos.

Para añadir una lista de prefijos a un recurso compartido existente mediante la consola de AWS RAM

Para agregar un prefijo administrado que sea de su propiedad a un recurso compartido existente, siga los pasos descritos en [Actualización de un recurso compartido](#) en la Guía del usuario de AWS RAM. En Select resource type (Seleccionar tipo de recurso), elija Prefix Lists (Listas de prefijos) y, a continuación, active la casilla de verificación de la lista de prefijos.

Para compartir una lista de prefijos de la que es propietario mediante la AWS CLI

Utilice los siguientes comandos para crear y actualizar un recurso compartido:

- [create-resource-share](#)
- [associate-resource-share](#)
- [update-resource-share](#)

Identificar una lista de prefijos compartida

Los propietarios y los consumidores pueden identificar listas de prefijos compartidas mediante la consola de Amazon VPC y AWS CLI.

Para identificar una lista de prefijos compartida mediante la consola de Amazon VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Managed Prefix Lists (Listas de prefijos administradas).
3. La página muestra las listas de prefijos de las que es propietario y las listas de prefijos que se comparten con usted. La columna Owner ID (ID del propietario) muestra el ID de la cuenta de AWS del propietario de la lista de prefijos.
4. Para ver la información de recurso compartido de una lista de prefijos, seleccione la lista de prefijos y elija Sharing (Compartir) en el panel inferior.

Para identificar una lista de prefijos compartida mediante la AWS CLI

Utilice el comando [describe-managed-prefix-lists](#). El comando devuelve las listas de prefijos de las que es propietario y las listas de prefijos que se comparten con usted. OwnerId muestra el ID de la cuenta de AWS del propietario de la lista de prefijos.

Identificar referencias a una lista de prefijos compartida

Los propietarios pueden identificar los recursos propiedad del consumidor que hacen referencia a una lista de prefijos compartida.

Para identificar referencias a una lista de prefijos compartida mediante la consola de Amazon VPC.

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Managed Prefix Lists (Listas de prefijos administradas).
3. Seleccione la lista de prefijos y elija Associations (Asociaciones) en el panel inferior.
4. Los ID de los recursos que hacen referencia a la lista de prefijos se muestran en la columna Resource ID (ID de recurso). Los propietarios de los recursos se muestran en la columna Resource Owner (Propietario del recurso).

Para identificar referencias a una lista de prefijos compartida mediante la AWS CLI

Utilice el comando [get-managed-prefix-list-associations](#).

Dejar de compartir una lista de prefijos compartida

Cuando deja de compartir una lista de prefijos, los consumidores ya no pueden ver la lista de prefijos ni sus entradas en su cuenta y no pueden hacer referencia a la lista de prefijos en sus recursos. Si ya hay referencias a la lista de prefijos en los recursos del consumidor, esas referencias seguirán funcionando con normalidad y podrá seguir [viendo esas referencias](#) (p. 79). Si actualiza la lista de prefijos a una nueva versión, las referencias utilizarán la versión más reciente.

Para dejar de compartir una lista de prefijos compartida que sea de su propiedad, debe quitarla del recurso compartido mediante AWS RAM.

Para dejar de compartir una lista de prefijos compartida de su propiedad mediante la consola de AWS RAM

Consulte [Actualización de un recurso compartido](#) en la Guía del usuario de AWS RAM.

Para dejar de compartir una lista de prefijos compartida de su propiedad mediante la AWS CLI

Utilice el comando [disassociate-resource-share](#).

Permisos de lista de prefijos compartida

Permisos de los propietarios

Los propietarios son responsables de administrar una lista de prefijos compartida y sus entradas. Los propietarios pueden ver los ID de los recursos de AWS que hacen referencia a la lista de prefijos. Sin embargo, no pueden agregar ni eliminar referencias a una lista de prefijos en los recursos de AWS que sean propiedad de los consumidores.

Los propietarios no pueden eliminar una lista de prefijos si esta tiene referencias en un recurso que es propiedad de un consumidor.

Permisos de los consumidores

Los consumidores pueden ver las entradas de una lista de prefijos compartida y pueden hacer referencia a una lista de prefijos compartida en sus recursos de AWS. Sin embargo, los consumidores no pueden modificar, restaurar o eliminar una lista de prefijos compartida.

Facturación y medición

No se aplican cargos adicionales por compartir listas de prefijos.

Cuotas para AWS RAM

Para obtener más información, consulte [Service Quotas](#).

Configurar tablas de enrutamiento

Las tablas de enrutamiento contienen conjuntos de reglas, denominadas rutas, que determinan adónde se dirige el tráfico de red desde la subred o puerta de enlace.

Contenido

- [Conceptos de las tablas de enrutamiento \(p. 81\)](#)
- [Tablas de enrutamiento de subred \(p. 82\)](#)
- [Tablas de ruteo de gateway \(p. 86\)](#)
- [Prioridad de la ruta \(p. 88\)](#)
- [Cuotas de la tabla de enrutamiento \(p. 90\)](#)
- [Opciones de enrutamiento de ejemplo \(p. 90\)](#)
- [Trabajar con tablas de ruteo \(p. 99\)](#)
- [Enrutamiento de Middlebox \(p. 106\)](#)

Conceptos de las tablas de enrutamiento

A continuación se enumeran los conceptos clave de las tablas de ruteo.

- **Tabla de enrutamiento principal:** la tabla de enrutamiento que viene de forma automática con la VPC. Controla el direccionamiento de todas las subredes que no están explícitamente asociadas a ninguna otra tabla de ruteo.
- **Tabla de enrutamiento personalizada:** una tabla de enrutamiento que se crea para la VPC.
- **Destino:** el intervalo de direcciones IP a las que desea que vaya el tráfico (CIDR de destino). Por ejemplo, una red corporativa externa con un CIDR 172.16.0.0/12.
- **Destino:** la gateway, interfaz de red o conexión a través de la cual enviar el tráfico de destino, por ejemplo, una gateway de Internet.
- **Asociación de tabla de enrutamiento:** la asociación entre una tabla de enrutamiento y una subred, gateway de Internet o gateway privada virtual.
- **Tabla de enrutamiento de subred:** una tabla de enrutamiento asociada con una subred.
- **Ruta local:** una ruta predeterminada para la comunicación dentro de la VPC.
- **Propagación:** la propagación de rutas permite que una gateway privada virtual propague rutas automáticamente a las tablas de enrutamiento. Esto significa que no es necesario introducir manualmente rutas de VPN en las tablas de ruteo. Para obtener más información acerca de las opciones de enrutamiento de VPN, consulte [Opciones de enrutamiento de Site-to-Site VPN](#) en la Guía del usuario de Site-to-Site VPN.
- **Tabla de enrutamiento de gateway:** una tabla de enrutamiento asociada con una gateway de Internet o gateway privada virtual.
- **Asociación de borde:** una tabla de enrutamiento que se utiliza para enrutar el tráfico de VPC entrante a un dispositivo. Asocie una tabla de ruteo a la gateway de Internet o a la gateway privada virtual y especifique la interfaz de red del dispositivo como objetivo para el tráfico de la VPC.
- **Tabla de enrutamiento de la transit gateway:** una tabla de enrutamiento asociada con una transit gateway. Para obtener más información, consulte [Tablas de enrutamiento de Transit Gateway](#) en Transit Gateways de Amazon VPC.

- Tabla de enrutamiento de gateway local: una tabla de enrutamiento asociada con una gateway local de Outposts. Para obtener más información, consulte [Gateways locales](#) en la Guía del usuario de AWS Outposts.

Tablas de enrutamiento de subred

Su VPC tiene un enrutador implícito y utiliza las tablas de ruteo para controlar dónde se dirige el tráfico de red. Cada subred de la VPC debe estar asociada a una tabla de ruteo que controla el direccionamiento de la subred (tabla de ruteo de la subred). Puede asociar de forma explícita una subred con una tabla de ruteo particular. De lo contrario, la subred se asocia de forma implícita con la tabla de ruteo principal. La subred solo puede asociarse a una tabla de ruteo a la vez. Sin embargo, puede asociar varias subredes a la misma tabla de ruteo de la subred.

Contenido

- [Rutas \(p. 82\)](#)
- [Tabla de enrutamiento principal \(p. 83\)](#)
- [Tablas de enrutamiento personalizadas \(p. 84\)](#)
- [Asociar una subred a la tabla de enrutamiento \(p. 84\)](#)

Rutas

Cada ruta en una tabla especifica un destino y un objetivo. Por ejemplo, para permitir que su subred acceda a Internet a través de una gateway de Internet, añada la siguiente ruta a su tabla de ruteo de la subred. El destino de la ruta es 0.0.0.0/0, que representa todas las direcciones IPv4. El objetivo es la gateway de Internet que se conecta a su VPC.

Destino	Objetivo
0.0.0.0/0	<i>igw-id</i>

Los bloques de CIDR para las direcciones IPv4 e IPv6 se tratan de forma individual. Por ejemplo, una ruta con un CIDR de destino de 0.0.0.0/0 no incluye de forma automática todas las direcciones IPv6. Por ello, debe crear una ruta con un CIDR de destino de ::/0 para todas las direcciones IPv6.

Si hace referencia con frecuencia al mismo conjunto de bloques de CIDR en sus recursos de AWS, puede crear una [lista de prefijos administrada por el cliente \(p. 70\)](#) para agruparlos. A continuación, puede especificar la lista de prefijos como destino en la entrada de la tabla de ruteo.

Cada tabla de ruteo contiene una ruta local para la comunicación con la VPC. Esta ruta se agrega de forma predeterminada a todas las tablas de ruteo. Si la VPC tiene varios bloques de CIDR IPv4, las tablas de ruteo contienen una ruta local para cada bloque de CIDR IPv4. Si ha asociado un bloque de CIDR IPv6 a su VPC, las tablas de ruteo contendrán una ruta local para el bloque de CIDR IPv6. No puede modificar ni eliminar estas rutas en una tabla de ruteo de la subred o en la tabla de ruteo principal.

Reglas y consideraciones

- No puede agregar una ruta a sus tablas de enrutamiento que es más específica que la ruta local. El destino debe coincidir con todo el bloque de CIDR IPv4 o IPv6 de una subred en su VPC. El destino debe ser una gateway NAT, una interfaz de red o un punto de enlace del balanceador de carga de la gateway.
- Si su ruta tiene varias rutas, para determinar cómo dirigir tráfico, se utiliza la ruta más específica que coincida con el tráfico en cuestión (coincidencia del prefijo más largo).

- No se pueden agregar rutas a direcciones IPv4 que coincidan de forma exacta o que sean un subconjunto del siguiente rango: 169.254.169.0/22. Este rango se encuentra dentro del espacio de direcciones de enlace local y está reservado para ser utilizado por los servicios de AWS. Por ejemplo, Amazon EC2 utiliza direcciones en este rango para servicios a los que solo se puede acceder desde instancias de EC2, como el servicio de metadatos de instancia (IMDS) y el servidor DNS de Amazon. Puede utilizar un bloque de CIDR que sea mayor que 169.254.169.0/22 pero los paquetes destinados a las direcciones de 169.254.169.0/22 no se reenviarán.
- No se pueden agregar rutas a direcciones IPv6 que coincidan de forma exacta o que sean un subconjunto del siguiente rango: fd00:ec2::/32. Este rango está dentro del espacio de direcciones locales únicas (ULA) y está reservado para que lo utilicen los servicios de AWS. Por ejemplo, Amazon EC2 utiliza direcciones en este rango para servicios a los que solo se puede acceder desde instancias de EC2, como el servicio de metadatos de instancia (IMDS) y el servidor DNS de Amazon. Puede utilizar un bloque de CIDR que sea mayor que fd00:ec2::/32 pero los paquetes destinados a las direcciones de fd00:ec2::/32 no se reenviarán.
- Puede agregar dispositivos middlebox a las vías de enrutamiento de su VPC. Para obtener más información, consulte [the section called “Enrutamiento para un dispositivo middlebox” \(p. 94\)](#).

Ejemplo

En el siguiente ejemplo, suponga que la VPC tiene tanto un bloque de CIDR IPv4 como un bloque de CIDR IPv6. En la tabla de enrutamiento:

- El tráfico IPv6 destinado a permanecer en la VPC (2001:db8:1234:1a00::/56) se gestiona con la ruta `Local` y se direcciona dentro de la VPC.
- El tráfico IPv4 e IPv6 se trata de manera individual; por lo tanto, todo el tráfico IPv6 (excepto el tráfico de la VPC) se direcciona a la gateway de Internet solo de salida.
- Hay una ruta para el tráfico IPv4 172.31.0.0/16 que apunta a una interconexión.
- Hay una ruta para todo el tráfico IPv4 (0.0.0.0/0) que apunta a una gateway de Internet.
- Hay una ruta para todo el tráfico IPv6 (::/0) que apunta a una gateway de Internet de solo salida.

Destino	Objetivo
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567
::/0	eigw-aabbccdde1122334

Tabla de enrutamiento principal

Al crear una VPC, esta cuenta de manera automática con una tabla de ruteo principal. Si una subred no está asociada de forma explícita a una tabla de enrutamiento, se utilizará la tabla de enrutamiento principal de forma predeterminada. En la página Route Tables (Tablas de ruteo) de la consola de Amazon VPC, puede consultar la tabla de enrutamiento principal de la VPC si busca el valor Yes (Sí) en la columna Main (Principal).

De forma predeterminada, cuando se crea una VPC no predeterminada, la tabla de ruteo principal contiene sólo una ruta local. Cuando utiliza el asistente de la VPC en la consola para crear una VPC no

predeterminada con una gateway NAT o una gateway privada virtual, el asistente añade de forma automática rutas a la tabla de ruteo principal para esas gateways.

Las siguientes reglas se aplican a la tabla de enrutamiento principal:

- La tabla de enrutamiento principal no se puede eliminar.
- No puede establecer una tabla de ruteo de gateway como la tabla de ruta principal.
- Puede reemplazar la tabla de enrutamiento principal por una tabla de enrutamiento de subred personalizada.
- De este modo, podrá añadir, quitar y modificar rutas en la tabla de ruteo principal.
- También podrá asociar de manera explícita una subred a la tabla de ruteo principal incluso si ya está asociada de manera implícita.

Es posible que desee hacerlo si cambia qué tabla es la tabla de ruteo principal. Cuando modifica la tabla que se considerará como tabla de ruteo principal, también modifica la opción predeterminada de las nuevas subredes adicionales o para las subredes que no están explícitamente asociadas a ninguna otra tabla de ruteo. Para obtener más información, consulte [Sustituir la tabla de enrutamiento principal](#) (p. 104).

Tablas de enrutamiento personalizadas

De forma predeterminada, una tabla de ruteo personalizada está vacía y agrega rutas según sea necesario. Cuando utiliza el asistente de la VPC en la consola para crear una VPC con una gateway de Internet, el asistente crea una tabla de ruteo personalizada y agrega una ruta a la gateway de Internet. Una forma de proteger la VPC es dejar la tabla de ruteo principal en su estado predeterminado original. Después, asocie de forma explícita cada nueva subred que cree a una de las tablas de ruteo personalizadas que haya creado. De este modo, se asegurará de que controla de manera explícita el modo en que cada subred direcciona el tráfico.

De este modo, podrá añadir, quitar y modificar rutas en la tabla de ruteo personalizada. Sólo puede eliminar una tabla de ruteo personalizada si no tiene asociaciones.

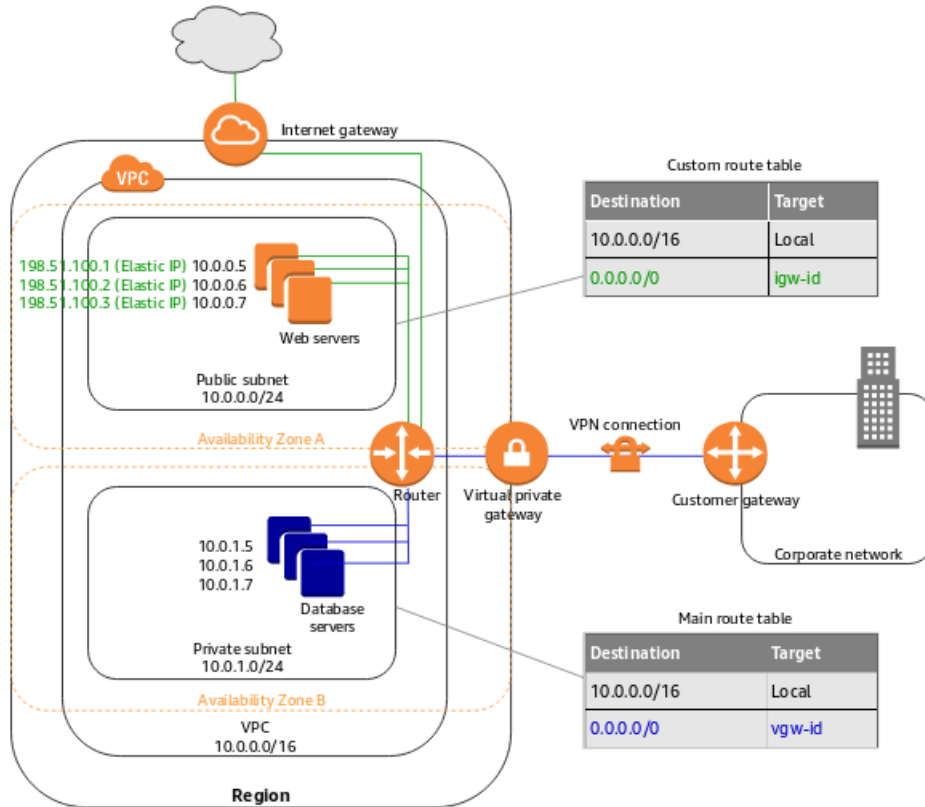
Asociar una subred a la tabla de enrutamiento

Cada subred de su VPC debe estar asociada a una tabla de ruteo. Una subred se puede asociar de forma explícita a la tabla de ruteo personalizada o de manera implícita o explícita a la tabla de ruteo principal. Para obtener más información sobre la visualización de las asociaciones de la subred y la tabla de enrutamiento, consulte [Determinar qué subredes o gateways están asociadas explícitamente a una tabla](#) (p. 99).

Las subredes que se encuentran en VPC asociadas a Outposts pueden tener un tipo de objetivo adicional de una gateway local. Esta es la única diferencia de direccionamiento con respecto a las subredes que no son de Outposts.

Ejemplo 1: asociación implícita y explícita de la subred

El diagrama siguiente muestra el direccionamiento de una VPC con una gateway de Internet, una gateway privada virtual, una subred pública y una subred de solo VPN. La tabla de ruteo principal tiene una ruta a la gateway privada virtual. La subred pública tiene asociada de forma explícita una tabla de ruteo personalizada. La tabla de ruteo personalizada tiene una ruta hacia Internet (0.0.0.0/0) a través de la gateway de Internet.

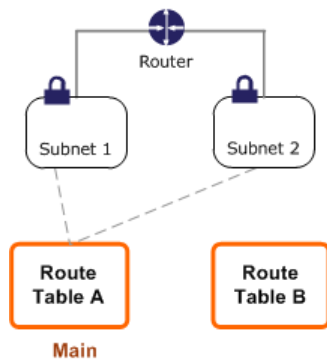


Si crea una nueva subred en esta VPC, esta se asociará automáticamente de forma implícita a la tabla de ruteo principal que dirige tráfico a la gateway privada virtual. Si establece la configuración inversa (en la que la tabla de ruteo principal tiene una ruta a la gateway de Internet y la tabla de ruteo personalizada tiene una ruta a la gateway privada virtual), la nueva subred tendría que disponer de manera automática de una ruta a la gateway de Internet.

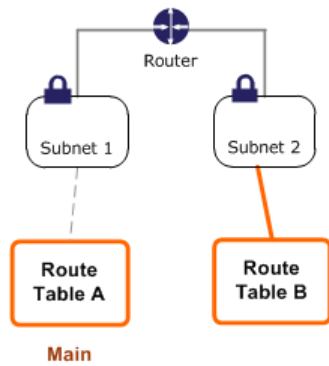
Ejemplo 2: sustitución de la tabla de enrutamiento principal

Es posible que desee realizar cambios en la tabla de ruteo principal. Para evitar cualquier interrupción en el tráfico, le recomendamos que pruebe primero los cambios de la ruta mediante una tabla de ruteo personalizada. De este modo, cuando esté satisfecho con las pruebas, puede sustituir la tabla de ruteo principal con la nueva tabla personalizada.

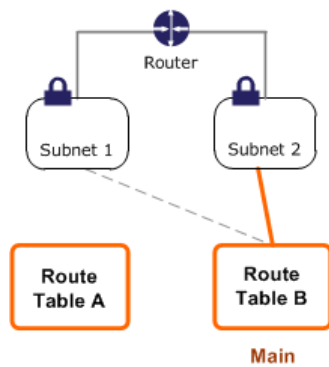
El diagrama siguiente muestra una VPC con dos subredes asociadas de manera implícita a una tabla de ruteo principal (tabla de ruteo A) y una tabla de ruteo personalizada (tabla de ruteo B) que no está asociada a ninguna subred.



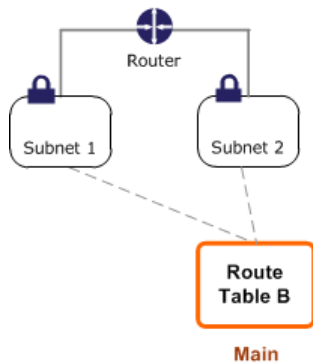
Puede crear una asociación explícita entre la subred 2 y la tabla de ruteo B.



Una vez probada la tabla de ruteo B, podrá convertirla en tabla de ruteo principal. Tenga en cuenta que la subred 2 aún tiene una asociación explícita con la tabla de ruteo B y que la subred 1 tiene una asociación implícita con la tabla de ruteo B porque es la nueva tabla de ruteo principal. La tabla de ruteo A ha dejado de utilizarse.



Si desasocia la subred 2 de la tabla de ruteo B, seguirá existiendo una asociación implícita entre la subred 2 y la tabla de ruteo B. Por lo tanto, si ya no necesita la tabla de ruteo A, puede eliminarla.



Tablas de ruteo de gateway

Puede asociar una tabla de ruteo a una gateway de Internet o a una gateway privada virtual. Cuando una tabla de ruteo está asociada a una gateway, se denomina tabla de ruteo de gateway. Puede crear una tabla de ruteo de gateway para el control detallado de la vía de direccionamiento del tráfico que entra a su VPC. Por ejemplo, puede interceptar el tráfico que entra en la VPC a través de una gateway de Internet redirigiendo ese tráfico a un dispositivo middlebox (como un dispositivo de seguridad) de la VPC.

Contenido

- [Rutas de la tabla de enrutamiento de gateway \(p. 87\)](#)
- [Reglas y consideraciones \(p. 88\)](#)

Rutas de la tabla de enrutamiento de gateway

Una tabla de enrutamiento de gateway asociada a una gateway de Internet admite enrutamientos con los siguientes destinos:

- La ruta local predeterminada
- Un [Punto de enlace del balanceador de carga de gateway](#)
- Una interfaz de red para un dispositivo middlebox

Una tabla de enrutamientos de gateway asociada a una gateway privada virtual admite rutas con los siguientes destinos:

- La ruta local predeterminada
- Una interfaz de red para un dispositivo middlebox

Cuando el destino es punto de enlace del balanceador de carga de gateway o una interfaz de red, se permiten los siguientes destinos:

- Todo el bloque de CIDR IPv4 o IPv6 de su VPC. En este caso, sustituye el objetivo de la ruta local predeterminada.
- Todo el bloque de CIDR IPv4 o IPv6 de una subred en su VPC. Es una ruta más específica que la ruta predeterminada local.

Si cambia el objetivo de la ruta local en una tabla de ruteo de gateway a una interfaz de red en su VPC, puede restaurarlo más adelante al objetivo `local` predeterminado. Para obtener más información, consulte [Reemplazar o restaurar el destino de una ruta local \(p. 105\)](#).

Ejemplo

En la siguiente tabla de ruteo de gateway, el tráfico destinado a una subred con el bloque de CIDR `172.31.0.0/20` se direcciona a una interfaz de red específica. El tráfico destinado a todas las demás subredes de la VPC utiliza la ruta local.

Destino	Objetivo
172.31.0.0/16	Local
172.31.0.0/20	<i>eni-id</i>

Ejemplo

En la siguiente tabla de ruteo de gateway, el objetivo de la ruta local se sustituye por un ID de interfaz de red. El tráfico destinado a todas las subredes de la VPC se direcciona a la interfaz de red.

Destino	Objetivo
172.31.0.0/16	<i>eni-id</i>

Reglas y consideraciones

No se puede asociar una tabla de ruteo con una gateway si se aplica alguna de las siguientes condiciones:

- La tabla de enrutamiento contiene rutas existentes con objetivos distintos a una interfaz de red, un punto de enlace del balanceador de carga de gateway o la ruta local predeterminada.
- La tabla de ruteo contiene rutas existentes a los bloques de CIDR fuera de los rangos de la VPC.
- La propagación de rutas está habilitada para la tabla de ruteo.

Además, se aplican las siguientes reglas y consideraciones:

- No puede agregar rutas a ningún bloque de CIDR fuera de los rangos de la VPC, incluidos rangos mayores que los bloques de CIDR de VPC individuales.
- Solo puede especificar como destino una `local`, un punto de enlace del balanceador de carga de gateway o una interfaz de red. No puede especificar ningún otro tipo de destino, incluidas las direcciones IP de host individuales. Para obtener más información, consulte [the section called “Opciones de enrutamiento de ejemplo” \(p. 90\)](#).
- No puede direccionar el tráfico de una gateway privada virtual a un punto de enlace del balanceador de carga de gateway. Si asocia la tabla de enrutamiento con una gateway privada virtual y agrega una ruta con un punto de enlace del balanceador de carga de gateway como destino, se elimina el tráfico destinado al punto de enlace.
- No se puede especificar una lista de prefijos como destino.
- No puede utilizar una tabla de ruteo de gateway para controlar o interceptar el tráfico fuera de la VPC, por ejemplo, el tráfico a través de una transit gateway conectada. Puede interceptar el tráfico que entra en la VPC y redirigirlo a otro objetivo en la misma VPC solamente.
- Para asegurarse de que el tráfico llega al dispositivo middlebox, la interfaz de red de destino debe estar asociada a una instancia en ejecución. Para el tráfico que fluya a través de una gateway de Internet, la interfaz de red de destino también debe tener una dirección IP pública.
- Al configurar el dispositivo Middlebox, tenga en cuenta las [consideraciones del dispositivo \(p. 95\)](#).
- Al enrutar el tráfico a través de un dispositivo Middlebox, el tráfico de retorno de la subred de destino debe enrutarse a través del mismo dispositivo. No se admite el enrutamiento asimétrico.
- Las reglas de tabla de enrutamiento se aplican a todo el tráfico que sale de una subred. El tráfico que sale de una subred se define como el tráfico destinado a la dirección MAC del enrutador de gateway de esa subred. El tráfico destinado a la dirección MAC de otra interfaz de red en la subred utiliza el enrutamiento de enlace de datos (capa 2) en lugar de la red (capa 3), por lo que las reglas no se aplican a este tráfico.

Prioridad de la ruta

En general, el tráfico se dirige mediante la ruta mas especifica que concuerde con el tráfico. Esto se conoce como la concordancia de prefijos más larga. Si la tabla de enrutamiento tiene rutas superpuestas o concordantes, se aplican las siguientes reglas:

Contenido

- [La concordancia de prefijo más larga \(p. 89\)](#)
- [Prioridad de ruta y rutas propagadas \(p. 89\)](#)
- [Listas de prefijos y prioridad de ruta \(p. 90\)](#)

La concordancia de prefijo más larga

Las rutas a direcciones IPv4 e IPv6 o bloques de CIDR son independientes entre sí. Para determinar cómo dirigir tráfico, se usa la ruta más específica que coincida con el tráfico de IPv4 o IPv6 en cuestión.

En el siguiente ejemplo, la tabla de enrutamiento de la subred tiene una ruta para el tráfico de Internet IPv4 (0.0.0.0/0), que apunta a una gateway de Internet, y una ruta para el tráfico IPv4 172.31.0.0/16 que apunta a una interconexión (pcx-11223344556677889). El tráfico de la subred cuyo destino sea el rango de direcciones IP 172.31.0.0/16 utiliza la interconexión, ya que esta ruta es más específica que la ruta para la gateway de Internet. El tráfico cuyo destino se encuentre en la VPC (10.0.0.0/16) se gestiona con la ruta `local` y, por lo tanto, se direcciona dentro de la VPC. El resto de tráfico de la subred usa la gateway de Internet.

Destino	Objetivo
10.0.0.0/16	local
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567

Prioridad de ruta y rutas propagadas

Si ha asociado una gateway privada virtual a la VPC y ha habilitado la propagación de rutas en la tabla de enrutamiento de la subred, las rutas que representan la conexión de Site-to-Site VPN aparecerán automáticamente como rutas propagadas en la tabla de enrutamiento.

Si el destino de una ruta propagada se superpone a la ruta local, la ruta local tiene prioridad incluso si la ruta propagada es más específica. Si el destino de una ruta propagada se superpone a una ruta estática, la ruta estática tiene prioridad.

Si el destino de una ruta propagada es idéntico al destino de una ruta estática, la ruta estática tiene prioridad si el destino es uno de los siguientes:

- gateway de Internet
- Puerta de enlace de NAT
- Interfaz de red
- ID de instancia
- Punto de enlace de la VPC de la gateway
- Transit gateway
- Interconexión de VPC
- Punto de enlace del balanceador de carga de gateway

Para obtener más información, consulte [Tablas de ruteo y prioridad de las rutas de VPN](#) en la Guía del usuario de AWS Site-to-Site VPN.

En el siguiente ejemplo, la tabla de enrutamiento tiene una ruta estática hacia una gateway de Internet y una ruta propagada hacia una gateway privada virtual. Ambas rutas tienen el destino 172.31.0.0/24. Dado que una ruta estática hacia una gateway de Internet tiene prioridad, todo el tráfico destinado a 172.31.0.0/24 se dirige a la gateway de Internet.

Destino	Objetivo	Propagado
10.0.0.0/16	local	No

Destino	Objetivo	Propagado
172.31.0.0/24	vgw-11223344556677889	Sí
172.31.0.0/24	igw-12345678901234567	No

Listas de prefijos y prioridad de ruta

Si la tabla de ruteo hace referencia a una lista de prefijos, se aplican las siguientes reglas:

- Si la tabla de enrutamiento contiene una ruta estática con un bloque CIDR de destino que se superpone a una ruta estática con una lista de prefijos, la ruta estática con el bloque de CIDR tiene prioridad.
- Si la tabla de enrutamiento contiene una ruta propagada que se superpone a una ruta con una lista de prefijos, la ruta que hace referencia a la lista de prefijos tiene prioridad.
- Si la tabla de ruteo hace referencia a varias listas de prefijos que tienen bloques CIDR superpuestos a diferentes destinos, elegimos aleatoriamente qué ruta tiene prioridad. A partir de entonces, la misma ruta siempre tiene prioridad.
- Si el bloque CIDR de una entrada de lista de prefijos no es válido para la tabla de enrutamiento, se omite ese bloque CIDR.

Cuotas de la tabla de enrutamiento

Existe una cuota en el número de tablas de ruteo que puede crear por VPC. Existe también una cuota en el número de rutas que puede añadir por tabla de ruteo. Para obtener más información, consulte [. Cuotas de Amazon VPC \(p. 378\)](#).

Opciones de enrutamiento de ejemplo

Los temas siguientes describen el direccionamiento de gateways o conexiones específicas de su VPC.

Contenido

- [Enrutar a una gateway de Internet \(p. 90\)](#)
- [Enrutar a un dispositivo NAT \(p. 91\)](#)
- [Enrutar a una gateway privada virtual \(p. 91\)](#)
- [Enrutamiento a una gateway local de AWS Outposts \(p. 92\)](#)
- [Enrutar a una interconexión de VPC \(p. 92\)](#)
- [Enrutar a un punto de enlace de la VPC de la gateway \(p. 93\)](#)
- [Enrutar a la gateway de Internet de solo salida \(p. 93\)](#)
- [Enrutar para una transit gateway \(p. 94\)](#)
- [Enrutamiento para un dispositivo middlebox \(p. 94\)](#)
- [Enrutamiento mediante una lista de prefijos \(p. 98\)](#)
- [Enrutamiento a un punto de enlace del balanceador de carga de gateway \(p. 98\)](#)

Enrutar a una gateway de Internet

Puede convertir una subred en una subred pública añadiendo una ruta en su tabla de ruteo de la subred hacia una gateway de Internet. Para ello, cree y adjunte una gateway de Internet a su VPC. A continuación,

añada una ruta con el destino 0.0.0.0/0 para el tráfico IPv4 o con el destino ::/0 para el tráfico IPv6, así como un objetivo para el ID de la gateway de Internet (igw-xxxxxxxxxxxxxxxxxx).

Destino	Objetivo
0.0.0.0/0	<i>igw-id</i>
::/0	<i>igw-id</i>

Para obtener más información, consulte [Conexión a Internet mediante una puerta de enlace de Internet](#) (p. 142).

Enrutar a un dispositivo NAT

Para habilitar instancias en una subred privada para conectarse a Internet, puede crear una gateway NAT o lanzar una instancia NAT en una subred pública. A continuación, agregue una ruta para la tabla de ruteo de la subred privada que dirija el tráfico de Internet de IPv4 (0.0.0.0/0) al dispositivo NAT.

Destino	Objetivo
0.0.0.0/0	<i>nat-gateway-id</i>

También puede crear rutas más específicas a otros objetivos para evitar cargos innecesarios de procesamiento de datos innecesarios por utilizar la gateway NAT o para dirigir el tráfico de forma privada. En el ejemplo siguiente, el tráfico de Amazon S3 (pl-xxxxxxx; un intervalo de direcciones IP específico para Amazon S3) se enruta al punto de enlace de la VPC de la gateway y el tráfico 10.25.0.0/16 se enruta a una interconexión de VPC. Los rangos de direcciones IP pl-xxxxxxx y 10.25.0.0/16 son más específicos que 0.0.0.0/0. Cuando las instancias envían tráfico a Amazon S3 o a la VPC interconectada, el tráfico se envía al punto de enlace de la VPC de la gateway o a la interconexión de la VPC. El resto del tráfico se envía a la gateway NAT.

Destino	Objetivo
0.0.0.0/0	<i>nat-gateway-id</i>
pl-xxxxxxx	<i>vpce-id</i>
10.25.0.0/16	<i>pcx-id</i>

Para obtener más información, consulte [Gateways NAT](#) (p. 157) y [Instancias NAT](#) (p. 184). Los dispositivos NAT No se pueden utilizar para el tráfico IPv6.

Enrutar a una gateway privada virtual

Puede utilizar una conexión de AWS Site-to-Site VPN para permitir que las instancias de su VPC se comuniquen con su propia red. Para ello, cree y adjunte una gateway privada virtual a su VPC. A continuación, agregue una ruta en la tabla de ruteo de subred con el destino de la red y un objetivo de la gateway privada virtual (vgw-xxxxxxxxxxxxxxxxxx).

Destino	Objetivo
10.0.0.0/16	<i>vgw-id</i>

A continuación, puede crear y configurar la conexión de Site-to-Site VPN. Para obtener más información, consulte [¿Qué es AWS Site-to-Site VPN?](#) y [Tablas de enrutamiento y prioridad de las rutas de VPN](#) en la Guía del usuario de AWS Site-to-Site VPN.

Una conexión de Site-to-Site VPN en una gateway privada virtual no admite tráfico IPv6. Sin embargo, sí que se admite el direccionamiento de tráfico IPv6 a través de gateways privadas virtuales a conexiones de AWS Direct Connect. Para obtener más información, consulte la [Guía del usuario de AWS Direct Connect](#).

Enrutamiento a una gateway local de AWS Outposts

Las subredes que se encuentran en VPC asociadas a AWS Outposts pueden tener un tipo de objetivo adicional de una gateway local. Tenga en cuenta el caso en el que desea que la gateway local dirija el tráfico con una dirección de destino de 192.168.10.0/24 a la red del cliente. Para ello, añada la siguiente ruta con la red de destino y un objetivo de la gateway local (lgw-xxxx).

Destino	Objetivo
192.168.10.0/24	lgw-id

Enrutar a una interconexión de VPC

Una interconexión de VPC es una conexión de redes entre dos VPC que permite direccionar el tráfico entre ellas mediante direcciones IPv4 privadas. Las instancias de ambas VPC se pueden comunicar entre sí si forman parte de la misma red.

Para permitir el direccionamiento de tráfico entre VPC en una interconexión de VPC, debe añadir una ruta hacia una o varias tablas de ruteo de la subred que apunten a la interconexión de VPC. Esto le permite acceder a todo o a parte del bloque de CIDR de la otra VPC en la interconexión. Del mismo modo, el propietario de la otra VPC deberá añadir una ruta a sus tablas de ruteo de la subred para direccionar el tráfico de vuelta a su VPC.

Supongamos que, por ejemplo, tiene una interconexión de VPC (pcx-11223344556677889) entre dos VPC con la información siguiente:

- VPC A: bloque de CIDR 10.0.0.0/16
- VPC B: bloque de CIDR 172.31.0.0/16

Para permitir el tráfico entre las VPC y facilitar el acceso a la totalidad del bloque de CIDR IPv4 de ambas VPC, la tabla de ruteo de la VPC A debe configurarse como se indica a continuación.

Destino	Objetivo
10.0.0.0/16	Local
172.31.0.0/16	pcx-11223344556677889

La tabla de ruteo de la VPC B debe configurarse como se indica a continuación.

Destino	Objetivo
172.31.0.0/16	Local
10.0.0.0/16	pcx-11223344556677889

La interconexión de la VPC también puede admitir la comunicación IPv6 entre instancias en las VPC, si las VPC y las instancias admiten la comunicación IPv6. Para permitir el direccionamiento de tráfico IPv6 entre las VPC, debe añadir una ruta a la tabla de ruteo que apunte a la interconexión de la VPC para, de este modo, obtener acceso a la totalidad o a parte del bloque de CIDR IPv6 de la VPC del mismo nivel.

Supongamos que, por ejemplo, con la misma interconexión de VPC (`pcx-11223344556677889`) anterior, las VPC tienen la información siguiente:

- VPC A: bloque de CIDR IPv6 `2001:db8:1234:1a00::/56`
- VPC B: bloque de CIDR IPv6 `2001:db8:5678:2b00::/56`

Para permitir la comunicación IPv6 a través de la interconexión de VPC, añada la ruta siguiente a la tabla de ruteo de la subred para la VPC A.

Destino	Objetivo
10.0.0.0/16	Local
172.31.0.0/16	pcx-11223344556677889
2001:db8:5678:2b00::/56	pcx-11223344556677889

Añada la siguiente ruta a la tabla de ruteo de la VPC B.

Destino	Objetivo
172.31.0.0/16	Local
10.0.0.0/16	pcx-11223344556677889
2001:db8:1234:1a00::/56	pcx-11223344556677889

Para obtener más información acerca de las interconexiones de VPC, consulte la [Guía de interconexión de Amazon VPC](#).

Enrutar a un punto de enlace de la VPC de la gateway

Un punto de enlace de la VPC de la gateway permite crear una conexión privada entre la VPC y otros servicios de AWS. Cuando crea un punto de enlace de la gateway, especifica las tablas de ruteo de la subred en su VPC que utiliza el punto de enlace de la gateway. Se añadirá automáticamente una ruta a cada una de las tablas de ruteo con el ID de la lista de prefijos del servicio (`p1-xxxxxxxx`) como destino y el ID del punto de conexión (`vpce-xxxxxxxxxxxxxxxxxx`) como objetivo. No es posible eliminar ni modificar de manera explícita la ruta del punto de conexión; sin embargo, es posible cambiar las tablas de ruteo que utiliza el punto de conexión.

Para obtener más información acerca del enrutamiento para puntos de enlace y las implicaciones de las rutas a servicios de AWS, consulte [Enrutamiento para puntos de enlace de gateway](#).

Enrutar a la gateway de Internet de solo salida

Puede crear gateways de Internet de solo salida para su VPC para permitir que las instancias de subredes privadas inicien comunicaciones salientes a Internet evitando que Internet inicie conexiones con dichas instancias. La gateway de Internet de solo salida se utiliza únicamente para el tráfico IPv6. Para configurar

el direccionamiento de la gateway de Internet de solo salida, añada una ruta a la tabla de ruteo de la subred privada que direcciona el tráfico de Internet IPv6 (:::/0) a la gateway de Internet de solo salida.

Destino	Objetivo
::/0	<i>eigw-id</i>

Para obtener más información, consulte [Habilitar el tráfico IPv6 saliente mediante una puerta de enlace de Internet de solo salida](#) (p. 153).

Enrutar para una transit gateway

Al asociar una VPC a una transit gateway, debe agregar una ruta a la tabla de enrutamiento de subredes para que el tráfico se enrute a través de la transit gateway.

Considere el siguiente escenario, en el que tiene tres VPC asociadas a una transit gateway. En este escenario, todas las conexiones se asocian a la tabla de enrutamiento de la transit gateway y se propagan a la tabla de enrutamiento de la transit gateway. Por lo tanto, todas las conexiones pueden enrutar paquetes entre sí y la transit gateway actúa como un simple hub de IP de capa 3.

Supongamos que, por ejemplo, tiene dos VPC con la información siguiente:

- VPC A: 10.1.0.0/16, ID de vinculación tgw-attach-1111111111111111
- VPC B: 10.2.0.0/16, ID de vinculación tgw-attach-2222222222222222

Para permitir el tráfico entre las VPC y permitir el acceso a la transit gateway, la tabla de enrutamiento de la VPC A debe configurarse como se muestra a continuación.

Destino	Objetivo
10.1.0.0/16	local
10.0.0.0/8	<i>tgw-id</i>

A continuación, se muestra un ejemplo de las entradas de las tablas de enrutamiento de transit gateway para las conexiones de VPC.

Destino	Objetivo
10.1.0.0/16	tgw-attach-1111111111111111
10.2.0.0/16	tgw-attach-2222222222222222

Para obtener más información acerca de las tablas de enrutamiento de la transit gateway, consulte [Enrutamiento](#) en Transit gateways de Amazon VPC.

Enrutamiento para un dispositivo middlebox

Puede agregar dispositivos middlebox a las vías de enrutamiento de su VPC. Estos son algunos casos de uso posibles:

- Intercepte el tráfico que ingresa a la VPC a través de una gateway de Internet o una gateway privada virtual, redirigiéndolo a un dispositivo middlebox en su VPC. Puede usar el asistente de enrutamiento

de middlebox para que AWS configure automáticamente las tablas de enrutamiento adecuadas para la gateway, el middlebox y la subred de destino. Para obtener más información, consulte [the section called “Trabaje con el asistente de enrutamiento de middlebox”](#) (p. 116).

- Dirija el tráfico entre dos subredes a un dispositivo de middlebox. Puede hacerlo creando una ruta para una tabla de enrutamientos de subred que coincida con la subred CIDR de la otra subred y especifique un punto de enlace del balanceador de carga de gateway, una gateway NAT, un punto de enlace de Network Firewall o la interfaz de red de un dispositivo como destino. Como alternativa, para redirigir todo el tráfico de la subred a cualquier otra subred, reemplace el destino de la ruta local por un punto de enlace del balanceador de carga de gateway, gateway NAT o interfaz de red.

Puede configurar el dispositivo para que se adapte a sus necesidades. Por ejemplo, puede configurar un dispositivo de seguridad que cribase todo el tráfico o un dispositivo de aceleración WAN. El dispositivo se implementa como una instancia Amazon EC2 en una subred de la VPC y se representa mediante una interfaz de red elástica (interfaz de red) en la subred.

Si habilita la propagación de enrutamientos en la tabla de enrutamiento de la subred de destino, tenga en cuenta la prioridad de las rutas. La ruta más específica es la que tiene mayor prioridad y, en caso de que coincidan, las rutas estáticas tendrán prioridad sobre las rutas propagadas. Revise las rutas para asegurarse de que el tráfico se direcciona correctamente y de que no produzcan consecuencias no deseadas si habilita o deshabilita la propagación de rutas (por ejemplo, la propagación de rutas es necesaria en una conexión AWS Direct Connect que admita tramas jumbo).

Para dirigir el tráfico de VPC entrante a un dispositivo, asocie una tabla de ruteo a la gateway de Internet o a la gateway privada virtual y especifique la interfaz de red del dispositivo como objetivo para el tráfico de la VPC. Para obtener más información, consulte [Tablas de ruteo de gateway](#) (p. 86). También puede dirigir el tráfico saliente de la subred a un dispositivo middlebox de otra subred.

Para ver ejemplos de enrutamiento de middlebox, consulte [Escenarios de enrutamiento de middlebox](#) (p. 106).

Contenido

- [Consideraciones sobre el dispositivo](#) (p. 95)
- [Enrutamiento del tráfico entre una gateway y un dispositivo](#) (p. 96)
- [Enrutamiento del tráfico entre subredes a un dispositivo](#) (p. 97)

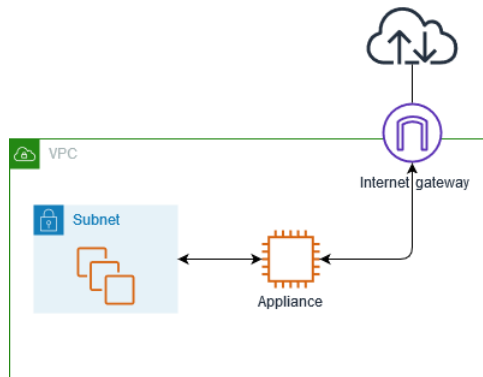
Consideraciones sobre el dispositivo

Puede elegir un dispositivo de terceros de [AWS Marketplace](#) o configurar su propio dispositivo. Al crear o configurar un dispositivo, tenga en cuenta lo siguiente:

- El dispositivo debe configurarse en una subred independiente para el tráfico de origen o destino.
- Debe deshabilitar la comprobación de origen/destino en el dispositivo. Para obtener más información, consulte [Cambio de la comprobación de origen o destino](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
- No se puede dirigir el tráfico entre hosts de la misma subred a través de un dispositivo.
- El dispositivo no tiene que realizar la conversión de las direcciones de red (NAT).
- Puede agregar una ruta a sus tablas de enrutamiento que sea más específica que la ruta local. Puede utilizar rutas más específicas para redirigir el tráfico entre subredes dentro de una VPC (tráfico Este-Oeste) a un dispositivo de Middlebox. El destino de la ruta debe coincidir con el bloque de CIDR IPv4 o IPv6 de una subred de su VPC.
- Para interceptar el tráfico IPv6, asegúrese de configurar la VPC, la subred y el dispositivo para IPv6. Para obtener más información, consulte [Trabajar con VPC](#) (p. 21). Las gateways privadas virtuales no admiten el tráfico IPv6.

Enrutamiento del tráfico entre una gateway y un dispositivo

Para dirigir el tráfico de VPC entrante a un dispositivo, asocie una tabla de ruteo a la gateway de Internet o a la gateway privada virtual y especifique la interfaz de red del dispositivo como objetivo para el tráfico de la VPC. En el ejemplo siguiente, la VPC tiene una gateway de Internet, un dispositivo y una subred con instancias. El tráfico de Internet se dirige a través de un dispositivo.



Asocie esta tabla de ruteo con su gateway de Internet o gateway privada virtual. La primera entrada es la ruta local. La segunda entrada envía el tráfico IPv4 destinado a la subred a la interfaz de red del dispositivo. Esta ruta es más específica que la ruta local.

Destino	Objetivo
<i>CIDR DE VPC</i>	Local
<i>CIDR de subred</i>	<i>ID de interfaz de red del dispositivo</i>

También puede sustituir el objetivo de la ruta local por la interfaz de red del dispositivo. Puede hacerlo para asegurarse de que todo el tráfico se dirige automáticamente al dispositivo, incluido el tráfico destinado a las subredes que agregue a la VPC más adelante.

Destino	Objetivo
<i>CIDR de VPC</i>	<i>ID de interfaz de red del dispositivo</i>

Para dirigir el tráfico de la subred a un dispositivo de otra subred, añada una ruta a la tabla de ruteo de la subred que dirige el tráfico a la interfaz de red del dispositivo. El destino debe ser menos específico que el destino de la ruta local. Por ejemplo, para el tráfico destinado a Internet, especifique 0.0.0.0/0 (todas las direcciones IPv4) para el destino.

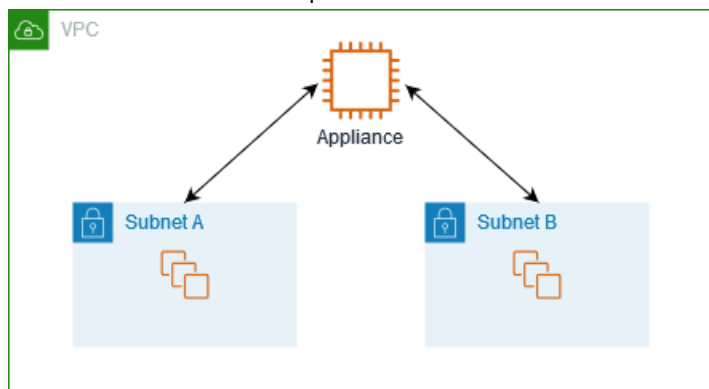
Destino	Objetivo
<i>CIDR DE VPC</i>	Local
0.0.0.0/0	<i>ID de interfaz de red del dispositivo</i>

A continuación, en la tabla de enrutamientos asociada a la subred del dispositivo, agregue una ruta que envíe el tráfico a la gateway de Internet o a la gateway privada virtual.

Destino	Objetivo
<i>CIDR DE VPC</i>	Local
0.0.0.0/0	<i>igw-id</i>

Enrutamiento del tráfico entre subredes a un dispositivo

Puede enrutar el tráfico destinado a una subred específica a la interfaz de red de un dispositivo. En el ejemplo siguiente, la VPC contiene dos subredes y un dispositivo. No se puede dirigir el tráfico entre subredes a través de un dispositivo.



Grupos de seguridad

Al enrutar el tráfico entre instancias en subredes diferentes a través de un dispositivo de middlebox, los grupos de seguridad de ambas instancias deben permitir que el tráfico fluya entre las instancias. El grupo de seguridad de cada instancia debe hacer referencia a la dirección IP privada de la otra instancia, o al rango CIDR de la subred que contiene la otra instancia, como fuente. Si hace referencia al grupo de seguridad de la otra instancia como fuente, esto no permite que el tráfico fluya entre las instancias.

Direccionamiento

A continuación se muestra un ejemplo de tabla de enrutamiento para la subred A. La primera entrada habilita a las instancias de la VPC para que se comuniquen entre sí. La segunda entrada dirige todo el tráfico de la subred A a la subred B a la interfaz de red del dispositivo.

Destino	Objetivo
<i>CIDR DE VPC</i>	Local
<i>CIDR de subred B</i>	<i>ID de interfaz de red del dispositivo</i>

A continuación se muestra un ejemplo de tabla de rutas para la subred B. La primera entrada habilita a las instancias de la VPC a comunicarse entre sí. La segunda entrada enruta todo el tráfico de la subred B a la subred A a la interfaz de red del dispositivo.

Destino	Objetivo
<i>CIDR DE VPC</i>	Local
<i>CIDR de subred A</i>	<i>ID de interfaz de red del dispositivo</i>

También puede sustituir el objetivo de la ruta local por la interfaz de red del dispositivo. Puede hacerlo para asegurarse de que todo el tráfico se dirige automáticamente al dispositivo, incluido el tráfico destinado a las subredes que agregue a la VPC más adelante.

Destino	Objetivo
<i>CIDR de VPC</i>	<i>ID de interfaz de red del dispositivo</i>

Enrutamiento mediante una lista de prefijos

Si hace referencia con frecuencia al mismo conjunto de bloques de CIDR en sus recursos de AWS, puede crear una [lista de prefijos administrada por el cliente \(p. 70\)](#) para agruparlos. A continuación, puede especificar la lista de prefijos como destino en la entrada de la tabla de ruteo. Posteriormente, puede agregar o quitar entradas para la lista de prefijos sin necesidad de actualizar las tablas de ruteo.

Por ejemplo, tiene una transit gateway con varios archivos adjuntos de VPC. Las VPC deben poder comunicarse con dos adjuntos VPC específicos que tengan los siguientes bloques CIDR:

- 10.0.0.0/16
- 10.2.0.0/16

Usted crea una lista de prefijos con ambas entradas. En las tablas de ruteo de subred, se crea una ruta y se especifica la lista de prefijos como destino y la transit gateway como destino.

Destino	Objetivo
172.31.0.0/16	Local
pl-123abc123abc123ab	<i>tgw-id</i>

El número máximo de entradas para las listas de prefijos es igual al mismo número de entradas en la tabla de ruteo.

Enrutamiento a un punto de enlace del balanceador de carga de gateway

Un balanceador de carga de gateway le permite distribuir tráfico a una flota de dispositivos virtuales, como firewalls. Puede configurar el balanceador de carga como servicio al crear una [configuración de servicio de punto de enlace de la VPC](#). A continuación, cree un [punto de enlace del balanceador de carga de gateway](#) en la VPC para conectar la VPC al servicio.

Para direccionar el tráfico al balanceador de carga de gateway (por ejemplo, para la inspección de seguridad), especifique el punto de enlace del balanceador de carga de gateway como destino en las tablas de enrutamiento.

Para obtener un ejemplo de dispositivos de seguridad detrás de un balanceador de carga de gateway, consulte [the section called “Dispositivo de seguridad detrás de un balanceador de carga de gateway en la VPC de seguridad” \(p. 110\)](#).

Para especificar el punto de enlace del balanceador de carga de gateway en la tabla de enrutamiento, utilice el ID del punto de enlace de la VPC. Por ejemplo, para dirigir el tráfico de 10.0.1.0/24 a un punto de enlace del balanceador de carga de gateway, agregue la siguiente ruta.

Destino	Objetivo
10.0.1.0/24	<i>vpc-endpoint-id</i>

Para obtener más información, consulte [Balanceadores de carga de gateway](#).

Trabajar con tablas de ruteo

En las tareas siguientes, se muestra cómo se trabaja con tablas de ruteo.

Note

Cuando utilice el asistente de la VPC de la consola para crear una VPC con una gateway, el asistente actualizará automáticamente las tablas de ruteo para utilizar la gateway. Si utiliza las herramientas de línea de comandos o la API para configurar su VPC, deberá actualizar las tablas de ruteo usted mismo.

Contenido

- [Determinar la tabla de enrutamiento de una subred \(p. 99\)](#)
- [Determinar qué subredes o gateways están asociadas explícitamente a una tabla \(p. 99\)](#)
- [Creación de una tabla de ruteo personalizada \(p. 100\)](#)
- [Agregar y eliminar rutas de una tabla de enrutamiento \(p. 101\)](#)
- [Habilitar o deshabilitar la propagación de rutas \(p. 102\)](#)
- [Asociación de una subred a una tabla de ruteo \(p. 102\)](#)
- [Cambiar la tabla de enrutamiento de una subred \(p. 103\)](#)
- [Desasociación de una subred de una tabla de ruteo \(p. 103\)](#)
- [Sustituir la tabla de enrutamiento principal \(p. 104\)](#)
- [Asociar una gateway a una tabla de enrutamiento \(p. 104\)](#)
- [Desasociar una gateway de una tabla de enrutamiento \(p. 105\)](#)
- [Reemplazar o restaurar el destino de una ruta local \(p. 105\)](#)
- [Eliminación de una tabla de ruteo \(p. 106\)](#)

Determinar la tabla de enrutamiento de una subred

Puede determinar la tabla de enrutamiento con la que se asocia la subred consultando los detalles de la subred en la consola de Amazon VPC.

Para determinar la tabla de enrutamiento de una subred

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets.
3. Elija la pestaña Route Table para ver el ID de la tabla de ruteo y sus rutas. En el caso de la tabla de ruteo principal, la consola no indicará si la asociación es implícita o explícita. Para determinar si la asociación a la tabla de ruteo principal es explícita, consulte [Determinar qué subredes o gateways están asociadas explícitamente a una tabla \(p. 99\)](#).

Determinar qué subredes o gateways están asociadas explícitamente a una tabla

Puede determinar el número y el tipo de subredes o gateways explícitamente asociadas a la tabla de ruteo.

La tabla de ruteo principal puede tener asociaciones de la subred implícitas y explícitas. Las tablas de ruteo principales solo tienen asociaciones explícitas.

Las subredes que no estén asociadas de manera explícita a ninguna tabla de ruteo tienen una asociación implícita a la tabla de ruteo principal. Puede asociar de forma explícita una subred con la tabla de ruteo principal. Para obtener un ejemplo de las razones para hacer eso, consulte [Sustituir la tabla de enrutamiento principal](#) (p. 104).

Para determinar las subredes que están asociadas de manera explícita utilizando la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables.
3. Consulte la columna Explicitly subnet association (Asociación de subred de forma explícita) para determinar las subredes asociadas de manera explícita.
4. Seleccione la tabla de ruteo obligatoria.
5. Elija la pestaña Subnet Associations en el panel de detalles. La pestaña mostrará las subredes asociadas explícitamente a la tabla. Las subredes que no estén asociadas a ninguna tabla de ruteo (y, por lo tanto, asociadas de manera implícita a la tabla de ruteo principal) también se muestran en la tabla.

Para determinar las gateways que están asociadas de manera explícita utilizando la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables.
3. Vea la columna Edge associations (Asociaciones de borde) para determinar las gateways asociadas.
4. Seleccione la tabla de ruteo obligatoria.
5. Elija la pestaña Edge Associations (Asociaciones de borde) en el panel de detalles. Se enumeran las gateways asociadas a la tabla de ruteo.

Para describir una o varias tablas de ruteo y ver sus asociaciones mediante la línea de comandos

- [describe-route-tables](#) (AWS CLI)
- [Get-EC2RouteTable](#) (AWS Tools for Windows PowerShell)

Creación de una tabla de ruteo personalizada

Puede crear una tabla de enrutamiento personalizada para la VPC mediante la consola de Amazon VPC.

Para crear una tabla de ruteo personalizada mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables.
3. Elija Create Route Table (Crear tabla de ruteo).
4. (Opcional) En Name tag (Etiqueta de nombre), escriba el nombre de la tabla de enrutamiento.
5. En VPC, elija su VPC.
6. (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 Value (Valor), escriba el valor de la clave.

[Eliminar una etiqueta] Elija el botón Eliminar ("X") situado a la derecha de la clave y valor de la etiqueta.

7. Seleccione Create (Crear).

Para crear una tabla de ruteo personalizada mediante la línea de comandos

- [create-route-table](#) (AWS CLI)
- [New-EC2RouteTable](#) (AWS Tools for Windows PowerShell)

Agregar y eliminar rutas de una tabla de enrutamiento

Puede añadir, eliminar y modificar rutas en las tablas de ruteo. Solo podrá modificar rutas que haya añadido.

Para obtener más información acerca de cómo trabajar con rutas estáticas para una conexión de Site-to-Site VPN, consulte [Edición de rutas estáticas para una conexión de Site-to-Site VPN](#) en la Guía del usuario de AWS Site-to-Site VPN.

Para modificar o añadir una ruta a una tabla de ruteo mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables (Tablas de ruteo) y, a continuación, seleccione la tabla de ruteo.
3. Elija Actions (Acciones), Edit routes (Editar rutas).
4. Para agregar una ruta, elija Add route (Añadir ruta). En Destination (Destino) introduzca el bloque CIDR de destino, una única dirección IP o el ID de una lista de prefijos.
5. Para modificar una ruta existente, para Destination (Destino), sustituya el bloque de CIDR de destino o la dirección IP única. En Target (Objetivo), elija un objetivo.
6. Elija Save routes (Guardar rutas).

Para añadir una ruta a una tabla de ruteo mediante la línea de comandos

- [create-route](#) (AWS CLI)
- [New-EC2Route](#) (AWS Tools for Windows PowerShell)

Note

Si agrega una ruta mediante una herramienta de línea de comandos o la API, el bloque de CIDR de destino se modifica automáticamente a su forma canónica. Por ejemplo, si especifica 100.68.0.18/18 para el bloque de CIDR, creamos una ruta con un bloque de CIDR de destino de 100.68.0.0/18.

Para sustituir una ruta existente en una tabla de ruteo mediante la línea de comandos

- [replace-route](#) (AWS CLI)
- [Set-EC2Route](#) (AWS Tools for Windows PowerShell)

Para eliminar una ruta de una tabla de ruteo mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.

2. En el panel de navegación, elija Route Tables (Tablas de ruteo) y, a continuación, seleccione la tabla de ruteo.
3. Elija Actions (Acciones), Edit routes (Editar rutas).
4. Seleccione el botón de eliminación (x) situado a la derecha de la ruta que desea eliminar.
5. Cuando haya terminado, elija Save routes (Guardar rutas).

Para eliminar una ruta de una tabla de ruteo mediante la línea de comandos

- [delete-route](#) (AWS CLI)
- [Remove-EC2Route](#) (AWS Tools for Windows PowerShell)

Habilitar o deshabilitar la propagación de rutas

La propagación de rutas permite que una gateway privada virtual propague automáticamente rutas a las tablas de ruteo. Esto significa que no es necesario introducir manualmente rutas de VPN en las tablas de ruteo. La propagación de rutas se puede habilitar ni deshabilitar.

Para completar este proceso, debe tener una gateway privada virtual.

Para obtener más información acerca de las opciones de enrutamiento de VPN, consulte [Opciones de enrutamiento de Site-to-Site VPN](#) en la Guía del usuario de Site-to-Site VPN.

Para habilitar la propagación de rutas utilizando la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables y, a continuación, seleccione la tabla de ruteo.
3. Elija Actions (Acciones), Edit route propagation (Editar propagación de rutas).
4. Seleccione la casilla de verificación Enable (Habilitar) situada junto a la gateway privada virtual y, a continuación, elija Save (Guardar).

Para habilitar la propagación de rutas mediante la línea de comandos

- [enable-vgw-route-propagation](#) (AWS CLI)
- [Enable-EC2VgwRoutePropagation](#) (AWS Tools for Windows PowerShell)

Para deshabilitar la propagación de rutas utilizando la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables y, a continuación, seleccione la tabla de ruteo.
3. Elija Actions (Acciones), Edit route propagation (Editar propagación de rutas).
4. Desactive la casilla de verificación Propagate y, a continuación, elija Save.

Para deshabilitar la propagación de rutas mediante la línea de comandos

- [disable-vgw-route-propagation](#) (AWS CLI)
- [Disable-EC2VgwRoutePropagation](#) (AWS Tools for Windows PowerShell)

Asociación de una subred a una tabla de ruteo

Para aplicar rutas de tablas de ruteo a una subred determinada, debe asociar la tabla de ruteo a la subred. Una tabla de ruteo se puede asociar con varias subredes. Sin embargo, una subred sólo puede asociarse

a una tabla de ruteo a la vez. Las subredes que no estén asociadas de manera explícita a ninguna tabla se asociarán implícitamente a la tabla de ruteo principal de forma predeterminada.

Para asociar una tabla de ruteo a una subred mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables y, a continuación, seleccione la tabla de ruteo.
3. En la pestaña Subnet associations (Asociaciones de subred), elija Edit subnet associations (Editar asociaciones de subred).
4. Seleccione la casilla de verificación para la subred que desee asociar a la tabla de enrutamiento. A continuación, elija Save associations (Guardar asociaciones).

Para asociar una subred a una tabla de ruteo mediante la línea de comandos

- [associate-route-table](#) (AWS CLI)
- [Register-EC2RouteTable](#) (AWS Tools for Windows PowerShell)

Cambiar la tabla de enrutamiento de una subred

Puede cambiar la asociación de la tabla de enrutamiento de una subred.

Al cambiar la tabla de enrutamiento, las conexiones existentes en la subred se eliminan a menos que la nueva tabla de enrutamiento contenga una ruta para el mismo tráfico al mismo destino.

Para cambiar la asociación de la tabla de ruteo de una subred mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets y, a continuación, seleccione la subred.
3. En la pestaña Route Table (Tabla de ruteo) elija Edit route table association (Editar asociación de la tabla de ruteo).
4. En la lista Route Table ID (ID de tabla de ruteo) seleccione la nueva tabla de ruteo a la que desea asociar la subred y, a continuación, elija Save (Guardar).

Para cambiar la tabla de ruteo asociada a una subred mediante el la línea de comandos

- [replace-route-table-association](#) (AWS CLI)
- [Set-EC2RouteTableAssociation](#) (AWS Tools for Windows PowerShell)

Desasociación de una subred de una tabla de ruteo

Puede desasociar una subred de una tabla de ruteo. Hasta que asocie la subred a otra tabla de ruteo, esta quedará implícitamente asociada a la tabla de ruteo principal.

Para desasociar una subred de una tabla de ruteo mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables y, a continuación, seleccione la tabla de ruteo.
3. En la pestaña Subnet associations (Asociaciones de subred), elija Edit subnet associations (Editar asociaciones de subred).
4. Desactive la casilla de verificación de la subred en cuestión y, a continuación, elija Save associations (Guardar asociaciones).

Para desasociar una subred de una tabla de ruteo mediante la línea de comandos

- [disassociate-route-table](#) (AWS CLI)
- [Unregister-EC2RouteTable](#) (AWS Tools for Windows PowerShell)

Sustituir la tabla de enrutamiento principal

Puede cambiar la tabla de ruteo principal de su VPC.

Para sustituir la tabla de ruteo principal mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables.
3. Seleccione la tabla de enrutamiento de la subred que será la nueva tabla de enrutamiento principal y, a continuación, elija Actions (Acciones), Set main route table (Configurar tabla de enrutamiento principal).
4. En el cuadro de diálogo de confirmación, elija Ok (Aceptar).

Para sustituir la tabla de ruteo principal mediante la línea de comandos

- [replace-route-table-association](#) (AWS CLI)
- [Set-EC2RouteTableAssociation](#) (AWS Tools for Windows PowerShell)

El procedimiento siguiente describe cómo quitar una asociación explícita entre una subred y la tabla de ruteo principal. El resultado es una asociación implícita entre la subred y la tabla de ruteo principal. El proceso es el mismo que el que se usa para desasociar subredes de tablas de ruteo.

Para quitar una asociación explícita a la tabla de ruteo principal

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables y, a continuación, seleccione la tabla de ruteo.
3. En la pestaña Subnet associations (Asociaciones de subred), elija Edit subnet associations (Editar asociaciones de subred).
4. Elija la subred y, a continuación, elija Save (Guardar).

Asociar una gateway a una tabla de enrutamiento

Puede asociar una gateway de Internet o a una gateway privada virtual a una tabla de ruteo. Para obtener más información, consulte [Tablas de ruteo de gateway](#) (p. 86).

Para asociar una gateway a la tabla de ruteo mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables y, a continuación, seleccione la tabla de ruteo.
3. Seleccione Actions (Acciones), Edit edge associations (Editar asociaciones de borde).
4. Seleccione la gateway y, a continuación, seleccione Save (Guardar).

Para asociar una gateway a la tabla de ruteo mediante la AWS CLI

Utilice el comando [associate-route-table](#). En el siguiente ejemplo se asocia una gateway de Internet `igw-11aa22bb33cc44dd1` a una tabla de ruteo `rtb-01234567890123456`.

```
aws ec2 associate-route-table --route-table-id rtb-01234567890123456 --gateway-id  
igw-11aa22bb33cc44dd1
```

Desasociar una gateway de una tabla de enrutamiento

Puede desasociar una gateway de Internet o a una gateway privada virtual de una tabla de ruteo.

Para asociar una gateway a la tabla de ruteo mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables y, a continuación, seleccione la tabla de ruteo.
3. Seleccione Actions (Acciones), Edit edge associations (Editar asociaciones de borde).
4. Elija la gateway que desea desasociar.
5. Seleccione Save.

Para desasociar una gateway de una tabla de ruteo mediante la línea de comandos

- [disassociate-route-table](#) (AWS CLI)
- [Unregister-EC2RouteTable](#) (AWS Tools for Windows PowerShell)

Reemplazar o restaurar el destino de una ruta local

Puede cambiar el objetivo de la ruta local predeterminada. Si reemplaza el destino de una ruta local, puede restaurarlo posteriormente al destino local predeterminado. Si la VPC tiene [varios bloques de CIDR \(p. 17\)](#), las tablas de enrutamiento tienen varias rutas locales (una por bloque de CIDR). Puede reemplazar o restaurar el destino de cada una de las rutas locales según sea necesario.

Para reemplazar el destino de una ruta local mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables y, a continuación, seleccione la tabla de ruteo.
3. Elija Actions (Acciones), Edit routes (Editar rutas).
4. En Target (Objetivo), elija un objetivo.
5. Elija Save routes (Guardar rutas).

Para restaurar el destino de una ruta local mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables y, a continuación, seleccione la tabla de ruteo.
3. Elija Actions (Acciones), Edit routes (Editar rutas).
4. En Target (Destino), elija local.
5. Elija Save routes (Guardar rutas).

Para reemplazar el destino de una ruta local mediante la AWS CLI

Utilice el comando [replace-route](#). En el ejemplo siguiente, se reemplaza el destino de la ruta local por `eni-11223344556677889`.

```
aws ec2 replace-route --route-table-id rtb-01234567890123456 --destination-cidr-block  
10.0.0.0/16 --network-interface-id eni-11223344556677889
```

Para restaurar el destino de una ruta local mediante la AWS CLI

En el ejemplo siguiente, se restaura el destino local en la tabla de ruteo `rtb-01234567890123456`.

```
aws ec2 replace-route --route-table-id rtb-01234567890123456 --destination-cidr-block 10.0.0.0/16 --local-target
```

Eliminación de una tabla de ruteo

Las tablas de ruteo solo se pueden eliminar si no tienen subredes asociadas. La tabla de ruteo principal no se puede eliminar.

Para eliminar una tabla de ruteo mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables.
3. Seleccione la tabla de ruteo y, a continuación, elija Actions (Acciones), Delete Route Table (Eliminar tabla de ruteo).
4. En el cuadro de diálogo de confirmación, elija Delete Route Table (Eliminar tabla de ruteo).

Para eliminar una tabla de ruteo mediante la línea de comandos

- [delete-route-table](#) (AWS CLI)
- [Remove-EC2RouteTable](#) (AWS Tools for Windows PowerShell)

Enrutamiento de Middlebox

Siga los pasos de esta sección para utilizar el enrutamiento de middlebox a fin de configurar el control preciso de la vía de enrutamiento del tráfico que entra o sale de la VPC.

Contenido

- [Escenarios de enrutamiento de middlebox \(p. 106\)](#)
- [Trabaje con el asistente de enrutamiento de middlebox \(p. 116\)](#)

Escenarios de enrutamiento de middlebox

Si desea configurar un control preciso sobre la vía de enrutamiento del tráfico dentro de la VPC, por ejemplo, redirigiendo el tráfico a un dispositivo de seguridad, puede utilizar el asistente de enrutamiento de middlebox en la consola de VPC. El asistente de enrutamiento de middlebox le ayuda a crear automáticamente las tablas de enrutamiento y rutas (saltos) necesarias para redirigir el tráfico según sea necesario.

Contenido

- [Inspeccione todo el tráfico destinado a una subred \(p. 107\)](#)
- [Dispositivo de seguridad detrás de un balanceador de carga de gateway en la VPC de seguridad \(p. 110\)](#)
- [Inspeccione el tráfico entre subredes \(p. 112\)](#)
- [Múltiples middleboxes en la misma VPC \(p. 114\)](#)

Inspeccione todo el tráfico destinado a una subred

Considere el escenario en el que tiene tráfico entrando en la VPC a través de una gateway de Internet y desea inspeccionar todo el tráfico destinado a una subred, por ejemplo la subred B, utilizando un dispositivo de firewall instalado en una instancia EC2. El dispositivo de firewall debe instalarse y configurarse en una instancia de Amazon EC2 en una subred independiente de la subred B de su VPC, por ejemplo, subred C. Puede utilizar el asistente de enrutamiento de middlebox para configurar rutas para el tráfico entre la subred B y la gateway de Internet.

El asistente de enrutamiento Middlebox realiza automáticamente las operaciones siguientes:

- Crea tres tablas de enrutamiento, una tabla de enrutamiento para la gateway de Internet (tabla de enrutamiento A), una tabla de enrutamiento para la subred B (tabla de enrutamiento B) y una tabla de enrutamiento para la subred C (tabla de enrutamiento C).
- Agrega las rutas necesarias a las nuevas tablas de enrutamiento como se describe en las siguientes secciones.
- Desasocia las tablas de enrutamiento actuales asociadas a la gateway de Internet, la subred B y la subred C.
- Asocia la tabla de enrutamiento A con la gateway de Internet (la fuente en el asistente de enrutamiento de middlebox), la tabla de enrutamiento C con la subred C (el Middlebox en el asistente de enrutamiento de middlebox) y la tabla de enrutamiento B con la subred B (el Destino en el asistente de enrutamiento de middlebox).
- Crea una etiqueta que indica que fue creada por el asistente de enrutamiento de middlebox y una etiqueta que indica la fecha de creación.

El asistente de enrutamiento de middlebox no modifica las tablas de enrutamiento existentes. Crea nuevas tablas de enrutamiento y, a continuación, las asocia con los recursos de la gateway y de la subred. Si los recursos ya están asociados explícitamente a las tablas de enrutamiento existentes, las tablas de enrutamiento existentes se desasocian primero y, a continuación, las nuevas tablas de enrutamiento se asocian a los recursos. Las tablas de enrutamiento existentes no se eliminan.

Si no utiliza el asistente de enrutamiento de middlebox, debe configurar manualmente y, a continuación, asignar las tablas de enrutamiento a las subredes y la gateway de Internet.

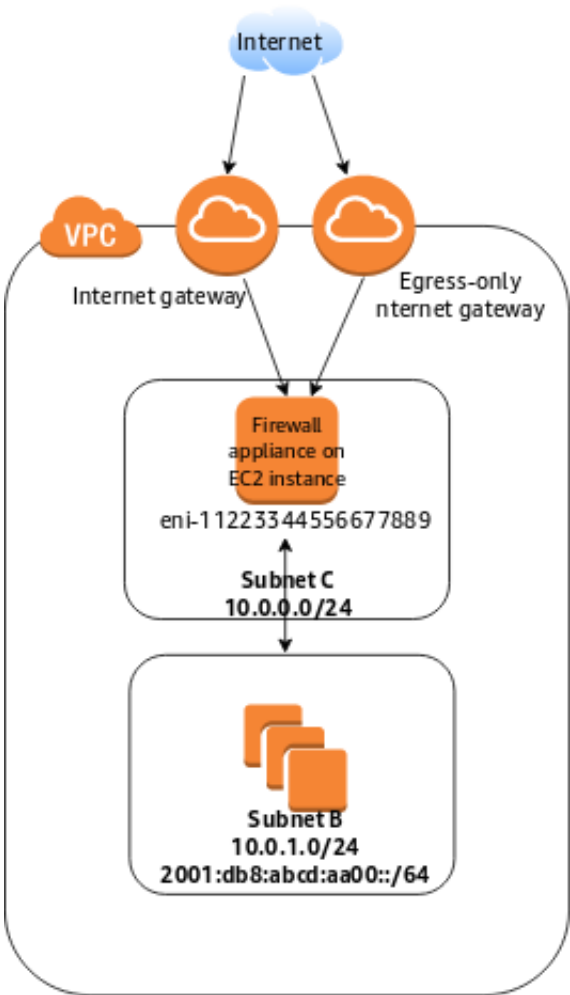


Tabla de enrutamiento de la gateway de Internet

La tabla de enrutamiento para la gateway de Internet contiene las siguientes rutas:

Destino	Objetivo	Finalidad
10.0.0.0/16	Local	Ruta local para IPv4
10.0.1.0/24	eni-11223344556677889	Dirija el tráfico IPv4 destinado a la subred B al middlebox
2001:db8:1234:1a00::/56	Local	Enrutamiento local de IPv6
2001:db8:1234:1a00::/64	eni-11223344556677889	Enrute el tráfico IPv6 destinado a la subred B al middlebox

Existe una asociación de borde entre la gateway de Internet y la VPC.

Cuando utiliza el asistente de enrutamiento de middlebox, las siguientes etiquetas están asociadas a la tabla de enrutamiento:

- Una etiqueta con una clave establecida en “Origen” y un Valor establecido en “Asistente de Middlebox”.

- Una etiqueta con una clave establecida en “date_created” y un valor establecido en el tiempo de creación, por ejemplo, “2021-02-18T22:25:49.137Z”.

Tabla de enrutamiento de la subred Middlebox

La tabla de enrutamiento para la subred de middlebox (Subred C) contiene las rutas siguientes:

Destino	Objetivo	Finalidad
10.0.0.0/16	Local	Ruta local para IPv4
0.0.0.0/0	igw-id	Dirija el tráfico de IPv4 a la gateway de Internet
2001:db8:1234:1a00::/56	Local	Enrutamiento local de IPv6
::/0	eigw-id	Dirija todo el tráfico de IPv6 a la gateway de Internet de solo salida.

Existe una asociación de subred con la subred B.

Cuando utiliza el asistente de enrutamiento de middlebox, las siguientes etiquetas están asociadas a la tabla de enrutamiento:

- Una etiqueta con una clave establecida en “Origen” y un Valor establecido en “Asistente de Middlebox”.
- Una etiqueta con una clave establecida en “date_created” y un valor establecido en el tiempo de creación, por ejemplo, “2021-02-18T22:25:49.137Z”.

Tabla de enrutamiento de subred

La tabla de enrutamiento para la subred de destino (Subred B) contiene las siguientes rutas:

Destino	Objetivo	Finalidad
10.0.0.0/16	Local	Ruta local
0.0.0.0/0	eni-11223344556677889	Dirija el tráfico IPv4 destinado a Internet al middlebox
2001:db8:1234:1a00::/56	Local	Enrutamiento local de IPv6
::/0	eni-11223344556677889	Dirija el tráfico IPv4 destinado a Internet al middlebox

Existe una asociación de subred con la subred C.

Cuando utiliza el asistente de enrutamiento de middlebox, las siguientes etiquetas están asociadas a la tabla de enrutamiento:

- Una etiqueta con una clave establecida en “Origen” y un Valor establecido en “Asistente de Middlebox”.
- Una etiqueta con una clave establecida en “date_created” y un valor establecido en el tiempo de creación, por ejemplo, “2021-02-18T22:25:49.137Z”.

Dispositivo de seguridad detrás de un balanceador de carga de gateway en la VPC de seguridad

En el siguiente ejemplo, desea inspeccionar el tráfico que entra a una VPC desde la gateway de Internet y destinado a la subred 1 mediante una flota de dispositivos de seguridad configurados detrás de un balanceador de carga de gateway en la VPC de seguridad. El propietario de la VPC del consumidor de servicios crea un punto de enlace del balanceador de carga de gateway en la subred 2 en su VPC (representada por una interfaz de red de punto de enlace). Todo el tráfico que entra en la VPC a través de la gateway de Internet se dirige primero al punto de enlace del balanceador de carga de gateway para su inspección en la VPC de seguridad antes de que se enrute a la subred 1 de destino. Del mismo modo, todo el tráfico que sale de la subred 1 se dirige primero al punto de enlace del balanceador de carga de gateway para su inspección en la VPC de seguridad antes de que se enrute a Internet.

El asistente de enrutamiento Middlebox realiza automáticamente las operaciones siguientes:

- Crea las tablas de enrutamiento.
- Agrega las rutas necesarias a las nuevas tablas de enrutamiento.
- Desasocia las tablas de enrutamiento actuales asociadas a las subredes.
- Asocia las tablas de enrutamiento que crea el asistente de enrutamiento de middlebox con las subredes.
- Crea una etiqueta que indica que fue creada por el asistente de enrutamiento de middlebox y una etiqueta que indica la fecha de creación.

El asistente de enrutamiento de middlebox no modifica las tablas de enrutamiento existentes. Crea nuevas tablas de enrutamiento y, a continuación, las asocia con los recursos de la gateway y de la subred. Si los recursos ya están asociados explícitamente a las tablas de enrutamiento existentes, las tablas de enrutamiento existentes se desasocian primero y, a continuación, las nuevas tablas de enrutamiento se asocian a los recursos. Las tablas de enrutamiento existentes no se eliminan.

Si no utiliza el asistente de enrutamiento de middlebox, debe configurar manualmente y, a continuación, asignar las tablas de enrutamiento a las subredes y la gateway de Internet.

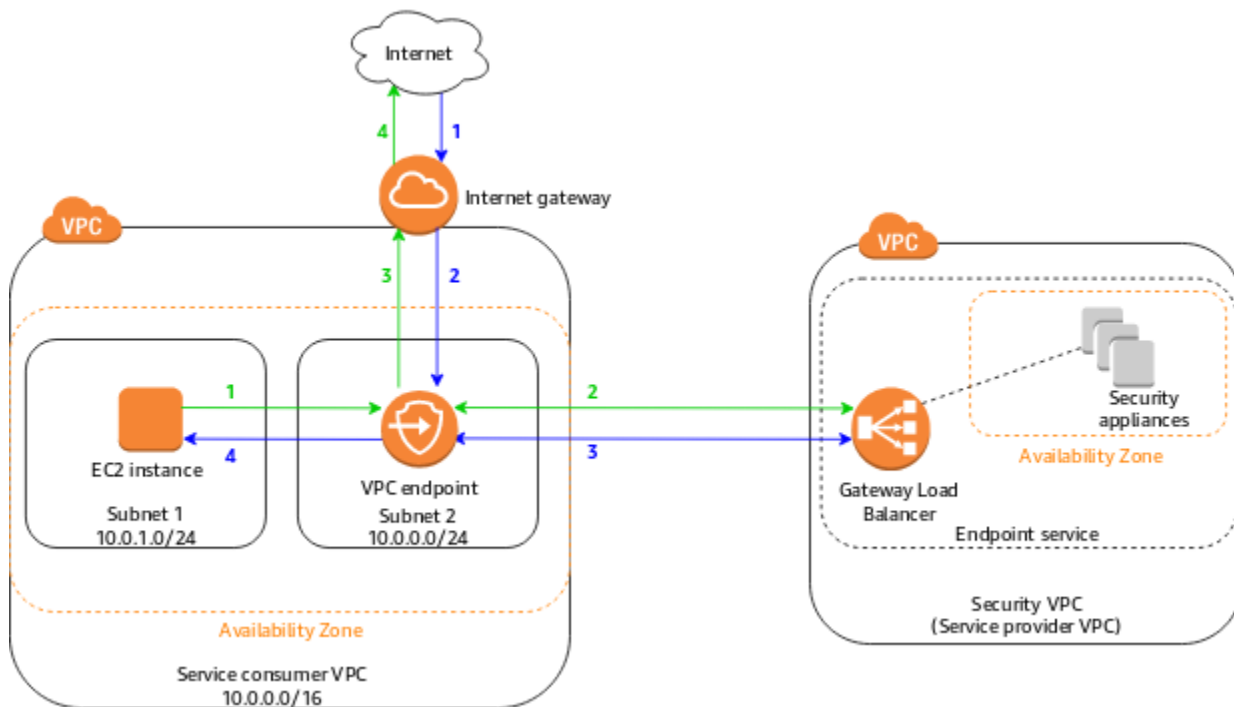


Tabla de enrutamiento de gateway

La tabla de enrutamiento de la gateway de internet tiene las siguientes rutas:

Destino	Objetivo	Finalidad
10.0.0.0/16	Local	Local
10.0.1.0/24	vpc-endpoint-id	Dirija el tráfico destinado a la subred 1 al punto de enlace del balanceador de carga de gateway.

Existe una asociación de borde con la gateway.

Cuando utiliza el asistente de enrutamiento de middlebox, las siguientes etiquetas están asociadas a la tabla de enrutamiento:

- Una etiqueta con una clave establecida en "Origen" y un Valor establecido en "Asistente de Middlebox".
- Una etiqueta con una clave establecida en "date_created" y un valor establecido en el tiempo de creación, por ejemplo, "2021-02-18T22:25:49.137Z".

Tabla de enrutamiento de subred 1

La tabla de enrutamiento de subred 1 tiene las siguientes rutas.

Destino	Objetivo	Finalidad
10.0.0.0/16	Local	Ruta local
0.0.0.0/0	vpc-endpoint-id	Dirija el tráfico no local al punto de enlace del balanceador de carga de gateway. Esto garantiza que todo el tráfico que sale de la subred (destinado a Internet) se dirija primero al punto de enlace del balanceador de carga de gateway.

Existe una asociación de subred con la subred 1.

Cuando utiliza el asistente de enrutamiento de middlebox, las siguientes etiquetas están asociadas a la tabla de enrutamiento:

- Una etiqueta con una clave establecida en "Origen" y un Valor establecido en "Asistente de Middlebox".
- Una etiqueta con una clave establecida en "date_created" y un valor establecido en el tiempo de creación, por ejemplo, "2021-02-18T22:25:49.137Z".

Tabla de enrutamiento de subred 2

La tabla de enrutamiento de subred 2 tiene las siguientes rutas.

Destino	Objetivo	Finalidad
10.0.0.0/16	Local	Ruta local: para el tráfico que se originó desde Internet, la ruta local garantiza que se dirija a su destino en la subred 1
0.0.0.0/0	igw-id	Dirige todo el tráfico a la gateway de Internet

Existe una asociación de subred con la subred 2.

Las siguientes etiquetas están asociadas a la tabla de enrutamiento:

- Una etiqueta con una clave establecida en "Origen" y un Valor establecido en "Asistente de Middlebox".
- Una etiqueta con una clave establecida en "date_created" y un valor establecido en el tiempo de creación, por ejemplo, "2021-02-18T22:25:49.137Z".

Inspeccione el tráfico entre subredes

Considere el escenario en el que tiene varias subredes en una VPC y desea inspeccionar el tráfico entre las subredes A y B mediante un dispositivo de firewall instalado en una instancia de EC2. Configure e instale el dispositivo de firewall en una instancia de EC2 en una subred C separada de la VPC. El dispositivo inspecciona todo el tráfico que circula entre las subredes A y B.

Utilice la ruta principal para la VPC y la subred de middlebox. Cada una de las subredes A y B tiene una tabla de rutas personalizada.

El asistente de enrutamiento Middlebox realiza automáticamente las operaciones siguientes:

- Crea las tablas de enrutamiento.
- Agrega las rutas necesarias a las nuevas tablas de enrutamiento.
- Desasocia las tablas de enrutamiento actuales asociadas a las subredes.
- Asocia las tablas de enrutamiento que crea el asistente de enrutamiento de middlebox con las subredes.
- Crea una etiqueta que indica que fue creada por el asistente de enrutamiento de middlebox y una etiqueta que indica la fecha de creación.

El asistente de enrutamiento de middlebox no modifica las tablas de enrutamiento existentes. Crea nuevas tablas de enrutamiento y, a continuación, las asocia con los recursos de la gateway y de la subred. Si los recursos ya están asociados explícitamente a las tablas de enrutamiento existentes, las tablas de enrutamiento existentes se desasocian primero y, a continuación, las nuevas tablas de enrutamiento se asocian a los recursos. Las tablas de enrutamiento existentes no se eliminan.

Si no utiliza el asistente de enrutamiento de middlebox, debe configurar manualmente y, a continuación, asignar las tablas de enrutamiento a las subredes y la gateway de Internet.

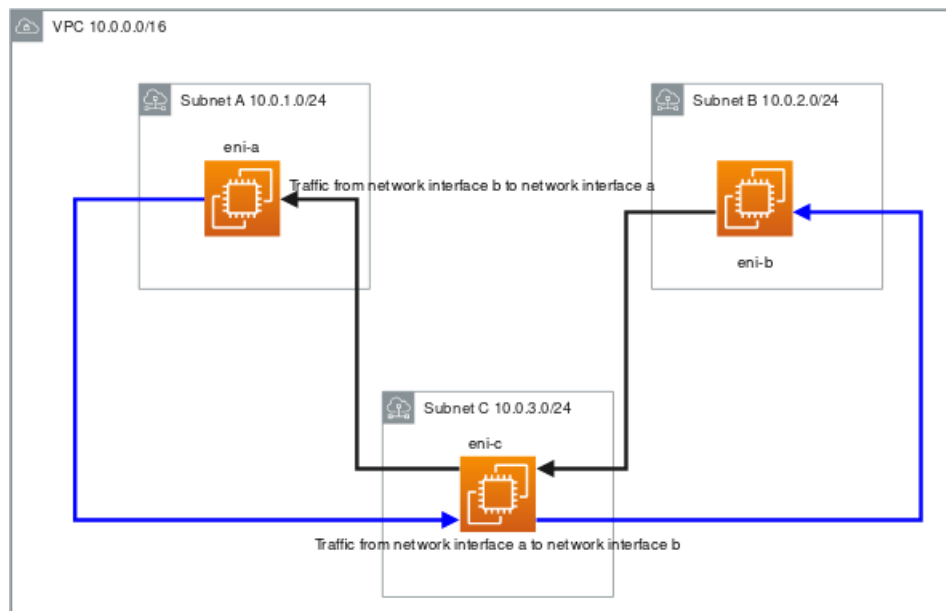


Tabla de rutas A de subred personalizada

Las tablas de enrutamiento de las subredes tienen las rutas siguientes.

Destino	Objetivo	Finalidad
10.0.0.0/16	Local	Ruta local
10.0.2.0/24	eni-c	Enrutar el tráfico destinado a la subred B a la caja intermedia

Existe una asociación de subred con la subred A.

Cuando utiliza el asistente de enrutamiento de middlebox, las siguientes etiquetas están asociadas a la tabla de enrutamiento:

- Una etiqueta con una clave establecida en “Origen” y un Valor establecido en “Asistente de Middlebox”.
- Una etiqueta con una clave establecida en “date_created” y un valor establecido en el tiempo de creación, por ejemplo, “2021-02-18T22:25:49.137Z”.

Tabla de enrutamiento de subred B personalizada

La tabla de enrutamiento de la subred B tienen las siguientes rutas:

Destino	Objetivo	Finalidad
10.0.0.0/16	Local	Ruta local
10.0.1.0/24	eni-c	Enrute el tráfico destinado a la subred A a la middlebox

Existe una asociación de subred con la subred B.

Cuando utiliza el asistente de enrutamiento de middlebox, las siguientes etiquetas están asociadas a la tabla de enrutamiento:

- Una etiqueta con una clave establecida en “Origen” y un Valor establecido en “Asistente de Middlebox”.
- Una etiqueta con una clave establecida en “date_created” y un valor establecido en el tiempo de creación, por ejemplo, “2021-02-18T22:25:49.137Z”.

Tabla de enrutamiento principal

La tabla de enrutamiento principal de la VPC y la subred C tiene la siguiente ruta.

Destino	Objetivo	Finalidad
10.0.0.0/16	Local	Ruta local

Existe una asociación de subred con la subred C.

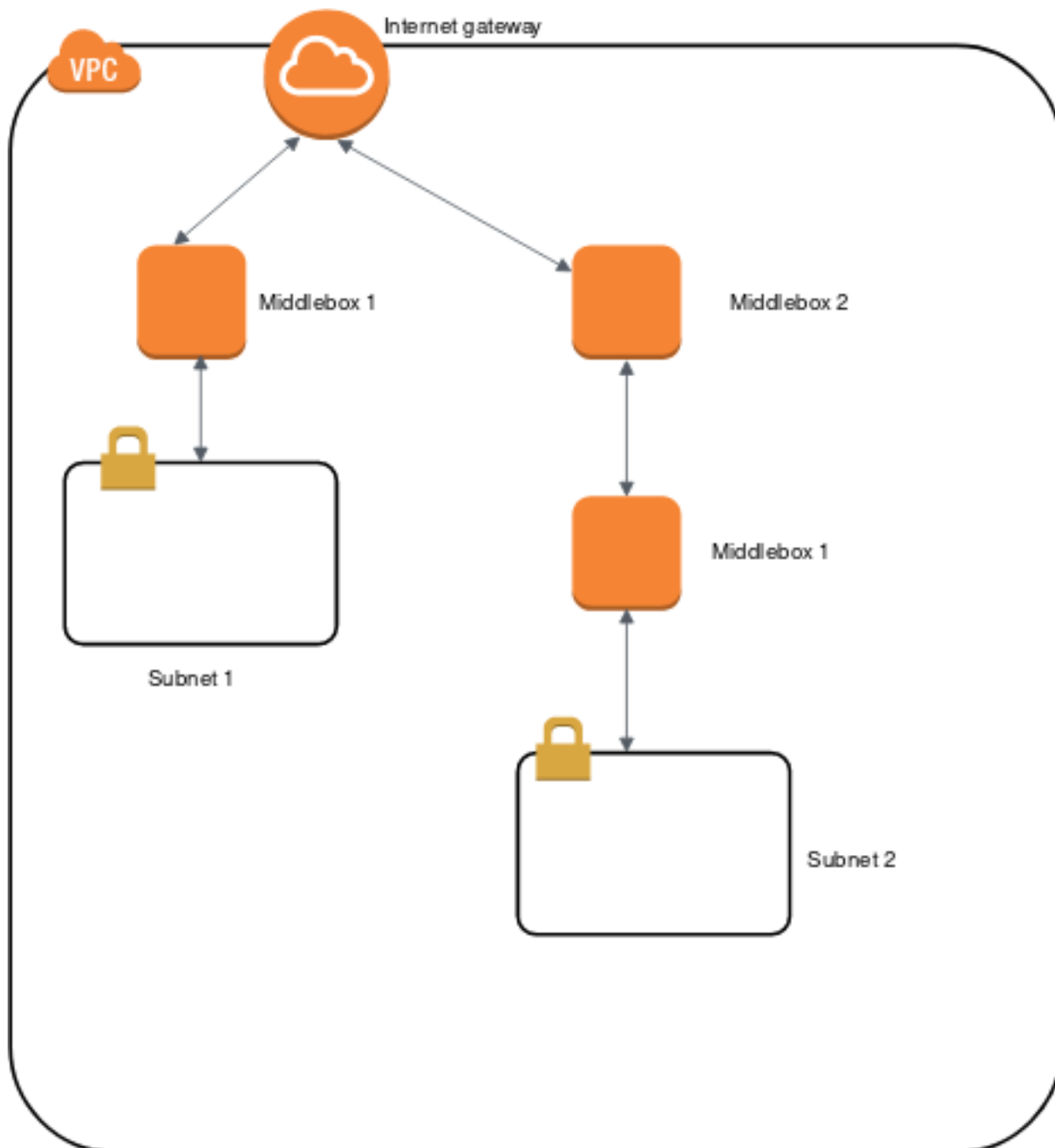
Cuando utiliza el asistente de enrutamiento de middlebox, las siguientes etiquetas están asociadas a la tabla de enrutamiento:

- Una etiqueta con una clave establecida en “Origen” y un Valor establecido en “Asistente de Middlebox”.
- Una etiqueta con una clave establecida en “date_created” y un valor establecido en el tiempo de creación, por ejemplo, “2021-02-18T22:25:49.137Z”.

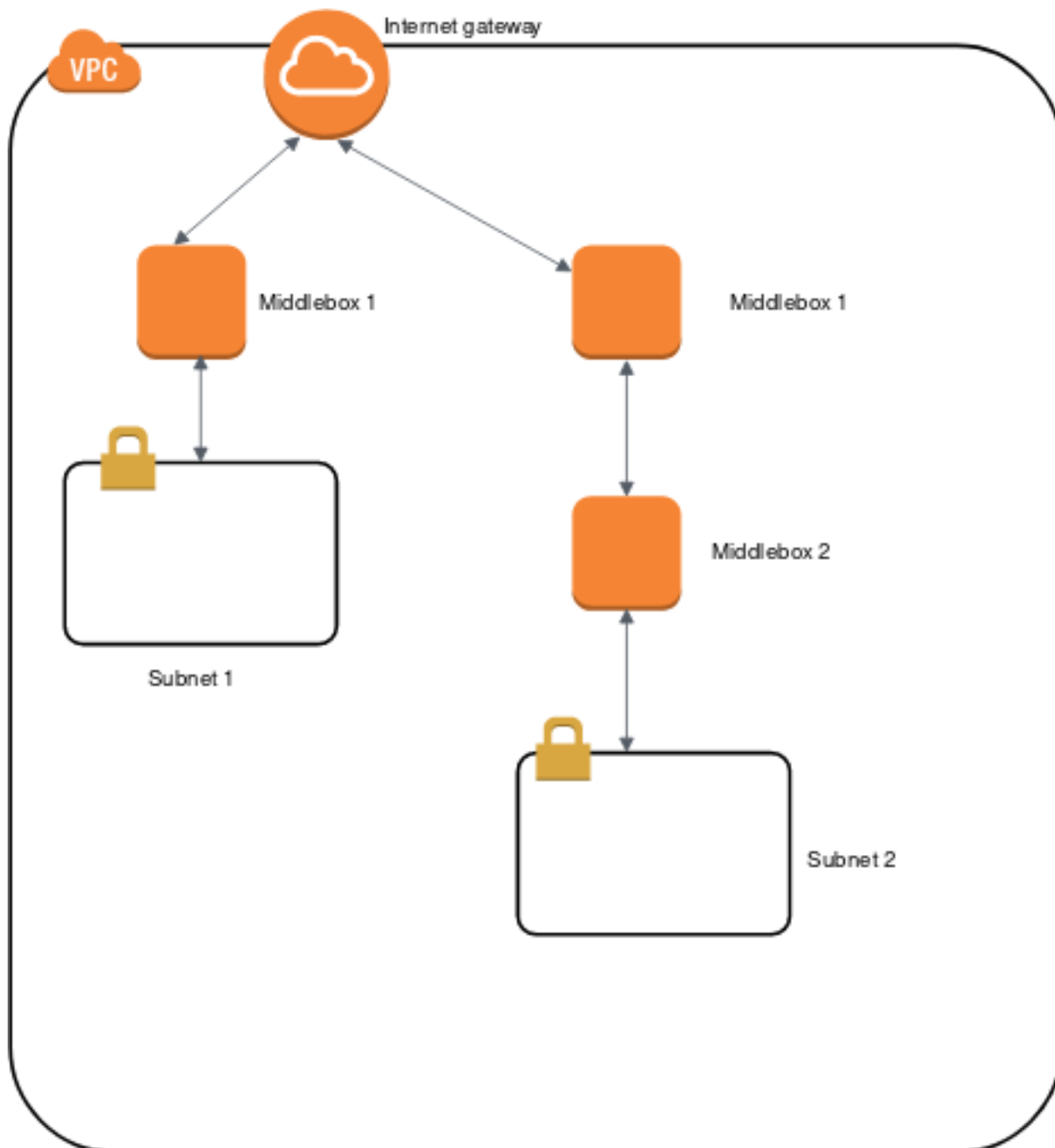
Múltiples middleboxes en la misma VPC

Misma Middlebox que inspecciona el tráfico de varias subredes en la misma VPC

Considere el escenario en el que tiene tráfico entrando en la VPC a través de una gateway de Internet y desea inspeccionar todo el tráfico destinado a la subred 1, utilizando el cuadro intermedio 1. Dentro de la misma VPC, desea utilizar middlebox 2 y middlebox 1 para inspeccionar el tráfico destinado a la subred 2. No se admite la siguiente configuración, ya que para las tablas de enrutamiento de las subredes asociadas con los middleboxes cada una necesita una ruta para 0.0.0.0/0 que dirige el tráfico a la gateway de Internet.



Si desea tener el mismo middlebox en esta configuración, entonces el middlebox debe estar en la misma posición de salto (por ejemplo, el salto después de la gateway de Internet) para ambas subredes. Esto significa que la tabla de enrutamiento para la subred asociada con middlebox 2 tiene una ruta para `0.0.0.0/0` que dirige el tráfico a la subred de middlebox 1. Hay una ruta en la tabla de enrutamiento asociada con el middlebox 1 que tiene una ruta para `0.0.0.0/0` que dirige el tráfico a la gateway de Internet.



Trabaje con el asistente de enrutamiento de middlebox

Si desea configurar un control preciso sobre la ruta de enrutamiento del tráfico que entra o sale de la VPC, por ejemplo, redirigiendo el tráfico a un dispositivo de seguridad, puede utilizar el asistente de enrutamiento de middlebox en la consola de VPC. El asistente de enrutamiento de middlebox le ayuda a crear automáticamente las tablas de enrutamiento y rutas (saltos) necesarias para redirigir el tráfico según sea necesario.

El asistente de enrutamiento de middlebox puede ayudarle a configurar el enrutamiento para los siguientes escenarios:

- Dirigir el tráfico a un dispositivo de middlebox, por ejemplo, una instancia de Amazon EC2 configurada como dispositivo de seguridad.
- Enrutamiento de tráfico a un balanceador de carga de gateway Para obtener más información, consulte la [User Guide for Gateway Load Balancers](#) (Guía del usuario para Gateway Load Balancers).

Para obtener más información, consulte [the section called “Escenarios de enrutamiento de middlebox”](#) (p. 106).

Contenido

- [Requisitos previos del asistente de enrutamiento de Middlebox](#) (p. 117)
- [Use el asistente de enrutamiento de middlebox](#) (p. 117)
- [Consideraciones del asistente de enrutamiento de Middlebox](#) (p. 119)
- [Información relacionada](#) (p. 120)

Requisitos previos del asistente de enrutamiento de Middlebox

Consulte el [the section called “Consideraciones del asistente de enrutamiento de Middlebox”](#) (p. 119). A continuación, asegúrese de que dispone de la siguiente información antes de utilizar el asistente de enrutamiento Middlebox.

- La VPC.
- El recurso en el que el tráfico se origina o entra en la VPC, por ejemplo, una gateway de Internet, una gateway privada virtual o una interfaz de red.
- La interfaz de red de middlebox o el punto de enlace del balanceador de carga de gateway.
- La subred de destino del tráfico.

Use el asistente de enrutamiento de middlebox

El asistente de enrutamiento de middlebox está disponible en el Amazon Virtual Private Cloud Console.

Contenido

- [Cree rutas mediante el asistente de enrutamiento de middlebox](#) (p. 117)
- [Modificar rutas de Middlebox](#) (p. 118)
- [Vea las tablas de enrutamiento del asistente de enrutamiento de middlebox](#) (p. 119)
- [Elimine la configuración del asistente de enrutamiento de middlebox](#) (p. 119)

Cree rutas mediante el asistente de enrutamiento de middlebox

Para crear rutas mediante el asistente de enrutamiento de middlebox

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs (Sus VPC).
3. Seleccione su VPC y, a continuación, elija Actions (Acciones), Manage middlebox routes (Administrar rutas de middlebox).
4. Elija Create routes (Crear rutas).
5. En la página Specify routes (Especificar rutas), haga lo siguiente:
 - Para Source (Fuente), elija la fuente de su tráfico. Si elige una gateway privada virtual, para Destination IPv4 CIDR (CIDR de destino IPv4), ingrese el CIDR para el tráfico en las instalaciones que entra a la VPC desde la gateway privada virtual.

- Para Middlebox, elija el ID de interfaz de red asociado con el dispositivo middlebox o, cuando utilice un punto de enlace del balanceador de carga de gateway, elija el ID de punto de enlace de la VPC.
 - Para Destination subnet (Subred de destino), elija la subred de destino.
6. (Opcional) Para agregar otra subred de destino, elija Add additional subnet (Agregado de subred adicional) y, a continuación, haga lo siguiente:
- Para Middlebox, elija el ID de interfaz de red asociado con el dispositivo middlebox o, cuando utilice un punto de enlace del balanceador de carga de gateway, elija el ID de punto de enlace de la VPC.
- Debe utilizar el mismo dispositivo middlebox para varias subredes.
- Para Destination subnet (Subred de destino), elija la subred de destino.
7. (Opcional) Para agregar otra fuente, elija Add source (Agregar fuente) y, a continuación, repita los pasos anteriores.
8. Elija Next (Siguiente).
9. En la página Review and create (Revisar y crear), compruebe las rutas y, a continuación, elija Create routes (Creación de rutas).

Modificar rutas de Middlebox

Puede editar la configuración de la ruta cambiando la gateway, el middlebox o la subred de destino.

Al realizar cualquier modificación, el asistente de enrutamiento de middlebox realiza automáticamente las siguientes operaciones:

- Crea nuevas tablas de enrutamiento para la gateway, el middlebox y la subred de destino.
- Agrega las rutas necesarias a las nuevas tablas de enrutamiento.
- Desasocia las tablas de enrutamiento actuales que el asistente de enrutamiento de middlebox asoció a los recursos.
- Asocia las nuevas tablas de enrutamientos que crea el asistente de enrutamiento de middlebox con los recursos.

Para modificar rutas de middlebox mediante el asistente de enrutamiento de middlebox

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs (Sus VPC).
3. Seleccione su VPC y, a continuación, elija Actions (Acciones), Manage middlebox routes (Administrar rutas de middlebox).
4. Elija Edit routes (Editar rutas).
5. Para cambiar la gateway, para Source (Fuente), elija la gateway a través de la cual el tráfico entra en su VPC. Si elige una gateway privada virtual, para Destination IPv4 CIDR (CIDR de destino IPv4), introduzca la subred CIDR de destino.
6. Para agregar otra subred de destino, elija Add additional subnet (Agregado de subred adicional) y, a continuación, haga lo siguiente:
 - Para Middlebox, elija el ID de interfaz de red asociado con el dispositivo middlebox o, cuando utilice un punto de enlace del balanceador de carga de gateway, elija el ID de punto de enlace de la VPC.Debe utilizar el mismo dispositivo middlebox para varias subredes.
 - Para Destination subnet (Subred de destino), elija la subred de destino.
7. Elija Next (Siguiente).
8. En la página Review and update (Realice la revisión y actualización), se muestra una lista de tablas de enrutamiento y sus rutas que creará el asistente de enrutamiento de middlebox. Compruebe las

rutas y, a continuación, en el cuadro de diálogo de confirmación, elija Update routes (Actualización de rutas).

Vea las tablas de enrutamiento del asistente de enrutamiento de middlebox

Para ver las tablas de enrutamiento del asistente de enrutamiento de middlebox

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs (Sus VPC).
3. Seleccione su VPC y, a continuación, elija Actions (Acciones), Manage middlebox routes (Administrar rutas de middlebox).
4. En Middlebox route tables (Tablas de enrutamiento de Middlebox), el número indica cuántas rutas creó el asistente de enrutamiento de middlebox. Elija el número para ver las rutas.

Mostramos las rutas del asistente de enrutamiento de middlebox en una página de tabla de enrutamiento separada.

Elimine la configuración del asistente de enrutamiento de middlebox

Si decide que ya no desea configurar el asistente de enrutamiento de Middlebox, debe eliminar manualmente las tablas de enrutamiento.

Para eliminar la configuración del asistente de enrutamiento de middlebox

1. Vea las tablas de enrutamiento del asistente de enrutamiento de middlebox. Para obtener más información, consulte [the section called “Vea las tablas de enrutamiento del asistente de enrutamiento de middlebox” \(p. 119\)](#).

Después de realizar la operación, las tablas de enrutamiento creadas por el asistente de enrutamiento de middlebox aparecen en una página de tabla de rutas independiente.

2. Elimine cada tabla de enrutamiento que aparezca. Para obtener más información, consulte [the section called “Eliminación de una tabla de ruteo” \(p. 106\)](#).

Consideraciones del asistente de enrutamiento de Middlebox

Tenga en cuenta lo siguiente cuando utilice el asistente de enrutamiento Middlebox:

- Si desea inspeccionar el tráfico, puede utilizar una gateway de Internet o una gateway privada virtual para la fuente.
- Si utiliza el mismo middlebox en una configuración de varios middlebox dentro de la misma VPC, asegúrese de que el middlebox esté en la misma posición de salto para ambas subredes.
- El dispositivo debe configurarse en una subred independiente para la subred de fuente o destino.
- Debe deshabilitar la comprobación de origen/destino en el dispositivo. Para obtener más información, consulte [Cambio de la comprobación de origen o destino](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
- Las tablas de enrutamiento y rutas que crea el asistente de enrutamiento de middlebox cuentan para las cuotas. Para obtener más información, consulte [the section called “Tablas de ruteo” \(p. 381\)](#).
- Si elimina un recurso, por ejemplo una interfaz de red, se eliminarán las asociaciones de tabla de enrutamiento con el recurso. Si el recurso es un destino, el aborrecimiento de la ruta se establece en agujero negro. Las tablas de enrutamiento no se eliminan.
- La subred Middlebox y la subred de destino deben estar asociadas a una tabla de enrutamiento no predeterminada.

Note

Se recomienda utilizar el asistente de enrutamiento de middlebox para modificar o eliminar cualquier tabla de enrutamiento creada mediante el asistente de enrutamiento de middlebox.

Información relacionada

Para obtener información adicional acerca de cómo crear los recursos que utiliza con el asistente de enrutamiento de middlebox, consulte lo siguiente:

- [the section called “Gateways de Internet” \(p. 142\)](#)
- [Asociar direcciones IP elásticas con recursos en la VPC \(p. 149\)](#)
- [Puntos de enlace del equilibrador de carga de gateway \(AWS PrivateLink\)](#)
- [Balanceadores de carga de gateway del Elastic Load Balancing](#)

Controlar el tráfico hacia las subredes utilizando las ACL de red

Una lista de control de acceso (ACL) de red es una capa de seguridad opcional para su VPC que actúa como firewall para controlar el tráfico entrante y saliente de una o varias subredes. Puede configurar ACL de red con reglas similares a sus grupos de seguridad para añadir una capa de seguridad adicional a su VPC. Para obtener más información acerca de las diferencias entre los grupos de seguridad y las ACL de red, consulte [Comparar grupos de seguridad y ACL de red \(p. 234\)](#).

Contenido

- [Conceptos básicos de la ACL de red \(p. 120\)](#)
- [Reglas de ACL de red \(p. 121\)](#)
- [ACL de red predeterminada \(p. 121\)](#)
- [ACL de red personalizada \(p. 123\)](#)
- [ACL de red personalizadas y otros servicios de AWS \(p. 133\)](#)
- [Puertos efímeros \(p. 133\)](#)
- [Detección de la MTU de la ruta \(p. 133\)](#)
- [Trabajar con ACL de red \(p. 134\)](#)
- [Ejemplo: controlar el acceso a las instancias de una subred \(p. 138\)](#)
- [Reglas recomendadas para casos de uso del asistente de la VPC \(p. 140\)](#)

Conceptos básicos de la ACL de red

A continuación se describen los conceptos básicos que debe saber acerca de las ACL de red:

- Su VPC incluye automáticamente una ACL de red predeterminada y modificable. De forma predeterminada, permite todo el tráfico IPv4 entrante y saliente y, si corresponde, el tráfico IPv6.
- Puede crear una ACL de red personalizada y asociarla a una subred. De forma predeterminada, todas las ACL de red personalizadas denegarán todo el tráfico entrante y saliente hasta que añada reglas.
- Cada subred de su VPC debe estar asociada a una ACL de red. Si no asocia una subred de forma explícita a una ACL de red, la subred se asociará automáticamente a la ACL de red predeterminada.

- Puede asociar una ACL de red con varias subredes. Sin embargo, una subred sólo puede asociarse a una ACL de red a la vez. Al asociar una ACL de red a una subred, se quita la asociación anterior.
- Una ACL de red contiene una lista numerada de reglas. Evaluamos las reglas por orden, empezando por la regla con el número más bajo, para determinar si se permite el tráfico entrante o saliente de alguna subred asociada a la ACL de red. El número más alto que puede utilizar para una regla es 32766. Le recomendamos que empiece creando reglas en incrementos (por ejemplo, incrementos de 10 o 100), de forma que pueda insertar reglas nuevas cuando lo necesite más adelante.
- Una ACL de red tiene reglas entrantes y salientes por separado, y cada regla puede permitir o denegar el tráfico.
- Las ACL de red son sin estado, lo que significa que las respuestas al tráfico entrante permitido están sujetas a las reglas de tráfico saliente (y viceversa).

Existen cuotas (límites) para el número de ACL de red por VPC y el número de reglas por ACL de red. Para obtener más información, consulte [Cuotas de Amazon VPC \(p. 378\)](#).

Reglas de ACL de red

Puede añadir o quitar reglas de la ACL de red predeterminada, o bien crear ACL de red adicionales para su VPC. Al añadir o quitar reglas de una ACL de red, los cambios se aplicarán automáticamente a las subredes con las que esté asociada.

Las siguientes son las partes de una regla de ACL de red:

- Número de regla. Las reglas se evalúan comenzando por la regla con el número más bajo. Cuando una regla coincide con el tráfico, esta se aplica independientemente de si hay una regla con un número más alto que la pueda contradecir.
- Tipo. El tipo de tráfico; por ejemplo, SSH. También puede especificar todo el tráfico o un rango personalizado.
- Protocolo. Puede especificar cualquier protocolo que tenga un número de protocolo estándar. Para obtener más información, consulte [Protocol Numbers](#). Si especifica ICMP como el protocolo, puede especificar cualquiera de los tipos y códigos de ICMP.
- Rango de puertos. El puerto de escucha o el rango de puertos para el tráfico. Por ejemplo, 80 para el tráfico HTTP.
- Source. [Solo reglas de entrada] Origen del tráfico (rango de CIDR).
- Destino. [Solo reglas de salida] Destino del tráfico (rango de CIDR).
- Permitir/Denegar. permitir o denegar el tráfico especificado.

Si agrega una regla mediante una herramienta de línea de comandos o la API de Amazon EC2, el intervalo de CIDR se modifica automáticamente a la forma canónica. Por ejemplo, si especifica `100.68.0.18/18` en el rango de CIDR, creamos una regla con un rango de CIDR `100.68.0.0/18`.

ACL de red predeterminada

La ACL de red predeterminada está configurada para permitir todo el tráfico entrante y saliente de las subredes con las que está asociada. Cada ACL de red también incluye una regla cuyo número de regla es un asterisco. Esta regla garantiza que si un paquete no coincide con ninguna de las reglas numeradas, se denegará. No es posible modificar ni quitar esta regla.

A continuación se muestra un ejemplo de una ACL de red predeterminada para una VPC que solo admite IPv4.

Entrada

Regla n.º	Tipo	Protocolo	Rango de puerto	Fuente	Permitir/Denegar
100	All IPv4 traffic	Todos	Todos	0.0.0.0/0	PERMITIR
*	All IPv4 traffic	Todos	Todos	0.0.0.0/0	DENEGAR
Salida					
Regla n.º	Tipo	Protocolo	Rango de puerto	Destino	Permitir/Denegar
100	All IPv4 traffic	Todos	Todos	0.0.0.0/0	PERMITIR
*	All IPv4 traffic	Todos	Todos	0.0.0.0/0	DENEGAR

Si crea una VPC con un bloque de CIDR IPv6 o si asocia un bloque de CIDR IPv6 con su VPC existente, añadiremos automáticamente reglas que permitan todo el tráfico IPv6 entrante y saliente de su subred. Asimismo, añadiremos reglas cuyos números de regla sean un asterisco que asegure que un paquete se denegará si no coincide con ninguno de las demás reglas numeradas. No es posible modificar ni quitar estas reglas. A continuación se muestra un ejemplo de una ACL de red predeterminada para una VPC que solo admite IPv4 e IPv6.

Note

Si ha modificado sus reglas entrantes predeterminadas de la ACL de red, no se añadirá automáticamente una regla permitir para el tráfico IPv6 entrante cuando asocie un bloque de IPv6 a su VPC. De forma similar, si ha modificado las reglas salientes, no añadiremos automáticamente una regla permitir para el tráfico IPv6 saliente.

Entrada					
Regla n.º	Tipo	Protocolo	Rango de puerto	Fuente	Permitir/Denegar
100	All IPv4 traffic	Todos	Todos	0.0.0.0/0	PERMITIR
101	Todo el tráfico IPv6	Todos	Todos	::/0	PERMITIR
*	All traffic	Todos	Todos	0.0.0.0/0	DENEGAR
*	Todo el tráfico IPv6	Todos	Todos	::/0	DENEGAR
Salida					
Regla n.º	Tipo	Protocolo	Rango de puerto	Destino	Permitir/Denegar
100	All traffic	Todos	Todos	0.0.0.0/0	PERMITIR
101	Todo el tráfico IPv6	Todos	Todos	::/0	PERMITIR
*	All traffic	Todos	Todos	0.0.0.0/0	DENEGAR
*	Todo el tráfico IPv6	Todos	Todos	::/0	DENEGAR

ACL de red personalizada

La siguiente tabla muestra un ejemplo de una ACL de red personalizada para una VPC que solo admite IPv4. Incluye reglas que permiten el tráfico HTTP y HTTPS entrante (reglas entrantes 100 y 110). Hay una regla saliente correspondiente que permite las respuestas a ese tráfico entrante (regla saliente 140, que cubre los puertos efímeros 32768-65535). Para obtener más información acerca de cómo seleccionar el rango de puerto efímero correcto, consulte [Puertos efímeros \(p. 133\)](#).

La ACL de red también incluye reglas entrantes que permiten el tráfico SSH y RDP en la subred. La regla saliente 120 permite que las respuestas dejen la subred.

La ACL de red tiene reglas salientes (100 y 110) que permiten que el tráfico saliente HTTP y HTTPS salga de la subred. Hay una regla entrante correspondiente que permite las respuestas a ese tráfico saliente (regla entrante 140, que cubre los puertos efímeros 32768-65535).

Note

Cada ACL de red incluye una regla predeterminada cuyo número de regla es un asterisco. Esta regla garantiza que si un paquete no coincide con ninguna de las demás reglas, se denegará. No es posible modificar ni quitar esta regla.

Entrada						
Regla n.º	Tipo	Protocolo	Rango de puerto	Fuente	Permitir/Denegar	Comentarios
100	HTTP	TCP	80	0.0.0.0/0	PERMITIR	Permite el tráfico HTTP entrante de cualquier dirección IPv4.
110	HTTPS	TCP	443	0.0.0.0/0	PERMITIR	Permite el tráfico HTTPS entrante de cualquier dirección IPv4.
120	SSH	TCP	22	192.0.2.0/24	PERMITIR	Permite el tráfico SSH entrante del rango del rango de direcciones IPv4 públicas de su red doméstica (a través de la gateway de Internet).
130	RDP	TCP	3389	192.0.2.0/24	PERMITIR	Permite el tráfico RDP entrante a

						servidores web desde el rango de direcciones IPv4 públicas de su red doméstica (a través del puerto de la gateway de Internet).
140	Custom TCP	TCP	32768-65535	0.0.0.0/0	PERMITIR	Permite el tráfico IPv4 de retorno entrante de Internet (es decir, para solicitudes que se originan en la subred). Este rango se proporciona solo como ejemplo. Para obtener más información acerca de cómo seleccionar el rango de puerto efímero correcto, consulte Puertos efímeros (p. 133) .
*	All traffic	Todos	Todos	0.0.0.0/0	DENEGAR	Deniega todo el tráfico IPv4 entrante no controlado por ninguna regla precedente (no modificable).
Salida						
Regla n.º	Tipo	Protocolo	Rango de puerto	Destino	Permitir/Denegar	Comentarios

100	HTTP	TCP	80	0.0.0.0/0	PERMITIR	Permite el tráfico HTTP IPv4 saliente de la subred a Internet.
110	HTTPS	TCP	443	0.0.0.0/0	PERMITIR	Permite el tráfico HTTPS IPv4 saliente de la subred a Internet.
120	SSH	TCP	1024 - 65535	192.0.2.0/24	PERMITIR	Permite el tráfico SSH saliente desde el rango de direcciones IPv4 públicas de la red doméstica (a través de la gateway de Internet).

140	Custom TCP	TCP	32768-65535	0.0.0.0/0	PERMITIR	<p>Permite las respuestas IPv4 salientes a clientes de Internet (por ejemplo, al ofrecer páginas web a usuarios que visitan los servidores web de la subred).</p> <p>Este rango se proporciona solo como ejemplo. Para obtener más información acerca de cómo seleccionar el rango de puerto efímero correcto, consulte Puertos efímeros (p. 133).</p>
*	All traffic	Todos	Todos	0.0.0.0/0	DENEGAR	<p>Deniega todo el tráfico IPv4 saliente no controlado por ninguna regla precedente (no modificable).</p>

Cuando un paquete llega a la subred, lo evaluamos según las reglas entrantes de la ACL con la que está asociada la subred (comenzando desde la parte superior de la lista de reglas, y desplazándose hasta la parte inferior). A continuación, se indica cómo se realiza la evaluación si el paquete está destinado al puerto HTTPS (443). El paquete no coincide con la primera regla evaluada (regla 100). No coincide con la segunda regla (110), que permite el paquete en la subred. Si el paquete se ha destinado al puerto 139 (NetBIOS), no se le aplica ninguna de las reglas y la regla * termina por rechazarlo.

Puede que desee añadir una regla denegar en el caso en que tenga la necesidad justificada de abrir un amplio rango de puertos, pero hay ciertos puertos en el rango que desea denegar. Asegúrese de colocar la regla denegar en la tabla antes de la regla que permita el rango amplio de tráfico de puerto.

Añade reglas permitir en función de su caso de uso. Por ejemplo, puede añadir una regla que permita TCP saliente y acceso UDP en el puerto 53 para resolución de DNS. Para todas las reglas que añada, asegúrese de que haya una regla de entrada o salida correspondiente que permita el tráfico de respuesta.

La siguiente tabla muestra el mismo ejemplo de una ACL de red personalizada para una VPC que tiene un bloque de CIDR IPv6 asociado. Esta ACL de red incluye reglas para todo el tráfico HTTP y HTTPS IPv6. En este caso, se insertaron nuevas reglas entre las reglas existentes para el tráfico IPv4. También puede agregar las reglas como reglas de número superior tras las reglas IPv4. El tráfico IPv4 y el IPv6 son independientes y, por lo tanto, ninguna de las reglas para el tráfico IPv4 se aplican a las del tráfico IPv6.

Entrada						
Regla n.º	Tipo	Protocolo	Rango de puerto	Fuente	Permitir/Denegar	Comentarios
100	HTTP	TCP	80	0.0.0.0/0	PERMITIR	Permite el tráfico HTTP entrante de cualquier dirección IPv4.
105	HTTP	TCP	80	::/0	PERMITIR	Permite el tráfico HTTP entrante de cualquier dirección IPv6.
110	HTTPS	TCP	443	0.0.0.0/0	PERMITIR	Permite el tráfico HTTPS entrante de cualquier dirección IPv4.
115	HTTPS	TCP	443	::/0	PERMITIR	Permite el tráfico HTTPS entrante de cualquier dirección IPv6.
120	SSH	TCP	22	192.0.2.0/24	PERMITIR	Permite el tráfico SSH entrante del rango del rango de direcciones IPv4 públicas de su red doméstica (a través de la gateway de Internet).

130	RDP	TCP	3389	192.0.2.0/24	PERMITIR	Permite el tráfico RDP entrante a servidores web desde el rango de direcciones IPv4 públicas de su red doméstica (a través del puerto de la gateway de Internet).
140	Custom TCP	TCP	32768-65535	0.0.0.0/0	PERMITIR	<p>Permite el tráfico IPv4 de retorno entrante de Internet (es decir, para solicitudes que se originan en la subred).</p> <p>Este rango se proporciona solo como ejemplo. Para obtener más información acerca de cómo seleccionar el rango de puerto efímero correcto, consulte Puertos efímeros (p. 133).</p>

145	Custom TCP	TCP	32768-65535	::/0	ALLOW	<p>Permite el tráfico IPv6 de retorno entrante de Internet (es decir, para solicitudes que se originan en la subred).</p> <p>Este rango se proporciona solo como ejemplo. Para obtener más información acerca de cómo seleccionar el rango de puerto efímero correcto, consulte Puertos efímeros (p. 133).</p>
*	All traffic	Todos	Todos	0.0.0.0/0	DENEGAR	Deniega todo el tráfico IPv4 entrante no controlado por ninguna regla precedente (no modificable).
*	Todo el tráfico	Todos	Todos	::/0	DENEGAR	Deniega todo el tráfico IPv6 entrante no controlado por ninguna regla precedente (no modificable).
Salida						
Regla n.º	Tipo	Protocolo	Rango de puerto	Destino	Permitir/Denegar	Comentarios

100	HTTP	TCP	80	0.0.0.0/0	PERMITIR	Permite el tráfico HTTP IPv4 saliente de la subred a Internet.
105	HTTP	TCP	80	::/0	PERMITIR	Permite el tráfico HTTP IPv6 saliente de la subred a Internet.
110	HTTPS	TCP	443	0.0.0.0/0	PERMITIR	Permite el tráfico HTTPS IPv4 saliente de la subred a Internet.
115	HTTPS	TCP	443	::/0	PERMITIR	Permite el tráfico HTTPS IPv6 saliente de la subred a Internet.

140	Custom TCP	TCP	32768-65535	0.0.0.0/0	PERMITIR	<p>Permite las respuestas IPv4 salientes a clientes de Internet (por ejemplo, al ofrecer páginas web a usuarios que visitan los servidores web de la subred).</p> <p>Este rango se proporciona solo como ejemplo. Para obtener más información acerca de cómo seleccionar el rango de puerto efímero correcto, consulte Puertos efímeros (p. 133).</p>
-----	------------	-----	-------------	-----------	----------	--

145	TCP personalizada	TCP	32768-65535	::/0	PERMITIR	<p>Permite las respuestas IPv6 salientes a clientes de Internet (por ejemplo, al ofrecer páginas web a usuarios que visitan los servidores web de la subred).</p> <p>Este rango se proporciona solo como ejemplo. Para obtener más información acerca de cómo seleccionar el rango de puerto efímero correcto, consulte Puertos efímeros (p. 133).</p>
*	All traffic	Todos	Todos	0.0.0.0/0	DENEGAR	Deniega todo el tráfico IPv4 saliente no controlado por ninguna regla precedente (no modificable).
*	Todo el tráfico	Todos	Todos	::/0	DENEGAR	Deniega todo el tráfico IPv6 saliente no controlado por ninguna regla precedente (no modificable).

Para obtener más ejemplos, consulte [Reglas recomendadas para casos de uso del asistente de la VPC](#) (p. 140).

ACL de red personalizadas y otros servicios de AWS

Si crea una ACL de red personalizada, tenga en cuenta cómo podría afectar a los recursos que crea que utilizan otros servicios de AWS.

Con Elastic Load Balancing, si la subred para las instancias backend tiene una ACL de red en la que ha agregado una regla denegar para todo el tráfico con un origen de 0.0.0.0/0 o el CIDR de la subred, el balanceador de carga no puede realizar ninguna comprobación de estado en las instancias. Para obtener más información acerca de las reglas de ACL de red recomendadas para los balanceadores de carga e instancias backend, consulte [ACL de red para balanceadores de carga en una VPC](#) en la Guía del usuario de balanceadores de carga clásicos.

Puertos efímeros

La ACL de red de ejemplo en la sección anterior utiliza un rango de puertos efímeros de 32768-65535. No obstante, puede que desee utilizar un rango diferente para sus ACL de red, dependiendo del tipo de cliente que esté utilizando o con el que se esté comunicando.

El cliente que inicia la solicitud elige el rango de puertos efímeros. El rango varía en función del sistema operativo del cliente.

- Muchos kernels de Linux (incluido el kernel de Amazon Linux) utilizan puertos 32768-61000.
- Las solicitudes que se originan desde Elastic Load Balancing utilizan puertos 1024-65535.
- Los sistemas operativos Windows con Windows Server 2003 utilizan los puertos 1025-5000.
- Windows Server 2008 y las versiones posteriores utilizan los puertos 49152-65535.
- Una gateway NAT utiliza los puertos 1024-65535.
- AWS LambdaLas funciones de utilizan los puertos 1024-65535.

Por ejemplo, si una solicitud llega a un servidor web en su VPC desde un cliente de Windows 10 en Internet, su ACL de red deberá tener una regla saliente para permitir el tráfico destinado a los puertos 49152 a 65535.

Si una instancia de la VPC es el cliente que inicia una solicitud, la ACL de red debe tener una regla entrante para habilitar el tráfico destinado a los puertos efímeros específicos del tipo de instancia (Amazon Linux, Windows Server 2008, etc.).

En la práctica, para cubrir los distintos tipos de clientes que pueden iniciar tráfico a instancias públicas en su VPC, puede abrir los puertos efímeros 1024-65535. Sin embargo, también puede añadir reglas a la ACL para denegar tráfico en puertos malintencionados en ese rango. Asegúrese de colocar las reglas denegar en la tabla antes de las reglas permitir que abren el amplio rango de puertos efímeros.

Detección de la MTU de la ruta

La detección de la MTU de la ruta se utiliza para determinar la MTU de la ruta entre dos dispositivos. La MTU de la ruta es tamaño máximo del paquete admitido en la ruta entre el host de origen y el host receptor.

Para IPv4, cuando un host envía un paquete mayor que la MTU del host receptor o que es mayor que la MTU de un dispositivo a lo largo de la ruta, el host o dispositivo receptor descarta el paquete y, a continuación, devuelve el siguiente mensaje ICMP: `Destination Unreachable: Fragmentation`

Needed and Don't Fragment was Set (Tipo 3, código 4). Esto indica al host transmisor que divida la carga útil en varios paquetes más pequeños y, a continuación, los retransmita.

El protocolo IPv6 no admite la fragmentación en la red. Cuando un host envía un paquete mayor que la MTU del host receptor o que es mayor que la MTU de un dispositivo a lo largo de la ruta, el host o dispositivo receptor descarta el paquete y, a continuación, devuelve el siguiente mensaje ICMP: `ICMPv6 Packet Too Big (PTB)` (Tipo 2). Esto indica al host transmisor que divida la carga útil en varios paquetes más pequeños y, a continuación, los retransmita.

Si la unidad de transmisión máxima (MTU) entre los anfitriones de las subredes es diferente o si las instancias se comunican con pares a través de Internet, debe agregar la siguiente regla de ACL de red, tanto entrante como saliente. Esta garantiza que la detección de la MTU de la ruta pueda funcionar correctamente y evita la pérdida de paquetes. Seleccione Custom ICMP Rule (Regla ICMP personalizada) para el tipo y Destination Unreachable (No se puede llegar al destino), fragmentation required (fragmentación obligatoria) y DF flag set (marca DF establecida) para el rango de puerto (tipo 3, código 4). Si utiliza el comando traceroute, añada también la siguiente regla: seleccione Custom ICMP Rule (Regla ICMP personalizada) para el tipo y Time Exceeded (Tiempo superado), TTL expired transit (TTL vencido en tránsito) para el rango de puerto (tipo 11, código 0). Para obtener más información, consulte [Unidad de transmisión máxima \(MTU\) de red para la instancia EC2](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Trabajar con ACL de red

En las siguientes tareas se muestra cómo trabajar con las ACL de red con la consola de Amazon VPC.

Tareas

- [Determinar las asociaciones de ACL de red \(p. 134\)](#)
- [Crear una ACL de red \(p. 135\)](#)
- [Agregar y eliminar reglas \(p. 135\)](#)
- [Asociar una subred a una ACL de red \(p. 136\)](#)
- [Desasociar una ACL de red de una subred \(p. 136\)](#)
- [Cambiar la ACL de red de una subred \(p. 137\)](#)
- [Eliminación de una ACL de red \(p. 137\)](#)
- [Información general de la API y de los comandos \(p. 137\)](#)

Determinar las asociaciones de ACL de red

Puede utilizar la consola de Amazon VPC para determinar la ACL de red asociada con una subred. Las ACL de red se pueden asociar a más de una subred, de modo que también puede determinar las subredes asociadas a una ACL de red.

Para determinar qué ACL de red está asociada a una subred

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets y, a continuación, seleccione la subred.

La ACL de red asociada a la subred se incluye en la pestaña Network ACL, junto con las reglas de la ACL de red.

Para determinar qué subredes están asociadas a una ACL de red

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.

2. En el panel de navegación, elija Network ACLs. La columna Associated With indica el número de subredes asociadas a cada ACL de red.
3. Seleccione una ACL de red.
4. En el panel de detalles, elija Subnet Associations (Asociaciones de subred) para mostrar las subredes asociadas a la ACL de red.

Crear una ACL de red

Puede crear una ACL de red personalizada para su VPC. De forma predeterminada, una ACL de red que cree bloqueará todo el tráfico entrante y saliente hasta que añada reglas, y no se asociará a ninguna subred hasta que le asocie una de forma explícita.

Para crear una regla ACL de red

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Network ACLs.
3. Elija Create Network ACL.
4. En el cuadro de diálogo Create Network ACL (Crear ACL de red), puede asignar, de forma opcional, un nombre a su ACL de red, y seleccionar el ID de su VPC en la lista VPC. Después seleccione Yes, Create (Sí, crear).

Agregar y eliminar reglas

Al añadir o eliminar una regla de una ACL, las subredes asociadas a la ACL estarán sujetas a ese cambio. No tiene que terminar ni relanzar las instancias de la subred. Los cambios surten efecto después de un corto período de tiempo.

Important

Tenga mucho cuidado si va a agregar y eliminar reglas al mismo tiempo. Las reglas de ACL de red definen qué tipos de tráfico de red pueden ingresar a las VPC o salir de ellas. Si elimina reglas de entrada o de salida y, a continuación, agrega más entradas nuevas de las permitidas en [Cuotas de Amazon VPC \(p. 378\)](#), se quitarán las entradas seleccionadas para eliminación y las nuevas entradas no se agregarán. Esto podría provocar problemas de conectividad inesperados e impedir involuntariamente el acceso a sus VPC y la conexión desde ellas.

Si utiliza la API de Amazon EC2 o una herramienta de línea de comandos, no puede modificar reglas. Sólo puede agregar y eliminar reglas. Si utiliza la consola de Amazon VPC, puede modificar las entradas de las reglas existentes. La consola elimina la regla existente y añade una regla nueva. Si necesita cambiar el orden de una regla en la ACL, deberá añadir una regla nueva con el número de la regla nueva, y luego eliminar la regla original.

Para añadir reglas a una ACL de red

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Network ACLs.
3. En el panel de detalles, elija la pestaña Inbound Rules o Outbound Rules, según el tipo de regla que necesite añadir, y luego elija Edit.
4. En Rule #, escriba un número de regla (por ejemplo, 100). El número de regla no debe estar ya en uso en la ACL de red. Las reglas se procesan por orden, empezando por el número más bajo.

Recomendamos dejar espacios entre los números de regla (como 100, 200, 300), en lugar de utilizar números secuenciales, (101, 102, 103). Esto le facilitará el añadir reglas nuevas sin tener que reenumerar las existentes.

5. Seleccione una regla de la lista Type. Por ejemplo, para añadir una regla para HTTP, elija HTTP. Para añadir una regla para permitir todo el tráfico TCP, elija All TCP. Para algunas de estas opciones (por ejemplo, HTTP), completaremos el puerto por usted. Para utilizar un protocolo que no aparezca en la lista, elija Custom Protocol Rule.
6. (Opcional) Si va a crear una regla de protocolo personalizada, seleccione el número de protocolo y asígnele un nombre en la lista Protocol. Para obtener más información, consulte [IANA List of Protocol Numbers](#).
7. (Opcional) Si el protocolo que ha seleccionado requiere un número de puerto, escriba el número de puerto o el rango de puertos separados por un guion (por ejemplo, 49152-65535).
8. En el campo Source o Destination (en función de si se trata de una regla entrante o saliente), escriba el rango de CIDR al que se aplica la regla.
9. En la lista Allow/Deny, seleccione ALLOW para permitir el tráfico especificado, o DENY para denegar el tráfico especificado.
10. (Opcional) Para añadir otra regla, elija Add another rule y repita los pasos del 4 al 9 según sea necesario.
11. Cuando haya terminado, elija Save.

Para eliminar una regla de una ACL de red

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Network ACLs y, a continuación, seleccione la ACL de red.
3. En el panel de detalles, seleccione la pestaña Inbound Rules o Outbound Rules y, a continuación, elija Edit. Elija Remove para la regla que desea eliminar y, a continuación, elija Save.

Asociar una subred a una ACL de red

Para aplicar las reglas de una ACL de red a una subred en particular, debe asociar la subred a la ACL de red. Puede asociar una ACL de red con varias subredes. Sin embargo, una subred sólo puede asociarse a una ACL de red. Las subredes no asociadas a una ACL concreta se asociarán automáticamente a la ACL de red predeterminada.

Para asociar una subred a una ACL de red

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Network ACLs y, a continuación, seleccione la ACL de red.
3. En el panel de detalles, en la pestaña Subnet Associations, elija Edit. Active la casilla de verificación Associate para la subred que desee asociar a la ACL de red y, a continuación, elija Save.

Desasociar una ACL de red de una subred

Puede desasociar una ACL de red personalizada de una subred. Cuando se ha desasociado la subred de la ACL de red personalizada, se asocia automáticamente a la ACL de red predeterminada.

Para anular la asociación de una subred a una ACL de red

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Network ACLs y, a continuación, seleccione la ACL de red.
3. En el panel de detalles, elija la pestaña Subnet Associations.
4. Elija Edit y anule la selección de la casilla de verificación Associate para la subred. Seleccione Save.

Cambiar la ACL de red de una subred

Puede cambiar la ACL de red asociada a una subred. Por ejemplo, al crear una subred, esta se asocia inicialmente a la ACL de red predeterminada. Puede que desee, en su lugar, asociarla a una ACL de red personalizada que ha creado.

Después de cambiar la ACL de red de una subred, no tiene que terminar ni relanzar las instancias de la subred. Los cambios surten efecto después de un corto período de tiempo.

Para cambiar la asociación de una ACL de red a una subred

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets y, a continuación, seleccione la subred.
3. Elija la pestaña Network ACL y, a continuación, elija Edit.
4. En la lista Change to (Cambiar a), seleccione la ACL de red con la que asociar la subred y, a continuación, elija Save (Guardar).

Eliminación de una ACL de red

La ACL de red solo se puede eliminar si no tiene subredes asociadas. La ACL de red predeterminada no se puede eliminar.

Para eliminar una ACL de red

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Network ACLs.
3. Seleccione la ACL de red y elija Delete.
4. En el cuadro de diálogo de confirmación, elija Yes, Delete.

Información general de la API y de los comandos

Puede realizar las tareas descritas en esta página utilizando la línea de comandos o una API. Para obtener más información acerca de las interfaces de la línea de comandos, junto con una lista de API disponibles, consulte [Acceder a Amazon VPC \(p. 2\)](#).

Creación de una ACL de red para su VPC

- [create-network-acl](#) (AWS CLI)
- [New-EC2NetworkAcl](#) (AWS Tools for Windows PowerShell)

Descripción de una o varias de sus ACL de red

- [describe-network-acls](#) (AWS CLI)
- [Get-EC2NetworkAcl](#) (AWS Tools for Windows PowerShell)

Adición de una regla a una ACL de red

- [create-network-acl-entry](#) (AWS CLI)
- [New-EC2NetworkAclEntry](#) (AWS Tools for Windows PowerShell)

Eliminación de una regla de una ACL de red

- [delete-network-acl-entry](#) (AWS CLI)
- [Remove-EC2NetworkAclEntry](#) (AWS Tools for Windows PowerShell)

Sustitución de una regla existente en una ACL de red

- [replace-network-acl-entry](#) (AWS CLI)
- [Set-EC2NetworkAclEntry](#) (AWS Tools for Windows PowerShell)

Sustitución de una asociación de ACL de red

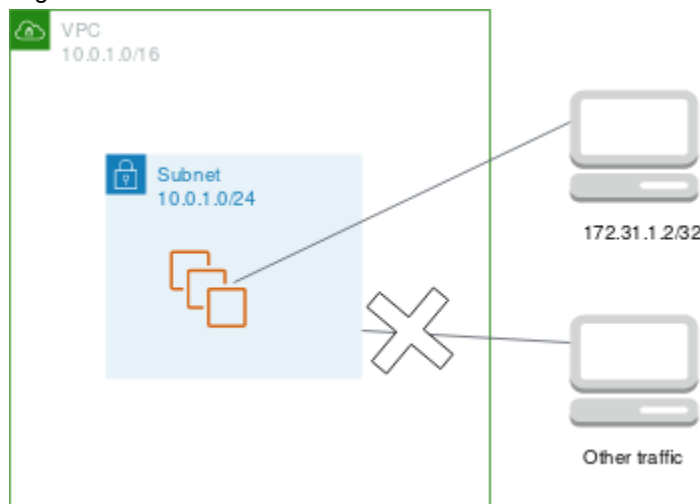
- [replace-network-acl-association](#) (AWS CLI)
- [Set-EC2NetworkAclAssociation](#) (AWS Tools for Windows PowerShell)

Eliminación de una ACL de red

- [delete-network-acl](#) (AWS CLI)
- [Remove-EC2NetworkAcl](#) (AWS Tools for Windows PowerShell)

Ejemplo: controlar el acceso a las instancias de una subred

En este ejemplo, las instancias de su subred se pueden comunicar entre sí, y se puede obtener acceso a ellas desde un equipo remoto de confianza. El equipo remoto puede ser un equipo en la red local o una instancia en una subred o VPC diferente. Se utiliza para conectarse a las instancias para realizar tareas administrativas. Las reglas de su grupo de seguridad y de ACL de red permiten el acceso desde la dirección IP de su equipo remoto (172.31.1.2/32). El resto del tráfico de Internet u otras redes se deniega. Este escenario le proporciona la flexibilidad necesaria para cambiar los grupos de seguridad o las reglas de grupos de seguridad de sus instancias, así como para tener la ACL de red como capa de copia de seguridad de defensa.



A continuación se muestra un ejemplo de grupo de seguridad para asociar a las instancias. Los grupos de seguridad son grupos con estado. Por lo tanto, no necesita una regla que permita respuestas al tráfico entrante.

Entrada				
Tipo de protocolo	Protocolo	Rango de puerto	Fuente	Comentarios
All traffic	All	All	sg-1234567890abcde	All instances associated with this security group can communicate with each other.
SSH	TCP	22	172.31.1.2/32	Allows inbound SSH access from the remote computer.
Salida				
Tipo de protocolo	Protocolo	Rango de puerto	Destino	Comentarios
All traffic	All	All	sg-1234567890abcde	All instances associated with this security group can communicate with each other.

A continuación se muestra un ejemplo de ACL de red para asociar a las subredes de las instancias. Las reglas de ACL de red se aplican a todas las instancias de la subred. Las ACL de red son sin estado. Por lo tanto, necesita una regla que permita respuestas al tráfico entrante.

Entrada						
Regla n.º	Tipo	Protocolo	Rango de puerto	Fuente	Permitir/Denegar	Comentarios
100	SSH	TCP	22	172.31.1.2/32	ALLOW	Allows inbound traffic from the remote computer.
*	All traffic	All	All	0.0.0.0/0	DENY	Denies all other inbound traffic.
Salida						
Regla n.º	Tipo	Protocolo	Rango de puerto	Destino	Permitir/Denegar	Comentarios
100	Custom TCP	TCP	1024-65535	172.31.1.2/32	ALLOW	Allows outbound responses to the remote computer.
*	All traffic	All	All	0.0.0.0/0	DENY	Denies all other

outbound
traffic.

En caso de crear por error reglas de grupos de seguridad demasiado permisivas, la ACL de red de este ejemplo seguirá permitiendo el acceso solo desde la dirección IP especificada. Por ejemplo, el siguiente grupo de seguridad contiene una regla que permite el acceso SSH entrante desde cualquier dirección IP. Sin embargo, si asocia este grupo de seguridad a una instancia de una subred que utiliza la ACL de red, solo otras instancias de la subred y el equipo remoto pueden acceder a la instancia, ya que las reglas de la ACL de red deniegan cualquier otro tráfico entrante a la subred.

Entrada				
Tipo	Protocolo	Rango de puerto	Fuente	Comentarios
All traffic	All	All	sg-1234567890abcde	All instances associated with this security group can communicate with each other.
SSH	TCP	22	0.0.0.0/0	Allows SSH access from any IP address.
Salida				
Tipo	Protocolo	Rango de puerto	Destino	Comentarios
All traffic	All	All	0.0.0.0/0	Allows all outbound traffic.

Reglas recomendadas para casos de uso del asistente de la VPC

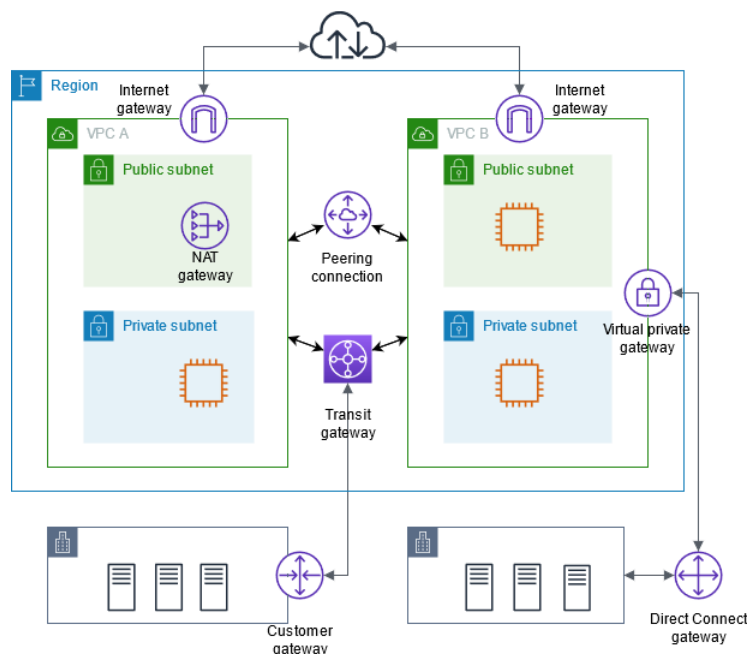
Puede utilizar el asistente de la VPC de la consola de Amazon VPC para implementar escenarios comunes para Amazon VPC. Al implementar estos escenarios tal como se describe en la documentación, se utiliza la lista de control de acceso (ACL) de red predeterminada, que permite todo el tráfico entrante y saliente. Si necesita una capa de seguridad adicional, puede crear una ACL de red y añadir reglas. Para obtener más información, consulte una de las siguientes:

- [the section called “Reglas de ACL de red recomendadas para una VPC con una única subred pública” \(p. 302\)](#)
- [the section called “Reglas ACL de red recomendadas para una VPC con subredes públicas y privadas \(NAT\)” \(p. 316\)](#)
- [the section called “Reglas ACL recomendadas para una VPC con subredes públicas y privadas y acceso de AWS Site-to-Site VPN” \(p. 340\)](#)
- [the section called “Reglas ACL de la red recomendadas para una VPC con una subred privada solamente y acceso a AWS Site-to-Site VPN” \(p. 357\)](#)

Conectar la VPC a otras redes

Puede conectar la nube virtual privada (VPC) a otras redes. Por ejemplo, otras VPC, Internet o la red en las instalaciones.

El siguiente diagrama muestra algunas de estas opciones de conectividad. La VPC A está conectada a Internet mediante de una puerta de enlace de Internet. La instancia de EC2 en la subred privada de la VPC A se puede conectar a Internet utilizando la puerta de enlace NAT de la subred pública de la VPC A. La VPC B está conectada a Internet mediante una puerta de enlace de Internet. La instancia de EC2 en la subred pública de la VPC B se puede conectar a Internet utilizando la puerta de enlace de Internet. La VPC A y la VPC B están conectadas entre sí mediante una conexión de emparejamiento de VPC y una puerta de enlace de tránsito. La puerta de enlace de tránsito tiene una conexión de VPN a un centro de datos. La VPC B tiene una conexión de AWS Direct Connect a un centro de datos.



Para obtener más información, consulte [Amazon Virtual Private Cloud Connectivity Options](#) (Opciones de conectividad de Amazon Virtual Private Cloud).

Contenido

- [Conexión a Internet mediante una puerta de enlace de Internet](#) (p. 142)
- [Habilitar el tráfico IPv6 saliente mediante una puerta de enlace de Internet de solo salida](#) (p. 153)
- [Conexión a Internet u otras redes mediante dispositivos NAT](#) (p. 156)
- [Conecte la VPC a otras VPC y redes utilizando una puerta de enlace de tránsito](#) (p. 194)
- [Conectar la VPC a redes remotas mediante AWS Virtual Private Network](#) (p. 194)
- [Conecte las VPC utilizando emparejamiento de VPC](#) (p. 195)

Conexión a Internet mediante una puerta de enlace de Internet

Una gateway de internet es un componente de la VPC de escalado horizontal, redundante y de alta disponibilidad que permite la comunicación entre su VPC e internet. Una puerta de enlace de Internet permite que los recursos (como las instancias de EC2) en las subredes públicas se conecten a Internet si el recurso tiene una dirección IPv4 pública o una dirección IPv6. Del mismo modo, los recursos de Internet pueden iniciar una conexión con los recursos de la subred utilizando la dirección IPv4 pública o la dirección IPv6. Por ejemplo, una puerta de enlace de Internet le permite conectarse a una instancia de EC2 en AWS utilizando su computadora local.

Un gateway de Internet sirve para dos fines: proporcionar un objetivo en sus tablas de ruteo de VPC para el tráfico direccionable de Internet y realizar la conversión de las direcciones de red (NAT) para las instancias que tengan asignadas direcciones IPv4 públicas. Para obtener más información, consulte [Habilitar el acceso a Internet \(p. 142\)](#).

Un gateway de Internet admite el tráfico IPv4 e IPv6. No genera riesgos de disponibilidad ni restricciones del ancho de banda del tráfico de red. No hay ningún cargo adicional por tener una gateway de Internet en su cuenta.

Habilitar el acceso a Internet

Para habilitar el acceso a Internet o desde Internet para instancias de una subred en una VPC, haga lo siguiente:

- Cree una gateway de Internet y asíciela a su VPC
- Agregue una ruta a la tabla de enrutamiento de la subred que dirija el tráfico vinculado a Internet a la gateway de Internet.
- Asegúrese de que las instancias de su subred tienen una dirección IP única global (dirección IPv4 pública, dirección IP elástica o dirección IPv6).
- Asegúrese de que las reglas de los grupos de seguridad y las listas de control de acceso a la red permitan el envío de tráfico relevante desde o hacia la instancia.

Subredes públicas y privadas

Si la subred está asociada a una tabla de enrutamiento que tiene una ruta a una gateway de Internet, esta se denomina subred pública. Si una subred está asociada a una tabla de enrutamiento que no tiene ninguna ruta a una gateway de Internet, se denomina subred privada.

En la tabla de enrutamiento de la subred pública, puede especificar la ruta de la gateway de Internet en todos los destinos que no se conocen explícitamente en la tabla (0.0.0.0/0 para IPv4 o :::/0 para IPv6). Si lo desea, también puede establecer el alcance de la ruta en un intervalo más pequeño de direcciones IP; por ejemplo, las direcciones IPv4 públicas de los puntos de enlace públicos de la empresa que estén fuera de AWS o las direcciones IP elásticas de otras instancias de Amazon EC2 externas a la VPC.

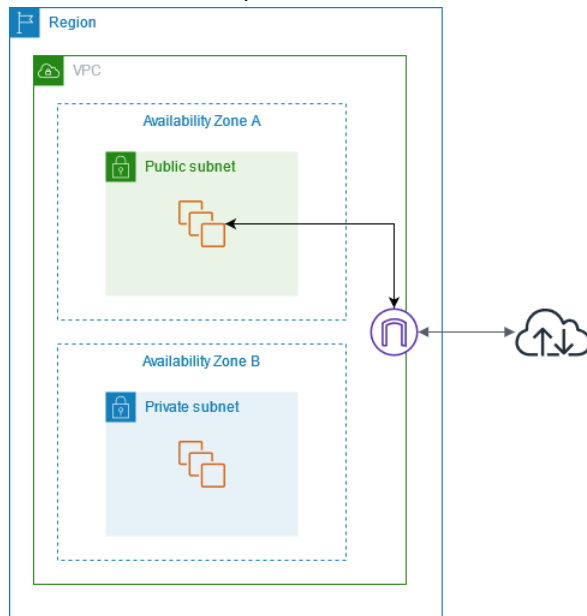
Direcciones IP y NAT

Para permitir la comunicación a través de Internet para IPv4, su instancia debe tener una dirección IPv4 pública o una dirección IP elástica asociada a una dirección IPv4 privada en su instancia. Su instancia solo tendrá en cuenta el espacio de dirección IP (interno) privado definido en la VPC y la subred. El gateway de Internet proporciona lógicamente la NAT individual en nombre de su instancia. Por lo tanto, cuando el tráfico sale de su subred de VPC a Internet, el campo de dirección de respuesta se configura con la dirección IPv4 pública o la dirección IP elástica de su instancia y no con su dirección IP privada. Por el

contrario, la dirección de destino del tráfico con destino a la dirección IP elástica o la dirección IPv4 pública de su instancia se convertirá a la dirección IPv4 privada de la instancia antes de que el tráfico se entregue a la VPC.

Para permitir la comunicación a través de Internet para IPv6, su VPC y su subred deben tener un bloque de CIDR IPv6 asociado y su instancia debe asignarse a una dirección IPv6 desde el rango de la subred. Las direcciones IPv6 son únicas de forma global y, por lo tanto, públicas de manera predeterminada.

En el siguiente diagrama, la subred de la zona de disponibilidad A es una subred pública. La tabla de enrutamiento de esta subred tiene una ruta que envía todo el tráfico IPv4 vinculado a Internet a la puerta de enlace de Internet. Las instancias de la subred pública deben tener direcciones IP públicas o direcciones IP elásticas para permitir la comunicación con Internet a través de la puerta de enlace de Internet. A modo de comparación, la subred de la zona de disponibilidad B es una subred privada porque su tabla de enrutamiento no tiene ninguna ruta hacia la puerta de enlace de Internet. Las instancias de la subred privada no pueden comunicarse con Internet a través de la puerta de enlace de Internet, incluso si tienen direcciones IP públicas.



Para proporcionar a sus instancias acceso a internet sin asignarles direcciones IP públicas, puede utilizar un dispositivo NAT en su lugar. Un dispositivo NAT permite que las instancias de una subred privada se conecten a Internet, pero evita que los anfitriones de Internet inicien conexiones con las instancias. Para obtener más información, consulte [Conexión a Internet u otras redes mediante dispositivos NAT \(p. 156\)](#).

Acceso a internet para VPC predeterminadas y no predeterminadas

La tabla siguiente ofrece información general acerca de si una VPC incluye automáticamente los componentes necesarios para el acceso a Internet a través de IPv4 o IPv6.

Componente	VPC predeterminada	VPC no predeterminada
Puerto de enlace a Internet	Sí	Sí, si creó la VPC utilizando la primera o la segunda opción del asistente para la creación de VPC. De lo contrario, deberá crear y adjuntar manualmente el gateway de Internet.

Componente	VPC predeterminada	VPC no predeterminada
Tabla de ruteo con ruta al gateway de Internet para el tráfico IPv4 (0.0.0.0/0)	Sí	Sí, si creó la VPC utilizando la primera o la segunda opción del asistente para la creación de VPC. De lo contrario, deberá crear manualmente la tabla de ruteo y añadir la ruta.
Tabla de ruteo con ruta al gateway de Internet para el tráfico IPv6 (::/0)	No	Sí, si creó la VPC utilizando la primera o la segunda opción del asistente para la creación de VPC y seleccionó la opción para asociar un bloque de CIDR IPv6 a la VPC. De lo contrario, deberá crear manualmente la tabla de ruteo y añadir la ruta.
Dirección IPv4 pública asignada automáticamente a una instancia iniciada en la subred	Sí (subred predeterminada)	No (subred no predeterminada)
Dirección IPv6 asignada automáticamente a una instancia iniciada en la subred	No (subred predeterminada)	No (subred no predeterminada)

Para obtener más información acerca de las VPC predeterminadas, consulte [VPC predeterminadas \(p. 28\)](#). Para obtener más información acerca de la utilización del asistente de VPC para crear una VPC con un gateway de Internet, consulte [VPC con una única subred pública \(p. 296\)](#) o [VPC con subredes privadas y públicas \(NAT\) \(p. 307\)](#).

Para obtener más información acerca del direccionamiento IP en su VPC y acerca del control de la asignación de direcciones IPv4 o IPv6 públicas a las instancias, consulte [Direccionamiento IP \(p. 4\)](#).

Al añadir una nueva subred a su VPC, deberá configurar el direccionamiento y la seguridad para dicha subred.

Acceso a Internet desde una subred de la VPC

A continuación, se describe cómo admitir el acceso a Internet desde una subred de la VPC mediante una puerta de enlace de Internet. Para eliminar el acceso a Internet, puede desconectar la puerta de enlace de Internet de la VPC y, a continuación, eliminarla.

Tareas

- [Creación de una subred \(p. 145\)](#)
- [Crear y adjuntar una gateway de Internet \(p. 145\)](#)
- [Creación de una tabla de ruteo personalizada \(p. 146\)](#)
- [Crear un grupo de seguridad para obtener acceso a Internet \(p. 146\)](#)
- [Asignar una dirección IP elástica a una instancia \(p. 147\)](#)
- [Separar una gateway de Internet de su VPC \(p. 147\)](#)
- [Eliminar un gateway de Internet \(p. 148\)](#)

Creación de una subred

Para añadir una subred a su VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets (Subredes), Create Subnet (Crear subred).
3. Especifique los detalles de la subred según sea necesario:
 - Name tag: indique, de manera opcional, un nombre para su subred. Esta acción creará una etiqueta con una clave de Name y el valor que especifique.
 - VPC: elija la VPC para la que va a crear la subred.
 - Availability Zone (Zona de disponibilidad): de forma opcional, elija la zona de disponibilidad o Local Zone en la que residirá la subred, o bien deje el valor predeterminado No Preference (Sin preferencias) para que AWS elija una zona de disponibilidad por usted.

Para obtener información acerca de las regiones que admiten zonas locales, consulte [Regiones disponibles](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

 - IPv4 CIDR block: especifique un bloque de CIDR IPv4 para su subred. Por ejemplo, 10.0.1.0/24. Para obtener más información, consulte [Ajuste de tamaño de VPC para IPv4 \(p. 16\)](#).
 - IPv6 CIDR block: (opcional) si ha asociado un bloque de CIDR IPv6 a su VPC, elija Specify a custom IPv6 CIDR. Especifique la pareja de valores hexadecimales de la subred, o bien deje el valor predeterminado.
4. Seleccione Create (Crear).

Para obtener más información, consulte [Subredes \(p. 60\)](#).

Crear y adjuntar una gateway de Internet

Para crear una gateway de internet y adjuntarla a su VPC.

Para crear un gateway de Internet y adjuntarlo a su VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Internet Gateways (Gateways de Internet) y, a continuación, elija Create internet gateway (Crear gateway de Internet).
3. Opcionalmente, asigne un nombre a su gateway de Internet.
4. Como opción, agregue 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 Value (Valor), escriba el valor de la clave.

[Eliminar una etiqueta] Elija Eliminar a la derecha de la clave y el valor de la etiqueta.
5. Elija Crear gateway de Internet.
6. Seleccione el gateway de Internet que acaba de crear y, a continuación, elija Actions, Attach to VPC (Acciones, Adjuntar a la VPC).
7. Seleccione la VPC de la lista y, a continuación, elija Asociar gateway de Internet.

Creación de una tabla de ruteo personalizada

Al crear una subred, esta se asocia automáticamente a la tabla de ruteo principal de la VPC. De manera predeterminada, la tabla de ruteo principal no contiene ninguna ruta al gateway de Internet. El procedimiento que se describe a continuación permite crear una tabla de ruteo personalizada con una ruta que enviará el tráfico cuyo destino esté fuera de la VPC al gateway de Internet para, a continuación, asociarlo a su subred.

Para crear una tabla de ruteo personalizada

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables (Tablas de enrutamiento) y, a continuación, elija Create route table (Crear tabla de enrutamiento).
3. En el cuadro de diálogo Create route table (Crear tabla de enrutamiento), podrá, de manera opcional, asignar un nombre a su tabla de enrutamiento, seleccionar su VPC y, a continuación, elegir Create route table (Crear tabla de enrutamiento).
4. Seleccione la tabla de ruteo personalizada que acaba de crear. El panel de detalles muestra pestañas para trabajar con sus rutas, sus asociaciones y la propagación de rutas.
5. En la pestaña Routes (Rutas), elija Edit routes (Editar rutas), Add route (Agregar ruta) y, a continuación, agregue las siguientes rutas según sea necesario. Cuando haya terminado, elija Save changes (Guardar cambios).
 - Para el tráfico IPv4, especifique 0.0.0.0/0 en el cuadro Destination (Destino) y seleccione el ID del gateway de Internet en la lista Target (Objetivo).
 - Para el tráfico IPv6, especifique ::/0 en el cuadro Destination (Destino) y seleccione el ID del gateway de Internet en la lista Target (Objetivo).
6. En la pestaña Subnet associations (Asociaciones de subred), elija Edit subnet associations (Editar asociaciones de subred), seleccione la casilla de verificación para la subred y, a continuación, elija Save associations (Guardar asociaciones).

Para obtener más información, consulte [Configurar tablas de enrutamiento \(p. 81\)](#).

Crear un grupo de seguridad para obtener acceso a Internet

De forma predeterminada, un grupo de seguridad de VPC permite todo el tráfico saliente. Puede crear un nuevo grupo de seguridad y agregar reglas que permitan el tráfico entrante desde Internet. A continuación, puede asociar el grupo de seguridad con instancias de la subred pública.

Para crear un grupo de seguridad y asociarlo con una instancia

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad) y, a continuación, elija Create Security Group (Crear grupo de seguridad).
3. Ingrese un nombre y una descripción para el grupo de seguridad.
4. En VPC, seleccione la VPC.
5. En Inbound Rules (Reglas entrantes), elija Add Rule (Agregar regla) y complete la información necesaria. Por ejemplo, seleccione HTTP o HTTPS en Type (Tipo) e ingrese Source (Origen) como 0.0.0.0/0 para el tráfico IPv4 o ::/0 para el tráfico IPv6.
6. Elija Create Security Group (Crear grupo de seguridad).
7. En el panel de navegación, elija Instances (Instancias).
8. Seleccione la instancia y, a continuación, elija Actions (Acciones), Security (Seguridad), Change security groups (Cambiar grupos de seguridad).

9. En Associated security groups (Grupos de seguridad asociados), seleccione un grupo de seguridad existente y luego elija Add security group (Agregar grupo de seguridad). Para quitar un grupo de seguridad que ya se asoció, elija Remove (Quitar). Cuando haya terminado de realizar los cambios, elija Save (Guardar).

Para obtener más información, consulte . [Controlar el tráfico hacia los recursos mediante grupos de seguridad \(p. 255\)](#).

Asignar una dirección IP elástica a una instancia

Tras lanzar la instancia en la subred, debe asignarle una dirección IP elástica si desea que esté disponible desde Internet a través de IPv4.

Note

Si asignó una dirección IPv4 pública a su instancia durante el lanzamiento, la instancia estará disponible desde Internet y no tendrá que asignarle ninguna dirección IP elástica. Para obtener más información acerca de la asignación de direcciones IP para su instancia, consulte [Direccionamiento IP \(p. 4\)](#).

Para asignar una dirección IP elástica y asignarla a una instancia utilizando la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Elastic IPs.
3. Elija Allocate new address (Allocate new address).
4. Elija Allocate.

Note

Si su cuenta es compatible con EC2-Classical, elija primero VPC.

5. Seleccione la dirección IP elástica de la lista, elija Actions y, a continuación, elija Associate address.
6. Elija Instance o Network interface y, a continuación, seleccione la instancia o el ID de interfaz de red. Seleccione la dirección IP privada a la que desea asociar la dirección IP elástica y, a continuación, elija Associate.

Para obtener más información, consulte [Asociar direcciones IP elásticas con recursos en la VPC \(p. 149\)](#).

Separar una gateway de Internet de su VPC

Si ya no necesita el acceso a Internet para las instancias que se lanzan en una VPC no predeterminada, puede separar el puerto de enlace a Internet de la VPC. Tenga en cuenta que no es posible separar el gateway de Internet si la VPC tiene recursos con las direcciones IP públicas o las direcciones IP elásticas.

Para separar un gateway de Internet

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Elastic IPs y seleccione la dirección IP elástica.
3. Elija Actions, Disassociate address. Elija Disassociate address.
4. En el panel de navegación, elija Internet Gateways.
5. Seleccione el gateway de Internet y elija Actions, Detach from VPC (Acciones, Separar de la VPC).
6. En el cuadro de diálogo Desconectar de VPC elija Desconectar gateway de Internet.

Eliminar un gateway de Internet

Si ya no necesita el gateway de Internet, puede eliminarlo. Tenga en cuenta que no podrá eliminar el gateway de Internet si sigue adjunto a la VPC.

Para eliminar un gateway de Internet

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Internet Gateways.
3. Seleccione el gateway de Internet y, a continuación, elija Actions (Acciones), Delete internet gateway (Eliminar gateway de Internet).
4. En el cuadro de diálogo Eliminar gateway de Internet escriba `delete` y elija Eliminar gateway de Internet.

Información general de la API y de los comandos

Puede realizar las tareas descritas en esta página utilizando la línea de comandos o una API. Para obtener más información acerca de las interfaces de la línea de comando, junto con una lista de las acciones de API disponibles, consulte [Acceder a Amazon VPC \(p. 2\)](#).

Cree un gateway de Internet

- [create-internet-gateway](#) (AWS CLI)
- [New-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

Adjuntar un gateway de Internet a una VPC

- [attach-internet-gateway](#) (AWS CLI)
- [Add-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

Descripción de un gateway de Internet

- [describe-internet-gateways](#) (AWS CLI)
- [Get-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

Separar un gateway de Internet de una VPC

- [detach-internet-gateway](#) (AWS CLI)
- [Dismount-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

Eliminar un gateway de Internet

- [delete-internet-gateway](#) (AWS CLI)
- [Remove-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

Asociar direcciones IP elásticas con recursos en la VPC

Las direcciones IP elásticas son direcciones IPv4 estáticas y públicas, diseñadas para la informática en la nube dinámica. Puede asociar una dirección IP elástica con cualquier instancia o interfaz de red de cualquier VPC de su cuenta. Con una dirección IP elástica, puede enmascarar los errores de las instancias reasignando rápidamente la dirección a otra instancia de su VPC.

Conceptos y reglas de direcciones IP elásticas

Para utilizar una dirección IP elástica, primero debe asignarla para utilizar en su cuenta. A continuación, puede asociarla con una instancia o interfaz de red en su VPC. La dirección IP elástica se mantiene asignada a su cuenta de AWS hasta que la libera de forma explícita.

Las direcciones IP elásticas son propiedad de una interfaz de red. Puede asociar una dirección IP elástica a una instancia actualizando la interfaz de red vinculada a la instancia. La ventaja de asociar la dirección IP elástica con la interfaz de red en lugar de directamente con la instancia es que puede mover todos los atributos de la interfaz de red de una instancia a otra en un solo paso. Para obtener más información, consulte [Interfaces de redes elásticas](#) en la Guía del usuario de Amazon EC2.

Se aplican las siguientes reglas:

- Una dirección IP elástica se puede asociar con una única instancia o interfaz de red a la vez.
- Puede mover una dirección IP elástica de una instancia o interfaz de red a otra.
- Si asocia una dirección IP elástica a la interfaz de red eth0 de su instancia, su dirección IPv4 pública actual (en caso de que la tenga) se liberará al grupo de direcciones IP públicas EC2-VPC. Si anula la asociación de la dirección IP elástica, a la interfaz de red eth0 se le asignará automáticamente una nueva dirección IPv4 pública en unos minutos. Esto no es aplicable si ha vinculado una segunda interfaz de red a su instancia.
- Para garantizar un uso eficiente de las direcciones IP elásticas, hemos establecido un pequeño cargo por horas cuando estas no están asociadas a una instancia en ejecución, o bien cuando están asociadas a una instancia detenida o a una interfaz de red no conectada. Mientras su instancia esté en ejecución, no se le cobrará por una dirección IP elástica asociada a la instancia, pero sí por las direcciones IP elásticas adicionales asociadas a la instancia. Para obtener más información, consulte [Precios de Amazon EC2](#).
- Se limita a cinco direcciones IP elásticas. Para ayudar a conservarlas, puede usar un dispositivo NAT. Para obtener más información, consulte [Conexión a Internet u otras redes mediante dispositivos NAT](#) (p. 156).
- No se admiten direcciones IP elásticas para IPv6.
- Puede etiquetar una dirección IP elástica asociada para usarse en una VPC, sin embargo, no se admiten etiquetas de asignación de costos. Si recupera una dirección IP elástica, las etiquetas no se recuperan.
- Puede acceder a una dirección IP elástica desde Internet cuando el grupo de seguridad y la ACL de red permiten el tráfico desde la dirección IP de origen. El tráfico de respuesta desde dentro la VPC de vuelta a Internet requiere una gateway de Internet. Para obtener más información, consulte [the section called "Grupos de seguridad" \(p. 255\)](#) y [the section called "ACL de red" \(p. 120\)](#).
- Puede utilizar cualquiera de las siguientes opciones para las direcciones IP elásticas:
 - Que Amazon proporcione las direcciones IP elásticas. Al seleccionar esta opción, puede asociar las direcciones IP elásticas a un grupo de bordes de red. Esta es la ubicación desde la que anunciamos el bloque CIDR. Establecer el grupo de bordes de red limita el bloque de CIDR a este grupo.
 - Utilice sus propias direcciones IP. Para obtener información sobre cómo traer sus propias direcciones IP, consulte [Traiga sus propias direcciones IP \(BYOIP\)](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Existen diferencias entre las direcciones IP elásticas que se utilizan en una VPC y las que se utilizan en EC2-Classic. Para obtener más información, consulte [Diferencias entre EC2-Classic y VPC](#) en la Guía del usuario de Amazon EC2 para instancias de Linux. Puede mover a la plataforma de VPC una dirección IP elástica que haya asignado para utilizarla en la plataforma de EC2-Classic. Para obtener más información, consulte [Migración de una dirección IP elástica de EC2-Classic](#).

Las direcciones IP elásticas son regionales. Para obtener más información acerca del uso de Global Accelerator para aprovisionar direcciones IP globales, consulte [Uso de direcciones IP estáticas globales en lugar de direcciones IP estáticas regionales](#) en la Guía para desarrolladores de AWS Global Accelerator.

Trabajar con direcciones IP elásticas

En las secciones siguientes, se describe cómo se utilizan las direcciones IP elásticas.

Tareas

- [Asignar una dirección IP elástica \(p. 150\)](#)
- [Asociar una dirección IP elástica \(p. 151\)](#)
- [Ver las direcciones IP elásticas \(p. 151\)](#)
- [Etiquetado de una dirección IP elástica \(p. 151\)](#)
- [Anulación de la asociación de una dirección IP elástica \(p. 151\)](#)
- [Liberación de una dirección IP elástica \(p. 152\)](#)
- [Recuperar una dirección IP elástica \(p. 152\)](#)

Asignar una dirección IP elástica

Antes de utilizar una IP elástica, debe asignar una para su uso en la VPC.

Para asignar una dirección IP elástica

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Elastic IPs.
3. Elija Allocate Elastic IP address (Asignar dirección IP elástica).
4. En Public IPv4 address pool (Grupo de direcciones IPv4 públicas) elija una de las siguientes opciones:
 - Amazon's pool of IP addresses (Grupo de direcciones IP de Amazon): si desea que una dirección de IPv4 se asigne desde un grupo de direcciones IP de Amazon.
 - My pool of public IPv4 addresses (Mi grupo de direcciones IPv4 públicas): si desea asignar una dirección IPv4 de un grupo de direcciones IP que trajo a su cuenta de AWS. Esta opción está deshabilitada si no tiene grupos de direcciones IP.
 - Customer owned pool of IPv4 addresses (Grupo de direcciones IPv4 propiedad del cliente): si desea asignar una dirección IPv4 de un grupo creado desde la red en las instalaciones para su uso con un Outpost. Esta opción solo está disponible si tiene un Outpost.
5. (Opcional) Añada o elimine una etiqueta.

[Agregar una etiqueta] Elija Agregar etiqueta y haga lo siguiente:

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

[Eliminar una etiqueta] Elija Eliminar a la derecha de la clave y el valor de la etiqueta.

6. Elija Allocate.

Note

Si su cuenta es compatible con EC2-Classic, elija primero VPC.

Asociar una dirección IP elástica

Puede asociar una IP elástica con una instancia en ejecución o interfaz de red en su VPC.

Después de asociar la dirección IP elástica con su instancia, la instancia recibe un nombre de host DNS público si los nombres de host DNS están habilitados. Para obtener más información, consulte [Atributos DNS para la VPC \(p. 42\)](#).

Para asociar una dirección IP elástica con una instancia o interfaz de red

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Elastic IPs.
3. Seleccione una dirección IP elástica asignada para su uso con una VPC (la columna Scope (Ámbito) tiene un valor de `vpc`) y, a continuación, elija Actions (Acciones), Associate Elastic IP address (Asociar dirección IP elástica).
4. Elija Instance o Network interface y, a continuación, seleccione la instancia o el ID de interfaz de red. Seleccione la dirección IP privada a la que desea asociar la dirección IP elástica. Elija Associate.

Ver las direcciones IP elásticas

Puede consultar las direcciones IP elásticas asignadas a su cuenta.

Para ver sus direcciones IP elásticas

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Elastic IPs.
3. Para filtrar la lista mostrada, comience escribiendo parte de la dirección IP elástica o uno de sus atributos en el cuadro de búsqueda.

Etiquetado de una dirección IP elástica

Puede aplicar etiquetas a las direcciones IP elásticas para poder identificarlas o clasificarlas según las necesidades de su organización.

Para etiquetar una dirección IP elástica

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Elastic IPs.
3. Seleccione las direcciones IP elásticas y elija Tags.
4. Elija Manage tags (Administrar etiquetas), escriba las claves y los valores de etiquetas necesarios y elija Save (Guardar).

Anulación de la asociación de una dirección IP elástica

Para cambiar el recurso con el que está asociada la dirección IP elástica, primero debe desasociarla del recurso asociado actualmente.

Para anular la asociación de una dirección IP elástica

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.

2. En el panel de navegación, elija Elastic IPs.
3. Seleccione la dirección IP elástica y, a continuación, elija Actions (Acciones), Disassociate Elastic IP address (Desvincular dirección IP elástica).
4. Cuando se le solicite, elija Disassociate (Desasociar).

Liberación de una dirección IP elástica

Si ya no necesita una dirección IP elástica, se recomienda que la libere. Se le cobrarán cargos por las direcciones IP elásticas asignadas para su uso con una VPC que no estén asociadas a una instancia. La dirección IP elástica no se debe asociar con una instancia o interfaz de red.

Para liberar una dirección IP elástica

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Elastic IPs.
3. Seleccione la dirección IP elástica y, a continuación, elija Actions (Acciones), Release Elastic IP addresses (Liberar direcciones IP elásticas).
4. Cuando se le solicite, elija Release.

Recuperar una dirección IP elástica

Si libera su dirección IP elástica, es posible que pueda recuperarla. No podrá recuperar la dirección IP elástica si se ha asignado a otra cuenta de AWS o si supera la cuota de direcciones IP elásticas.

Puede recuperar una dirección IP elástica mediante la API de Amazon EC2 o una herramienta de línea de comandos.

Para recuperar una dirección IP elástica con la AWS CLI

Utilice el comando [allocate-address](#) y especifique la dirección IP con el parámetro `--address`.

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

Información general de la API y de los comandos

Puede realizar las tareas descritas en esta página utilizando la línea de comandos o una API. Para obtener más información acerca de las interfaces de la línea de comando, junto con una lista de las acciones de API disponibles, consulte [Acceder a Amazon VPC \(p. 2\)](#).

Asignar una dirección IP elástica

- [allocate-address](#) (AWS CLI)
- [New-EC2Address](#) (AWS Tools for Windows PowerShell)

Asociación de una dirección IP elástica a una instancia o una interfaz de red

- [associate-address](#) (AWS CLI)
- [Register-EC2Address](#) (AWS Tools for Windows PowerShell)

Ver las direcciones IP elásticas

- [describe-addresses](#) (AWS CLI)

- [Get-EC2Address](#) (AWS Tools for Windows PowerShell)

Etiquetado de una dirección IP elástica

- [create-tags](#) (AWS CLI)
- [New-EC2Tag](#) (AWS Tools for Windows PowerShell)

Anulación de la asociación de una dirección IP elástica

- [disassociate-address](#) (AWS CLI)
- [Unregister-EC2Address](#) (AWS Tools for Windows PowerShell)

Liberación de una dirección IP elástica

- [release-address](#) (AWS CLI)
- [Remove-EC2Address](#) (AWS Tools for Windows PowerShell)

Habilitar el tráfico IPv6 saliente mediante una puerta de enlace de Internet de solo salida

La gateway de internet de solo salida es un componente de VPC de escalado horizontal, redundante y de alta disponibilidad que permite la comunicación saliente a través de IPv6 desde instancias de su VPC a internet. Asimismo, impide que internet inicie conexiones IPv6 con sus instancias.

Note

La gateway de internet de solo salida se utiliza solo para el tráfico IPv6. Para habilitar la comunicación con internet de solo salida mediante IPv4, utilice una gateway NAT. Para obtener más información, consulte [Gateways NAT](#) (p. 157).

Contenido

- [Conceptos básicos de las gateways de Internet de solo salida](#) (p. 153)
- [Trabajar con gateways de Internet de solo salida](#) (p. 154)
- [Información general de la API y de la CLI](#) (p. 156)

Conceptos básicos de las gateways de Internet de solo salida

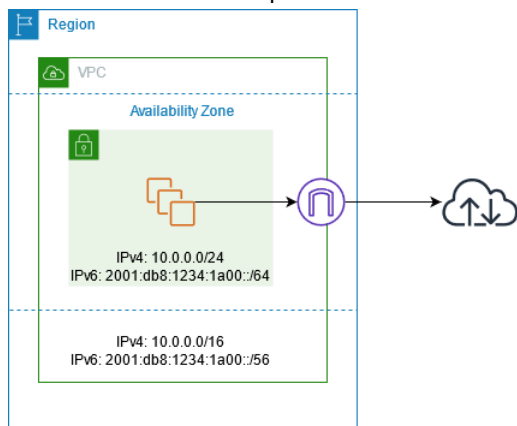
Las direcciones IPv6 son únicas de forma global y, por lo tanto, son públicas de manera predeterminada. Si desea que su instancia pueda obtener acceso a internet pero desea evitar que los recursos de internet inicien comunicaciones con su instancia, utilice una gateway de internet de solo salida. Para ello, cree una gateway de internet de solo salida en su VPC y, a continuación, añada una ruta a su tabla de enrutamiento que apunte a todo el tráfico IPv6 (:::/0) o un rango específico de direcciones IPv6 a la gateway de internet de solo salida. El tráfico IPv6 de la subred asociado a la tabla de enrutamiento se direcciona a la gateway de internet de solo salida.

La gateway de internet de solo salida tiene estado: reenvía el tráfico desde las instancias de la subred a internet o a otros servicios de AWS y, a continuación, envía la respuesta de nuevo a las instancias.

La gateway de internet de solo salida tiene las características siguientes:

- No puede asociar un grupo de seguridad a una gateway de internet de solo salida. Puede utilizar grupos de seguridad para sus instancias de la subred privada para controlar el tráfico entrante y saliente de estas instancias.
- Puede usar una ACL de red para controlar el tráfico hacia la subred y procedente de esta para la que la gateway de internet de solo salida direcciona el tráfico.

En el siguiente diagrama, la VPC tiene bloques de CIDR IPv4 e IPv6 y la subred bloques de CIDR IPv4 e IPv6. La VPC tiene una puerta de enlace de Internet de solo salida.



A continuación se muestra un ejemplo de la tabla de enrutamiento asociada a la subred. Hay una ruta que envía todo el tráfico IPv6 de internet (::/0) a la puerta de enlace de Internet de solo salida.

Destino	Objetivo
10.0.0.0/16	Local
2001:db8:1234:1a00::/64	Local
::/0	<i>eigw-id</i>

Trabajar con gateways de Internet de solo salida

Las tareas siguientes describen cómo crear una gateway de Internet de solo salida (saliente) para su subred privada y configurar el enrutamiento para la subred.

Tareas

- [Creación de una gateway de internet de solo salida \(p. 154\)](#)
- [Ver la gateway de Internet de solo salida \(p. 155\)](#)
- [Creación de una tabla de ruteo personalizada \(p. 155\)](#)
- [Eliminación de una gateway de internet de solo salida \(p. 156\)](#)

Creación de una gateway de internet de solo salida

Puede crear una gateway de Internet de solo salida para la VPC mediante la consola de Amazon VPC.

Para crear una gateway de internet de solo salida

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.

2. En el panel de navegación, elija Egress Only Internet Gateways.
3. Elija Create Egress Only Internet Gateway.
4. (Opcional) Añada o elimine una etiqueta.

[Agregar una etiqueta] Elija Agregar etiqueta y haga lo siguiente:

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

[Eliminar una etiqueta] Elija Eliminar a la derecha de la clave y el valor de la etiqueta.

5. Seleccione la VPC en la que desea crear el puerto de enlace a Internet de solo salida.
6. Seleccione Create (Crear).

Ver la gateway de Internet de solo salida

Puede consultar información acerca de la gateway de Internet de solo salida en la consola de Amazon VPC.

Para ver la información acerca de la gateway de internet de solo salida

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Egress Only Internet Gateways.
3. Seleccione la gateway de internet de solo salida para ver su información en el panel de detalles.

Creación de una tabla de ruteo personalizada

Para enviar el tráfico con destino fuera de la VPC a la gateway de internet de solo salida, debe crear una tabla de enrutamiento personalizada, añadir una ruta que envíe el tráfico a la gateway y, a continuación, asociarla a la subred.

Para crear una tabla de enrutamiento personalizada y añadir una ruta a la gateway de internet de solo salida

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables (Tablas de enrutamiento) y Create route table (Crear tabla de enrutamiento).
3. En el cuadro de diálogo Create route table (Crear tabla de enrutamiento), podrá, de manera opcional, asignar un nombre a su tabla de enrutamiento y, a continuación, seleccionar su VPC y elegir Create route table (Crear tabla de enrutamiento).
4. Seleccione la tabla de ruteo personalizada que acaba de crear. El panel de detalles muestra pestañas para trabajar con sus rutas, sus asociaciones y la propagación de rutas.
5. En la pestaña Routes (Rutas), elija Edit routes (Editar rutas), especifique `::/0` en el cuadro Destination (Destino), seleccione el ID de la puerta de enlace de Internet de solo salida en la lista Target (Objetivo) y, a continuación, elija Save changes (Guardar cambios).
6. En la pestaña Subnet associations (Asociaciones de subred), elija Edit subnet associations (Editar asociaciones de subred) y seleccione la casilla de verificación de la subred. Seleccione Save.

De manera alternativa, puede añadir una ruta a la tabla de ruteo existente asociada a su subred. Seleccione la tabla de enrutamiento existente y siga los pasos 5 y 6 anteriores para añadir una ruta a la gateway de internet de solo salida.

Para obtener más información acerca de las tablas de ruteo, consulte [Configurar tablas de enrutamiento \(p. 81\)](#).

Eliminación de una gateway de internet de solo salida

Si ya no necesita la gateway de internet de solo salida, puede eliminarla. Las rutas de la tabla de enrutamiento que apuntan a la gateway de internet de solo salida permanecerán con el estado `blackhole` hasta que elimine o actualice manualmente la ruta.

Para eliminar la gateway de internet de solo salida

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Gateways de Internet de solo salida y seleccione la gateway de internet de solo salida.
3. Elija Eliminar.
4. Elija Delete Egress Only Internet Gateway en el cuadro de diálogo de confirmación.

Información general de la API y de la CLI

Puede realizar las tareas descritas en esta página utilizando la línea de comandos o una API. Para obtener más información acerca de las interfaces de la línea de comando, junto con una lista de las acciones de API disponibles, consulte [Acceder a Amazon VPC \(p. 2\)](#).

Creación de una gateway de internet de solo salida

- [create-egress-only-internet-gateway](#) (AWS CLI)
- [New-EC2EgressOnlyInternetGateway](#) (AWS Tools for Windows PowerShell)

Descripción de una gateway de internet de solo salida

- [describe-egress-only-internet-gateways](#) (AWS CLI)
- [Get-EC2EgressOnlyInternetGatewayList](#) (AWS Tools for Windows PowerShell)

Eliminación de una gateway de internet de solo salida

- [delete-egress-only-internet-gateway](#) (AWS CLI)
- [Remove-EC2EgressOnlyInternetGateway](#) (AWS Tools for Windows PowerShell)

Conexión a Internet u otras redes mediante dispositivos NAT

Puede utilizar un dispositivo NAT para permitir que los recursos de las subredes privadas se conecten a Internet, a otras VPC o a las redes en las instalaciones. Estas instancias pueden comunicarse con servicios fuera de la VPC, pero no pueden recibir solicitudes de conexión no solicitadas.

El dispositivo NAT reemplaza la dirección IPv4 de origen de las instancias con la dirección del dispositivo NAT. Cuando envía tráfico de respuesta a las instancias, el dispositivo NAT traduce las direcciones a las primeras direcciones IPv4 de origen.

Puede utilizar un dispositivo NAT administrado ofrecido por AWS, denominado gateway NAT, o bien crear su propio dispositivo NAT en una instancia EC2, llamada instancia NAT. Le recomendamos que utilice las gateways NAT, ya que proporcionan mayor disponibilidad y ancho de banda y requieren menos esfuerzo de administración por su parte.

Consideraciones

- Los dispositivos NAT no son compatibles con el tráfico IPv6; en su lugar, utilice una gateway de Internet de solo salida. Para obtener más información, consulte [Habilitar el tráfico IPv6 saliente mediante una puerta de enlace de Internet de solo salida](#) (p. 153).
- Usamos el término NAT en esta documentación para seguir la práctica de TI común, aunque el rol real de un dispositivo NAT es tanto la traducción de direcciones como la traducción de direcciones de puerto (PAT).

Contenido

- [Gateways NAT](#) (p. 157)
- [Instancias NAT](#) (p. 184)
- [Comparar las gateways NAT con las instancias NAT](#) (p. 192)

Gateways NAT

Una gateway NAT es un servicio de traducción de direcciones de red (NAT). Puede utilizar una gateway NAT para que las instancias de una subred privada puedan conectarse a servicios fuera de la VPC, pero los servicios externos no pueden iniciar una conexión con esas instancias.

Cuando se crea una gateway NAT, se especifica uno de los siguientes tipos de conectividad:

- **Pública (predeterminado):** las instancias de subredes privadas pueden conectarse a Internet a través de una gateway NAT pública, pero no pueden recibir conexiones entrantes no solicitadas de Internet. Crea una gateway NAT pública en una subred pública y debe asociar una dirección IP elástica con la gateway NAT en el momento de la creación. El tráfico se dirige desde la gateway NAT a la gateway de Internet de la VPC. También puede utilizar una gateway NAT pública para conectarse a otras VPC o a la red en las instalaciones. En este caso, el tráfico se dirige desde la gateway NAT a través de una gateway de tránsito o una gateway privada virtual.
- **Privada:** las instancias de subredes privadas pueden conectarse a otras VPC o a la red en las instalaciones a través de una gateway NAT privada. El tráfico se dirige desde la gateway NAT a través de una gateway de tránsito o una gateway privada virtual. No puede asociar una dirección IP elástica a una gateway NAT privada. Puede adjuntar una gateway de Internet a una VPC con una gateway NAT privada, pero si dirige el tráfico desde la gateway NAT privada a la gateway de Internet, esta última reduce el tráfico.

La gateway NAT reemplaza la dirección IP de fuente de las instancias con la dirección IP de la gateway NAT. Para una gateway NAT pública, esta es la dirección IP elástica de la gateway NAT. Para una gateway NAT privada, esta es la dirección IP privada de la gateway NAT. Cuando envía tráfico de respuesta a las instancias, el dispositivo NAT traduce las direcciones a las primeras direcciones IP fuente.

Precios

Cuando aprovisiona una gateway NAT, se le cobrará por cada hora que esté disponible y por cada Gigabyte de datos que procese. Para obtener más información, consulte [Precios de Amazon VPC](#).

Las siguientes estrategias pueden servir de ayuda para reducir los cargos por transferencia de datos de su gateway NAT:

- Si sus recursos de AWS envían o reciben un volumen significativo de tráfico entre las zonas de disponibilidad, asegúrese de que los recursos se encuentran en la misma zona de disponibilidad que la gateway NAT o cree una gateway NAT en la misma zona de disponibilidad que los recursos.
- Si la mayor parte del tráfico que fluye a través de la gateway NAT se dirige a los servicios de AWS que admiten puntos de enlace de interfaz o puntos de enlace de gateway, considere la posibilidad de crear un punto de enlace de interfaz o un punto de enlace de gateway para estos servicios. Para obtener más información sobre el posible ahorro de costos, consulte [Precios de AWS PrivateLink](#).

Contenido

- [Conceptos básicos de la gateway NAT \(p. 158\)](#)
- [Controlar el uso de gateways NAT \(p. 159\)](#)
- [Trabajar con gateways NAT \(p. 159\)](#)
- [Información general de la API y de la CLI \(p. 161\)](#)
- [Casos de uso de puerta de enlace NAT \(p. 161\)](#)
- [DNS64 y NAT64 \(p. 169\)](#)
- [Monitorear las puertas de enlace NAT mediante Amazon CloudWatch \(p. 172\)](#)
- [Solucionar problemas de las gateways NAT \(p. 178\)](#)

Conceptos básicos de la gateway NAT

Cada gateway NAT se crea en una zona de disponibilidad específica, y se implementa con redundancia en dicha zona. Hay una cuota establecida en la cantidad de gateways NAT que puede crear en cada zona de disponibilidad. Para obtener más información, consulte [Cuotas de Amazon VPC \(p. 378\)](#).

Si tiene recursos en varias zonas de disponibilidad que comparten una gateway NAT y la zona de disponibilidad de la gateway NAT no funciona, los recursos de las demás zonas de disponibilidad perderán el acceso a Internet. Para crear una arquitectura independiente de la zona de disponibilidad, cree una gateway NAT en cada zona de disponibilidad y configure el direccionamiento para asegurarse de que los recursos utilicen la gateway NAT de la misma zona de disponibilidad.

Las siguientes características y reglas se aplican a las gateways NAT:

- Una gateway NAT admite los siguientes protocolos: TCP, UDP e ICMP.
- Las gateways NAT son compatibles con el tráfico IPv4 o IPv6. Para el tráfico IPv6, la gateway NAT ejecuta NAT64. Al utilizarla en combinación con DNS64 (disponible en Route 53 Resolver), las cargas de trabajo de IPv6 de una subred de Amazon VPC pueden comunicarse con los recursos de IPv4. Estos servicios IPv4 pueden existir en la misma VPC (en una subred independiente) o en una VPC diferente, en su entorno en las instalaciones o en Internet.
- Las gateways NAT admiten 5 Gbps de ancho de banda y se amplían automáticamente hasta 45 Gbps. Si necesita más ancho de banda, puede dividir los recursos en varias subredes y crear una gateway NAT en cada subred.
- Una gateway NAT puede procesar un millón de paquetes por segundo y escalar automáticamente hasta cuatro millones de paquetes por segundo. Más allá de este límite, una gateway NAT descartará paquetes. Para evitar la pérdida de paquetes, divida los recursos en varias subredes y cree una gateway NAT independiente para cada subred.
- Una gateway NAT puede admitir hasta 55,000 conexiones simultáneas a cada destino único. Este límite se aplica también cuando se crean aproximadamente 900 conexiones por segundo hacia un único destino (sobre 55 000 conexiones por minuto). Si la dirección IP de destino, el puerto de destino o el protocolo (TCP/UDP/ICMP) cambian, puede crear 55 000 conexiones adicionales. Cuando hay más de 55 000 conexiones, las probabilidades de errores de conexión aumentan debido a errores de asignación de puertos. Estos errores se pueden monitorear examinando la métrica de CloudWatch

`ErrorPortAllocation` para la gateway NAT. Para obtener más información, consulte [Monitorear las puertas de enlace NAT mediante Amazon CloudWatch](#) (p. 172).

- Puede asociar exactamente una dirección IP elástica a una gateway NAT pública. No puede desasociar una dirección IP elástica de una gateway NAT después de crearla. Para usar una dirección IP elástica distinta para su gateway NAT, debe crear una nueva gateway NAT con la dirección necesaria, actualizar sus tablas de ruteo y, a continuación, eliminar la gateway NAT existente si ya no la necesita.
- Una gateway NAT privada recibe una dirección IP privada disponible de la subred en la que está configurada. No puede desconectar esta dirección IP privada ni adjuntar direcciones IP privadas adicionales.
- No puede asociar un grupo de seguridad a una gateway NAT. Puede asociar grupos de seguridad a las instancias para controlar su tráfico entrante y saliente.
- Puede usar una ACL de red para controlar el tráfico hacia la subred y procedente de esta en su gateway NAT. Las gateways NAT utilizan los puertos 1024-65535. Para obtener más información, consulte [Controlar el tráfico hacia las subredes utilizando las ACL de red](#) (p. 120).
- Una gateway NAT recibe una interfaz de red a la que se asigna de forma automática una dirección IP privada del rango de direcciones IP de la subred. Puede consultar la interfaz de red de la gateway NAT con la consola de Amazon EC2. Para obtener más información, consulte [Visualización de los detalles de una interfaz de red](#). No se pueden modificar los atributos de esta interfaz de red.
- No se puede obtener acceso a una gateway NAT mediante una conexión de ClassicLink asociada a su VPC.
- No se puede dirigir el tráfico a una gateway NAT mediante una interconexión de VPC, una conexión de Site-to-Site VPN ni AWS Direct Connect. No es posible utilizar una gateway NAT con recursos situados en el otro lado de dichas conexiones.

Controlar el uso de gateways NAT

De forma predeterminada, los usuarios de IAM no tienen permiso para trabajar con gateways NAT. Puede crear una política de usuario de IAM que conceda permisos a los usuarios para crear, describir y eliminar gateways NAT. Para obtener más información, consulte [Identity and Access Management para Amazon VPC](#) (p. 237).

Trabajar con gateways NAT

Puede utilizar la consola de Amazon VPC para crear y administrar sus gateways NAT. También puede utilizar el asistente de Amazon VPC para crear una VPC con una subred pública, una subred privada y una gateway NAT. Para obtener más información, consulte [VPC con subredes privadas y públicas \(NAT\)](#) (p. 307).

Tareas

- [Creación de una gateway NAT](#) (p. 159)
- [Etiquetar una gateway NAT](#) (p. 160)
- [Eliminación de una gateway NAT](#) (p. 160)

Creación de una gateway NAT

Para crear una gateway NAT, ingrese un nombre opcional, una subred y un tipo de conectividad opcional. Con una gateway NAT pública, debe especificar una dirección IP elástica disponible. Una gateway NAT privada recibe una dirección IP privada principal que se selecciona de forma aleatoria de su subred. No puede desconectar la dirección IP privada principal ni agregar direcciones IP privadas secundarias.

Para crear una gateway NAT

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.

2. En el panel de navegación, elija NAT Gateways.
3. Elija Create a NAT Gateway (Crear una gateway NAT) y haga lo siguiente:
 - a. (Opcional) Especifique un nombre para la gateway NAT. Esto crea una etiqueta en la que la clave es **Name** y el valor es el nombre que especifique.
 - b. Seleccione la subred en la que crear la gateway NAT.
 - c. En Connectivity type (Tipo de conectividad), seleccione Private (Privada) para crear una gateway NAT privada o (la opción predeterminada) Public (Pública) para crear una gateway NAT pública.
 - d. (Solo para la gateway NAT pública) En Elastic IP allocation ID (ID de asignación de IP elástica), seleccione una dirección IP elástica para asociarla con la gateway NAT.
 - e. (Opcional) Para cada etiqueta, elija Add new tag (Agregar nueva etiqueta) e ingrese el nombre y el valor de la clave.
 - f. Elija Create a NAT Gateway (Crear una gateway NAT).
4. El estado inicial de la gateway NAT es Pending. Una vez que el estado cambia a Available, la gateway NAT está lista para su uso. Agregue una ruta a la gateway NAT para las tablas de enrutamiento para las subredes privadas y agregue rutas a la tabla de enrutamiento para la gateway NAT.

Si el estado de la gateway NAT cambia a Failed, es que ha habido un error durante la creación. Para obtener más información, consulte [La creación de la gateway NAT produce un error \(p. 178\)](#).

Etiquetar una gateway NAT

Puede etiquetar la gateway NAT como ayuda para identificarla o clasificarla según las necesidades de su organización. Para obtener información sobre cómo trabajar con etiquetas, consulte [Etiquetado de los recursos de Amazon EC2](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Las etiquetas de asignación de costos son compatibles con las gateways NAT. Por lo tanto, también puede utilizar etiquetas para organizar su factura de AWS y reflejar su propia estructura de costos. Para obtener más información, consulte [Uso de etiquetas de asignación de costos](#) en la Guía del usuario de AWS Billing and Cost Management. Para obtener más información acerca de la configuración de un informe de asignación de costos con etiquetas, consulte [Informe de asignación de costos mensual](#) en la sección de Facturación de cuentas de AWS.

Eliminación de una gateway NAT

Si ya no necesita una gateway NAT, puede eliminarla. Una vez que se elimine la gateway NAT, la entrada permanece visible en la consola de Amazon VPC durante aproximadamente una hora, hasta que se elimine de forma automática. No puede quitar esta entrada por sí mismo.

Al eliminar una gateway NAT, se desasocia su dirección IP elástica, pero no se libera la dirección de su cuenta. Si elimina una gateway NAT, sus rutas permanecerán con el estado blackhole hasta que las elimine o las actualice.

Para eliminar una gateway NAT

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija NAT Gateways.
3. Seleccione el botón de opción de la gateway NAT y, a continuación, elija Actions (Acciones), Delete NAT gateway (Eliminar gateway NAT).
4. Cuando se le pida confirmación, ingrese **delete** y elija Delete (Eliminar).
5. Si ya no necesita la dirección IP elástica asociada con la gateway NAT pública, es recomendable liberarla. Para obtener más información, consulte [Liberación de una dirección IP elástica \(p. 152\)](#).

Información general de la API y de la CLI

Puede realizar las tareas descritas en esta página utilizando la línea de comandos o al API. Para obtener más información acerca de las interfaces de la línea de comandos, junto con una lista de las operaciones de API disponibles, consulte [Acceder a Amazon VPC \(p. 2\)](#).

Creación de una gateway NAT

- [create-nat-gateway](#) (AWS CLI)
- [New-EC2NatGateway](#) (AWS Tools for Windows PowerShell)
- [CreateNatGateway](#) (API de consulta de Amazon EC2)

Descripción de una gateway NAT

- [describe-nat-gateways](#) (AWS CLI)
- [Get-EC2NatGateway](#) (AWS Tools for Windows PowerShell)
- [DescribeNatGateways](#) (API de consulta de Amazon EC2)

Etiquetar una gateway NAT

- [create-tags](#) (AWS CLI)
- [New-EC2Tag](#) (AWS Tools for Windows PowerShell)
- [CreateTags](#) (API de consulta de Amazon EC2)

Eliminación de una gateway NAT

- [delete-nat-gateway](#) (AWS CLI)
- [Remove-EC2NatGateway](#) (AWS Tools for Windows PowerShell)
- [DeleteNatGateway](#) (API de consulta de Amazon EC2)

Casos de uso de puerta de enlace NAT

Los siguientes son ejemplos de casos de uso de gateways NAT públicas y privadas.

Situaciones

- [Acceso a Internet desde una subred privada \(p. 161\)](#)
- [Acceso a la red mediante las direcciones IP permitidas \(p. 165\)](#)
- [Habilitar la comunicación entre redes superpuestas \(p. 166\)](#)

Acceso a Internet desde una subred privada

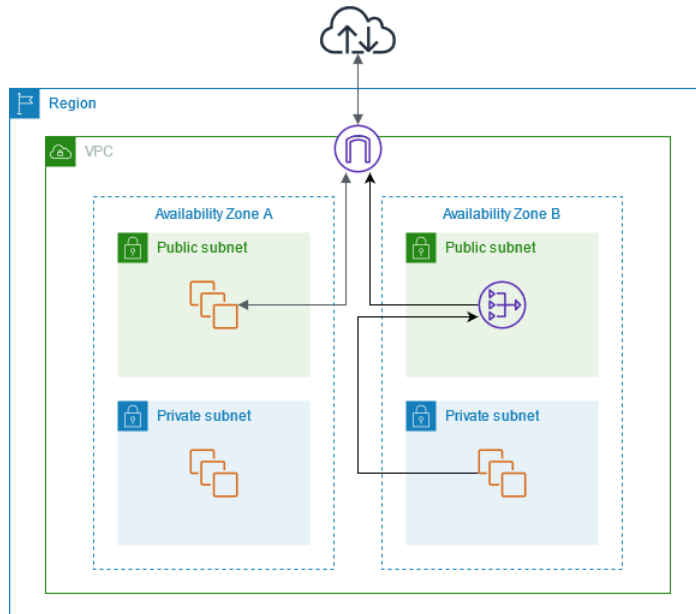
Puede utilizar una puerta de enlace NAT pública para permitir que las instancias de una subred privada envíen tráfico de salida a Internet, además de evitar que Internet establezca conexiones a dichas instancias.

Contenido

- [Información general \(p. 162\)](#)
- [Direccionamiento \(p. 162\)](#)
- [Prueba de la gateway NAT pública \(p. 163\)](#)

Información general

El siguiente diagrama ilustra este caso de uso. Hay dos zonas de disponibilidad, con dos subredes en cada zona de disponibilidad. La tabla de enrutamiento de cada subred determina cómo se dirige el tráfico. En la zona de disponibilidad A, las instancias de la subred pública pueden conectarse a Internet a través de una ruta a la puerta de enlace de Internet, mientras que las instancias de la subred privada no tienen ruta a Internet. En la zona de disponibilidad B, la subred pública contiene una puerta de enlace NAT y las instancias de la subred privada pueden conectarse a Internet a través de una ruta a la puerta de enlace NAT de la subred pública. La puerta de enlace NAT envía el tráfico a la puerta de enlace de Internet mediante la dirección IP elástica como la dirección IP de origen.



Direccionamiento

La siguiente es la tabla de enrutamiento asociada a la subred pública en la zona de disponibilidad A. La primera entrada es la ruta local. Esta permite a las instancias de la subred comunicarse con otras instancias de la VPC mediante las direcciones IP privadas. La segunda entrada envía el resto del tráfico de la subred a la puerta de enlace de Internet, lo que permite a las instancias de la subred acceder a Internet.

Destino	Objetivo
<i>CIDR DE VPC</i>	local
0.0.0.0/0	<i>internet-gateway-id</i>

La siguiente es la tabla de enrutamiento asociada a la subred privada de la zona de disponibilidad A. La entrada es la ruta local que permite a las instancias de la subred comunicarse con otras instancias de la VPC mediante las direcciones IP privadas. Las instancias de esta subred no tienen acceso a Internet.

Destino	Objetivo
<i>CIDR DE VPC</i>	local

La siguiente es la tabla de enrutamiento asociada a la subred pública en la zona de disponibilidad B. La primera entrada es la ruta local que permite a las instancias de la subred comunicarse con otras instancias

de la VPC mediante las direcciones IP privadas. La segunda entrada envía el resto del tráfico de la subred a la puerta de enlace de Internet, lo que permite a la puerta de enlace de NAT de la subred acceder a Internet.

Destino	Objetivo
<i>CIDR DE VPC</i>	local
0.0.0.0/0	<i>internet-gateway-id</i>

La siguiente es la tabla de enrutamiento asociada a la subred privada en la zona de disponibilidad B. La primera entrada es la ruta local. Esta permite a las instancias de la subred comunicarse con otras instancias de la VPC mediante las direcciones IP privadas. La segunda entrada envía el resto del tráfico de subred a la gateway NAT.

Destino	Objetivo
<i>CIDR DE VPC</i>	local
0.0.0.0/0	<i>nat-gateway-id</i>

Para obtener más información, consulte [the section called “Trabajar con tablas de ruteo” \(p. 99\)](#).

Prueba de la gateway NAT pública

Una vez que ha creado su gateway NAT y ha actualizado sus tablas de enrutamiento, puede hacer ping a direcciones remotas de Internet desde una instancia de su subred privada para comprobar si puede conectarse a Internet. Para ver un ejemplo práctico, consulte [Comprobación de la conexión a Internet \(p. 163\)](#).

Si puede conectarse a Internet, también podrá probar si el tráfico de Internet se dirige a través de la gateway NAT:

- Trace la ruta de tráfico desde una instancia de su subred privada. Para ello, ejecute el comando `traceroute` desde una instancia de Linux en su subred privada. En el resultado, debería ver la dirección IP privada de la gateway NAT en uno de los saltos (suele ser el primero).
- Puede utilizar un sitio web o una herramienta de terceros que muestre la dirección IP de origen al conectarse desde una instancia de su subred privada. La dirección IP de origen debería ser la dirección IP elástica de la gateway NAT.

Si estas pruebas no son satisfactorias, consulte [Solucionar problemas de las gateways NAT \(p. 178\)](#).

Comprobación de la conexión a Internet

En el siguiente ejemplo se muestra cómo comprobar si una instancia en una subred privada se puede conectar a Internet.

1. Lance una instancia en su subred pública (la usará como alojamiento bastión). En el asistente de lanzamiento, asegúrese de seleccionar una AMI de Amazon Linux y de asignar una dirección IP pública a la instancia. Asegúrese de que las reglas de su grupo de seguridad admiten el tráfico SSH entrante del rango de direcciones IP de su red local y el tráfico SSH saliente al rango de direcciones IP de su subred privada (también puede utilizar 0.0.0.0/0 para el tráfico SSH tanto entrante como saliente en esta prueba).
2. Lance una instancia en su subred privada. En el asistente de lanzamiento, asegúrese de seleccionar una AMI de Amazon Linux. No asigne una dirección IP pública a su instancia. Asegúrese de que

las reglas de su grupo de seguridad admiten el tráfico SSH entrante de la dirección IP privada de la instancia que lanzó en la subred pública, así como todo el tráfico ICMP saliente. Debe elegir el mismo par de claves que utilizó para lanzar su instancia en la subred pública.

3. Configure el reenvío de agentes SSH en su equipo local, y conéctese a su host bastión en la subred pública. Para obtener más información, consulte [Para configurar el reenvío de agentes SSH para Linux o macOS \(p. 164\)](#) o [Para configurar el reenvío de agentes SSH para Windows \(PuTTY\) \(p. 164\)](#).
4. Desde el host bastión, conéctese a su instancia en la subred privada y, a continuación, compruebe la conexión a Internet desde su instancia en la subred privada. Para obtener más información, consulte [Para comprobar la conexión a Internet \(p. 164\)](#).

Para configurar el reenvío de agentes SSH para Linux o macOS

1. Desde su equipo local, añada su clave privada al agente de autenticación.

Para Linux, utilice el siguiente comando.

```
ssh-add -c mykeypair.pem
```

Para macOS, utilice el siguiente comando.

```
ssh-add -K mykeypair.pem
```

2. Conéctese a su instancia en la subred pública utilizando la opción `-A` para habilitar el reenvío de agentes SSH y utilice la dirección pública de la instancia, como se muestra en el ejemplo siguiente.

```
ssh -A ec2-user@54.0.0.123
```

Para configurar el reenvío de agentes SSH para Windows (PuTTY)

1. Descargue e instale Pageant desde la [página de descargas de PuTTY](#), si aún no lo tiene instalado.
2. Convierta su clave privada al formato .ppk. Para obtener más información, consulte [Conversión de la clave privada mediante PuTTYgen](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
3. Inicie Pageant, haga clic con el botón derecho en el icono de Pageant de la barra de tareas (puede estar oculto) y elija Add Key. Seleccione el archivo .ppk que ha creado, escriba la frase de contraseña si es necesario y elija Open (Abrir).
4. Inicie una sesión de PuTTY y conéctese a su instancia en la subred pública utilizando su dirección IP pública. Para obtener más información, consulte [Conexión a la instancia de Linux](#). En la categoría Auth, asegúrese de seleccionar la opción Allow agent forwarding y deje el cuadro Private key file for authentication en blanco.

Para comprobar la conexión a Internet

1. Desde su instancia en la subred pública, conéctese a su instancia en la subred privada utilizando su dirección IP privada, como se muestra en el ejemplo siguiente.

```
ssh ec2-user@10.0.1.123
```

2. Desde su instancia privada, compruebe que puede conectarse a Internet ejecutando el comando `ping` para un sitio web que tenga ICMP habilitado.

```
ping ietf.org
```

```
PING ietf.org (4.31.198.44) 56(84) bytes of data.  
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=1 ttl=47 time=86.0 ms  
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=2 ttl=47 time=75.6 ms  
...
```

Pulse Ctrl+C en su teclado para cancelar el comando ping. Si el comando ping da error, consulte [Las instancias no pueden obtener acceso a Internet \(p. 181\)](#).

3. (Opcional) Si ya no necesita las instancias, térmelas. Para obtener más información, consulte [Terminar la instancia](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Acceso a la red mediante las direcciones IP permitidas

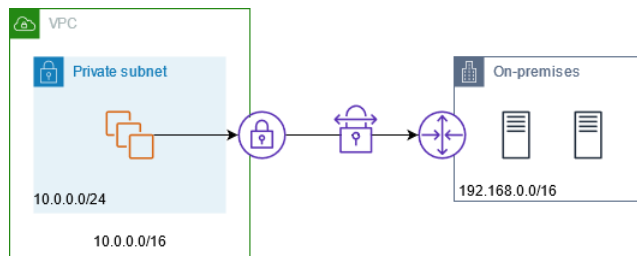
Puede utilizar una puerta de enlace NAT privada para habilitar la comunicación desde las VPC a su red en las instalaciones mediante un grupo de direcciones permitidas. En lugar de asignar a cada instancia una dirección IP independiente del rango de direcciones IP permitidas, puede dirigir el tráfico desde la subred destinada a la red en las instalaciones a través de una puerta de enlace NAT privada con una dirección IP del rango de direcciones IP permitidas.

Contenido

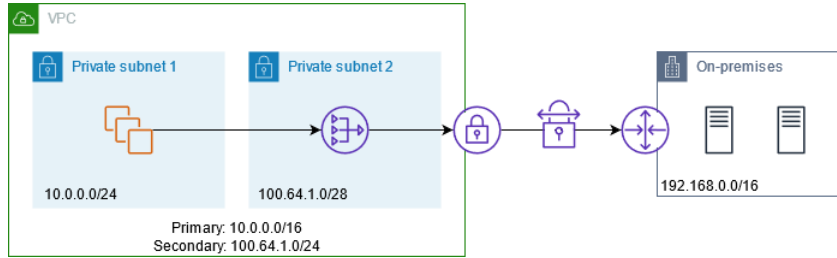
- [Información general \(p. 165\)](#)
- [Recursos \(p. 166\)](#)
- [Direccionamiento \(p. 166\)](#)

Información general

En el siguiente diagrama se muestra cómo las instancias pueden acceder a los recursos en las instalaciones mediante AWS VPN. El tráfico de las instancias se dirige a una puerta de enlace privada virtual, a través de la conexión VPN, a la puerta de enlace de cliente y, a continuación, al destino de las redes en las instalaciones. Sin embargo, supongamos que el destino permite tráfico solo desde un rango de direcciones IP específico, como 100.64.1.0/28. Esto evitaría que el tráfico de estas instancias llegue a la red en las instalaciones.



El siguiente diagrama muestra los componentes clave de la configuración de este escenario. La VPC tiene su rango de direcciones IP original más el rango de direcciones IP permitido. La VPC tiene una subred del rango de direcciones IP permitido con una puerta de enlace NAT privada. El tráfico de las instancias destinadas a la red en las instalaciones se envía a la puerta de enlace NAT antes de dirigirse a la conexión VPN. La red en las instalaciones recibe el tráfico de las instancias con la dirección IP de origen de la puerta de enlace NAT, que proviene del rango de direcciones IP permitido.



Recursos

Cree o actualice recursos de la siguiente manera:

- Asocie el rango de direcciones IP permitido a la VPC.
- Cree una subred en la VPC a partir del rango de direcciones IP permitido.
- Cree una puerta de enlace NAT privada en la nueva subred.
- Actualice la tabla de enrutamiento de la subred con las instancias para enviar el tráfico destinado a la red en las instalaciones hacia la puerta de enlace NAT. Agregue una ruta a la tabla de enrutamiento de la subred con la puerta de enlace NAT privada que envía tráfico destinado a la red en las instalaciones hacia la puerta de enlace privada virtual.

Direccionamiento

La siguiente es la tabla de enrutamiento principal asociada a la primera subred. Hay una ruta local para cada CIDR de VPC. Las rutas locales permiten a los recursos de la subred comunicarse con otros recursos de la VPC mediante direcciones IP privadas. La tercera entrada envía el tráfico destinado a la red en las instalaciones a la puerta de enlace NAT privada.

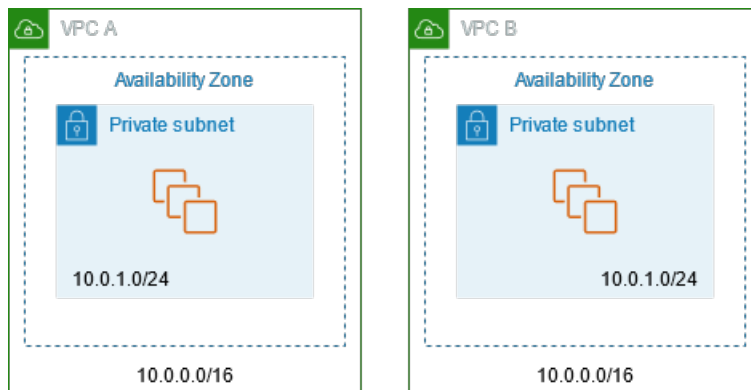
Destino	Objetivo
<i>10.0.0.0/16</i>	local
10.0.1.0/24	local
<i>192.168.0.0/16</i>	<i>nat-gateway-id</i>

La siguiente es la tabla de enrutamiento principal asociada a la segunda subred. Hay una ruta local para cada CIDR de VPC. Las rutas locales permiten a los recursos de la subred comunicarse con otros recursos de la VPC mediante direcciones IP privadas. La tercera entrada envía el tráfico destinado a la red en las instalaciones a la puerta de enlace privada virtual.

Destino	Objetivo
<i>10.0.0.0/16</i>	local
10.0.1.0/24	local
<i>192.168.0.0/16</i>	<i>vgw-id</i>

Habilitar la comunicación entre redes superpuestas

Puede utilizar una puerta de enlace NAT privada para habilitar la comunicación entre redes incluso si tienen rangos de CIDR superpuestos. Por ejemplo, supongamos que las instancias de la VPC A necesitan acceder a los servicios proporcionados por las instancias de la VPC B.



Contenido

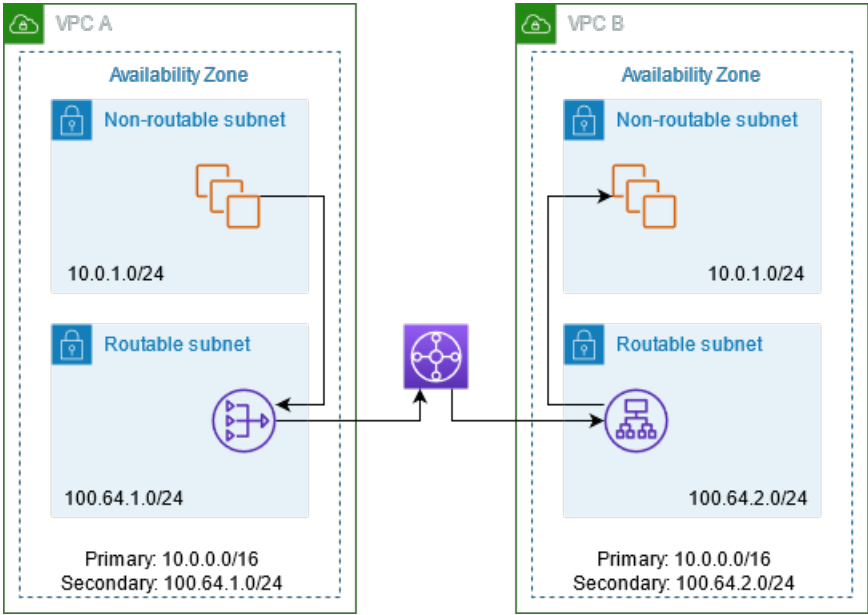
- [Información general \(p. 167\)](#)
- [Recursos \(p. 168\)](#)
- [Direccionamiento \(p. 168\)](#)

Información general

El siguiente diagrama muestra los componentes clave de la configuración de este escenario. En primer lugar, su equipo de administración de IP determina qué rangos de direcciones pueden superponerse (rangos de direcciones no enrutables) y cuáles no (rangos de direcciones enrutables). El equipo de administración de IP asigna rangos de direcciones desde el grupo de rangos de direcciones enrutables a proyectos por petición.

Cada VPC tiene su rango de direcciones IP original, que no es enrutable, más el rango de direcciones IP enrutable que le ha asignado el equipo de administración de IP. La VPC A tiene una subred de su rango enrutable con una puerta de enlace NAT privada. La puerta de enlace NAT privada obtiene su dirección IP de su subred. La VPC B tiene una subred de su rango enrutable con un Application Load Balancer. El Application Load Balancer obtiene las direcciones IP de sus subredes.

El tráfico de una instancia de la subred no enrutable de la VPC A destinada a las instancias de la subred no enrutable de la VPC B se envía a través de la puerta de enlace NAT privada y, a continuación, se dirige a la puerta de enlace de tránsito. La puerta de enlace de tránsito envía el tráfico al Application Load Balancer, que dirige el tráfico a una de las instancias de destino de la subred no enrutable de la VPC B. Este tráfico tiene la dirección IP de origen de la puerta de enlace NAT privada. Por lo tanto, el tráfico de respuesta del equilibrador de carga utiliza la dirección de la puerta de enlace NAT privada como destino. El tráfico de respuesta se envía a la puerta de enlace de tránsito y, luego, se dirige a la puerta de enlace NAT privada, lo que traduce el destino a la instancia de la subred no enrutable de la VPC A.



Recursos

Cree o actualice recursos de la siguiente manera:

- Asocie los rangos de direcciones IP enrutables asignados a sus respectivas VPC.
- Cree una subred en la VPC A a partir de su rango de direcciones IP enrutable y cree una puerta de enlace NAT privada en esta nueva subred.
- Cree una subred en la VPC B a partir de su rango de direcciones IP enrutable y cree un Application Load Balancer en esta nueva subred. Registre las instancias en la subred no enrutable con el grupo de destino del equilibrador de carga.
- Cree una puerta de enlace de tránsito para conectar las VPC. Asegúrese de desactivar la propagación de rutas. Cuando adjunte cada VPC a la puerta de enlace de tránsito, utilice el rango de direcciones enrutables de la VPC.
- Actualice la tabla de enrutamiento de la subred no enrutable de la VPC A para enviar todo el tráfico destinado al rango de direcciones enrutables de la VPC B hacia la puerta de enlace NAT privada. Actualice la tabla de enrutamiento de la subred enrutable de la VPC A para enviar todo el tráfico destinado al rango de direcciones enrutables de la VPC B hacia la puerta de enlace de tránsito.
- Actualice la tabla de enrutamiento de la subred enrutable de la VPC B para enviar todo el tráfico destinado al rango de direcciones enrutables de la VPC A hacia la puerta de enlace de tránsito.

Direccionamiento

La siguiente es la tabla de enrutamiento de la subred no enrutable de la VPC A.

Destino	Objetivo
<i>10.0.0.0/16</i>	local
10.0.1.0/24	local
192.0.2.0/24	<i>nat-gateway-id</i>

La siguiente es la tabla de enrutamiento de la subred enrutable de la VPC A.

Destino	Objetivo
<i>10.0.0.0/16</i>	local
10.0.1.0/24	local
192.0.2.0/24	<i>transit-gateway-id</i>

La siguiente es la tabla de enrutamiento de la subred no enrutable de la VPC B.

Destino	Objetivo
<i>10.0.0.0/16</i>	local
192.0.2.0/24	local

La siguiente es la tabla de enrutamiento de la subred enrutable de la VPC B.

Destino	Objetivo
<i>10.0.0.0/16</i>	local
192.0.2.0/24	local
10.0.1.0/24	<i>transit-gateway-id</i>

A continuación, se muestra la tabla de enrutamiento de la puerta de enlace de tránsito.

CIDR	Attachment	Tipo de ruta
10.0.1.0/24	<i>Vinculación de la VPC A</i>	Estático
192.0.2.0/24	<i>Vinculación de la VPC B</i>	Estático

DNS64 y NAT64

Una puerta de enlace NAT admite la traducción de direcciones de red de IPv6 a IPv4, y se la conoce popularmente como NAT64. La NAT64 ayuda a los recursos IPv6 de AWS a comunicarse con los recursos IPv4 en la misma VPC o en una VPC diferente, en la red en las instalaciones o en Internet. Puede utilizar NAT64 con DNS64 en Amazon Route 53 Resolver o puede utilizar su propio servidor DNS64.

Contenido

- [¿Qué es DNS64? \(p. 169\)](#)
- [¿Qué es NAT64? \(p. 170\)](#)
- [Configuración de DNS64 y NAT64 \(p. 170\)](#)

¿Qué es DNS64?

Las cargas de trabajo solo de IPv6 que se ejecutan en las VPC solo pueden enviar y recibir paquetes de red IPv6. Sin DNS64, una consulta de DNS para un servicio solo de IPv4 producirá una dirección de

destino IPv4 en respuesta, y su servicio exclusivo IPv6 no puede comunicarse con esta. Para reducir esta brecha de comunicación, puede habilitar DNS64 para una subred y se aplicará a todos los recursos de AWS dentro de esa subred. Con DNS64, Amazon Route 53 Resolver busca el registro DNS del servicio para el cual realizó la consulta y realiza una de las siguientes acciones:

- Si el registro contiene una dirección IPv6, devuelve el registro original y la conexión se establece sin ninguna traducción a través de IPv6.
- Si no hay ninguna dirección IPv6 asociada al destino en el registro DNS, Route 53 Resolver sintetiza una al anteponer el conocido prefijo /96, definido en RFC6052 (64::ff9b::/96), a la dirección IPv4 del registro. El servicio solo de IPv6 envía paquetes de red a la dirección IPv6 sintetizada. A continuación, deberá dirigir este tráfico a través de la gateway NAT, que realiza la traducción necesaria del tráfico para permitir que los servicios IPv6 de su subred accedan a los servicios IPv4 fuera de esa subred.

Puede habilitar o desactivar DNS64 en una subred mediante [modify-subnet-attribute](#) con AWS CLI o la consola de la VPC al seleccionar una subred y elegir Actions > Edit subnet settings (Acciones > Editar configuración de subred).

¿Qué es NAT64?

NAT64 permite que los servicios solo de IPv6 en Amazon VPC se comuniquen con servicios solo de IPv4 dentro de la misma VPC (en distintas subredes) o VPC conectadas, en sus redes en las instalaciones o en Internet.

NAT64 está disponible automáticamente en las gateways NAT actuales o en cualquier gateway NAT nueva que cree. No puede habilitar o desactivar esta característica.

Una vez que habilitó DNS64 y el servicio solo de IPv6 envía paquetes de red a la dirección IPv6 sintetizada a través de la gateway NAT, ocurre lo siguiente:

- Desde el prefijo 64::ff9b::/96, la gateway NAT reconoce que el destino original es IPv4 y traduce los paquetes IPv6 a IPv4 al reemplazar:
 - La IPv6 fuente con su propia IP privada, que la gateway de Internet traduce a una dirección IP elástica.
 - La IPv6 de destino a IPv4 al truncar el prefijo 64::ff9b::/96.
- La gateway NAT envía los paquetes IPv4 traducidos al destino a través de la gateway de Internet, la gateway privada virtual o la gateway de tránsito e inicia una conexión.
- El host solo de IPv4 envía paquetes de respuesta IPv4. Una vez establecida una conexión, la gateway NAT acepta los paquetes IPv4 de respuesta de los hosts externos.
- Los paquetes IPv4 de respuesta están destinados a la gateway NAT, que recibe los paquetes y revierte la traducción de NAT al reemplazar su IP (IP de destino) por la dirección IPv6 del host y anteponiendo nuevamente 64::ff9b::/96 en la dirección IPv4 fuente. A continuación, el paquete fluye hacia el host siguiendo la ruta local.

De este modo, la gateway NAT permite que las cargas de trabajo solo de IPv6 de una subred de Amazon VPC se comuniquen con los servicios solo de IPv4 en cualquier lugar fuera de la subred.

Configuración de DNS64 y NAT64

Siga los pasos de esta sección para configurar DNS64 y NAT64 a fin de habilitar la comunicación con los servicios solo de IPv4.

Contenido

- [Habilitar la comunicación con los servicios solo de IPv4 en Internet con AWS CLI \(p. 171\)](#)
- [Habilitar la comunicación con los servicios solo de IPv4 en su entorno en las instalaciones \(p. 171\)](#)

Habilitar la comunicación con los servicios solo de IPv4 en Internet con AWS CLI

Si tiene una subred con cargas de trabajo solo de IPv6 que necesita comunicarse con servicios solo de IPv4 fuera de la subred, en este ejemplo se muestra cómo habilitar estos servicios solo de IPv6 para comunicarse con servicios solo de IPv4 en Internet.

Primero debe configurar una gateway NAT en una subred pública (independiente de la subred que contiene las cargas de trabajo solo de IPv6). Por ejemplo, la subred que contiene la gateway NAT debe tener una ruta `0.0.0.0` con dirección a la gateway de Internet.

Siga estos pasos para permitir que estos servicios solo de IPv6 se conecten con servicios solo de IPv4 en Internet:

1. Agregue las tres rutas siguientes a la tabla de enrutamiento de la subred que contiene las cargas de trabajo solo de IPv6:
 - Ruta IPv4 (si la hay) en dirección a la gateway NAT.
 - `64:ff9b::/96` Ruta en dirección a la gateway NAT. Esto permitirá que el tráfico de las cargas de trabajo solo de IPv6 destinadas a servicios solo de IPv4 se enrute a través de la gateway NAT.
 - Ruta IPv6 `::/0` en dirección a la gateway de Internet solo de salida (o gateway de Internet).

Tenga en cuenta que dirigir `::/0` a la gateway de Internet permitirá que los hosts IPv6 externos (fuera de la VPC) inicien la conexión a través de IPv6.

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-cidr-block  
0.0.0.0/0 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block  
64:ff9b::/96 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block  
::/0 --egress-only-internet-gateway-id eigw-c0a643a9
```

2. Habilite la función de DNS64 en la subred que contiene las cargas de trabajo solo de IPv6.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-1a2b3c4d --enable-dns64
```

Ahora, los recursos de su subred privada pueden establecer conexiones con estado con servicios IPv4 e IPv6 en Internet. Configure el grupo de seguridad y las NACL de manera apropiada para permitir el tráfico de salida e entrada a `64:ff9b::/96`.

Habilitar la comunicación con los servicios solo de IPv4 en su entorno en las instalaciones

Amazon Route 53 Resolver le permite reenviar consultas de DNS desde la VPC a una red en las instalaciones y viceversa. Para hacerlo, siga estos pasos:

- Cree un punto de enlace de salida de Route 53 Resolver en una VPC y asígnelo a las direcciones IPv4 desde las que desea que Route 53 Resolver reenvíe las consultas. Para su solucionador de DNS en las instalaciones, estas son las direcciones IP desde las que se originan las consultas de DNS y, por lo tanto, deben ser direcciones IPv4.

- Cree una o más reglas que especifiquen los nombres de dominio de las consultas de DNS que desea que Route 53 Resolver reenvíe a los solucionadores en las instalaciones. También debe especificar las direcciones IPv4 de los solucionadores en las instalaciones.
- Ahora que ha configurado un punto de enlace de salida de Route 53 Resolver, debe habilitar DNS64 en la subred que contiene sus cargas de trabajo solo de IPv6 y dirigir los datos destinados a la red en las instalaciones a través de una gateway NAT.

Cómo funciona DNS64 para destinos solo de IPv4 en redes en las instalaciones:

1. Asigne una dirección IPv4 al punto de enlace de salida de Route 53 Resolver de la VPC.
2. La consulta de DNS de su servicio IPv6 va a Route 53 Resolver a través de IPv6. Route 53 Resolver coteja la consulta con la regla de reenvío y obtiene una dirección IPv4 para el solucionador en las instalaciones.
3. Route 53 Resolver convierte el paquete de consulta de IPv6 a IPv4 y lo reenvía al punto de enlace de salida. Cada dirección IP del punto de enlace representa una ENI que reenvía la solicitud a la dirección IPv4 en las instalaciones de su solucionador DNS.
4. El solucionador en las instalaciones envía el paquete de respuesta a través de IPv4 nuevamente a través del punto de enlace de salida a Route 53 Resolver.
5. Suponiendo que la consulta se realizó desde una subred habilitada para DNS64, Route 53 Resolver realiza dos cosas:
 - a. Verifica el contenido del paquete de respuestas. Si hay una dirección IPv6 en el registro, mantiene el contenido tal cual, pero si contiene solo un registro IPv4. Sintetiza también un registro IPv6 al anteponer `64:ff9b::/96` a la dirección IPv4.
 - b. Vuelve a empaquetar el contenido y lo envía al servicio de la VPC a través de IPv6.

Monitorear las puertas de enlace NAT mediante Amazon CloudWatch

Puede monitorear la gateway NAT con CloudWatch, que recopila información de la gateway NAT y crea métricas legibles casi en tiempo real. Puede utilizar esta información para monitorizar la gateway NAT y solucionar sus problemas. Los datos de las métricas de gateway NAT se proporcionan en intervalos de un minuto y las estadísticas se registran durante un periodo de 15 meses.

Para obtener más información sobre Amazon CloudWatch, consulte la [Guía del usuario de Amazon CloudWatch](#). Para obtener más información sobre precios, consulte [Precios de Amazon CloudWatch](#).

Métricas y dimensiones de gateway NAT

Las siguientes métricas están disponibles para las gateways de NAT.

Métrica	Descripción
<code>ActiveConnectionCount</code>	<p>Número total de conexiones TCP simultáneas activas a través de la gateway NAT.</p> <p>Si el valor es cero, indica que no hay conexiones activas a través de la gateway NAT.</p> <p>Unidades: recuento</p> <p>Estadísticas: la estadística más útil es <code>Max</code>.</p>

Métrica	Descripción
<code>BytesInFromDestination</code>	<p>Número de bytes recibidos por la gateway NAT desde el destino.</p> <p>Si el valor de <code>BytesOutToSource</code> es menor que el valor de <code>BytesInFromDestination</code>, puede que se estén perdiendo datos durante el procesamiento de la gateway NAT o que la gateway NAT esté bloqueando el tráfico.</p> <p>Unidades: bytes</p> <p>Estadísticas: la estadística más útil es Sum.</p>
<code>BytesInFromSource</code>	<p>Número de bytes recibidos por la gateway NAT desde los clientes de la VPC.</p> <p>Si el valor de <code>BytesOutToDestination</code> es menor que el valor de <code>BytesInFromSource</code>, puede que se estén perdiendo datos durante el procesamiento de la gateway NAT.</p> <p>Unidades: bytes</p> <p>Estadísticas: la estadística más útil es Sum.</p>
<code>BytesOutToDestination</code>	<p>Número de bytes enviados a través de la gateway NAT al destino.</p> <p>Un valor mayor que cero indica que hay tráfico en dirección a Internet desde los clientes que se encuentran detrás de la gateway NAT. Si el valor de <code>BytesOutToDestination</code> es menor que el valor de <code>BytesInFromSource</code>, puede que se estén perdiendo datos durante el procesamiento de la gateway NAT.</p> <p>Unidades: bytes</p> <p>Estadísticas: la estadística más útil es Sum.</p>
<code>BytesOutToSource</code>	<p>Número de bytes enviados a través de la gateway NAT a los clientes de la VPC.</p> <p>Un valor mayor que cero indica que hay tráfico procedente de Internet a los clientes que se encuentran detrás de la gateway NAT. Si el valor de <code>BytesOutToSource</code> es menor que el valor de <code>BytesInFromDestination</code>, puede que se estén perdiendo datos durante el procesamiento de la gateway NAT o que la gateway NAT esté bloqueando el tráfico.</p> <p>Unidades: bytes</p> <p>Estadísticas: la estadística más útil es Sum.</p>

Métrica	Descripción
<code>ConnectionAttemptCount</code>	<p>Número de intentos de conexión realizados a través de la gateway NAT.</p> <p>Si el valor de <code>ConnectionEstablishedCount</code> es menor que el valor de <code>ConnectionAttemptCount</code>, esto indica que los clientes que se encuentran detrás de la gateway NAT han intentado establecer nuevas conexiones, pero que no han obtenido respuesta.</p> <p>Unidad: recuento</p> <p>Estadísticas: la estadística más útil es Sum.</p>
<code>ConnectionEstablishedCount</code>	<p>Número de conexiones establecidas a través de la gateway NAT.</p> <p>Si el valor de <code>ConnectionEstablishedCount</code> es menor que el valor de <code>ConnectionAttemptCount</code>, esto indica que los clientes que se encuentran detrás de la gateway NAT han intentado establecer nuevas conexiones, pero que no han obtenido respuesta.</p> <p>Unidad: recuento</p> <p>Estadísticas: la estadística más útil es Sum.</p>
<code>ErrorPortAllocation</code>	<p>Número de veces que la gateway NAT no pudo asignar un puerto de origen.</p> <p>Un valor mayor que cero indica que hay demasiadas conexiones simultáneas abiertas a través de la gateway NAT.</p> <p>Unidades: recuento</p> <p>Estadísticas: la estadística más útil es Sum.</p>
<code>IdleTimeoutCount</code>	<p>El número de conexiones que pasaron correctamente del estado Active al estado Idle. Una conexión con el estado Active pasa al estado Idle si no se cierra bien y no hay ninguna actividad en los últimos 350 segundos.</p> <p>Un valor mayor que cero indica que hay conexiones han entrado en el estado de inactividad. Si el valor de <code>IdleTimeoutCount</code> aumenta, podría indicar que los clientes que se encuentran detrás de la gateway NAT están reutilizando conexiones obsoletas.</p> <p>Unidad: recuento</p> <p>Estadísticas: la estadística más útil es Sum.</p>

Métrica	Descripción
<code>PacketsDropCount</code>	<p>Número de paquetes que la gateway NAT ha perdido.</p> <p>Un valor mayor que cero puede indicar que existe un problema transitorio con la gateway NAT. Si este valor supera el 0,01 % del tráfico total en la puerta de enlace NAT, consulte el AWS Service Health Dashboard (Panel de estado del servicio de AWS).</p> <p>Unidades: recuento</p> <p>Estadísticas: la estadística más útil es Sum.</p>
<code>PacketsInFromDestination</code>	<p>Número de paquetes recibidos por la gateway NAT desde el destino.</p> <p>Si el valor de <code>PacketsOutToSource</code> es menor que el valor de <code>PacketsInFromDestination</code>, puede que se estén perdiendo datos durante el procesamiento de la gateway NAT o que la gateway NAT esté bloqueando el tráfico.</p> <p>Unidad: recuento</p> <p>Estadísticas: la estadística más útil es Sum.</p>
<code>PacketsInFromSource</code>	<p>Número de paquetes recibidos por la gateway NAT desde los clientes de la VPC.</p> <p>Si el valor de <code>PacketsOutToDestination</code> es menor que el valor de <code>PacketsInFromSource</code>, puede que se estén perdiendo datos durante el procesamiento de la gateway NAT.</p> <p>Unidad: recuento</p> <p>Estadísticas: la estadística más útil es Sum.</p>
<code>PacketsOutToDestination</code>	<p>Número de paquetes enviados a través de la gateway NAT al destino.</p> <p>Un valor mayor que cero indica que hay tráfico en dirección a Internet desde los clientes que se encuentran detrás de la gateway NAT. Si el valor de <code>PacketsOutToDestination</code> es menor que el valor de <code>PacketsInFromSource</code>, puede que se estén perdiendo datos durante el procesamiento de la gateway NAT.</p> <p>Unidad: recuento</p> <p>Estadísticas: la estadística más útil es Sum.</p>

Métrica	Descripción
PacketsOutToSource	<p>Número de paquetes enviados a través de la gateway NAT a los clientes de la VPC.</p> <p>Un valor mayor que cero indica que hay tráfico procedente de Internet a los clientes que se encuentran detrás de la gateway NAT. Si el valor de PacketsOutToSource es menor que el valor de PacketsInFromDestination, puede que se estén perdiendo datos durante el procesamiento de la gateway NAT o que la gateway NAT esté bloqueando el tráfico.</p> <p>Unidad: recuento</p> <p>Estadísticas: la estadística más útil es Sum.</p>

Para filtrar los datos de las métricas, use la siguiente dimensión.

Dimensión	Descripción
NatGatewayId	Filtra los datos de las métricas en función del ID de gateway NAT.

Consultar las métricas de CloudWatch para las gateways NAT

Las métricas de la gateway NAT se envían a CloudWatch en intervalos de un minuto. Las métricas se agrupan primero por el espacio de nombres de servicio y, a continuación, por las posibles combinaciones de dimensiones dentro de cada espacio de nombres. Puede ver las métricas de las gateways NAT de la manera siguiente.

Para consultar métricas mediante la consola de CloudWatch

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, seleccione Metrics (Métricas) y, a continuación, All metrics (Todas las métricas).
3. Elija el espacio de nombres de la métrica NATGateway.
4. Elija la dimensión de la métrica.

Para ver métricas mediante la AWS CLI

En el símbolo del sistema, use el siguiente comando para enumerar las métricas que están disponibles para el servicio de gateway NAT.

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

Crear alarmas de CloudWatch para monitorear una gateway NAT

Puede crear una alarma de CloudWatch que envíe un mensaje de Amazon SNS cuando la alarma cambie de estado. Una alarma vigila una métrica determinada durante el periodo especificado. Envía una notificación a un tema de Amazon SNS en función del valor de la métrica con respecto a un umbral determinado durante varios periodos de tiempo.

Por ejemplo, puede crear una alarma que monitorice el volumen de tráfico que entra o sale de la gateway NAT. La alarma siguiente monitoriza el volumen de tráfico saliente de los clientes de la VPC a través de la gateway NAT a Internet. Envía una notificación cuando el número de bytes alcanza un umbral de 5 000 000 durante un periodo de 15 minutos.

Para crear una alarma para el tráfico saliente a través de la gateway NAT

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Alarms (Alarmas) y, luego, Create Alarm (Crear alarma).
3. Elija Create alarm (Crear alarma).
4. Elija Select Metric (Seleccionar métrica).
5. Elija el espacio de nombres de la métrica NATGateway y, a continuación, elija una dimensión de métrica. Cuando llegue a las métricas, seleccione la casilla de verificación situada junto a la métrica BytesOutToDestination para la gateway NAT y, a continuación, elija Select metric (Seleccionar métrica).
6. Configure la alarma como se indica a continuación y, luego, elija Next (Siguiente):
 - En Statistic (Estadística), elija Sum (Suma).
 - En Period (Período), seleccione 15 minutes (15 minutos).
 - En Whenever (Cada vez que), elija Greater/Equal (Mayor o igual) e ingrese 5000000 para el umbral.
7. Para Notification (Notificación), seleccione un tema de SNS existente o elija Create new topic (Crear tema nuevo) para crear uno nuevo. Elija Next (Siguiente).
8. Ingrese un nombre y una descripción para la alarma y, a continuación, elija Next (Siguiente).
9. Cuando haya terminado de configurar la alarma, elija Create alarm (Crear alarma).

Como un ejemplo adicional, puede crear una alarma que monitoree los errores de asignación de puertos y que envíe una notificación cuando el valor sea mayor que cero (0) durante tres periodos consecutivos de 5 minutos.

Para crear una alarma para monitorizar los errores de asignación de puertos

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Alarms (Alarmas) y, luego, Create Alarm (Crear alarma).
3. Elija Create alarm (Crear alarma).
4. Elija Select Metric (Seleccionar métrica).
5. Elija el espacio de nombres de la métrica NATGateway y, a continuación, elija una dimensión de métrica. Cuando llegue a las métricas, seleccione la casilla de verificación situada junto a la métrica ErrorPortAllocation para la gateway NAT y, a continuación, elija Select metric (Seleccionar métrica).
6. Configure la alarma como se indica a continuación y, luego, elija Next (Siguiente):
 - En Statistic (Estadística), elija Maximum (Máximo).
 - En Period (Período), elija 1 minutes (5 minutos).
 - En Whenever (Cada vez que), elija Greater (Mayor) e ingrese 0 para el umbral.
 - En Additional configuration (Configuración adicional), Datapoints to alarm (Puntos de datos para alarma), ingrese 3.
7. Para Notification (Notificación), seleccione un tema de SNS existente o elija Create new topic (Crear tema nuevo) para crear uno nuevo. Elija Next (Siguiente).
8. Ingrese un nombre y una descripción para la alarma y, a continuación, elija Next (Siguiente).
9. Cuando haya terminado de configurar la alarma, elija Create alarm (Crear alarma).

Para obtener más información, consulte [Uso de las alarmas de Amazon CloudWatch](#) en la Guía del usuario de Amazon CloudWatch.

Solucionar problemas de las gateways NAT

Los siguientes temas le ayudarán a solucionar problemas comunes que podría encontrarse a la hora de crear o utilizar una gateway NAT.

Problemas

- [La creación de la gateway NAT produce un error \(p. 178\)](#)
- [Cuota de gateways NAT \(p. 179\)](#)
- [Cuota de direcciones IP elásticas \(p. 180\)](#)
- [La zona de disponibilidad no es compatible \(p. 180\)](#)
- [La gateway NAT ya no está visible \(p. 180\)](#)
- [La gateway NAT no responde a un comando ping \(p. 181\)](#)
- [Las instancias no pueden obtener acceso a Internet \(p. 181\)](#)
- [Error de la conexión TCP a un destino \(p. 182\)](#)
- [La salida del comando traceroute no muestra la dirección IP privada de la gateway NAT \(p. 183\)](#)
- [La conexión a Internet se pierde después de 350 segundos \(p. 183\)](#)
- [La conexión IPsec no se puede establecer \(p. 184\)](#)
- [No se pueden iniciar más conexiones \(p. 184\)](#)

La creación de la gateway NAT produce un error

Problema

Al crear una gateway NAT, esta cambia al estado `Failed`.

Note

Una gateway NAT que falle se elimina automáticamente, normalmente en aproximadamente una hora.

Causa

Se produjo un error al crear la gateway NAT. El mensaje de estado devuelto proporciona el motivo del error.

Solución

Para ver el mensaje de error, abra la consola de Amazon VPC y, a continuación, elija NAT Gateways (Gateways NAT). Seleccione el botón de opción de la gateway NAT y, a continuación, busque State message (Mensaje de estado) en la ficha Details (Detalles).

En la siguiente tabla se muestran las causas posibles del error según lo que se indique en la consola de Amazon VPC. Tras aplicar los pasos recomendados como solución, puede intentar volver a crear una gateway NAT.

Error mostrado	Causa	Solución
Subnet has insufficient free addresses to create this NAT gateway	La subred que ha especificado no tiene ninguna dirección IP privada libre. La gateway NAT requiere una interfaz de red con una dirección IP privada	Vaya a la página Subnets (Subredes) de la consola de Amazon VPC para comprobar cuántas direcciones IP hay disponibles en la subred.

Error mostrado	Causa	Solución
	asignada desde el rango de la subred.	Puede ver las Available IPs (IP disponibles) en el panel de detalles de su subred. Para crear direcciones IP libres en su subred, puede eliminar las interfaces de red que no utilice, o bien terminar las instancias que no necesite.
Network vpc-xxxxxxx has no internet gateway attached	Debe haber una gateway NAT creada en una VPC con un puerto de enlace a Internet.	Cree un puerto de enlace a Internet y vincúlelo a su VPC. Para obtener más información, consulte Crear y adjuntar una gateway de Internet (p. 145) .
Elastic IP address eipalloc-xxxxxxx could not be associated with this NAT gateway	La dirección IP elástica que ha especificado no existe o no se puede encontrar.	Compruebe el ID de asignación de la dirección IP elástica para asegurarse de haberlo escrito correctamente. Asegúrese de haber especificado una dirección IP elástica que se encuentre en la misma región de AWS en la que esté creando la gateway NAT.
Elastic IP address eipalloc-xxxxxxx is already associated	La dirección IP elástica que ha especificado ya está asociada a otro recurso, y no se puede asociar a la gateway NAT.	Compruebe qué recurso está asociado a la dirección IP elástica. Vaya a la página Elastic IPs (Direcciones IP elásticas) de la consola de Amazon VPC y consulte los valores especificados para el ID de instancia o el ID de la interfaz de red. Si no necesita la dirección IP elástica para ese recurso, puede desasociarla. De forma alternativa, puede asignar una nueva dirección IP elástica a su cuenta. Para obtener más información, consulte Trabajar con direcciones IP elásticas (p. 150) .
Network interface eni-xxxxxxx, created and used internally by this NAT gateway is in an invalid state. Inténtelo de nuevo.	Ha habido un problema al crear o utilizar la interfaz de red para la gateway NAT.	No puede resolver este error. Intente crear de nuevo una gateway NAT.

Cuota de gateways NAT

Cuando intenta crear una gateway NAT, obtiene el siguiente error.

```
Performing this operation would exceed the limit of 5 NAT gateways
```

Causa

Ha alcanzado la cuota correspondiente al número de gateways NAT para esa zona de disponibilidad.

Solución

Si ha alcanzado esta cuota gateways NAT para su cuenta, puede hacer una de estas cosas:

- Solicite un aumento de la [cuota de gateways NAT por zona de disponibilidad](#) mediante la consola de Service Quotas.
- Compruebe el estado de su gateway NAT. Una gateway con los estados Pending, Available o Deleting cuenta al calcular la cuota. Si ha eliminado recientemente una gateway NAT, espere unos minutos para que el estado cambie de Deleting a Deleted. A continuación, intente crear una nueva gateway NAT.
- Si no necesita que su gateway NAT esté en una zona de disponibilidad específica, intente crear una gateway NAT en una zona de disponibilidad en la que no haya alcanzado la cuota.

Para obtener más información, consulte [Cuotas de Amazon VPC \(p. 378\)](#).

Cuota de direcciones IP elásticas

Problema

Cuando intenta asignar una dirección IP elástica a su gateway NAT pública, obtiene el siguiente error.

The maximum number of addresses has been reached.

Causa

Ha alcanzado la cuota de direcciones IP elásticas para su cuenta en esa región.

Solución

Si ha alcanzado la cuota de direcciones IP elásticas, puede anular la asociación de una dirección IP elástica de otro recurso. También puede solicitar un aumento de la [cuota de IP elásticas](#) mediante la consola de Service Quotas.

La zona de disponibilidad no es compatible

Problema

Cuando intenta crear una gateway NAT, obtiene el siguiente mensaje de error: NotAvailableInZone.

Causa

Es posible que intente crear la gateway NAT en una zona de disponibilidad limitada, es decir, una zona en la que la capacidad de ampliación esté restringida.

Solución

Las gateways NAT no son compatibles en estas zonas de disponibilidad. Puede crear una gateway NAT en una zona de disponibilidad diferente y usarla para subredes privadas en la zona limitada. También puede mover los recursos a una zona de disponibilidad no limitada para que sus recursos y su gateway NAT estén en la misma zona.

La gateway NAT ya no está visible

Problema

Ha creado una gateway NAT, pero ya no está visible en la consola de Amazon VPC.

Causa

Es posible que haya habido un error durante la creación de la gateway NAT y que haya fallado la creación. Una gateway NAT cuyo estado sea `Failed` está visible en la consola de Amazon VPC durante una hora aproximadamente. Después de una hora, se elimina automáticamente.

Solución

Revise la información en [La creación de la gateway NAT produce un error \(p. 178\)](#) e intente crear una nueva gateway NAT.

La gateway NAT no responde a un comando ping

Problema

Cuando intenta hacer ping a la dirección IP elástica de una gateway NAT o en la dirección IP privada desde Internet (por ejemplo, desde su equipo doméstico) o desde alguna instancia en su VPC, no obtiene ninguna respuesta.

Causa

Una gateway NAT solo pasa el tráfico desde una instancia de una subred privada a Internet.

Solución

Para comprobar si su gateway NAT está funcionando, consulte [Prueba de la gateway NAT pública \(p. 163\)](#).

Las instancias no pueden obtener acceso a Internet

Problema

Ha creado una gateway NAT pública y ha seguido los pasos para probarla, pero el comando `ping` produce un error, o bien sus instancias de la subred privada no pueden acceder a Internet.

Causas

Este problema podría deberse a una de las siguientes causas:

- La gateway NAT no está lista para dirigir tráfico.
- Sus tablas de ruteo no se han configurado correctamente.
- Sus grupos de seguridad o las ACL de red están bloqueando el tráfico entrante o saliente.
- Está utilizando un protocolo no admitido.

Solución

Compruebe la siguiente información:

- Compruebe que la gateway NAT tiene el estado `Available`. En la consola Amazon VPC, vaya a la página NAT Gateways (Gateways NAT) y consulte la información de estado en el panel de detalles. Si la gateway NAT tiene un estado de error, puede que haya habido un error durante su creación. Para obtener más información, consulte [La creación de la gateway NAT produce un error \(p. 178\)](#).
- Asegúrese de haber configurado las tablas de ruteo correctamente:

- La gateway NAT debe estar en una subred pública con una tabla de ruteo que direcciona el tráfico de Internet a un puerto de enlace a Internet.
- Su instancia debe estar en una subred privada con una tabla de ruteo que direcciona el tráfico de Internet a la gateway NAT.
- Compruebe que no haya otras entradas de tabla de ruteo que dirijan todo o parte del tráfico de Internet a otro dispositivo en lugar de a la gateway NAT.
- Asegúrese de que las reglas de su grupo de seguridad para su instancia privada permiten el tráfico de salida de Internet. Para que el comando `ping` funcione, las reglas también deben permitir el tráfico ICMP saliente.

La gateway NAT permite por sí misma todo el tráfico de salida, y el tráfico recibido en respuesta a una solicitud saliente (por tanto, es con estado).

- Asegúrese de que las ACL de red estén asociadas a la subred privada y de que las subredes públicas no tengan reglas que bloqueen el tráfico de entrada y salida de Internet. Para que el comando `ping` funcione, las reglas también deben permitir el tráfico ICMP entrante y saliente.

Puede habilitar los logs de flujo para que le ayuden a diagnosticar las conexiones perdidas a causa de las reglas de grupos de seguridad o de ACL de red. Para obtener más información, consulte [Registro del tráfico de IP con registros de flujo de la VPC \(p. 197\)](#).

- Si va a utilizar el comando `ping`, asegúrese de hacer `ping` a un host con ICMP habilitado. Si ICMP no se ha habilitado, no recibirá paquetes de respuesta. Para comprobar esto, ejecute el mismo comando `ping` desde el terminal de línea de comandos en su propio equipo.
- Asegúrese de que su instancia puede hacer `ping` a otros recursos, como, por ejemplo, otras instancias de la subred privada (suponiendo que las reglas de ese grupo de seguridad lo permitan).
- Asegúrese de que su conexión esté utilizando únicamente un protocolo TCP, UDP o ICMP.

Error de la conexión TCP a un destino

Problema

Algunas de sus conexiones TCP desde instancias de una subred privada a un destino específico a través de una gateway de NAT se realizan correctamente, pero otras producen errores o se agota el tiempo de espera.

Causas

Este problema podría deberse a una de las siguientes causas:

- El punto de enlace de destino responde con paquetes TCP fragmentados. Las gateways NAT no admiten la fragmentación de IP para TCP o ICMP. Para obtener más información, consulte [Comparar las gateways NAT con las instancias NAT \(p. 192\)](#).
- La opción `tcp_tw_recycle`, de la que se sabe que causa problemas cuando hay varias conexiones desde detrás de un dispositivo NAT, está habilitada en el servidor remoto.

Soluciones

Haga lo siguiente para comprobar si el punto de enlace al que intenta conectarse está respondiendo con paquetes TCP fragmentados:

1. Utilizar una instancia en una subred pública con una dirección IP pública para desencadenar una respuesta lo suficientemente grande para provocar la fragmentación desde el punto de enlace específico.
2. Utilizar `tcpdump` para verificar que el punto de conexión esté enviando paquetes fragmentados.

Important

Debe utilizar una instancia en una subred pública para realizar estas comprobaciones. No puede utilizar la instancia desde la que estaba fallando la conexión original ni una instancia en una subred privada detrás de una gateway NAT o una instancia NAT.

Las herramientas de diagnóstico que envían o reciben grandes paquetes ICMP informarán de la pérdida de paquetes. Por ejemplo, el comando `ping -s 10000 example.com` no funciona tras una gateway NAT.

3. Si el punto de conexión está enviando paquetes TCP fragmentados, puede utilizar una instancia NAT en lugar de una gateway NAT.

Si tiene acceso al servidor remoto, haga lo siguiente para comprobar si la opción `tcp_tw_recycle` está habilitada:

1. Desde el servidor, ejecute el comando siguiente.

```
cat /proc/sys/net/ipv4/tcp_tw_recycle
```

Si el resultado es 1, la opción `tcp_tw_recycle` está habilitada.

2. Si se ha habilitado `tcp_tw_recycle`, le recomendamos deshabilitarla. Si necesita reutilizar las conexiones, `tcp_tw_reuse` es una opción más segura.

Si no tiene acceso al servidor remoto, pruebe a deshabilitar temporalmente la opción `tcp_timestamps` en una instancia de la subred privada. A continuación, vuelva a conectarse al servidor remoto. Si la conexión se realiza correctamente, puede que el error anterior se deba a que la opción `tcp_tw_recycle` está habilitada en el servidor remoto. Si es posible, póngase en contacto con el propietario del servidor remoto para comprobar si esta opción está habilitada y solicitar que se deshabilite.

La salida del comando `traceroute` no muestra la dirección IP privada de la gateway NAT

Problema

Su instancia puede obtener acceso a Internet, pero al ejecutar el comando `traceroute`, la salida no muestra la dirección IP privada de la gateway NAT.

Causa

Su instancia está obteniendo acceso a Internet mediante una gateway distinta, como una gateway de Internet.

Solución

En la tabla de ruteo de la subred en la que se encuentra su instancia, compruebe la siguiente información:

- Asegúrese de que hay una ruta que envía el tráfico de Internet a la gateway NAT.
- Asegúrese de que no hay una ruta más específica que esté enviando el tráfico de Internet a otros dispositivos, como una gateway privada virtual o un puerto de enlace a Internet.

La conexión a Internet se pierde después de 350 segundos

Problema

Sus instancias pueden obtener acceso a Internet, pero la conexión se interrumpe transcurridos 350 segundos.

Causa

Si una conexión que está utilizando una gateway NAT se queda inactiva durante 350 segundos o más, su tiempo de espera se agota.

Cuando el tiempo de espera de una conexión finaliza, una gateway NAT devuelve un paquete RST a los recursos situados detrás de la gateway NAT que intenten continuar la conexión (no envía un paquete FIN).

Solución

Para impedir que se pierda la conexión, puede iniciar más tráfico a través de esta. También puede habilitar conexiones keepalive de TCP en la instancia con un valor inferior a 350 segundos.

La conexión IPsec no se puede establecer

Problema

No puede establecer una conexión IPsec a un destino.

Causa

Las gateways NAT actualmente no admiten el protocolo IPsec.

Solución

Puede usar NAT-Traversal (NAT-T) para encapsular el tráfico IPsec en UDP, que es un protocolo admitido para las gateways NAT. Asegúrese de probar la configuración de NAT-T e IPsec para verificar que el tráfico IPsec no se elimina.

No se pueden iniciar más conexiones

Problema

Ya tiene conexiones a un destino a través de una gateway NAT, pero no se pueden establecer más.

Causa

Puede que haya alcanzado el límite de conexiones simultáneas para una sola gateway NAT. Para obtener más información, consulte [Conceptos básicos de la gateway NAT \(p. 158\)](#). Si sus instancias de la subred privada crean un gran número de conexiones, puede que alcance este límite.

Solución

Realice alguna de las siguientes acciones:

- Cree una gateway NAT por zona de disponibilidad y reparta sus clientes entre estas zonas.
- Cree gateways NAT adicionales en la subred pública y divida sus clientes en varias subredes privadas, cada una con una ruta a una gateway NAT distinta.
- Limite el número de conexiones que pueden crear sus clientes al destino.
- Utilice la métrica `IdleTimeoutCount` (p. 172) en CloudWatch para monitorear los aumentos de las conexiones inactivas. Cierre las conexiones inactivas para liberar capacidad.

Instancias NAT

Important

NAT AMI se basa en la última versión de Amazon Linux, 2018.03, cuya compatibilidad estándar llegó a su fin el 31 de diciembre de 2020. Para obtener más información, consulte la siguiente

entrada del blog: [Amazon Linux AMI end of life](#). Esta AMI solo recibirá actualizaciones de seguridad críticas (no habrá actualizaciones regulares).

Si utiliza una AMI NAT existente, AWS recomienda que [migre a una gateway NAT \(p. 194\)](#). Las gateway NAT ofrecen una mejor disponibilidad, un mayor ancho de banda y que requieren menos esfuerzo administrativo. Si las instancias NAT coinciden mejor con su caso de uso, puede crear su propia AMI NAT. Para obtener más información, consulte [. Comparar las gateways NAT con las instancias NAT \(p. 192\)](#).

Puede crear su propia AMI que proporcione traducción de direcciones de red y utilizar su AMI para iniciar una instancia EC2 como instancia NAT. Puede utilizar una instancia NAT en una subred pública para permitir que las instancias de la subred privada inicien el tráfico IPv4 saliente a la internet o a otros servicios de AWS, pero impedir que las instancias reciban tráfico entrante iniciado por alguien en internet.

Limitaciones

- Su cuota de instancias NAT depende de la cuota de instancias para la región. Para obtener más información, consulte [Amazon EC2 Service Quotas](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
- NAT no es compatible con el tráfico IPv6, en su lugar, utilice una gateway de Internet de solo salida. Para obtener más información, consulte [Habilitar el tráfico IPv6 saliente mediante una puerta de enlace de Internet de solo salida \(p. 153\)](#).

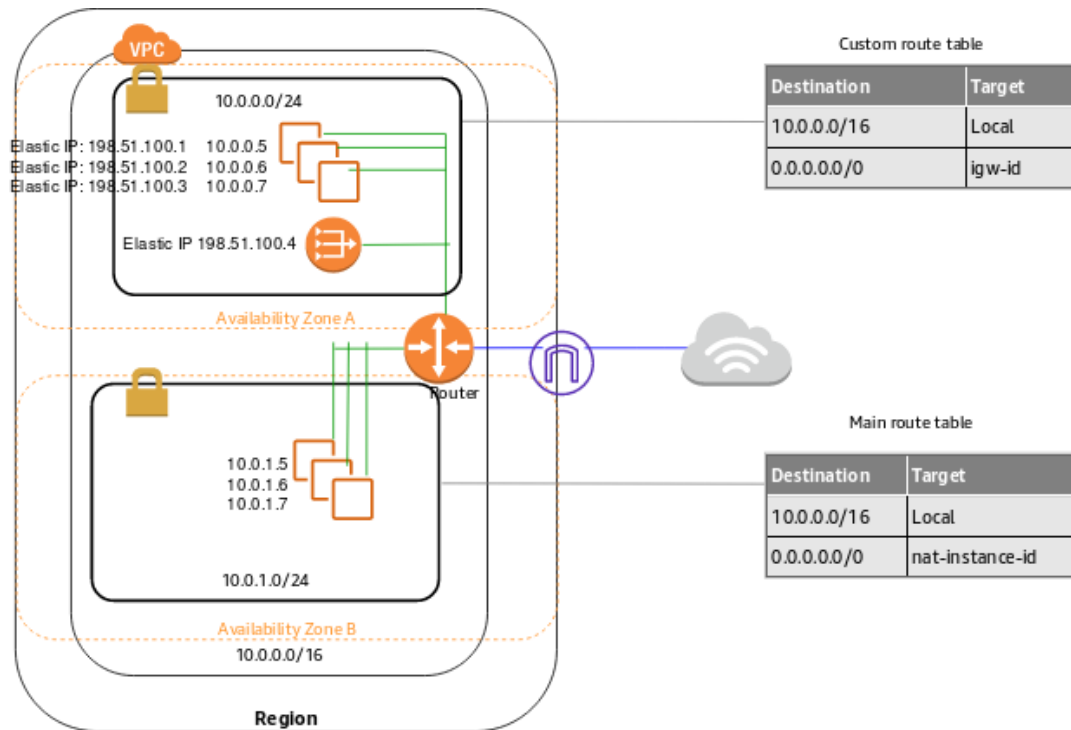
Contenido

- [Conceptos básicos de las instancias NAT \(p. 185\)](#)
- [Configurar la instancia NAT \(p. 186\)](#)
- [Crear el grupo de seguridad de NATSG \(p. 187\)](#)
- [Deshabilitar las comprobaciones de origen/destino \(p. 189\)](#)
- [Actualizar la tabla de ruteo principal \(p. 189\)](#)
- [Comprobar la configuración de su instancia NAT \(p. 190\)](#)

Conceptos básicos de las instancias NAT

El siguiente gráfico muestra los conceptos básicos de las instancias NAT. La tabla de ruteo principal está asociada a la subred privada y envía el tráfico de las instancias de la subred privada a la instancia NAT en la subred pública. La instancia NAT envía el tráfico a continuación a la gateway de internet para la VPC. El tráfico se atribuye a la dirección IP elástica de la instancia NAT. La instancia NAT especifica un número de puerto alto para la respuesta; si la respuesta vuelve, la instancia NAT la envía a una instancia de la subred privada en función del número de puerto de la respuesta.

El tráfico de Internet desde las instancias en la subred privada se direcciona a la instancia NAT, que luego se comunica con Internet. Por lo tanto, la instancia NAT debe tener acceso a Internet. Debe estar en una subred pública (una subred que tiene una tabla de enrutamiento con una ruta a la gateway de Internet) y debe tener una dirección IP pública o una dirección IP elástica.



Configurar la instancia NAT

Utilice el siguiente procedimiento para configurar una VPC y una instancia NAT.

Requisito

Antes de comenzar, cree una AMI configurada para que se ejecute como instancia NAT. Los comandos específicos para configurar NAT dependen del sistema operativo que utiliza. Por ejemplo, para Amazon Linux 2, utilice los siguientes comandos:

```
sudo sysctl -w net.ipv4.ip_forward=1
sudo /sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo yum install iptables-services
sudo service iptables save
```

Para configurar una instancia NAT

1. Cree una VPC con dos subredes.
 - a. Cree una VPC (consulte [Creación de una VPC \(p. 21\)](#)).
 - b. Cree dos subredes (consulte [Creación de una subred \(p. 145\)](#)).
 - c. Asocie una gateway de Internet a la VPC (consulte [Crear y adjuntar una gateway de Internet \(p. 145\)](#)).
 - d. Cree una tabla de enrutamiento personalizada que envíe el tráfico cuyo destino esté fuera de la VPC a la gateway de Internet y, a continuación, asóciela con una subred, lo que la convierte en una subred pública (consulte [Creación de una tabla de ruteo personalizada \(p. 146\)](#)).
2. Cree el grupo de seguridad de NATSG (consulte [Crear el grupo de seguridad de NATSG \(p. 187\)](#)). Este grupo de seguridad se especifica al lanzar la instancia NAT.
3. Lance una instancia en su subred pública desde una AMI que se haya configurado para ejecutarse como instancia NAT.

- a. Abra la consola de Amazon EC2.
- b. En el panel, elija el botón Launch Instance y complete el asistente de la siguiente forma:
 - i. En la página Elegir una Amazon Machine Image (AMI), establezca el filtro en De mi propiedad, a continuación, seleccione la AMI.
 - ii. En la página Choose an Instance Type, seleccione el tipo de instancia y, a continuación, elija Next: Configure Instance Details.
 - iii. En la página Configure Instance Details, seleccione la VPC que creó en la lista Network y seleccione la subred pública desde la lista Subnet.
 - iv. (Opcional) Seleccione la casilla de verificación Public IP para solicitar que la instancia NAT reciba una dirección IP pública. Si elige no asignar una dirección IP pública ahora, puede asignar una dirección IP elástica y asignarla a su instancia una vez lanzada. Elija Next: Add Storage (Siguiente: Agregar almacenamiento).
 - v. Puede elegir añadir almacenamiento a su instancia y, en la página siguiente, añadir etiquetas. Elija Next: Configure Security Group cuando haya terminado.
 - vi. En la página Configure Security Group, seleccione la opción Select an existing security group y seleccione el grupo de seguridad NATSG que ha creado. Elija Review and Launch.
 - vii. Revise los ajustes que ha elegido. Realice los cambios que necesite y, a continuación, elija Launch para seleccionar un par de claves y lanzar su instancia.
4. Deshabilite el atributo `SrcDestCheck` para la instancia NAT (consulte [Deshabilitar las comprobaciones de origen/destino \(p. 189\)](#)).
5. Si no ha asignado una dirección IP pública a su instancia NAT durante el lanzamiento (paso 3), debe asociarle una dirección IP elástica.
 - a. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
 - b. En el panel de navegación, elija Elastic IPs y, a continuación, elija Allocate new address.
 - c. Elija Allocate.
 - d. Seleccione la dirección IP elástica de la lista y, a continuación, elija Actions, Associate address.
 - e. Seleccione el recurso de interfaz de red y, a continuación, seleccione la interfaz de red para la instancia NAT. Seleccione la dirección a la que desea asociar la IP elástica en la lista Private IP y, a continuación, elija Associate.
6. Actualice la tabla de ruteo principal para enviar el tráfico a la instancia NAT. Para obtener más información, consulte [Actualizar la tabla de ruteo principal \(p. 189\)](#).

Lanzar una instancia NAT mediante la línea de comandos

Para lanzar una instancia NAT en su red, utilice uno de los siguientes comandos. Para obtener más información, consulte [Acceder a Amazon VPC \(p. 2\)](#). Puede utilizar el ID de AMI de la AMI que configuró para ejecutarse como una instancia NAT. Para obtener información acerca de cómo crear una AMI en Amazon Linux 2, consulte [Creación de AMI de Amazon con respaldo EBS](#) en la Guía del usuario de Amazon EC2 para instancias Linux.

- `run-instances` (AWS CLI)
- `New-EC2Instance` (AWS Tools for Windows PowerShell)

Crear el grupo de seguridad de NATSG

Defina el grupo de seguridad de NATSG según lo descrito en la siguiente tabla para permitir a su instancia NAT recibir tráfico vinculado a internet desde instancias de una subred privada, así como tráfico SSH de su red. La instancia NAT también puede enviar tráfico a internet, lo que permite que las instancias de la subred privada obtengan actualizaciones de software.

A continuación, se muestran las reglas recomendadas.

Entrada			
Fuente	Protocolo	Rango de puerto	Comentarios
<i>CIDR de subred privada</i>	TCP	80	Allow inbound HTTP traffic from servers in the private subnet
<i>CIDR de subred privada</i>	TCP	443	Allow inbound HTTPS traffic from servers in the private subnet
<i>Rango de direcciones IP públicas de su red</i>	TCP	22	Allow inbound SSH access to the NAT instance from your network (over the internet gateway)
Salida			
Destino	Protocolo	Rango de puerto	Comentarios
0.0.0.0/0	TCP	80	Allow outbound HTTP access to the internet
0.0.0.0/0	TCP	443	Allow outbound HTTPS access to the internet

Para crear el grupo de seguridad de NATSG

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Security Groups y, a continuación, elija Create Security Group.
3. En el cuadro de diálogo Create Security Group, especifique NATSG como el nombre del grupo de seguridad y proporcione una descripción. Seleccione el ID de su VPC de la lista VPC y, a continuación, elija Yes, Create.
4. Seleccione el grupo de seguridad NATSG que acaba de crear. El panel de detalles muestra información detallada del grupo de seguridad, además de pestañas que permiten usar las reglas entrantes y salientes.
5. Añada reglas para el tráfico entrante utilizando la pestaña Inbound Rules, tal y como se indica a continuación:
 - a. Elija Edit.
 - b. Elija Add another rule y seleccione HTTP en la lista Type. En el campo Source, especifique el rango de direcciones IP de su subred privada.
 - c. Elija Add another rule y seleccione HTTPS en la lista Type. En el campo Source, especifique el rango de direcciones IP de su subred privada.
 - d. Elija Add another rule y seleccione SSH en la lista Type. En el campo Source, especifique el rango de direcciones IP públicas de su red.
 - e. Seleccione Save.
6. Añada reglas para el tráfico saliente utilizando la pestaña Outbound Rules, tal y como se indica a continuación:
 - a. Elija Edit.

- b. Elija Add another rule y seleccione HTTP en la lista Type. En el campo Destination (Destino), especifique 0.0.0.0/0
- c. Elija Add another rule y seleccione HTTPS en la lista Type. En el campo Destination, especifique 0.0.0.0/0
- d. Seleccione Save.

Para obtener más información, consulte [Controlar el tráfico hacia los recursos mediante grupos de seguridad \(p. 255\)](#).

Deshabilitar las comprobaciones de origen/destino

Cada instancia EC2 realiza las comprobaciones de origen/destino de forma predeterminada. Esto significa que la instancia debe ser el origen o el destino de todo tráfico que envíe o reciba. No obstante, una instancia NAT debe poder enviar y recibir tráfico cuando el origen o el destino no sea la propia instancia. Por lo tanto, debe deshabilitar las comprobaciones de origen/destino en la instancia NAT.

Puede deshabilitar el atributo `SrcDestCheck` para una instancia NAT que se esté ejecutando o se haya detenido mediante la consola o la línea de comandos.

Para deshabilitar la comprobación de origen/destino mediante la consola

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione la instancia NAT, elija Actions (Acciones), Networking (Redes), Change source/destination check (Cambiar comprobación de origen/destino).
4. Compruebe que se ha detenido la comprobación de origen/destino. De lo contrario, elija Stop (Detener).
5. Seleccione Save.
6. Si la instancia NAT tiene una interfaz de red secundaria, selecciónela en Network interfaces (Interfaces de red) en la pestaña Networking (Redes). Elija el ID de interfaz para ir a la página de interfaces de red. Elija Actions (Acciones), Change source/des. check (Cambiar comprobación de origen y destino), borrar Enable (Habilitar) y elija Save (Guardar).

Para deshabilitar la comprobación de origen/destino mediante la línea de comandos

Puede utilizar uno de los siguientes comandos. Para obtener más información, consulte [Acceder a Amazon VPC \(p. 2\)](#).

- `modify-instance-attribute` (AWS CLI)
- `Edit-EC2InstanceAttribute` (AWS Tools for Windows PowerShell)

Actualizar la tabla de ruteo principal

La subred privada de su VPC no está asociada a una tabla de ruteo personalizada; por tanto, utiliza la tabla de ruteo principal. De forma predeterminada, la tabla de ruteo principal permite que las instancias de su VPC se comuniquen entre sí. Debe agregar una ruta que envíe el resto del tráfico de la subred a la instancia NAT.

Para actualizar la tabla de ruteo principal

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables.

3. Seleccione la tabla de enrutamiento principal para su VPC (la columna Main [Principal] mostrará Yes [Sí]). El panel de detalles muestra pestañas para trabajar con sus rutas, sus asociaciones y la propagación de rutas.
4. En la pestaña Routes (Rutas), haga lo siguiente:
 - a. Elija la pestaña Edit routes (Editar rutas) y, a continuación, Add routes (Agregar rutas).
 - b. Especifique 0.0.0.0/0 para Destination (Destino) y el ID de instancia de la instancia NAT de Target (Objetivo).
 - c. Elija Save changes.
5. En la pestaña Subnet associations (Asociaciones de subred), elija Edit subnet associations (Editar asociaciones de subred). Seleccione la casilla de verificación de la subred privada y, a continuación, elija Save associations (Guardar asociaciones).

Para obtener más información, consulte . [Configurar tablas de enrutamiento \(p. 81\)](#).

Comprobar la configuración de su instancia NAT

Después de haber iniciado una instancia NAT y completado los pasos de configuración anteriores, puede realizar una prueba para comprobar si una instancia de su subred privada puede obtener acceso a internet a través de la instancia NAT utilizando la instancia NAT como servidor bastión. Para ello, actualice las reglas del grupo de seguridad de NATSG para que permitan el tráfico ICMP entrante y saliente y el tráfico SSH saliente, lance una instancia en su subred privada, configure el reenvío de agentes SSH para obtener acceso a las instancias de su subred privada, conéctese a su instancia y, a continuación, pruebe la conectividad a internet.

Para actualizar el grupo de seguridad de su instancia NAT

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Security Groups.
3. Seleccione la casilla de verificación del grupo de seguridad NATSG asociado a la instancia NAT.
4. En la pestaña Inbound rules (Reglas de entrada), seleccione Edit inbound rules (Editar reglas de entrada).
5. Seleccione Add rule (Agregar regla). Seleccione All ICMP IPv4 (Todos los ICMP IPv4) para Type (Tipo). Seleccione Custom (Personalizado) para Source (Fuente) y escriba el rango de direcciones IP de la subred privada (por ejemplo, 10.0.1.0/24). Seleccione Save rules (Guardar reglas).
6. Seleccione Edit outbound rules (Editar reglas salientes) en la pestaña Outbound rules (Reglas salientes).
7. Seleccione Add rule (Agregar regla). Seleccione SSH para Type (Tipo). Seleccione Custom (Personalizado) para Destination (Destino) y escriba el rango de direcciones IP de la subred privada (por ejemplo, 10.0.1.0/24).
8. Seleccione Add rule (Agregar regla). Seleccione All ICMP IPv4 (Todos los ICMP IPv4) para Type (Tipo). Seleccione Anywhere - IPv4 (En cualquier lugar: IPv4) para Destination (Destino). Seleccione Save rules (Guardar reglas).

Para lanzar una instancia en su subred privada

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Lance una instancia en su subred privada. Asegúrese de configurar las siguientes opciones en el asistente de lanzamiento y, a continuación, elija Launch:
 - En la página Choose an Amazon Machine Image (AMI), seleccione una AMI de Amazon Linux en la categoría Quick Start.

- En la página Configure Instance Details, seleccione su subred privada de la lista Subnet y no asigne una dirección IP pública a su instancia.
- En la página Configure Security Group, asegúrese de que su grupo de seguridad incluye una regla entrante que permita el acceso al SSH desde la dirección IP privada de su instancia NAT o desde el rango de direcciones IP de su subred pública, y asegúrese de tener una regla saliente que permita el tráfico ICMP saliente.
- En el cuadro de diálogo Select an existing key pair or create a new key pair, seleccione el mismo par de claves que utilizó para lanzar la instancia NAT.

Para configurar el reenvío de agentes SSH para Linux u OS X

1. Desde su equipo local, añada su clave privada al agente de autenticación.

Para Linux, utilice el siguiente comando:

```
ssh-add -c mykeypair.pem
```

Para OS X, utilice el siguiente comando:

```
ssh-add -K mykeypair.pem
```

2. Conéctese a su instancia NAT utilizando la opción `-A` para habilitar el reenvío de agentes SSH; por ejemplo:

```
ssh -A ec2-user@54.0.0.123
```

Para configurar el reenvío de agentes SSH para Windows (PuTTY)

1. Descargue e instale Pageant desde la [página de descargas de PuTTY](#), si aún no lo tiene instalado.
2. Convierta su clave privada al formato .ppk. Para obtener más información, consulte [Convertir la clave privada mediante PuTTYgen](#).
3. Inicie Pageant, haga clic con el botón derecho en el icono de Pageant de la barra de tareas (puede estar oculto) y elija Add Key. Seleccione el archivo .ppk que ha creado, escriba la frase de contraseña si es necesario, y elija Open.
4. Inicie una sesión de PuTTY para conectarse a su instancia NAT. En la categoría Auth asegúrese de seleccionar la opción Allow agent forwarding y deje el campo Private key file for authentication en blanco.

Para comprobar la conexión a Internet

1. Compruebe que su instancia NAT puede conectarse a internet ejecutando el comando ping para un sitio web que tenga ICMP habilitado; por ejemplo:

```
ping ietf.org
```

```
PING ietf.org (4.31.198.44) 56(84) bytes of data.  
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=1 ttl=48 time=74.9 ms  
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=2 ttl=48 time=75.1 ms  
...
```

Pulse Ctrl+C en su teclado para cancelar el comando ping.

- Desde su instancia NAT, conéctese a su instancia en su subred privada utilizando su dirección IP privada. Por ejemplo:

```
ssh ec2-user@10.0.1.123
```

- Desde su instancia privada, compruebe que puede conectarse a internet ejecutando el comando ping:

```
ping ietf.org
```

```
PING ietf.org (4.31.198.44) 56(84) bytes of data.  
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=1 ttl=47 time=86.0 ms  
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=2 ttl=47 time=75.6 ms  
...
```

Pulse Ctrl+C en su teclado para cancelar el comando ping.

En caso de error en el comando ping, compruebe la información siguiente:

- Compruebe que las reglas de grupo de seguridad de su instancia NAT permiten el tráfico ICMP entrante desde su subred privada. En caso contrario, su instancia NAT no podrá recibir el comando ping desde su instancia privada.
 - Asegúrese de haber configurado las tablas de ruteo correctamente. Para obtener más información, consulte [Actualizar la tabla de ruteo principal \(p. 189\)](#).
 - Asegúrese de haber deshabilitado la comprobación de origen/destino para su instancia NAT. Para obtener más información, consulte [Deshabilitar las comprobaciones de origen/destino \(p. 189\)](#).
 - Asegúrese de estar haciendo ping a un sitio web que tiene ICMP habilitado. En caso contrario, no recibirá paquetes de respuesta. Para comprobar esto, ejecute el mismo comando ping desde el terminal de línea de comandos en su propio equipo.
- (Opcional) Termine su instancia privada si ya no la necesita. Para obtener más información, consulte [Terminar la instancia](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Comparar las gateways NAT con las instancias NAT

A continuación se proporciona un resumen general de las diferencias entre las gateways NAT y las instancias NAT. Le recomendamos que utilice las gateways NAT, ya que proporcionan mayor disponibilidad y ancho de banda y requieren menos esfuerzo de administración por su parte.

Atributo	Gateway NAT	Instancia NAT
Disponibilidad	Altamente disponibles. Las gateways NAT de cada zona de disponibilidad se implementan con redundancia. Cree una gateway NAT en cada zona de disponibilidad para garantizar una arquitectura independiente de zonas.	Utilice un script para administrar la conmutación por error entre instancias.
Ancho de banda	Puede escalar hasta 45 Gbps.	Dependen del ancho de banda del tipo de instancia.
Mantenimiento	Administrada por AWS. No necesita realizar ningún mantenimiento.	Administradas por usted. Por ejemplo, al instalar actualizaciones de software o parches de sistema operativo en la instancia.

Atributo	Gateway NAT	Instancia NAT
Desempeño	El software está optimizado para la gestión del tráfico de NAT.	Una AMI configurada para realizar la NAT.
Costo	Se cobra en función del número de gateways NAT que utilice, la duración del uso y la cantidad de datos que envíe mediante las gateways NAT.	Se cobra en función del número de instancias NAT que utilice, la duración del uso y el tamaño y el tipo de instancia.
Tipo y tamaño	Oferta uniforme; no necesita decidir el tamaño ni el tipo.	Elija un tipo de instancia y un tamaño adecuados, acordes con la estimación de su carga de trabajo.
Direcciones IP públicas	Elija la dirección IP elástica para asociar a la gateway NAT pública en el momento de la creación.	Utilice una dirección IP elástica o una dirección IP pública con una instancia NAT. Puede cambiar la dirección IP pública en el momento de asociar una nueva dirección IP elástica a la instancia.
Direcciones IP privadas	Se seleccionan automáticamente del rango de direcciones IP de la subred al crear la gateway.	Al lanzar la instancia, asigne una dirección IP privada específica del rango de direcciones IP de la subred.
Grupos de seguridad	No puede asociar los grupos de seguridad a las gateways NAT. Puede asociarlos a los recursos detrás de la gateway NAT para controlar el tráfico entrante y saliente.	Asocie su instancia NAT y los recursos detrás de su instancia NAT para controlar el tráfico entrante y saliente.
ACL de red	Utilice una ACL de red para controlar el tráfico hacia la subred y procedente de esta en la que se encuentra su gateway NAT.	Utilice una ACL de red para controlar el tráfico hacia la subred y procedente de esta en la que se encuentra su instancia NAT.
Logs de flujo	Utilice los logs de flujo para capturar el tráfico.	Utilice los logs de flujo para capturar el tráfico.
Enrutamiento de puertos	No es compatible.	Personalice manualmente la configuración para que admita el reenvío de puertos.
Servidores bastión	No es compatible.	Se pueden utilizar como servidor bastión.
Métricas de tráfico	Consulte métricas de CloudWatch para la gateway NAT (p. 172) .	Consulte métricas de CloudWatch para la instancia.
Comportamiento de los tiempos de espera	Cuando el tiempo de espera de una conexión finaliza, una gateway NAT devuelve un paquete RST a los recursos situados detrás de la gateway NAT que intenten continuar la conexión (no envía un paquete FIN).	Cuando el tiempo de espera de una conexión finaliza, una instancia NAT envía un paquete FIN a los recursos situados detrás de la instancia NAT para cerrar la conexión.
Fragmentación de IP	Admiten el reenvío de paquetes IP fragmentados para el protocolo UDP. No admiten la fragmentación para los protocolos ICMP y TCP. Los paquetes fragmentados para estos protocolos se retirarán.	Admiten el reensamblado de paquetes IP fragmentados para los protocolos ICMP, UDP y TCP.

Migrar desde una instancia NAT a una gateway NAT

Si ya está utilizando una instancia NAT, recomendamos que la reemplace por una gateway NAT. Para ello, puede crear una gateway NAT en la misma subred que su instancia NAT, y luego reemplazar la ruta existente en su tabla de enrutamiento que apunta a la instancia NAT por una ruta que apunte a la gateway NAT. Para usar la misma dirección IP elástica para la gateway NAT que utiliza actualmente para su instancia NAT, primero debe desasociar la dirección IP elástica de su instancia NAT y después asociarla a su gateway NAT al crear la gateway.

Si cambia su direccionamiento de una instancia NAT a una gateway NAT, o si desasocia la dirección IP elástica de su instancia NAT, las conexiones actuales se perderán y tendrá que volver a establecerlas. Asegúrese de no estar ejecutando ninguna tarea crítica (o cualquier otra tarea que opere mediante la instancia NAT).

Conecte la VPC a otras VPC y redes utilizando una puerta de enlace de tránsito

Puede conectar las nubes virtuales privadas (VPC) y las redes en las instalaciones utilizando una puerta de enlace de tránsito, que actúa como un concentrador central, para dirigir el tráfico entre las VPC, las conexiones VPN y las conexiones de AWS Direct Connect. Para obtener más información, consulte [AWS Transit Gateway](#).

En la siguiente tabla se describen algunos casos de uso comunes de puertas de enlace de tránsito y se proporcionan vínculos a más información en las Puertas de enlace de tránsito de Amazon VPC.

Ejemplo	Uso
Router centralizado	Puede configurar su transit gateway como un enrutador centralizado que conecta todas las VPC, AWS Direct Connect y las conexiones de AWS Site-to-Site VPN. Para obtener más información, consulte Ejemplo: enrutador centralizado .
VPC aisladas	Configure la transit gateway como varios enrutadores aislados. Es similar a utilizar varias puertas de enlace de tránsito, pero ofrece mayor flexibilidad en aquellos casos en los que es posible que las rutas y las conexiones cambien. Para obtener más información, consulte Ejemplo: VPC aisladas .
VPC aisladas con servicios compartidos	Configure su transit gateway como varios enrutadores aislados que utilizan un servicio compartido. Es similar a utilizar varias puertas de enlace de tránsito, pero ofrece mayor flexibilidad en aquellos casos en los que es posible que las rutas y las conexiones cambien. Para obtener más información, consulte Ejemplo: VPC aisladas con servicios compartidos .

Conectar la VPC a redes remotas mediante AWS Virtual Private Network

Puede conectar Amazon VPC a redes y usuarios remotos usando las siguientes opciones de conectividad de VPN.

Opción de conectividad de VPN	Descripción
AWS Site-to-Site VPN	Puede crear una conexión de VPN IPsec entre su VPC y su red remota. En el lado de AWS de la conexión de Site-to-Site VPN, una puerta de enlace privada virtual o transit gateway proporciona dos puntos de enlace de VPN (túneles) para la conmutación por error automática. Configure su dispositivo de puerta de enlace del cliente en el lado remoto de la conexión de Site-to-Site VPN. Para obtener más información, consulte la Guía del usuario de AWS Site-to-Site VPN .
AWS Client VPN	AWS Client VPN es un servicio administrado de VPN basado en el cliente que le permite acceder de manera segura a sus recursos de AWS o a su red en las instalaciones. Con AWS Client VPN, se configura un punto de enlace al que se pueden conectar sus usuarios para establecer una sesión de VPN TLS segura. De este modo, los clientes pueden acceder a los recursos de AWS o los de las instalaciones desde cualquier ubicación mediante un cliente de VPN basado en OpenVPN. Para obtener más información, consulte la Guía de administración de AWS Client VPN .
AWS VPN CloudHub	Si tiene más de una red remota (por ejemplo, varias sucursales), podrá crear varias conexiones de AWS Site-to-Site VPN a través de su gateway privada virtual para habilitar la comunicación entre estas redes. Para obtener más información, consulte Comunicaciones seguras entre sitios mediante VPN CloudHub en la Guía del usuario de AWS Site-to-Site VPN.
Dispositivo de VPN por software de terceros	Puede crear una conexión de VPN a su red remota usando una instancia de Amazon EC2 de su VPC que ejecute un dispositivo de VPN por software de terceros. AWS no proporciona ni mantiene dispositivos de VPN por software de terceros; sin embargo, puede elegir de una gama de productos proporcionados por socios y comunidades de código abierto. Puede buscar dispositivos de VPN por software de terceros en AWS Marketplace .

También puede utilizar AWS Direct Connect para crear una conexión privada dedicada desde la red remota a su VPC. Esta conexión se puede combinar con una AWS Site-to-Site VPN para crear una conexión con cifrado IPsec. Para obtener más información, consulte [¿Qué es AWS Direct Connect?](#) en la Guía del usuario de AWS Direct Connect.

Conecte las VPC utilizando emparejamiento de VPC

Una interconexión de VPC es una conexión de redes entre dos VPC que permite direccionar el tráfico entre ellas de forma privada. Las instancias de ambas VPC se pueden comunicar entre sí siempre que se encuentren en la misma red. Puede crear una interconexión de VPC entre sus propias VPC, con una VPC de otra cuenta de AWS o con una VPC de otra región de AWS.

AWS utiliza la infraestructura existente de una VPC para crear una interconexión de VPC. No se trata de ninguna gateway o conexión de AWS Site-to-Site VPN y no usa ningún hardware físico individual. Por lo tanto, no existen puntos de error de comunicaciones ni cuellos de botella de ancho de banda.

Para obtener más información acerca del uso de interconexiones de VPC y ejemplos de escenarios de utilización de interconexiones de VPC, consulte la [Guía de interconexión de Amazon VPC](#).

Ejemplos: servicios que utilizan emparejamiento de VPC y AWS PrivateLink

El emparejamiento de VPC le permite conectar las VPC de forma privada, mientras que AWS PrivateLink le permite configurar aplicaciones o servicios en las VPC como puntos de conexión a los que se pueden conectar las conexiones de emparejamiento de VPC.

Un proveedor de servicios de AWS PrivateLink configura las instancias que ejecutan servicios en la VPC con un Network Load Balancer como frontend. Utilice la interconexión de VPC dentro de la región (VPC que están en la misma región) y la interconexión de VPC entre regiones (VPC que están en regiones distintas) con AWS PrivateLink para permitir el acceso privado a consumidores en conexiones con interconexión de VPC.

Los consumidores de VPC remotas no pueden usar nombres de DNS privados en interconexiones. Sin embargo, pueden crear su propia zona alojada privada en Route 53 y asociarla a las VPC para usar el mismo nombre DNS privado. Para obtener información acerca del uso de la transit gateway con Amazon Route 53 Resolver, para compartir los puntos de enlace de interfaz de PrivateLink entre varias VPC conectadas y un entorno en las instalaciones, consulte [Integrating AWS Transit Gateway with AWS PrivateLink and Amazon Route 53 Resolver](#).

Para obtener información sobre los siguientes casos de uso, consulte [Securely Access Services Over AWS PrivateLink](#):

- Acceso privado a aplicaciones SaaS
- Servicios compartidos
- Servicios híbridos
- Servicios de punto de enlace entre regiones
- Acceso a servicios de punto de enlace entre regiones

Recursos adicionales

Los temas siguientes pueden ayudarle a configurar los componentes necesarios para los casos de uso:

- [Servicios de punto de conexión de la VPC](#)
- [Introducción a los balanceadores de carga de red](#)
- [Funcionamiento de interconexiones de VPC](#)
- [Crear un punto de enlace de interfaz](#)

Para obtener más ejemplos de interconexión de VPC, consulte los siguientes temas en la Guía de interconexiones de Amazon VPC:

- [Configuraciones de interconexión de VPC](#)
- [Configuraciones de interconexión de VPC no admitidas](#)

Supervisión de la VPC

Puede utilizar las siguientes herramientas para supervisar el tráfico o el acceso a la red en la nube virtual privada (VPC).

Logs de flujo de VPC

Puede utilizar los registros de flujo de VPC para recopilar información detallada sobre el tráfico entrante y saliente de las interfaces de red en las VPC.

Amazon VPC IP Address Manager (IPAM)

Puede utilizar IPAM para planificar, rastrear y supervisar las direcciones IP de las cargas de trabajo. Para obtener más información, consulte [Administrador de direcciones IP](#).

Replicación de tráfico

Puede utilizar esta característica para copiar el tráfico desde una interfaz de red de una instancia de Amazon EC2 y enviarlo a dispositivos de seguridad y supervisión fuera de banda para una inspección profunda de paquetes. Puede detectar anomalías de red y seguridad, obtener información operativa, aplicar controles de conformidad y seguridad, además de solucionar problemas. Para obtener más información, consulte [Replicación de tráfico](#).

VPC Reachability Analyzer

Puede utilizar esta herramienta para analizar y depurar la accesibilidad de la red entre dos recursos en la VPC. Después de especificar los recursos de origen y destino, Reachability Analyzer produce detalles salto a salto de la ruta virtual entre ellos cuándo son accesibles e identifica el componente de bloqueo cuándo son inalcanzables. Para obtener más información, consulte [VPC Reachability Analyzer](#).

Analizador de acceso a la red

Puede utilizar el analizador de acceso a la red para comprobar el acceso de la red a los recursos. Esto le ayuda a identificar mejoras en la posición de seguridad de la red y a demostrar que esta cumple con los requisitos específicos de conformidad. Para obtener más información, consulte [Analizador de acceso a la red](#).

Registros de CloudTrail

Puede utilizar AWS CloudTrail para recopilar información detallada sobre las llamadas realizadas a la API de Amazon VPC. Puede utilizar los registros de CloudTrail generados para determinar qué llamadas se han efectuado, la dirección IP de origen de la que procede la llamada, quién la ha realizado, cuándo, etc. Para obtener más información, consulte [Registrar llamadas a la API de Amazon EC2, Amazon EBS y Amazon VPC con AWS CloudTrail](#) en la Referencia de las API de Amazon EC2.

Registro del tráfico de IP con registros de flujo de la VPC

Los logs de flujo de VPC son una característica que permite capturar información acerca del tráfico IP que entra y sale de las interfaces de red en la VPC. Los datos del registro de flujo se pueden publicar en

Amazon CloudWatch Logs o Amazon S3. Una vez creado un registro de flujo, puede recuperarlo y ver sus datos en el destino elegido.

Los logs de flujo pueden ayudarle en una serie de tareas, tales como:

- Diagnosticar reglas de grupo de seguridad muy restrictivas
- Monitorizar el tráfico que llega a su instancia
- Determinar la dirección del tráfico hacia y desde las interfaces de red

Los datos de registro de flujo se recopilan fuera de la ruta del tráfico de red y, por lo tanto, no afectan al rendimiento ni a la latencia de la red. Puede crear o eliminar registros de flujo sin ningún riesgo de impacto en el rendimiento de la red.

Contenido

- [Conceptos básicos de logs de flujo \(p. 198\)](#)
- [Registros de log de flujo \(p. 200\)](#)
- [Ejemplos de registros de log de flujo \(p. 205\)](#)
- [Limitaciones de los logs de flujo \(p. 210\)](#)
- [Precios de registros de flujo \(p. 210\)](#)
- [Publicar registros de flujo en CloudWatch Logs \(p. 211\)](#)
- [Publicar registros de flujo en Amazon S3 \(p. 216\)](#)
- [Trabajar con registros de flujo \(p. 222\)](#)
- [Realizar consultas en los registros de flujo mediante Amazon Athena \(p. 226\)](#)
- [Solucionar problemas de los registros de flujo de VPC \(p. 229\)](#)

Conceptos básicos de logs de flujo

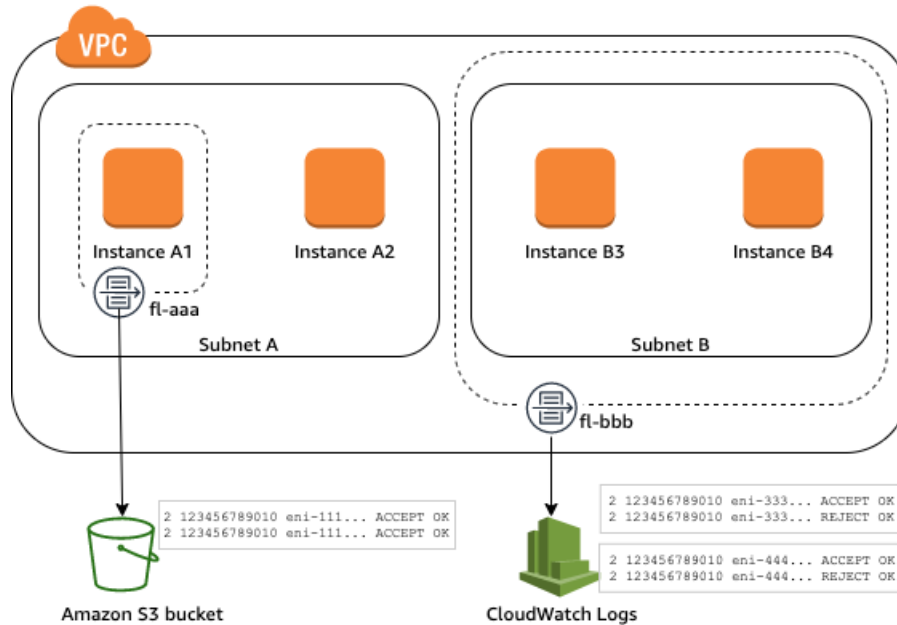
Puede crear un log de flujo para una VPC, una subred o una interfaz de red. Si crea un log de flujo para una subred o VPC, se supervisará cada interfaz de red de la VPC o la subred.

Los datos de logs de flujo de una interfaz de red monitoreada se registran como registros de logs de flujo, que son eventos de registro que constan de campos que describen el flujo de tráfico. Para obtener más información, consulte [Registros de log de flujo \(p. 200\)](#).

Para crear un log de flujo, especifique:

- El recurso para el que desea crear el log de flujo
- El tipo de tráfico que capturar (tráfico aceptado, tráfico rechazado o todo el tráfico)
- Los destinos a los que desea publicar los datos de log de flujo

En el ejemplo siguiente, se crea una entrada de registro (f1-aaa) que captura el tráfico aceptado para la interfaz de red para la instancia A1 y publica las entradas de registro de flujo en un bucket de Amazon S3. Se crea una segunda entrada de registro de flujo que captura todo el tráfico de la subred B y publica las entradas de registro de flujo en Amazon CloudWatch Logs. El log de flujo (f1-bbb) captura el tráfico de todas las interfaces de red de la subred B. No hay logs de flujo que capturen tráfico, por ejemplo, la interfaz de red de A2.



Después de crear un registro de flujo, pueden transcurrir varios minutos hasta que se empiecen a recopilar datos y a publicarse en los destinos elegidos. Los logs de flujo no capturan los flujos de logs en tiempo real de las interfaces de red. Para obtener más información, consulte [Crear un log de flujo \(p. 223\)](#).

Si lanza una instancia en la subred después de haber creado un registro de flujo para la subred o la VPC, creamos un nuevo flujo de registros (para CloudWatch Logs) o un objeto de archivo de registros (para Amazon S3) para la nueva interfaz de red apenas haya tráfico de red para la interfaz de red.

Puede crear registros de flujo para interfaces de red creadas por otros servicios de AWS, tales como:

- Elastic Load Balancing
- Amazon RDS
- Amazon ElastiCache
- Amazon Redshift
- Amazon WorkSpaces
- Gateways NAT
- Transit gateways

Con independencia del tipo de interfaz de red, debe utilizar la consola de Amazon EC2 o la API de Amazon EC2 para crear un registro de flujo para una interfaz de red.

Puede aplicar etiquetas a los registros de flujo. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario. Las etiquetas pueden ayudarle a organizar los registros de flujo, por ejemplo, por finalidad o propietario.

Si ya no necesita un log de flujo, puede eliminarlo. La eliminación de un registro de flujo desactiva el servicio del registro de flujo para el recurso y no se crean nuevas entradas de registros ni se publican en CloudWatch Logs o Amazon S3. La eliminación del registro de flujo no elimina ninguna entrada de registro de flujo existente ni secuencias de registros (para CloudWatch Logs) u objetos de archivos de registro (para Amazon S3) de una interfaz de red. Para eliminar una secuencia de registro existente, utilice la consola de CloudWatch Logs. Para eliminar objetos de archivos de registro, utilice la consola de Amazon S3. Tras haber eliminado un log de flujo, puede que se necesiten varios minutos para que se dejen de recopilar los datos. Para obtener más información, consulte [Eliminación de un log de flujo \(p. 225\)](#).

Registros de log de flujo

Un registro de log de flujo representa un flujo de red en su VPC. De forma predeterminada, cada registro captura un flujo de tráfico del protocolo de Internet (IP) de red (caracterizado por 5 tuplas para cada interfaz de red) que tiene lugar dentro de un intervalo de agregación, lo también se conoce como período de captura.

Cada registro es una cadena con campos separados por espacios. Un registro incluye valores para los distintos componentes del flujo de IP, por ejemplo, el origen, el destino y el protocolo.

Al crear un registro de flujo, puede utilizar el formato predeterminado para el registro del registro de flujo o puede especificar un formato personalizado.

Contenido

- [Intervalo de agregación \(p. 200\)](#)
- [Formato predeterminado \(p. 200\)](#)
- [Formato personalizado \(p. 200\)](#)
- [Campos disponibles \(p. 201\)](#)

Intervalo de agregación

El intervalo de agregación es el período de tiempo durante el que se captura un flujo determinado y se agrega a un registro de flujo. De forma predeterminada, el intervalo de agregación máximo es de 10 minutos. Cuando cree un registro de flujo, si lo desea, puede especificar un intervalo máximo de agregación de 1 minuto. Los registros de flujo con un intervalo de agregación máximo de 1 minuto producen un volumen mayor de registros que los que tienen un intervalo de agregación máximo de 10 minutos.

Cuando una interfaz de red está asociada a una [instancia basada en Nitro](#), el intervalo de agregación siempre es igual o inferior a 1 minuto, independientemente del intervalo de agregación máximo especificado.

Una vez que los datos se han capturado durante el intervalo de agregación, se necesita más tiempo para procesarlos y publicarlos en CloudWatch Logs o Amazon S3. El servicio de registros de flujo suele entregar registros a CloudWatch Logs en unos 5 minutos y a Amazon S3 en unos 10 minutos. No obstante, aunque se hace todo lo posible para realizar la entrega de los registros, puede que se produzcan retrasos y se necesite más tiempo del habitual para entregarlos.

Formato predeterminado

Con el formato predeterminado, los registros del log de flujo incluyen los campos de la versión 2, en el orden mostrado en la tabla de [campos disponibles \(p. 201\)](#). No puede personalizar o cambiar el formato predeterminado. Para capturar los campos adicionales o un subconjunto de campos distinto, especifique un formato personalizado.

Formato personalizado

Con un formato personalizado, especifique qué campos se incluyen en los registros del log de flujo y en qué orden. De este modo, puede crear registros de flujo específicos con arreglo a sus necesidades y omitir los campos que no resulten relevantes. El uso de un formato personalizado puede reducir la necesidad de procesos separados para extraer información específica de logs de flujo publicados. Puede especificar cualquier número de campos de log de flujo disponibles, pero debe especificar al menos uno.

Campos disponibles

La tabla siguiente describe todos los campos disponibles para un registro de logs de flujo. La columna Version (Versión) indica la versión de los registros de flujo de VPC en la que se introdujo el campo. El formato predeterminado incluye todos los campos de la versión 2, en el mismo orden en que aparecen en la tabla.

Al publicar datos de registro de flujo en Amazon S3, el tipo de datos de los campos depende del formato del registro de flujo. Si el formato es texto sin formato, todos los campos son de tipo STRING. Si el formato es Parquet, consulte la tabla de los tipos de datos de campo.

Si un campo no es aplicable o no se pudo calcular para un registro específico, el registro muestra un símbolo “-” en esa entrada. Los campos de metadatos que no provienen directamente del encabezado del paquete son aproximaciones de mejor esfuerzo y sus valores pueden faltar o ser inexactos.

Campo	Descripción	Versión
version	La versión de los registros de flujo de VPC. Si utiliza el formato predeterminado, la versión es 2. Si utiliza un formato personalizado, la versión es la más alta entre los campos especificados. Por ejemplo, si especifica sólo campos de la versión 2, la versión es 2. Si especifica una combinación de campos de las versiones 2, 3 y 4, la versión es 4. Tipo de datos de Parquet: INT_32	2
account-id	El ID de la cuenta de AWS del propietario de la interfaz de red de origen en la que se registra el tráfico. Si un servicio de AWS crea la interfaz de red, por ejemplo, al momento de crear un punto de conexión de VPC o Network Load Balancer, el registro puede mostrar unknown para este campo. Tipo de datos de Parquet: STRING	2
interface-id	El ID de la interfaz de red para la que se registra el tráfico. Tipo de datos de Parquet: STRING	2
srcaddr	La dirección de origen para tráfico entrante o la dirección IPv4 o IPv6 de la interfaz de red para tráfico saliente en la interfaz de red. La dirección IPv4 de la interfaz de red es siempre su dirección IPv4 privada. Véase también pkt-srcaddr. Tipo de datos de Parquet: STRING	2
dstaddr	La dirección de destino para tráfico saliente o la dirección IPv4 o IPv6 de la interfaz de red para tráfico entrante en la interfaz de red. La dirección IPv4 de la interfaz de red es siempre su dirección IPv4 privada. Véase también pkt-dstaddr. Tipo de datos de Parquet: STRING	2
srcport	El puerto de origen del tráfico. Tipo de datos de Parquet: INT_32	2
dstport	El puerto de destino del tráfico. Tipo de datos de Parquet: INT_32	2

Campo	Descripción	Versión
protocol	El número de protocolo IANA del tráfico. Para obtener más información, consulte Assigned Internet Protocol Numbers . Tipo de datos de Parquet: INT_32	2
packets	El número de paquetes transferidos durante el flujo. Tipo de datos de Parquet: INT_64	2
bytes	El número de bytes transferidos durante el flujo. Tipo de datos de Parquet: INT_64	2
start	Momento, en segundos Unix, en que se recibió el primer paquete del flujo dentro del intervalo de agregación. El tiempo transcurrido puede ser como máximo de 60 segundos una vez que el paquete se ha transmitido o recibido en la interfaz de red. Tipo de datos de Parquet: INT_64	2
end	Momento, en segundos Unix, en que se recibió el último paquete del flujo dentro del intervalo de agregación. El tiempo transcurrido puede ser como máximo de 60 segundos una vez que el paquete se ha transmitido o recibido en la interfaz de red. Tipo de datos de Parquet: INT_64	2
action	La acción asociada al tráfico: <ul style="list-style-type: none"> ACCEPT: los grupos de seguridad o las ACL de red permitieron el tráfico registrado. REJECT: los grupos de seguridad o las ACL de red no permitieron el tráfico registrado. Tipo de datos de Parquet: STRING	2
log-status	El estado de registro del registro de flujo: <ul style="list-style-type: none"> OK: los datos se registran normalmente en los destinos elegidos. NODATA: no hubo tráfico de red hacia o desde la interfaz de red durante el intervalo de agregación. SKIPDATA: algunos registros de flujo se omitieron durante el intervalo de agregación. Esto se puede deber a una restricción de capacidad interna, o a un error interno. Tipo de datos de Parquet: STRING	2
vpc-id	El ID de la VPC que contiene la interfaz de red para la que se registra el tráfico. Tipo de datos de Parquet: STRING	3
subnet-id	El ID de la subred que contiene la interfaz de red para la que se registra el tráfico. Tipo de datos de Parquet: STRING	3

Campo	Descripción	Versión
instance-id	<p>El ID de la instancia que está asociado a la interfaz de red para la que se registra el tráfico, si la instancia es de su propiedad. Devuelve un símbolo "-" para una interfaz de red administrada por el solicitante; por ejemplo, la interfaz de red para una gateway NAT.</p> <p>Tipo de datos de Parquet: STRING</p>	3
tcp-flags	<p>El valor de máscara de bits de las siguientes marcas TCP:</p> <ul style="list-style-type: none"> • SYN: 2 • SYN-ACK: 18 • FIN: 1 • RST: 4 <p>ACK se notifica solo cuando va acompañado de SYN.</p> <p>Se puede aplicar OR a las marcas TCP durante el intervalo de agregación. Para conexiones breves, los marcadores se pueden establecer en la misma línea en el registro de flujo, por ejemplo 19 para SYN-ACK y FIN y 3 para SYN y FIN. Para ver un ejemplo, consulte Secuencia de marca TCP (p. 207).</p> <p>Tipo de datos de Parquet: INT_32</p>	3
type	<p>El tipo de tráfico. Los valores posibles son: IPv4 IPv6 EFA. Para obtener más información, consulte Elastic Fabric Adapter.</p> <p>Tipo de datos de Parquet: STRING</p>	3
pkt-srcaddr	<p>La dirección IP de origen (original) del nivel de paquete del tráfico. Utilice este campo con el campo srcaddr para distinguir entre la dirección IP de una capa intermedia a través de la que fluye el tráfico y la dirección IP de origen original del tráfico. Por ejemplo, cuando el tráfico fluye a través de una interfaz de red para una gateway NAT (p. 208) o si la dirección IP de un pod de Amazon EKS es distinta de la dirección IP de la interfaz de red del nodo de instancia en el que se ejecuta el pod (para permitir la comunicación dentro de una VPC).</p> <p>Tipo de datos de Parquet: STRING</p>	3
pkt-dstaddr	<p>La dirección IP de destino (original) del nivel de paquete para el tráfico. Utilice este campo con el campo dstaddr para distinguir entre la dirección IP de una capa intermedia a través de la que fluye el tráfico y la dirección IP de destino final del tráfico. Por ejemplo, cuando el tráfico fluye a través de una interfaz de red para una gateway NAT (p. 208) o si la dirección IP de un pod de Amazon EKS es distinta de la dirección IP de la interfaz de red del nodo de instancia en el que se ejecuta el pod (para permitir la comunicación dentro de una VPC).</p> <p>Tipo de datos de Parquet: STRING</p>	3
region	<p>La región que contiene la interfaz de red para la que se registra el tráfico.</p> <p>Tipo de datos de Parquet: STRING</p>	4

Campo	Descripción	Versión
az-id	El ID de la zona de disponibilidad que contiene la interfaz de red para la que se registra el tráfico. Si el tráfico procede de una ubicación secundaria, el registro muestra un símbolo '-' en este campo. Tipo de datos de Parquet: STRING	4
sublocation-type	El tipo de ubicación secundaria que se devuelve en el sublocation-id campo. Los valores posibles son: longitud de onda outpost zona local . Si el tráfico no procede de una ubicación secundaria, el registro muestra un símbolo '-' en este campo. Tipo de datos de Parquet: STRING	4
sublocation-id	El ID de la ubicación secundaria que contiene la interfaz de red para la que se registra el tráfico. Si el tráfico no procede de una ubicación secundaria, el registro muestra un símbolo '-' en este campo. Tipo de datos de Parquet: STRING	4
pkt-src-aws-service	El nombre del subconjunto de intervalos de direcciones IP para el campo pkt-srcaddr, si la dirección IP de origen está destinada a un servicio de AWS. Los valores posibles son: AMAZON AMAZON_APPFLOW AMAZON_CONNECT API_GATEWAY CHIME_MEETINGS CHIME_VOICECONNECTOR CLOUD9 CLOUDFRONT CODEBUILD DYNAMODB EBS EC2 EC2_INSTANCE_CONNECT GLOBALACCELERATOR KINESIS_VIDEO_STREAMS ROUTE53 ROUTE53_HEALTHCHECKS ROUTE53_HEALTHCHECKS_PUBLISHING ROUTE53_RESOLVER S3 WORKSPACES_GATEWAYS. Tipo de datos de Parquet: STRING	5
pkt-dst-aws-service	El nombre del subconjunto de intervalos de direcciones IP para el campo pkt-dstaddr, si la dirección IP de destino está destinada a un servicio de AWS. Para obtener una lista de posibles valores, consulte el pkt-src-aws-service campo. Tipo de datos de Parquet: STRING	5
flow-direction	La dirección del flujo con respecto a la interfaz donde se captura el tráfico. Los valores posibles son: ingress egress. Tipo de datos de Parquet: STRING	5

Campo	Descripción	Versión
traffic-path	<p>La ruta que el tráfico de salida toma al destino. Para determinar si el tráfico es de salida, marque el flow-direction campo. Los valores posibles son los siguientes: Si no se aplica ninguno de los valores, el campo se establece en -.</p> <ul style="list-style-type: none"> 1: a través de otro recurso en la misma VPC 2: a través de una gateway de Internet o un punto de enlace de la VPC de gateway 3: a través de una gateway privada virtual 4: a través de una interconexión de VPC dentro de la región 5: a través de una interconexión de VPC entre regiones 6: a través de una gateway local 7 — A través de un punto de enlace de la VPC de gateway (solo instancias basadas en Nitro) 8 — A través de una gateway de Internet (solo instancias basadas en Nitro) <p>Tipo de datos de Parquet: INT_32</p>	5

Ejemplos de registros de log de flujo

A continuación se muestran ejemplos de registros de logs de flujo que capturan flujos de tráfico específicos.

Para obtener información sobre el formato de entradas de registro de flujo, consulte [Registros de log de flujo \(p. 200\)](#). Para obtener información sobre cómo crear registros de flujo, consulte [Trabajar con registros de flujo \(p. 222\)](#).

Contenido

- [Tráfico aceptado y rechazado \(p. 205\)](#)
- [Registros sin datos y omitidos \(p. 206\)](#)
- [Reglas de grupos de seguridad y ACL de red \(p. 206\)](#)
- [Tráfico IPv6 \(p. 207\)](#)
- [Secuencia de marca TCP \(p. 207\)](#)
- [Tráfico a través de una gateway NAT \(p. 208\)](#)
- [Tráfico a través de una transit gateway \(p. 208\)](#)
- [Nombre del servicio, ruta de tráfico y dirección del flujo \(p. 209\)](#)

Tráfico aceptado y rechazado

Los siguientes ejemplos son registros de logs de flujo predeterminados.

En este ejemplo, se ha permitido el tráfico SSH (puerto de destino 22, protocolo TCP) a la interfaz de red eni-1235b8ca123456789 en la cuenta 123456789010.

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 172.31.16.21 20641 22 6 20 4249
1418530010 1418530070 ACCEPT OK
```

En este ejemplo, se ha rechazado el tráfico RDP (puerto de destino 3389, protocolo TCP) a la interfaz de red eni-1235b8ca123456789 en la cuenta 123456789010.

```
2 123456789010 eni-1235b8ca123456789 172.31.9.69 172.31.9.12 49761 3389 6 20 4249
1418530010 1418530070 REJECT OK
```

Registros sin datos y omitidos

Los siguientes ejemplos son registros de logs de flujo predeterminados.

En este ejemplo, no se registraron datos durante el intervalo de agregación.

```
2 123456789010 eni-1235b8ca123456789 - - - - - 1431280876 1431280934 - NODATA
```

En este ejemplo, se omitieron los registros durante el intervalo de agregación. Los registros de flujo de la VPC omite registros cuando no puede capturar datos del registro de flujo durante un intervalo de integración porque supera la capacidad interna. Un único registro que se omite puede representar varios flujos que no se capturaron para la interfaz de red durante el intervalo de integración.

```
2 123456789010 eni-11111111aaaaaaaa - - - - - 1431280876 1431280934 - SKIPDATA
```

Reglas de grupos de seguridad y ACL de red

Si va a utilizar logs de flujo para diagnosticar reglas excesivamente restrictivas o permisivas de grupos de seguridad o ACL de red, tenga en cuenta el estado de estos recursos. Los grupos de seguridad son grupos con estado: esto significa que las respuestas al tráfico permitido también están permitidas, incluso si las reglas del grupo de seguridad no lo permiten. Por otro lado, las ACL de red son sin estado, y por lo tanto las respuestas al tráfico permitido están sujetas a las reglas de la ACL de red.

Por ejemplo, supongamos que utiliza el comando ping desde su equipo doméstico (la dirección IP es 203.0.113.12) hasta su instancia (la dirección IP privada de la interfaz de red es 172.31.16.139). Las reglas entrantes del grupo de seguridad permiten el tráfico ICMP, pero las reglas salientes no permiten el tráfico ICMP. Dado que los grupos de seguridad son grupos con estado, se permite el ping de respuesta de su instancia. Su ACL de red permite el tráfico ICMP entrante, pero no permite el tráfico ICMP saliente. Puesto que las ACL de red son sin estado, se descarta el ping de respuesta y no llegará a su equipo doméstico. En un log de flujo predeterminado, esto se muestra como dos registros de logs de flujo:

- Un registro de ACCEPT para el ping de origen que han permitido tanto la ACL de red como el grupo de seguridad, y que por tanto puede llegar a su instancia.
- Un registro de REJECT para el ping de respuesta que ha denegado la ACL de red.

```
2 123456789010 eni-1235b8ca123456789 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027
1432917142 ACCEPT OK
```

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094
1432917142 REJECT OK
```

Si su ACL de red permite el tráfico ICMP saliente, el log de flujo muestra dos registros ACCEPT (uno para el ping de origen y otro para el ping de respuesta). Si su grupo de seguridad deniega el tráfico ICMP entrante, el log de flujo mostrará un único recurso REJECT, ya que el tráfico no tiene permiso para llegar a su instancia.

Tráfico IPv6

A continuación se muestra un ejemplo de un registro de log de flujo predeterminado. En el ejemplo, se permitió el tráfico SSH (puerto 22) desde la dirección IPv6 2001:db8:1234:a100:8d6e:3477:df66:f105 a la interfaz de red eni-1235b8ca123456789 en la cuenta 123456789010.

```
2 123456789010 eni-1235b8ca123456789 2001:db8:1234:a100:8d6e:3477:df66:f105
2001:db8:1234:a102:3304:8879:34cf:4071 34892 22 6 54 8855 1477913708 1477913820 ACCEPT OK
```

Secuencia de marca TCP

A continuación se muestra un ejemplo de un log de flujo personalizado que captura los campos siguientes en el orden que se indica seguidamente.

```
version vpc-id subnet-id instance-id interface-id account-id type srcaddr dstaddr srcport
dstport pkt-srcaddr pkt-dstaddr protocol bytes packets start end action tcp-flags log-
status
```

El campo tcp-flags puede ayudarle a identificar la dirección del tráfico, por ejemplo, el servidor que inició la conexión. En los registros siguientes (empezando a las 7:47:55 PM y terminando a las 7:48:53 PM), un cliente inició dos conexiones a un servidor que se ejecuta en el puerto 5001. El servidor recibió dos marcas SYN (2) del cliente desde puertos de origen distintos en el cliente (43416 y 43418). Para cada SYN, se envió una marca SYN-ACK desde el servidor al cliente (18) en el puerto correspondiente.

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456 eni-1235b8ca123456789
123456789010 IPv4 52.213.180.42 10.0.0.62 43416 5001 52.213.180.42 10.0.0.62 6 568 8
1566848875 1566848933 ACCEPT 2 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456 eni-1235b8ca123456789
123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43416 10.0.0.62 52.213.180.42 6 376 7
1566848875 1566848933 ACCEPT 18 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456 eni-1235b8ca123456789
123456789010 IPv4 52.213.180.42 10.0.0.62 43418 5001 52.213.180.42 10.0.0.62 6 100701 70
1566848875 1566848933 ACCEPT 2 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456 eni-1235b8ca123456789
123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62 52.213.180.42 6 632 12
1566848875 1566848933 ACCEPT 18 OK
```

En el segundo intervalo de agregación, una de las conexiones que se estableció durante el flujo anterior ahora está cerrada. El cliente envió una marca FIN (1) al servidor para la conexión en el puerto 43418. El servidor envió una marca FIN al cliente en el puerto 43418.

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456 eni-1235b8ca123456789
123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62 52.213.180.42 6 63388 1219
1566848933 1566849113 ACCEPT 1 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456 eni-1235b8ca123456789
123456789010 IPv4 52.213.180.42 10.0.0.62 43418 5001 52.213.180.42 10.0.0.62 6 23294588
15774 1566848933 1566849113 ACCEPT 1 OK
```

En las conexiones breves (de unos cuantos segundos, por ejemplo) que se abren y cierran en un mismo intervalo de agregación, las marcas podrían establecerse en la misma línea del registro del flujo de tráfico que tiene lugar en la misma dirección. En el ejemplo siguiente, la conexión se establece y termina en el mismo intervalo de agregación. En la primera línea, el valor de la marca TCP es 3, que indica que se envió SYN y un mensaje FIN desde el cliente al servidor. En la segunda línea, el valor de la marca TCP es 19, que indica que se envió SYN-ACK y un mensaje FIN desde el servidor al cliente

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456 eni-1235b8ca123456789
123456789010 IPv4 52.213.180.42 10.0.0.62 43638 5001 52.213.180.42 10.0.0.62 6 1260 17
1566933133 1566933193 ACCEPT 3 OK
```

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456 eni-1235b8ca123456789
123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43638 10.0.0.62 52.213.180.42 6 967 14
1566933133 1566933193 ACCEPT 19 OK
```

Tráfico a través de una gateway NAT

En este ejemplo, una instancia en una subred privada accede a Internet a través de una gateway NAT que está en una subred pública.

El siguiente log de flujo personalizado para la interfaz de red de gateway de NAT captura los campos siguientes en el orden siguiente.

```
instance-id interface-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

El log de flujo muestra el flujo de tráfico desde la dirección IP de la instancia (10.0.1.5) a través de la interfaz de red de la gateway de NAT a un host en Internet (203.0.113.5). La interfaz de red de gateway de NAT es una interfaz de red administrada por el solicitante, por tanto, el registro de logs de flujo muestra un símbolo «-» para el campo instance-id. La línea siguiente muestra tráfico desde la instancia de origen a la interfaz de red de la gateway de NAT. Los valores para los campos dstaddr y pkt-dstaddr son distintos. El campo dstaddr muestra la dirección IP privada de la interfaz de red de la gateway de NAT y el campo pkt-dstaddr muestra la dirección IP de destino final del host en Internet.

```
- eni-1235b8ca123456789 10.0.1.5 10.0.0.220 10.0.1.5 203.0.113.5
```

Las dos líneas siguientes muestra el tráfico desde la interfaz red de gateway de NAT al host de destino en Internet y el tráfico de respuesta desde el host a la interfaz de red de la gateway de NAT.

```
- eni-1235b8ca123456789 10.0.0.220 203.0.113.5 10.0.0.220 203.0.113.5
- eni-1235b8ca123456789 203.0.113.5 10.0.0.220 203.0.113.5 10.0.0.220
```

La línea siguiente muestra tráfico de respuesta desde la interfaz de red de la gateway de NAT a la instancia de origen. Los valores para los campos srcaddr y pkt-srcaddr son distintos. El campo srcaddr muestra la dirección IP privada de la interfaz de red de la gateway de NAT y el campo pkt-srcaddr muestra la dirección IP del host en Internet.

```
- eni-1235b8ca123456789 10.0.0.220 10.0.1.5 203.0.113.5 10.0.1.5
```

Puede crear otro log de flujo personalizado utilizando el mismo conjunto de campos que con anterioridad. Puede crear el log de flujo para la interfaz de red para la instancia en la subred privada. En este caso, el campo instance-id devuelve el ID de la instancia que está asociado a la interfaz de red y no hay ninguna diferencia entre los campos dstaddr y pkt-dstaddr y los campos srcaddr y pkt-srcaddr. A diferencia de la interfaz de red para la gateway de NAT, esta interfaz de red no es una interfaz de red intermedia para el tráfico.

```
i-01234567890123456 eni-1111aaaa2222bbbb3 10.0.1.5 203.0.113.5 10.0.1.5 203.0.113.5
#Traffic from the source instance to host on the internet
i-01234567890123456 eni-1111aaaa2222bbbb3 203.0.113.5 10.0.1.5 203.0.113.5 10.0.1.5
#Response traffic from host on the internet to the source instance
```

Tráfico a través de una transit gateway

En este ejemplo, un cliente en VPC A se conecta a un servidor web en VPC B a través de una transit gateway. El cliente y el servidor están en zonas de disponibilidad distintas. Por tanto, el tráfico

llega al servidor en la VPC B utilizando eni-1111111111111111 y sale de la VPC B utilizando eni-2222222222222222.

Puede crear un log de flujo personalizado para VPC B con el formato siguiente.

```
version interface-id account-id vpc-id subnet-id instance-id srcaddr dstaddr srcport
dstport protocol tcp-flags type pkt-srcaddr pkt-dstaddr action log-status
```

Las líneas siguientes de los registros de logs de flujo muestran el flujo de tráfico en la interfaz de red para el servidor web. La primera línea es el tráfico de solicitudes del cliente y la última línea es el tráfico de respuesta del servidor web.

```
3 eni-3333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbbb
i-01234567890123456 10.20.33.164 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164 10.40.2.236
ACCEPT OK
...
3 eni-3333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbbb
i-01234567890123456 10.40.2.236 10.20.33.164 80 39812 6 19 IPv4 10.40.2.236 10.20.33.164
ACCEPT OK
```

La línea siguiente es el tráfico de solicitudes en eni-1111111111111111, una interfaz de red administrada el por solicitante para la transit gateway en la subred subnet-11111111aaaaaaaa. El registro de logs de flujo por tanto muestra un símbolo «-» para el campo instance-id. El campo srcaddr muestra la dirección IP privada de la interfaz de red de transit gateway y el campo pkt-srcaddr muestra la dirección IP de origen del cliente en VPC A.

```
3 eni-1111111111111111 123456789010 vpc-abcdefab012345678 subnet-11111111aaaaaaaa -
10.40.1.175 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164 10.40.2.236 ACCEPT OK
```

La línea siguiente es el tráfico de respuesta en eni-2222222222222222, una interfaz de red administrada por el solicitante para la transit gateway en la subred subnet-22222222bbbbbbbbbb. El campo dstaddr muestra la dirección IP privada de la interfaz de red de transit gateway y el campo pkt-dstaddr muestra la dirección IP del cliente en VPC A.

```
3 eni-2222222222222222 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbbb -
10.40.2.236 10.40.2.31 80 39812 6 19 IPv4 10.40.2.236 10.20.33.164 ACCEPT OK
```

Nombre del servicio, ruta de tráfico y dirección del flujo

A continuación se presenta un ejemplo de los campos para un registro de log de flujo personalizado.

```
version srcaddr dstaddr srcport dstport protocol start end type packets bytes account-id
vpc-id subnet-id instance-id interface-id region az-id sublocation-type sublocation-id
action tcp-flags pkt-srcaddr pkt-dstaddr pkt-src-aws-service pkt-dst-aws-service traffic-
path flow-direction log-status
```

En el ejemplo siguiente, la versión es 5 porque los registros incluyen campos de la versión 5. Una instancia EC2 llama al servicio Amazon S3. Los logs de flujo se capturan en la interfaz de red de la instancia. El primer registro tiene una dirección de flujo de ingress y el segundo registro tiene una dirección de flujo de egress. Para el registro egress, traffic-path es 8, lo que indica que el tráfico pasa a través de un gateway de Internet. El campo traffic-path no es compatible con el tráfico de ingress. Cuando pkt-srcaddr o pkt-dstaddr es una dirección IP pública, se muestra el nombre del servicio.

```
5 52.95.128.179 10.0.0.71 80 34210 6 1616729292 1616729349 IPv4 14 15044 123456789012 vpc-
abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b eni-1235b8ca123456789 ap-
southeast-2 apse2-az3 - - ACCEPT 19 52.95.128.179 10.0.0.71 S3 - - ingress OK
```

```
5 10.0.0.71 52.95.128.179 34210 80 6 1616729292 1616729349 IPv4 7 471 123456789012 vpc-
abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b eni-1235b8ca123456789 ap-
southeast-2 apse2-az3 - - ACCEPT 3 10.0.0.71 52.95.128.179 - S3 8 egress OK
```

Limitaciones de los logs de flujo

Para utilizar los logs de flujo, debe conocer las siguientes limitaciones:

- No se pueden habilitar logs de flujo para interfaces de red que se encuentren en la plataforma EC2-Classic. Esto incluye las instancias de EC2-Classic vinculadas a una VPC a través de ClassicLink.
- No se pueden habilitar los logs de flujo para VPC interconectadas con su VPC a menos que la VPC del mismo nivel se encuentre en su cuenta.
- Después de haber creado un registro de flujo, no puede cambiar su configuración ni el formato de registro de los registros de flujo. Por ejemplo, no puede asociar un rol de IAM diferente con el registro de flujo ni agregar o quitar campos en la entrada de registro de flujo. En su lugar, puede eliminar el log de flujo y crear uno nuevo con la configuración necesaria.
- Si su interfaz de red tiene varias direcciones IPv4 y el tráfico se envía a una dirección IPv4 privada secundaria, el log de flujo mostrará la dirección IPv4 privada principal en el campo `dstaddr`. Para capturar la dirección IP de destino original, cree un log de flujo con el campo `pkt-dstaddr`.
- Si el tráfico se envía a una interfaz de red y el destino no es ninguna de las direcciones IP de la interfaz de red, el log de flujo muestra la dirección IPv4 privada principal en el campo `dstaddr`. Para capturar la dirección IP de destino original, cree un log de flujo con el campo `pkt-dstaddr`.
- Si el tráfico se envía a una interfaz de red y el origen no es ninguna de las direcciones IP de la interfaz de red, el log de flujo muestra la dirección IPv4 privada principal en el campo `srcaddr`. Para capturar la dirección IP de origen original, cree un log de flujo con el campo `pkt-srcaddr`.
- Si el tráfico se envía a una interfaz de red o desde una interfaz de red, los campos `srcaddr` y `dstaddr` del registro de flujo muestran siempre la dirección IPv4 privada principal, con independencia del origen o destino del paquete. Para capturar el origen o destino del paquete, cree un log de flujo con los campos `pkt-srcaddr` y `pkt-dstaddr`.
- Cuando la interfaz de red está asociada a una [instancia basada en Nitro](#), el intervalo de agregación siempre es igual o menor a 1 minuto, independientemente del intervalo máximo de agregación especificado.

Los logs de flujo no capturan todo el tráfico IP. Los siguientes tipos de tráfico no se registran:

- Tráfico generado por instancias al contactar con el servidor DNS de Amazon. Si utiliza su propio servidor DNS, sí se registrará el tráfico a ese servidor DNS.
- Tráfico generado por una instancia de Windows para la activación de licencia de Windows para Amazon.
- Tráfico entrante y saliente de 169.254.169.254 para metadatos de instancias.
- Tráfico entrante y saliente de 169.254.169.123 para el servicio Amazon Time Sync.
- Tráfico DHCP.
- Tráfico reflejado.
- Tráfico a la dirección IP reservada para el router VPC predeterminado.
- El tráfico entre una interfaz de red de punto de enlace y una interfaz de red de Network Load Balancer.

Precios de registros de flujo

Los costos por incorporación y archivo de datos para los registros a la venta se aplican cuando se publican registros de flujo en CloudWatch Logs o en Amazon S3. Para obtener más información y ejemplos, consulte [Precios de Amazon CloudWatch](#).

Para realizar un seguimiento de los cargos de publicación de los registros de flujo en los buckets de Amazon S3, puede aplicar etiquetas de asignación de costos a las suscripciones de registros de flujo. Para realizar un seguimiento de los cargos de publicación de los registros de flujo en CloudWatch Logs, puede aplicar etiquetas de asignación de costos al grupo de registros de CloudWatch de destino. A partir de entonces, el informe de asignación de costos de AWS incluirá el uso y los costos agregados por estas etiquetas. Puede aplicar etiquetas que representen categorías de negocio (por ejemplo, centros de costos, nombres de aplicación o propietarios) para organizar los costos. Para obtener más información, consulte [Uso de etiquetas de asignación de costos](#) en la Guía del usuario de AWS Billing and Cost Management.

Publicar registros de flujo en CloudWatch Logs

Los registros de flujo pueden publicar datos de registro de flujo directamente en Amazon CloudWatch.

Al publicar en CloudWatch Logs, los datos de registro de flujo se publican en un grupo de registros y cada interfaz de red tiene una secuencia de registro única en el grupo de registros. Los flujos de logs contienen registros de logs de flujo. Puede crear varios logs de flujo que publiquen datos en el mismo grupo de logs. Si la misma interfaz de red está presente en uno o varios logs de flujo en el mismo grupo de logs, tendrá un flujo de logs combinado. Si ha especificado que un log de flujo debe capturar el tráfico rechazado y otro log de flujo debe capturar el tráfico aceptado, el flujo de logs combinado capturará todo el tráfico.

Se aplican costos por incorporación y archivo de datos para los registros a la venta cuando se publican registros de flujo en CloudWatch Logs. Para obtener más información, consulte los [precios de Amazon CloudWatch](#).

En CloudWatch Logs, el campo timestamp (marca temporal) corresponde a la hora de inicio capturada en la entrada de registro de flujo. El campo ingestionTime indica la fecha y hora en que CloudWatch Logs recibió la entrada de registro de flujo. Esta marca de tiempo es posterior a la hora de finalización capturada en el registro de flujo.

Para obtener más información acerca de CloudWatch Logs, consulte [Registros enviados a CloudWatch Logs](#) en la Guía del usuario de Amazon CloudWatch Logs.

Contenido

- [Roles de IAM para publicar registros de flujo en CloudWatch Logs \(p. 211\)](#)
- [Permisos para que los usuarios de IAM pasen un rol \(p. 213\)](#)
- [Crear un registro de flujo que se publique en CloudWatch Logs \(p. 213\)](#)
- [Procesar entradas de registro de flujo en CloudWatch Logs \(p. 215\)](#)

Roles de IAM para publicar registros de flujo en CloudWatch Logs

El rol de IAM asociado con el registro de flujo debe tener permisos suficientes para publicar registros de flujo en el grupo de registros especificado en CloudWatch Logs. El rol de IAM debe pertenecer a la cuenta de AWS.

La política de IAM asociada al rol de IAM debe incluir al menos los siguientes permisos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
```

```
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
    ],
    "Resource": "*"
  }
]
```

Asegúrese también de que el rol tiene una relación de confianza que permite al servicio de logs de flujo asumir ese rol.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Le recomendamos que utilice las claves de condición `aws:SourceAccount` y `aws:SourceArn` para protegerse contra el [problema del suplente confuso](#). Por ejemplo, podría agregar el siguiente bloque de condición a la política de confianza anterior. La cuenta fuente es la propietaria del registro de flujo y el ARN fuente es el ARN del registro de flujo. Si no conoce el ID del registro de flujo, puede reemplazar esa parte del ARN por un comodín (*) y, a continuación, actualizar la política después de crear el registro de flujo.

```
"Condition": {
  "StringEquals": {
    "aws:SourceAccount": "account_id"
  },
  "ArnLike": {
    "aws:SourceArn": "arn:aws:ec2:region:account_id:vpc-flow-log/flow-log-id"
  }
}
```

Creación o actualización de un rol de IAM para registros de flujo

Puede actualizar una función existente o utilizar el procedimiento siguiente para crear una nueva función y utilizarla con los logs de flujo.

Para crear un rol de IAM para registros de flujo

1. Abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. En el panel de navegación, elija Roles, Create role.
3. En Select type of trusted entity (Seleccionar tipo de entidad de confianza), elija AWS service (Servicio de AWS). En Use case (Caso de uso), elija EC2. Elija Next: Permissions.
4. En la página Attach permissions policies (Asociar políticas de permisos), elija Next: Review (Siguiente: Revisar). Elija Next: Review.
5. Ingrese un nombre para el rol y, opcionalmente, especifique una descripción. Elija Create role (Crear rol).
6. Seleccione el nombre de su función. En Permissions (Permisos), elija Add inline policy (Añadir política insertada), JSON.

7. Copie la primera política de [Roles de IAM para publicar registros de flujo en CloudWatch Logs](#) (p. 211) y péguela en la ventana. Elija Review policy (Revisar política).
8. Escriba un nombre para la política y elija Create policy (Crear política).
9. Seleccione el nombre de su función. En Trust relationships (Relaciones de confianza), seleccione Edit trust relationship (Editar relación de confianza). En el documento de la política existente, cambie el servicio de `ec2.amazonaws.com` a `vpc-flow-logs.amazonaws.com`. Elija Update Trust Policy.
10. En la página Summary (Resumen), tome nota del ARN de la función. Necesita este ARN para crear su propio log de flujo.

Permisos para que los usuarios de IAM pasen un rol

Los usuarios también deben tener permisos para utilizar la acción `iam:PassRole` para el rol de IAM que está asociado con registro de flujo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iam:PassRole"],
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    }
  ]
}
```

Crear un registro de flujo que se publique en CloudWatch Logs

Puede crear registros de flujo para sus VPC, subredes o interfaces de red. Si realiza estos pasos como usuario de IAM, asegúrese de que tiene permisos para usar la acción `iam:PassRole`. Para obtener más información, consulte [Permisos para que los usuarios de IAM pasen un rol](#) (p. 213).

Requisito previo

Cree el grupo de registros de destino. Abra la [página de grupos de registro](#) en la consola de CloudWatch y elija Create log group (Crear grupo de registro). Escriba un nombre para el grupo de registros y elija Create (Crear).

Para crear un log de flujo para una interfaz de red utilizando la consola

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione las casillas de verificación de una o más interfaces de red y elija Actions (Acciones), Create flow log (Crear registro de flujo).
4. Para Filter (Filtro), especifique el tipo de tráfico que desea registrar. Elija All (Todos) para registrar el tráfico aceptado y rechazado, Reject (Rechazar) a fin de registrar sólo el tráfico rechazado o Accept (Aceptar) con el objetivo de registrar sólo el tráfico aceptado.
5. En Maximum aggregation interval (Intervalo máximo de agregación), elija el período de tiempo máximo durante el que se va a capturar el flujo y se va a agregar a un registro de flujo.
6. En Destination (Destino), elija Send to CloudWatch Logs (Enviar a CloudWatch Logs).
7. Para Destination log group (Grupo de registros de destino), elija el nombre del grupo de registros de destino que ha creado.
8. En IAM role (Rol de IAM), especifique el nombre del rol que tiene permisos para publicar registros en CloudWatch Logs.

9. Para Log record format (Formato de registro de registro), seleccione el formato para el registro de flujo.
 - Para utilizar el formato predeterminado, elija AWS default format (Formato predeterminado de AWS).
 - Para utilizar un formato personalizado, elija Custom format (Formato personalizado) y, a continuación, seleccione campos de Log format (Formato de registro).
10. (Opcional) Elija Add new tag (Agregar etiqueta nueva) para aplicar etiquetas al registro de flujo.
11. Elija Create flow log (Crear registro de flujo).

Para crear un log de flujo para una VPC o una subred utilizando la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs (Sus VPC) o Subnets (Subredes).
3. Seleccione la casilla de verificación para una o más VPC o subredes y, a continuación, elija Actions (Acciones), Create flow log (Crear registro de flujo).
4. Para Filter (Filtro), especifique el tipo de tráfico que desea registrar. Elija All (Todos) para registrar el tráfico aceptado y rechazado, Reject (Rechazar) a fin de registrar sólo el tráfico rechazado o Accept (Aceptar) con el objetivo de registrar sólo el tráfico aceptado.
5. En Maximum aggregation interval (Intervalo máximo de agregación), elija el período de tiempo máximo durante el que se va a capturar el flujo y se va a agregar a un registro de flujo.
6. En Destination (Destino), elija Send to CloudWatch Logs (Enviar a CloudWatch Logs).
7. Para Destination log group (Grupo de registros de destino), elija el nombre del grupo de registros de destino que ha creado.
8. En IAM role (Rol de IAM), especifique el nombre del rol que tiene permisos para publicar registros en CloudWatch Logs.
9. Para Log record format (Formato de registro de registro), seleccione el formato para el registro de flujo.
 - Para utilizar el formato predeterminado, elija AWS default format (Formato predeterminado de AWS).
 - Para utilizar un formato personalizado, elija Custom format (Formato personalizado) y, a continuación, seleccione campos de Log format (Formato de registro).
10. (Opcional) Elija Add new tag (Agregar etiqueta nueva) para aplicar etiquetas al registro de flujo.
11. Elija Create flow log (Crear registro de flujo).

Para crear un registro de flujo mediante la línea de comandos

Utilice uno de los siguientes comandos.

- [create-flow-logs](#) (AWS CLI)
- [New-EC2FlowLogs](#) (AWS Tools for Windows PowerShell)
- [CreateFlowLogs](#) (API de consulta de Amazon EC2)

El siguiente ejemplo de la AWS CLI crea un log de flujo que captura todo el tráfico aceptado para la subred subnet-1a2b3c4d. Los registros de flujo se envían a un grupo de registro en CloudWatch Logs denominado my-flow-logs, en la cuenta 123456789101, mediante el rol de IAM publishFlowLogs.

```
aws ec2 create-flow-logs --resource-type Subnet --resource-ids subnet-1a2b3c4d --
traffic-type ACCEPT --log-group-name my-flow-logs --deliver-logs-permission-arn
arn:aws:iam::123456789101:role/publishFlowLogs
```

Procesar entradas de registro de flujo en CloudWatch Logs

Puede trabajar con las entradas de registro de flujo al igual que con los demás eventos de registro recopilados por CloudWatch Logs. Para obtener más información acerca de los datos de registro y filtros de métricas de monitoreo, consulte [Búsqueda y filtrado de datos de registros](#) en la Guía del usuario de Amazon CloudWatch.

Ejemplo: crear un filtro de métrica y una alarma de CloudWatch para un registro de flujo

En este ejemplo, tiene un log de flujo para `eni-1a2b3c4d`. Desea crear una alarma que le avise si ha habido 10 o más intentos rechazados para conectar con su instancia a través del puerto TCP 22 (SSH) en un periodo de 1 hora. En primer lugar, debe crear un filtro de métrica que coincida con el patrón de tráfico para el que va a crear la alarma. A continuación, puede crear una alarma para el filtro de métrica.

Para crear un filtro de métrico para el tráfico SSH rechazado y una alarma para el filtro

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Logs (Registros), Log groups (Grupos de registros).
3. Seleccione la casilla de verificación para el grupo de registro y, a continuación, elija Actions (Acciones), Create metric filter (Crear filtro de métricas).
4. En Filter Pattern (Patrón de filtro), escriba lo siguiente.

```
[version, account, eni, source, destination, srcport, destport="22", protocol="6", packets, bytes, windowstart, windowend, action="REJECT", flowlogstatus]
```

5. En Select Log Data to Test (Seleccionar datos de registro para prueba), seleccione el flujo de registro para la interfaz de red. (Opcional) Para ver las líneas de los datos de registro que concuerdan con el patrón de filtro, elija Test Pattern (Probar patrón). Cuando esté preparado para continuar, seleccione Next (Siguiente).
6. Ingrese un nombre de filtro, un espacio de nombres de métrica y un nombre de métrica. Establezca el valor de la métrica en 1. Cuando haya terminado, elija Next (Siguiente) y, luego, elija Create metric filter (Crear filtro de métricas).
7. En el panel de navegación, elija Alarms (Alarmas), Create Alarm (Crear alarma).
8. Elija Create alarm (Crear alarma).
9. Elija el espacio de nombres para el filtro de métricas que ha creado.

Puede que la nueva métrica tarde unos minutos en mostrarse en la consola.

10. Seleccione el nombre de métrica que ha creado y elija Next (Siguiente).
11. Configure la alarma como se indica a continuación y, luego, elija Next (Siguiente):
 - En Statistic (Estadística), elija Sum (Suma). Asegura que esté capturando el número total de puntos de datos para el período especificado.
 - En Period (Período), seleccione 1 Hour (1 hora).
 - En Whenever (Siempre), elija Greater/Equal (Mayor o igual) e ingrese 10 en el umbral.
 - En Additional configuration (Configuración adicional), Datapoints to alarm (Puntos de datos para alarma), deje el valor predeterminado 1.
12. En Notification (Notificación), seleccione un tema de SNS existente o elija Create new topic (Crear tema nuevo) para crear uno nuevo. Elija Next (Siguiente).
13. Ingrese un nombre y una descripción para la alarma y, a continuación, elija Next (Siguiente).
14. Cuando haya terminado de configurar la alarma, elija Create alarm (Crear alarma).

Publicar registros de flujo en Amazon S3

Los registros de flujo pueden publicar datos de registros de flujo en Amazon S3.

Al publicar en Amazon S3, los datos de registro de flujo se publican en un bucket de Amazon S3 existente que especifique. Los registros de logs de flujo de todas las interfaces de red monitoreadas se publican en una serie de objetos de archivos log que se almacenan en el bucket. Si el log de flujo captura datos de una VPC, se publican los registros de logs de flujo de todas las interfaces de red de la VPC seleccionada.

Se aplican costos por incorporación y archivo de datos para los registros a la venta cuando se publican registros de flujo en Amazon S3. Para obtener más información, consulte los [precios de Amazon CloudWatch](#).

Para crear un bucket de Amazon S3 a fin de utilizarlo con registros de flujo, consulte [Create a bucket](#) (Crear un bucket) en la Guía de introducción de Amazon Simple Storage Service.

Para obtener más información acerca del registro de varias cuentas, consulte [Registro central](#) en la Biblioteca de soluciones de AWS.

Para obtener más información acerca de CloudWatch Logs, consulte [Registros enviados a Simple Storage Service \(Amazon S3\)](#) en la Guía del usuario de Amazon CloudWatch Logs.

Contenido

- [Archivos log de flujo \(p. 216\)](#)
- [Política de IAM para entidades principales de IAM que publican registros de flujo en Amazon S3 \(p. 218\)](#)
- [Permisos del bucket de Amazon S3 para registros de flujo \(p. 218\)](#)
- [Política de clave requerida para el uso con SSE-KMS \(p. 219\)](#)
- [Permisos de archivos de registro de Amazon S3 \(p. 220\)](#)
- [Crear un registro de flujo que se publique en Amazon S3 \(p. 220\)](#)
- [Procesar entradas de registro de flujo en Amazon S3 \(p. 222\)](#)

Archivos log de flujo

VPC Flow Logs recopila colecciones de datos de registros de flujo, las consolidan en archivos de registro y, a continuación, publican los archivos de registro en el bucket de Amazon S3 en intervalos de cinco minutos. Cada archivo log contiene registros de logs de flujo del tráfico IP registrado en los cinco minutos anteriores.

El tamaño de archivo máximo de un archivo log es de 75 MB. Si el archivo log alcanza el límite de tamaño de archivo en el periodo de cinco minutos, el log de flujo deja de añadirle registros de logs de flujo. A continuación, publica el registro de flujo en el bucket de Amazon S3 y crea un nuevo archivo de registro.

En Amazon S3, el campo Last modified (Última modificación) del archivo de registro de flujo indica la fecha y la hora en que el archivo se cargó en el bucket de Amazon S3. Este valor es posterior a la marca temporal del nombre de archivo y difiere en la cantidad de tiempo invertido en cargar el archivo en el bucket de Amazon S3.

Formato de archivo de registro

Puede especificar uno de los siguientes formatos para los archivos de registro. Cada archivo se comprime en un único archivo Gzip.

- **Texto:** Texto sin formato. Este es el formato predeterminado.
- **Parquet:** Apache Parquet es un formato de datos columnar. Las consultas sobre los datos en formato Parquet son de 10 a 100 veces más rápidas en comparación con las consultas de datos en texto sin

formato. Los datos en formato Parquet con compresión Gzip ocupan un 20 por ciento menos de espacio de almacenamiento que el texto sin formato con compresión Gzip.

Opciones de archivo de registro

Puede especificar las siguientes opciones:

- Prefijos de S3 compatibles con Hive: Habilite los prefijos compatibles con Hive en lugar de importar las particiones a las herramientas compatibles con Hive. Antes de ejecutar las consultas, utilice el comando `MSCK REPAIR TABLE`.
- Particiones por horas: Si tiene un gran volumen de registros y, por lo general, orienta las consultas a una hora en específico, puede obtener resultados más rápidos y ahorrar en costos de consulta si particiona los registros por hora.

Estructura del bucket de S3 del archivo de registro

Los archivos de registro se guardan en el bucket de Amazon S3 especificado con una estructura de carpetas basada en el ID del registro de flujo, la Región, la fecha en que se crearon y en las opciones de destino.

De forma predeterminada, los archivos se entregan en la siguiente ubicación.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/
```

Si habilita los prefijos de S3 compatibles con Hive, los archivos se entregan en la siguiente ubicación.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/service=vpcflowlogs/aws-region=region/year=year/month=month/day=day/
```

Si habilita particiones por hora, los archivos se entregan en la siguiente ubicación.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/hour/
```

Si habilita particiones compatibles con Hive y particiona el registro de flujo por hora, los archivos se entregan en la siguiente ubicación.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/service=vpcflowlogs/aws-region=region/year=year/month=month/day=day/hour=hour/
```

Nombre de archivo de registro

El nombre de archivo de un archivo de registro se basa en el ID del registro de flujo, la Región y en la fecha y hora de creación. Los nombres de archivo utilizan el formato siguiente.

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

A continuación, se muestra un ejemplo de un archivo de registros para un registro de flujo que la cuenta 123456789012 de AWS ha creado para un recurso en la Región us-east-1, el June 20, 2018 a las 16:20 UTC. El archivo contiene las colecciones de datos del registro de flujo con una hora de finalización entre las 16:20:00 y las 16:24:59.

```
123456789012_vpcflowlogs_us-east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

Política de IAM para entidades principales de IAM que publican registros de flujo en Amazon S3

Una entidad principal de IAM en la cuenta, como un usuario de IAM, debe tener permisos suficientes para publicar registros de flujo en el bucket de Amazon S3. Esto incluye permisos para trabajar con acciones de logs: específicas para crear y publicar los registros de flujo. La política de IAM debe incluir los permisos siguientes.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs>DeleteLogDelivery"
      ],
      "Resource": "*"
    }
  ]
}
```

Permisos del bucket de Amazon S3 para registros de flujo

De forma predeterminada, los buckets de Amazon S3 y los objetos que contienen son privados. Solo el propietario del bucket puede tener acceso al bucket y a los objetos almacenados en él. Sin embargo, el propietario del bucket puede conceder acceso a otros recursos y usuarios escribiendo una política de acceso.

Si el usuario que crea el registro de flujo es el propietario del bucket y tiene permisos `PutBucketPolicy` y `GetBucketPolicy` para el bucket, adjuntamos de forma automática la siguiente política al bucket. Esta política sobrescribe cualquier política existente asociada al bucket.

De otra manera, el propietario del bucket debe agregar esta política al bucket, al especificar el ID de cuenta de AWS del creador del registro de flujo o fallará la creación del registro de flujo. Para obtener más información, consulte [Uso de políticas de bucket](#) en la Guía del usuario de Amazon Simple Storage Service.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {"Service": "delivery.logs.amazonaws.com"},
      "Action": "s3:PutObject",
      "Resource": "my-s3-arn",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": account_id
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:logs:region:account_id:*"
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryCheck",
```



```
{
  "Effect": "Allow",
  "Principal": { "Service": "delivery.logs.amazonaws.com" },
  "Action": [ "s3:GetBucketAcl", "s3:ListBucket" ],
  "Resource": "arn:aws:s3:::bucket_name",
  "Condition": {
    "StringEquals": {
      "aws:SourceAccount": account_id
    },
    "ArnLike": {
      "aws:SourceArn": "arn:aws:logs:region:account_id:*"
    }
  }
}
```

El ARN que especifique para *my-s3-arn* depende de si utiliza prefijos de S3 compatibles con HIVE.

- Prefijos predeterminados

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*
```

- Prefijos de S3 compatibles con HIVE

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/aws-account-id=account_id/*
```

Recomendamos que conceda estos permisos a la entidad principal del servicio de entrega de registros en lugar de a los ARN individuales de la cuenta de AWS. También es una práctica recomendada utilizar las claves de condición `aws:SourceAccount` y `aws:SourceArn` para protegerse del [problema del suplente confuso](#). La cuenta fuente es la propietaria del registro de flujo y el ARN fuente es el ARN comodín (*) del servicio de registros.

Política de clave requerida para el uso con SSE-KMS

Para proteger los datos del bucket de Amazon S3, habilite el cifrado del lado del servidor con las claves administradas de Amazon S3 (SSE-S3) o con el cifrado del lado del servidor con claves de KMS (SSE-KMS). Para obtener más información, consulte [Protección de datos mediante cifrado del lado del servidor](#) en la Guía del usuario de Amazon S3.

Con SSE-KMS, puede utilizar una clave administrada por AWS o una clave administrada por el cliente. Con una clave administrada por AWS, no puede utilizar la entrega en cuentas cruzadas. Los registros de flujo se entregan desde la cuenta de entrega de registros, por lo que debe conceder acceso para la entrega entre cuentas. Para conceder acceso de cuentas cruzadas al bucket de S3, utilice una clave administrada por el cliente y especifique el nombre de recurso de Amazon (ARN) de la clave administrada por el cliente cuando habilite el cifrado del bucket. Para obtener más información, consulte [Especificación del cifrado del lado del servidor con AWS KMS](#) en la Guía del usuario de Amazon S3.

Cuando utilice SSE-KMS con una clave administrado por el cliente, debe agregar lo siguiente a la política de clave destinada a su clave (no la política de bucket para el bucket de S3), de modo que VPC Flow Logs pueda realizar registros en el bucket de S3.

```
{
  "Sid": "Allow VPC Flow Logs to use the key",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "delivery.logs.amazonaws.com"
    ]
  }
}
```

```
    },  
    "Action": [  
        "kms:Encrypt",  
        "kms:Decrypt",  
        "kms:ReEncrypt*",  
        "kms:GenerateDataKey*",  
        "kms:DescribeKey"  
    ],  
    "Resource": "*" }  
}
```

Permisos de archivos de registro de Amazon S3

Además de las políticas de bucket necesarias, Amazon S3 utiliza listas de control de acceso (ACL) para administrar el acceso a los archivos de registro creados por un registro de flujo. De forma predeterminada, el propietario del bucket tiene los permisos `FULL_CONTROL` en cada archivo log. El propietario de la entrega de logs, si es diferente del propietario del bucket, no tiene permisos. La cuenta de entrega de logs tiene los permisos `READ` y `WRITE`. Para obtener más información, consulte [Access Control List \(ACL\) Overview](#) (Información general de la Lista de control de acceso [ACL]) en la Guía del usuario de Amazon Simple Storage Service.

Crear un registro de flujo que se publique en Amazon S3

Después de haber creado y configurado el bucket de Amazon S3, puede crear registros de flujo para las interfaces de red, las subredes y las VPC.

Para crear un log de flujo para una interfaz de red utilizando la consola

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione las casillas de verificación para una o más interfaces de red.
4. Seleccione Actions (Acciones) y, a continuación, Create flow log (Crear registro de flujo).
5. Establezca la configuración del registro de flujo. Para obtener más información, consulte [To configure flow log settings \(p. 221\)](#) (Configuración de los ajustes del registro de flujo).

Para crear un registro de flujo para una subred mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets.
3. Seleccione las casillas de verificación de una o más subredes.
4. Elija Actions (Acciones) y, a continuación, Create flow log (Crear registro de flujo).
5. Establezca la configuración del registro de flujo. Para obtener más información, consulte [To configure flow log settings \(p. 221\)](#) (Configuración del registro de flujo).

Para crear un registro de flujo para una VPC mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs (Sus VPC).
3. Seleccione las casillas de verificación de una o más VPC.
4. Seleccione Actions (Acciones) y, a continuación, Create flow log (Crear registro de flujo).
5. Establezca la configuración del registro de flujo. Para obtener más información, consulte [To configure flow log settings \(p. 221\)](#) (Configuración del registro de flujo).

Configuración del registro de flujo mediante la consola

1. En **Filter (Filtro)**, especifique el tipo de datos de tráfico IP que desea registrar.
 - **Accepted (Aceptado)**: Solo tráfico aceptado.
 - **Rejected (Rechazado)**: Solo tráfico rechazado.
 - **All (Todo)**: Tráfico aceptado y rechazado
2. En **Maximum aggregation interval (Intervalo máximo de agregación)**, elija el período de tiempo máximo durante el que se va a capturar el flujo y se va a agregar a un registro de flujo.
3. En **Destination (Destino)**, elija **Send to an Amazon S3 bucket (Enviar a un bucket de S3)**.
4. En **S3 bucket ARN (ARN de bucket de S3)**, especifique el nombre de recurso de Amazon (ARN) de un bucket de Amazon S3 existente. Si lo desea, puede incluir una subcarpeta. Por ejemplo, para especificar una subcarpeta llamada `my-logs` de un bucket denominado `my-bucket`, utilice el siguiente ARN:

```
arn:aws:s3::my-bucket/my-logs/
```

El bucket no puede utilizar `AWLogs` como nombre de subcarpeta, ya que se trata de un término reservado.

Si posee el bucket, crearemos automáticamente una política de recursos y la asociaremos al bucket. Para obtener más información, consulte [. Permisos del bucket de Amazon S3 para registros de flujo \(p. 218\)](#).

5. Para **Log record format (Formato de registro)**, seleccione el formato para el registro de flujo.
 - Para utilizar el formato de registro predeterminado del registro de flujo, elija **AWS default format (Formato predeterminado de AWS)**.
 - Para crear un formato personalizado, seleccione **Formato personalizado**. En **Log format (Formato de log)**, elija los campos que desea incluir en el registro de logs de flujo.
6. Para **Log file format (Formato de archivo de registro)**, especifique el formato del archivo de registro.
 - **Text (Texto)**: Texto sin formato. Este es el formato predeterminado.
 - **Parquet**: Apache Parquet es un formato de datos columnar. Las consultas sobre los datos en formato Parquet son de 10 a 100 veces más rápidas en comparación con las consultas de datos en texto sin formato. Los datos en formato Parquet con compresión Gzip ocupan un 20 por ciento menos de espacio de almacenamiento que el texto sin formato con compresión Gzip.
7. (Opcional) Para utilizar prefijos de S3 compatibles con Hive, elija **Hive-compatible S3 prefix (Prefijo de S3 compatible con Hive)** y, a continuación, **Enable (Habilitar)**.
8. (Opcional) Para particionar los registros de flujo por hora, elija **Every 1 hour (60 mins) (Cada 1 hora [60 minutos])**.
9. (Opcional) Para agregar una etiqueta al registro de flujo, elija **Add new tag (Añadir nueva etiqueta)** y especifique la clave y el valor de etiqueta.
10. Elija **Create flow log (Crear registro de flujo)**.

Para crear un registro de flujo que publica en Amazon S3 mediante una herramienta de línea de comandos

Utilice uno de los siguientes comandos.

- [create-flow-logs](#) (AWS CLI)
- [New-EC2FlowLogs](#) (AWS Tools for Windows PowerShell)
- [CreateFlowLogs](#) (API de consulta de Amazon EC2)

En el siguiente ejemplo de AWS CLI, se crea un registro de flujo que captura todo el tráfico de la VPC `vpc-00112233344556677` y envía los registros de flujo a un bucket de Amazon S3 denominado `flow-log-bucket`. El parámetro `--log-format` especifica un formato personalizado para las entradas de registros de flujo.

```
aws ec2 create-flow-logs --resource-type VPC --resource-ids vpc-00112233344556677 --
traffic-type ALL --log-destination-type s3 --log-destination arn:aws:s3:::flow-log-
bucket/my-custom-flow-logs/ --log-format '${version} ${vpc-id} ${subnet-id} ${instance-
id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${tcp-flags} ${type} ${pkt-
srcaddr} ${pkt-dstaddr}'
```

Procesar entradas de registro de flujo en Amazon S3

Los archivos log están comprimidos. Si abre los archivos de registro con la consola de Amazon S3, se descomprimen y se muestran las entradas de registro de flujo. Si descarga los archivos, debe descomprimirlos para ver los registros de logs de flujo.

También puede consultar las entradas de registro de flujo en los archivos de registro mediante Amazon Athena. Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar. Para obtener más información, consulte [Consulta de registros de flujo de Amazon VPC](#) en la Guía del usuario de Amazon Athena.

Trabajar con registros de flujo

Puede trabajar con registros de flujo con las consolas de Amazon EC2, Amazon VPC, CloudWatch y Amazon S3.

Tareas

- [Controlar el uso de los registros de flujo \(p. 222\)](#)
- [Crear un log de flujo \(p. 223\)](#)
- [Ver los registros de flujo \(p. 223\)](#)
- [Agregar o quitar etiquetas para los registros de flujo \(p. 223\)](#)
- [Ver entradas de registros de flujo \(p. 224\)](#)
- [Buscar entradas de registros de flujo \(p. 224\)](#)
- [Eliminación de un log de flujo \(p. 225\)](#)
- [Información general de la API y de la CLI \(p. 225\)](#)

Controlar el uso de los registros de flujo

De forma predeterminada, los usuarios de IAM no tienen permiso para trabajar con registros de flujo. Puede crear una política de usuarios de IAM que conceda permisos a los usuarios para crear, describir y eliminar registros de flujo. Para obtener más información, consulte [Concesión a los usuarios de IAM de los permisos necesarios para los recursos de Amazon EC2](#) en la Referencia de la API de Amazon EC2.

A continuación se muestra una política de ejemplo que concede a los usuarios permisos completos para crear, describir y eliminar logs de flujo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
```

```
        "ec2:DescribeFlowLogs"  
      ],  
      "Resource": "*"   
    }  
  ]  
}
```

Se requiere alguna configuración adicional de permisos y roles de IAM, en función de si se publica en CloudWatch Logs o Amazon S3. Para obtener más información, consulte [Publicar registros de flujo en CloudWatch Logs \(p. 211\)](#) y [Publicar registros de flujo en Amazon S3 \(p. 216\)](#).

Crear un log de flujo

Puede crear registros de flujo para sus VPC, subredes o interfaces de red. Los registros de flujo pueden publicar datos en CloudWatch Logs o Amazon S3.

Para obtener más información, consulte [Crear un registro de flujo que se publique en CloudWatch Logs \(p. 213\)](#) y [Crear un registro de flujo que se publique en Amazon S3 \(p. 220\)](#).

Ver los registros de flujo

Puede consultar información acerca de los registros de flujo en las consolas de Amazon EC2 y Amazon VPC en la pestaña Flow Logs (Registros de flujo) para un recurso específico. Al seleccionar el recurso, se mostrarán todos los logs de flujo de ese recurso. La información mostrada incluye el ID del log de flujo, la configuración del log de flujo y la información acerca del estado del log de flujo.

Para ver información acerca de los registros de flujo para sus interfaces de red

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione una interfaz de red y elija Flow Logs (Logs de flujo). Se mostrará información acerca de los logs de flujo en la pestaña. La columna Destination type (Tipo de destino) indica el destino en el que se publican los logs de flujo.

Para ver información acerca de los registros de flujo para sus VPC o subredes

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs (Sus VPC) o Subnets (Subredes).
3. Seleccione su VPC o subred y elija Flow Logs (Logs de flujo). Se mostrará información acerca de los logs de flujo en la pestaña. La columna Destination type (Tipo de destino) indica el destino en el que se publican los logs de flujo.

Agregar o quitar etiquetas para los registros de flujo

Puede agregar o quitar etiquetas para un registro de flujo en las consolas de Amazon EC2 y Amazon VPC.

Para agregar o quitar etiquetas en un registro de flujo para una interfaz de red

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Network Interfaces.
3. Seleccione una interfaz de red y elija Flow Logs (Logs de flujo).
4. Elija Manage tags (Administrar etiquetas) para el registro de flujo requerido.
5. Para agregar una etiqueta nueva, elija Create Tag. Para quitar una etiqueta, elija el icono de eliminación (x).

6. Seleccione Save.

Para agregar o quitar etiquetas en un registro de flujo para una VPC o una subred

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs (Sus VPC) o Subnets (Subredes).
3. Seleccione su VPC o subred y elija Flow Logs (Logs de flujo).
4. Seleccione el registro de flujo y elija Actions (Acciones), Add/Edit Tags (Agregar o editar etiquetas).
5. Para agregar una etiqueta nueva, elija Create Tag. Para quitar una etiqueta, elija el icono de eliminación (x).
6. Seleccione Save.

Ver entradas de registros de flujo

Puede consultar las entradas de registro de flujo mediante la consola de CloudWatch Logs o la consola de Amazon S3, en función del tipo de destino elegido. Es posible que, después de crear su registro de flujo, se necesiten unos minutos para que se encuentre visible en la consola.

Para consultar las entradas de registro de flujo publicados en CloudWatch Logs

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Logs y seleccione el grupo de logs que contiene el log de flujo. Aparecerá una lista de flujos de log para cada interfaz de red.
3. Seleccione el flujo de logs que contiene el ID de la interfaz de red para la que desea ver los registros de logs de flujo. Para obtener más información, consulte [Registros de log de flujo \(p. 200\)](#).

Para consultar las entradas de registro de flujo publicadas en Amazon S3

1. Abra la consola de Amazon S3 en <https://console.aws.amazon.com/s3>.
2. En Bucket name (Nombre del bucket), seleccione el bucket en el que se van a publicar los logs de flujo.
3. En Name (Nombre), active la casilla de verificación situada junto al archivo log. En el panel de información general del objeto, elija Download (Descargar).

Buscar entradas de registros de flujo

Puede buscar las entradas de registro de flujo que se publican en CloudWatch Logs mediante la consola de CloudWatch Logs. Puede utilizar [filtros de métricas](#) para filtrar entradas de registro de flujo. Los registros de log de flujo están delimitados por espacios.

Para buscar entradas de registro de flujo mediante la consola de CloudWatch Logs

1. Abra la consola de CloudWatch en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, elija Grupos de registros y seleccione el grupo de registros que contiene el registro de flujo. Aparecerá una lista de flujos de log para cada interfaz de red.
3. Seleccione la secuencia de registro individual si conoce la interfaz de red que está buscando. Otra opción, elija Buscar en el grupo de registros para buscar en todo el grupo de registros. Esto puede tardar algún tiempo si hay muchas interfaces de red en el grupo de registro o en función del intervalo de tiempo que seleccione.
4. En Filtrar los eventos, escriba la siguiente cadena. Esto supone que el registro de log de flujo utiliza el [formato predeterminado \(p. 200\)](#).

```
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport, protocol, packets, bytes, start, end, action, logstatus]
```

5. Modifique el filtro según sea necesario especificando valores para los campos. En los siguientes ejemplos se filtra por direcciones IP de origen específicas.

```
[version, accountid, interfaceid, srcaddr = 10.0.0.1, dstaddr, srcport, dstport, protocol, packets, bytes, start, end, action, logstatus]  
[version, accountid, interfaceid, srcaddr = 10.0.2.*, dstaddr, srcport, dstport, protocol, packets, bytes, start, end, action, logstatus]
```

En los siguientes ejemplos se filtra por puerto de destino, el número de bytes y si se ha rechazado el tráfico.

```
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport = 80 || dstport = 8080, protocol, packets, bytes, start, end, action, logstatus]  
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport = 80 || dstport = 8080, protocol, packets, bytes >= 400, start, end, action = REJECT, logstatus]
```

Eliminación de un log de flujo

Puede eliminar un registro de flujo mediante las consolas de Amazon EC2 y Amazon VPC.

Estos procedimientos deshabilitan el servicio de logs de flujo para un recurso. La eliminación de un registro de flujo no elimina las secuencias de registro existentes de CloudWatch Logs y los archivos de registro de Amazon S3. Los datos de los logs de flujo existentes deben eliminarse con la consola del servicio correspondiente. Además, la eliminación de un registro de flujo que publica en Amazon S3 no quita las políticas de bucket ni las listas de control de acceso (ACL) de los archivos de registro.

Para eliminar un log de flujo para una interfaz de red

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Network Interfaces y seleccione la interfaz de red.
3. Elija Flow Logs (Logs de flujo) y, a continuación, elija el botón de eliminación (una cruz) para el log de flujo que desea eliminar.
4. En el cuadro de diálogo de confirmación, elija Yes, Delete.

Para eliminar un log de flujo para una VPC o subred

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs (Sus VPC) o Subnets (Subredes) y, a continuación, seleccione el recurso.
3. Elija Flow Logs (Logs de flujo) y, a continuación, elija el botón de eliminación (una cruz) para el log de flujo que desea eliminar.
4. En el cuadro de diálogo de confirmación, elija Yes, Delete.

Información general de la API y de la CLI

Puede realizar las tareas descritas en esta página utilizando la línea de comandos o al API. Para obtener más información acerca de las interfaces de la línea de comando, junto con una lista de las acciones de API disponibles, consulte [Acceder a Amazon VPC \(p. 2\)](#).

Crear un log de flujo

- [create-flow-logs](#) (AWS CLI)
- [New-EC2FlowLog](#) (AWS Tools for Windows PowerShell)
- [CreateFlowLogs](#) (API de consulta de Amazon EC2)

Descripción de sus logs de flujo

- [describe-flow-logs](#) (AWS CLI)
- [Get-EC2FlowLog](#) (AWS Tools for Windows PowerShell)
- [DescribeFlowLogs](#) (API de consulta de Amazon EC2)

Visualización de sus registros de logs de flujo (eventos de log)

- [get-log-events](#) (AWS CLI)
- [Get-CWLogEvent](#) (AWS Tools for Windows PowerShell)
- [GetLogEvents](#) (API de CloudWatch)

Eliminación de un log de flujo

- [delete-flow-logs](#) (AWS CLI)
- [Remove-EC2FlowLog](#) (AWS Tools for Windows PowerShell)
- [DeleteFlowLogs](#) (API de consulta de Amazon EC2)

Realizar consultas en los registros de flujo mediante Amazon Athena

Amazon Athena es un servicio de consulta interactivo que le permite analizar datos en Amazon S3, como los logs de flujo, mediante SQL estándar. Puede utilizar Athena con los logs de flujo de VPC para obtener rápidamente información útil sobre el tráfico que fluye a través de su VPC. Por ejemplo, puede identificar qué recursos de sus virtual private clouds (VPC) son los principales interlocutores o puede identificar las direcciones IP con las conexiones TCP más rechazadas.

Opciones

- Puede optimizar y automatizar la integración de los registros de flujo de VPC con Athena generando una plantilla de CloudFormation que cree los recursos de AWS necesarios, además de consultas predefinidas que puede ejecutar para obtener información sobre el tráfico que fluye a través de la VPC.
- Puede crear sus propias consultas con Athena. Para obtener más información, consulte [Realizar consultas en los registros de flujo mediante Amazon Athena](#) en la Guía del usuario de Amazon Athena.

Precios

Incurrir en [cargos estándar de Amazon Athena](#) por ejecutar consultas. Incurrir en [cargos estándar de AWS Lambda](#) por la función de Lambda que carga nuevas particiones en una programación periódica (cuando especifica una frecuencia de carga de partición pero no especifica una fecha de inicio y finalización).

Para utilizar las consultas predefinidas

- [Generar la plantilla de CloudFormation mediante la consola](#) (p. 227)
- [Generar la plantilla de CloudFormation mediante la AWS CLI](#) (p. 228)

- [Ejecutar una consulta predefinida \(p. 228\)](#)

Generar la plantilla de CloudFormation mediante la consola

Después de entregar los primeros logs de flujo a su bucket de S3, puede integrarse con Athena generando una plantilla de CloudFormation y utilizando la plantilla para crear una pila.

Requisitos

- Debe seleccionar una región que admita AWS Lambda y Amazon Athena.
- Los buckets de Amazon S3 deben estar en la región seleccionada.

Para generar la plantilla mediante la consola

1. Aplique alguna de las siguientes acciones:
 - Abra la consola de Amazon VPC. En el panel de navegación, elija Your VPCs (Sus VPC) y, a continuación seleccione su VPC,
 - Abra la consola de Amazon VPC. En el panel de navegación, elija Subnets (Subredes) y, a continuación, seleccione la suya.
 - Abra la consola de Amazon EC2. En el panel de navegación, elija Network Interfaces (Interfaces de red) y, a continuación, seleccione su interfaz de red.
2. En la pestaña Flow logs (Logs de flujo) , seleccione un log de flujo que se publique en Amazon S3 y, a continuación, elija Actions (Acciones), Generate Athena integration (Generar integración de Athena).
3. Especifique la frecuencia de carga de la partición. Si elige None (Ninguno), debe especificar la fecha de inicio y finalización de la partición, utilizando fechas anteriores. Si elige Daily (Diaria), Weekly (Semanal) o Monthly (Mensual), las fechas de inicio y finalización de la partición son opcionales. Si no especifica fechas de inicio y finalización, la plantilla de CloudFormation crea una función Lambda que carga nuevas particiones con una programación recurrente.
4. Seleccione o cree un bucket de S3 para la plantilla generada y un bucket de S3 para los resultados de la consulta.
5. Elija Generate Athena Integration (Generar integración de Athena).
6. (Opcional) En el mensaje de éxito, elija el vínculo para navegar al bucket especificado para la plantilla de CloudFormation y personalice la plantilla.
7. En el mensaje de éxito, elija Create CloudFormation stack (Crear pila de CloudFormation) para abrir el asistente Create Stack (Crear pila) en la consola de AWS CloudFormation. La dirección URL de la plantilla de CloudFormation generada se especifica en la sección Template (Plantilla) . Complete el asistente para crear los recursos especificados en la plantilla.

Recursos creados por la plantilla de CloudFormation

- Una base de datos de Athena. El nombre de la base de datos es `vpcflowlogsathenadatabase<flow-logs-subscription-id>`.
- Un grupo de trabajo de Athena. El nombre del grupo de trabajo es `<flow-log-subscription-id><partition-load-frequency><start-date><end-date>workgroup`
- Una tabla Athena particionada que corresponde a sus registros del log de flujo. El nombre de la tabla es `<flow-log-subscription-id><partition-load-frequency><start-date><end-date>`.
- Un conjunto de consultas llamadas Athena. Para obtener más información, consulte [Consultas predefinidas \(p. 228\)](#).
- Una función Lambda que carga nuevas particiones en la tabla según la programación especificada (diaria, semanal o mensual).
- Una función de IAM que otorga permiso para ejecutar las funciones Lambda.

Generar la plantilla de CloudFormation mediante la AWS CLI

Después de entregar los primeros logs de flujo a su bucket de S3, puede generar y utilizar una plantilla de CloudFormation para integrarse con Athena.

Utilice el siguiente comando [get-flow-logs-integration-template](#) para generar la plantilla de CloudFormation.

```
aws ec2 get-flow-logs-integration-template --cli-input-json file://config.json
```

A continuación se muestra un ejemplo del archivo `config.json`.

```
{
  "FlowLogId": "fl-12345678901234567",
  "ConfigDeliveryS3DestinationArn": "arn:aws:s3:::my-flow-logs-athena-integration/
templates/",
  "IntegrateServices": {
    "AthenaIntegrations": [
      {
        "IntegrationResultS3DestinationArn": "arn:aws:s3:::my-flow-logs-analysis/
athena-query-results/",
        "PartitionLoadFrequency": "monthly",
        "PartitionStartDate": "2021-01-01T00:00:00",
        "PartitionEndDate": "2021-12-31T00:00:00"
      }
    ]
  }
}
```

Utilice el siguiente comando [create-stack](#) para crear una pila utilizando la plantilla de CloudFormation generada.

```
aws cloudformation create-stack --stack-name my-vpc-flow-logs --template-body file://my-
cloudformation-template.json
```

Ejecutar una consulta predefinida

La plantilla de CloudFormation generada proporciona un conjunto de consultas predefinidas que puede ejecutar para obtener rápidamente información significativa sobre el tráfico de su red de AWS. Después de crear la pila y comprobar que todos los recursos se han creado correctamente, puede ejecutar una de las consultas predefinidas.

Para ejecutar una consulta predefinida mediante la consola

1. Abra la consola de Athena. En el panel Workgroups (Grupos de trabajo), seleccione el grupo de trabajo creado por la plantilla de CloudFormation.
2. Seleccione una de las [consultas predefinidas](#) (p. 228), modifique los parámetros según sea necesario y, a continuación, ejecute la consulta.
3. Abra la consola de Amazon S3. Avance hasta el bucket especificado para los resultados de la consulta y vea los resultados de la consulta.

Consultas predefinidas

Las siguientes son las consultas con el nombre Athena proporcionadas por la plantilla generada de CloudFormation:

- `vpcFlowLogsAcceptedTraffic`: las conexiones TCP permitidas en función de los grupos de seguridad y las ACL de red.

- `vpcFlowLogsAdminPortTraffic`: las 10 direcciones IP con más tráfico, registradas por las aplicaciones que atienden solicitudes en los puertos administrativos.
- `vpcFlowLogsIpv4Traffic`: el total de bytes del tráfico IPv4 registrado.
- `vpcFlowLogsIpv6Traffic`: el total de bytes del tráfico IPv6 registrado.
- `vpcFlowLogsRejectedTCPTraffic`: las conexiones TCP que se rechazaron en función de los grupos de seguridad o las ACL de red.
- `vpcFlowLogsRejectedTraffic`: el tráfico que se rechazó en función de los grupos de seguridad o las ACL de red.
- `vpcFlowLogssShrdpTraffic`: el tráfico SSH y RDP.
- `vpcFlowLogStopTalkers`: las 50 direcciones IP con la mayor cantidad de tráfico registrado.
- `vpcFlowLogStopTalkerSpacketLevel`: las 50 direcciones IP de nivel de paquete con la mayor cantidad de tráfico registrado.
- `vpcFlowLogStopTalkingInstances`: las ID de las 50 instancias con la mayor cantidad de tráfico registrado.
- `vpcFlowLogStopTalkingSubnets`: las ID de las 50 subredes con la mayor cantidad de tráfico registrado.
- `vpcflowLogStoptCPTraffic`: todo el tráfico TCP registrado para una dirección IP de origen.
- `vpcFlowLogsTotalByteTransferred`: los 50 pares de direcciones IP de origen y destino con la mayoría de bytes registrados.
- `vpcFlowLogsTotalByTestransferredPacketLevel`: los 50 pares de direcciones IP de origen y destino a nivel de paquete con la mayor cantidad de bytes registrados.
- `vpcFlowLogsTrafficFrmsrcAddr`: el tráfico registrado para una dirección IP de origen específica.
- `vpcFlowLogsTrafficToStaddr`: el tráfico registrado para una dirección IP de destino específica.

Solucionar problemas de los registros de flujo de VPC

A continuación se indican los posibles problemas que pueden surgir al trabajar con registros de flujo.

Problemas

- [Registros de logs de flujo incompletos \(p. 229\)](#)
- [El log de flujo está activo, pero no hay registros de logs de flujo ni grupo de logs \(p. 230\)](#)
- [Error 'LogDestinationNotFoundException' o 'Access Denied for LogDestination' \(p. 230\)](#)
- [Superación del límite de la política de bucket de Amazon S3 \(p. 231\)](#)

Registros de logs de flujo incompletos

Problema

Sus registros de flujo están incompletos o ya no se publican.

Causa

Es posible que haya un problema con la entrega de registros de flujo al grupo de registros de CloudWatch Logs.

Solución

En la consola de Amazon EC2 o en la consola de Amazon VPC, elija la pestaña Flow Logs (Registros de flujo) para el recurso correspondiente. Para obtener más información, consulte [Ver los registros de flujo \(p. 223\)](#). La tabla de logs de flujo muestra los errores en la columna Status. Otra opción, utilice el

comando [describe-flow-logs](#) y compruebe el valor devuelto en el campo `DeliverLogsErrorMessage`. Es posible que se muestre uno de los siguientes errores:

- `Rate limited`: este error se puede producir si se ha aplicado una limitación controlada de CloudWatch Logs, cuando el número de entradas de registro de flujo para una interfaz de red es superior al número máximo de registros que se pueden publicar en un periodo determinado. Este error también se puede producir si ha alcanzado la cuota del número de grupos de registro de CloudWatch Logs que puede crear. Para obtener más información, consulte [Service Quotas de CloudWatch](#) en la Guía del usuario de Amazon CloudWatch.
- `Access error`: este error puede producirse por las razones siguientes:
 - El rol de IAM del registro de flujo no tiene permisos suficientes para publicar entradas de registros de flujo en el grupo de registros de CloudWatch
 - El rol de IAM no tiene una relación de confianza con el servicio de registros de flujo
 - La relación de confianza no especifica el servicio de logs de flujo como elemento principal

Para obtener más información, consulte [Roles de IAM para publicar registros de flujo en CloudWatch Logs](#) (p. 211).

- `Unknown error`: se ha producido un error interno en el servicio de logs de flujo.

El log de flujo está activo, pero no hay registros de logs de flujo ni grupo de logs

Problema

Usted creó un registro de flujo y la consola de Amazon VPC o Amazon EC2 muestra el registro de flujo como `Active`. Sin embargo, no puede ver ninguna secuencia de registro en CloudWatch Logs ni en los archivos de registro del bucket de Amazon S3.

Causas posibles

- El registro de flujo sigue en proceso de creación. En algunos casos, pueden necesitarse diez minutos o más después de crear el registro de flujo para que se cree el grupo de registros y para que se muestren los datos.
- Aún no se ha registrado tráfico en sus interfaces de red. El grupo de registros de CloudWatch Logs solo se crea cuando se registra el tráfico.

Solución

Esperar unos minutos a que se cree el grupo de registros o a que se registre el tráfico.

Error 'LogDestinationNotFoundException' o 'Access Denied for LogDestination'

Problema

Aparece un error `Access Denied for LogDestination` o `LogDestinationNotFoundException` cuando crea un registro de flujo.

Causas posibles

- Al crear un registro de flujo que publica datos en un bucket de Amazon S3, este error indica que no se pudo encontrar el bucket de S3 especificado o que la política de bucket no permite que los registros se entreguen al bucket.

- Al crear un registro de flujo que publica datos en Amazon CloudWatch Logs, este error indica que el rol de IAM no permite que los registros se entreguen al grupo de registros.

Solución

- Al publicar en Amazon S3, asegúrese de que ha especificado el ARN de un bucket de S3 existente y de que el ARN tiene el formato correcto. Si no es propietario del bucket de S3, compruebe que la [política de bucket](#) (p. 218) cuente con los permisos necesarios y utilice el ID de cuenta y el nombre de bucket correctos en el ARN.
- Al publicar en CloudWatch Logs, compruebe que el [rol de IAM](#) (p. 211) cuente con los permisos necesarios.

Superación del límite de la política de bucket de Amazon S3

Problema

Cuando intenta crear un registro de flujo, obtiene el siguiente mensaje de error:
`LogDestinationPermissionIssueException`.

Causas posibles

Las políticas de bucket de Amazon S3 tienen un límite de tamaño de 20 KB.

Cada vez que crea un registro de flujo que publica en un bucket de Amazon S3, se agrega automáticamente el ARN del bucket especificado, que incluye la ruta de la carpeta, al elemento `Resource` de la política del bucket.

La creación de varios registros de flujo que publican en el mismo bucket podría provocar que se superara el límite de la política de bucket.

Solución

- Elimine la política de bucket al quitar las entradas del registro de flujo que ya no se necesitan.
- Otorgue permisos a todo el bucket reemplazando las entradas individuales del log de flujo por las siguientes:

```
arn:aws:s3:::bucket_name/*
```

Si concede permisos a todo el bucket, las nuevas suscripciones de registro de flujo no añaden nuevos permisos a la política de bucket.

Seguridad en Amazon Virtual Private Cloud

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y un centro de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El [modelo de responsabilidad compartida](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta los servicios de AWS en la nube de AWS. AWS también proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los [AWS Programas de conformidad de](#) . Para obtener información sobre los programas de conformidad que se aplican a Amazon Virtual Private Cloud, consulte [Servicios de AWS en el alcance del programa de conformidad](#).
- Seguridad en la nube: su responsabilidad se determina según el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Amazon VPC. En los siguientes temas, se le muestra cómo configurar Amazon VPC para satisfacer los objetivos de seguridad y conformidad. También descubrirá cómo se utilizan otros servicios de AWS que le ayudan a monitorear y proteger los recursos de Amazon VPC.

Contenido

- [Protección de datos en Amazon Virtual Private Cloud \(p. 232\)](#)
- [Seguridad de la infraestructura en Amazon VPC \(p. 235\)](#)
- [Identity and Access Management para Amazon VPC \(p. 237\)](#)
- [Controlar el tráfico hacia los recursos mediante grupos de seguridad \(p. 255\)](#)
- [Resiliencia en Amazon Virtual Private Cloud \(p. 265\)](#)
- [Validación de conformidad para Amazon Virtual Private Cloud \(p. 265\)](#)
- [Configuración y análisis de vulnerabilidades en Amazon Virtual Private Cloud \(p. 266\)](#)
- [Prácticas recomendadas de seguridad de la VPC \(p. 266\)](#)

Protección de datos en Amazon Virtual Private Cloud

El [modelo de responsabilidad compartida](#) de AWS se aplica a la protección de los datos en Amazon Virtual Private Cloud. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Este contenido incluye la configuración de seguridad y las tareas de administración de los Servicios de AWS que utilice. Para obtener más información sobre la privacidad de

los datos, consulte las [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog [AWSShared Responsibility Model and GDPR](#) en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de Cuenta de AWS y configurar cuentas de usuario individuales con AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de las siguientes formas:

- Utilice Multi-Factor Authentication (MFA) con cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Recomendamos TLS 1.2 o una versión posterior.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de AWS.
- Utilice avanzados servicios de seguridad administrados, como Amazon Macie, que lo ayuden a detectar y proteger los datos personales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de enlace de FIPS. Para obtener más información sobre los puntos de enlace de FIPS disponibles, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-2](#).

Recomendamos encarecidamente que nunca introduzca información de identificación confidencial, como, por ejemplo, direcciones de email de sus clientes, en etiquetas o en los campos de formato libre, como el campo Name (Nombre). Esto incluye cuando trabaja con Amazon VPC u otros servicios de AWS mediante la consola, la API, la AWS CLI o los AWS SDK. Los datos que ingresa en etiquetas o campos de formato libre utilizados para los nombres se pueden utilizar 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.

Privacidad del tráfico entre redes en Amazon VPC

Amazon Virtual Private Cloud ofrece características que puede utilizar para aumentar y monitorear la seguridad de Virtual Private Cloud (VPC):

- Grupos de seguridad: los grupos de seguridad actúan como firewall para las instancias Amazon EC2 asociadas, al controlar el tráfico entrante y saliente en el nivel de la instancia. Cuando lanza una instancia, puede asociarla a uno o varios grupos de seguridad que haya creado. Cada instancia de su VPC podría pertenecer a un conjunto distinto de grupos de seguridad. Si no especifica ningún grupo de seguridad al lanzar una instancia, esta se asocia automáticamente al grupo de seguridad predeterminado de la VPC. Para obtener más información, consulte [Controlar el tráfico hacia los recursos mediante grupos de seguridad](#) (p. 255).
- Listas de control de acceso (ACL) de red: las ACL de red actúan como firewall para las subredes asociadas y controlan el tráfico entrante y saliente en el ámbito de la subred. Para obtener más información, consulte [Controlar el tráfico hacia las subredes utilizando las ACL de red](#) (p. 120).
- Registros de flujo: los registros de flujo capturan información acerca del tráfico IP entrante y saliente de las interfaces de red en su VPC. Puede crear un registro de flujo para una VPC, una subred o una interfaz de red individual. Los datos del registro de flujo se publican en CloudWatch Logs o Amazon S3 y pueden ayudarle a diagnosticar reglas de ACL de red y de grupos de seguridad excesivamente restrictivas o permisivas. Para obtener más información, consulte [Registro del tráfico de IP con registros de flujo de la VPC](#) (p. 197).
- Replicación del tráfico: puede copiar el tráfico de red desde una interfaz de red elástica de una instancia de Amazon EC2. A continuación, puede enviar el tráfico a dispositivos de supervisión y seguridad fuera de banda. Para obtener más información, consulte la [Guía de replicación de tráfico](#).

Puede utilizar AWS Identity and Access Management (IAM) para controlar quién de su organización tiene permiso para crear y administrar grupos de seguridad, ACL de red y registros de flujo. Por ejemplo, puede conceder ese permiso a sus administradores de red, pero no dar permiso al personal que solo necesita lanzar instancias. Para obtener más información, consulte [Identity and Access Management para Amazon VPC](#) (p. 237).

Los grupos de seguridad y las ACL de red de Amazon no filtran el tráfico destinado a los siguientes servicios de Amazon ni desde los mismos:

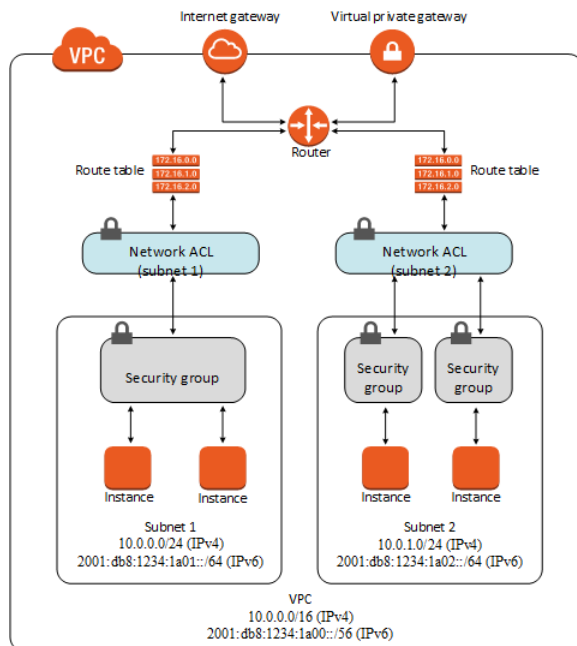
- Servicios de nombres de dominio de Amazon (DNS)
- Protocolo de configuración dinámica de host de Amazon (DHCP)
- Metadatos de la instancia de Amazon EC2
- Activación de licencia de Windows para Amazon
- Amazon Time Sync Service
- Dirección IP reservada del enrutador de la VPC predeterminado

Comparar grupos de seguridad y ACL de red

La siguiente tabla resume las diferencias básicas entre grupos de seguridad y ACL de red.

Security group (Grupo de seguridad)	ACL de red
Opera en el nivel de la instancia	Opera en el nivel de la subred
Solo admite reglas de permiso	Admite reglas de permiso y de denegación
Es con estado: el tráfico de retorno se admite automáticamente, independientemente de las reglas	Es sin estado: las reglas deben permitir de forma explícita el tráfico de retorno
Evaluamos todas las normas antes de decidir si permitir el tráfico	Procesamos las reglas en orden, empezando por la regla numerada más baja, al decidir si permitir el tráfico
Se aplica a una instancia únicamente si alguien especifica el grupo de seguridad al lanzar la instancia, o asocia el grupo de seguridad a la instancia más adelante	Se aplica automáticamente a todas las instancias de las subredes con las que se ha asociado (por lo tanto, proporciona una capa de defensa adicional si las reglas del grupo de seguridad son demasiado permisivas)

El siguiente diagrama muestra las capas de seguridad proporcionadas por los grupos de seguridad y las ACL de red. Por ejemplo, el tráfico de un puerto de enlace a Internet se dirige a la subred correspondiente mediante las rutas de la tabla de ruteo. Las reglas de la ACL de red que se asocian a la subred controlan el tráfico que se permite en la subred. Las reglas del grupo de seguridad que se asocian a una instancia controlan el tráfico que se permite en la instancia.



Puede proteger sus instancias utilizando sólo grupos de seguridad. Sin embargo, puede añadir ACL de red como una capa adicional de defensa. Para ver un ejemplo, consulte [Ejemplo: controlar el acceso a las instancias de una subred](#) (p. 138).

Cifrado en tránsito

AWS proporciona conectividad privada y segura entre instancias EC2 de todo tipo. Además, en algunos tipos de instancia, se utilizan las capacidades de descarga del hardware Nitro System subyacente para cifrar de manera automática el tráfico en tránsito entre instancias. Para obtener más información, consulte [Cifrado en tránsito](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Seguridad de la infraestructura en Amazon VPC

Como servicio administrado, Amazon VPC está protegido por los procedimientos de seguridad de la red global de AWS que se detallan en el documento técnico [Amazon Web Services: Información general acerca de los procesos de seguridad](#).

Puede utilizar llamadas a la API publicadas de AWS para acceder a Amazon VPC a través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.0 o una versión posterior. Le recomendamos TLS 1.2 o una versión posterior. 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 puede utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Aislamiento de red

Una nube virtual privada (VPC) es una red virtual en su propia área, aislada lógicamente en la nube de AWS. Utilice VPC separados para aislar la infraestructura por carga de trabajo o unidad organizativa.

Una subred es un rango de direcciones IP de una VPC. Al lanzar una instancia, la lanza a una subred en su VPC. Utilice subredes para aislar los niveles de la aplicación (por ejemplo, web, aplicación y base de datos) en una VPC individual. Utilice subredes privadas para las instancias si no se debe acceder a ellas directamente desde Internet.

Para llamar a la API de Amazon EC2 desde su VPC sin enviar tráfico a través del Internet público, use AWS PrivateLink.

Controlar el tráfico de red

Tenga en cuenta las siguientes opciones para controlar el tráfico de red a las instancias EC2:

- Restrinja el acceso a sus subredes mediante [the section called “Grupos de seguridad” \(p. 255\)](#). Por ejemplo, puede permitir el tráfico únicamente desde rangos de direcciones para su red corporativa.
- Aproveche los grupos de seguridad como mecanismo principal para controlar el acceso de la red a las VPC. Cuando sea necesario, utilice las ACL de red con moderación para proporcionar un control de red sin estado y amplio. Los grupos de seguridad son más versátiles que las ACL de red debido a su capacidad de realizar un filtrado de paquetes con estado y crear reglas que hagan referencia a otros grupos de seguridad. Sin embargo, las ACL de red pueden ser eficaces como control secundario para denegar un subconjunto específico de tráfico o proporcionar medidas de protección de subred de alto nivel. Además, dado que las ACL de red se aplican a toda una subred, se pueden utilizar como defensa en profundidad en caso de que una instancia se lance involuntariamente sin un grupo de seguridad correcto.
- Utilice subredes privadas para las instancias si no se debe acceder a ellas directamente desde Internet. Utilice un host bastión o gateway NAT para acceder a Internet desde una instancia en una subred privada.
- Configure tablas de enrutamiento de subred de Amazon VPC con las rutas de red mínimas requeridas. Por ejemplo, coloque solo las instancias de Amazon EC2 que requieran acceso directo a Internet en subredes con rutas a una gateway de Internet, y coloque solo las instancias de Amazon EC2 que necesiten acceso directo a redes internas en subredes con rutas a una gateway privada virtual.
- Considere la posibilidad de utilizar grupos de seguridad adicionales o interfaces de red para controlar y auditar el tráfico de administración de instancias de Amazon EC2 con independencia del tráfico normal de aplicaciones. Este enfoque permite a los clientes implementar políticas especiales de IAM para el control de cambios, lo que facilita la auditoría de los cambios en reglas de grupos de seguridad o en los scripts automatizados de verificación de reglas. Múltiples interfaces de red también ofrecen opciones adicionales para controlar el tráfico de red, incluida la capacidad de crear políticas de direccionamiento basadas en el host o aprovechar diferentes reglas de direccionamiento de la subred VPC basadas en interfaces de red asignadas a una subred.
- Utilice AWS Virtual Private Network o AWS Direct Connect para establecer conexiones privadas desde sus redes remotas a sus VPC. Para obtener más información, consulte [Opciones de conectividad de red a Amazon VPC](#).
- Utilice [registros de flujo de VPC](#) para monitorear el tráfico que llegue a sus instancias.
- Utilice [AWS Security Hub](#) para verificar la accesibilidad accidental a la red desde sus instancias.

Además de restringir el acceso a la red a cada instancia de Amazon EC2, Amazon VPC admite la implementación de controles de seguridad de red adicionales. Para obtener más información, consulte [Protección de redes](#).

Identity and Access Management para Amazon VPC

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Amazon VPC. IAM es un Servicio de AWS que se puede utilizar sin cargo adicional.

Contenido

- [Público \(p. 237\)](#)
- [Autenticarse con identidades \(p. 237\)](#)
- [Administrar el acceso con políticas \(p. 239\)](#)
- [Cómo funciona Amazon VPC con IAM \(p. 241\)](#)
- [Ejemplos de políticas de Amazon VPC \(p. 245\)](#)
- [Solucionar problemas de identidad y acceso de Amazon VPC \(p. 252\)](#)
- [AWS Políticas administradas por para Amazon Virtual Private Cloud \(p. 254\)](#)

Público

La forma en que utiliza AWS Identity and Access Management (IAM) difiere en función del trabajo que realiza en Amazon VPC.

Usuario de servicio: si utiliza el servicio de Amazon VPC para realizar su trabajo, el administrador le proporcionará las credenciales y los permisos que necesita. A medida que utilice más características de Amazon VPC para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos a su administrador. Si no puede acceder a una característica de Amazon VPC, consulte [Solucionar problemas de identidad y acceso de Amazon VPC \(p. 252\)](#).

Administrador de servicio: si está a cargo de los recursos de Amazon VPC de su empresa, probablemente tenga acceso completo a Amazon VPC. Su trabajo consiste en determinar a qué características y recursos de Amazon VPC pueden acceder los empleados. Debe enviar solicitudes al administrador de IAM para cambiar los permisos de los usuarios de los servicios. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo la empresa puede utilizar IAM con Amazon VPC, consulte [Cómo funciona Amazon VPC con IAM \(p. 241\)](#).

Administrador de IAM: si es un administrador de IAM, es posible que desee obtener información sobre cómo escribir políticas para administrar el acceso a Amazon VPC. Para ver ejemplos de políticas, consulte [Ejemplos de políticas de Amazon VPC \(p. 245\)](#).

Autenticarse con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Para obtener más información acerca de cómo iniciar sesión con la AWS Management Console, consulte [Inicio de sesión en la AWS Management Console como usuario de IAM o usuario raíz](#) en la Guía del usuario de IAM.

Debe estar autenticado (haber iniciado sesión en AWS) como el usuario raíz de la Cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM. También puede utilizar la autenticación de inicio de sesión único de la empresa o incluso iniciar sesión con Google o Facebook. En estos casos, su administrador

habrá configurado previamente la federación de identidad mediante roles de IAM. Cuando obtiene acceso a AWS mediante credenciales de otra empresa, asume un rol indirectamente.

Para iniciar sesión directamente en la [AWS Management Console](#), utilice la contraseña con su dirección de email de usuario raíz o con su nombre de usuario de IAM. Puede acceder a AWS mediante programación utilizando sus claves de acceso de usuario raíz o usuario de IAM. AWS proporciona SDK y herramientas de línea de comandos para firmar criptográficamente su solicitud con sus credenciales. Si no utiliza las herramientas de AWS, debe firmar usted mismo la solicitud. Para ello, utilice Signature Version 4, un protocolo para autenticar solicitudes de API de entrada. Para obtener más información acerca de cómo autenticar solicitudes, consulte [Proceso de firma de Signature Version 4](#) en la Referencia general de AWS.

Independientemente del método de autenticación que utilice, es posible que también deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte [Uso de la autenticación multifactor \(MFA\) en AWS](#) en la Guía del usuario de IAM.

Cuenta de AWS usuario raíz

Cuando se crea una Cuenta de AWS por primera vez, se comienza con una única identidad de inicio de sesión que tiene acceso completo a todos los recursos y Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz en sus tareas cotidianas, ni siquiera en las tareas administrativas. En lugar de ello, es mejor ceñirse a la [práctica recomendada de utilizar el usuario final exclusivamente para crear al primer usuario de IAM](#). A continuación, guarde las credenciales del usuario raíz en un lugar seguro y utilícelas tan solo para algunas tareas de administración de cuentas y servicios.

Usuarios y grupos de IAM

Un [usuario de IAM](#) es una identidad de la Cuenta de AWS que dispone de permisos específicos para una sola persona o aplicación. Un usuario de IAM puede tener credenciales a largo plazo, como un nombre de usuario y una contraseña o un conjunto de claves de acceso. Para obtener información sobre cómo generar claves de acceso, consulte [Administración de claves de acceso de los usuarios de IAM](#) en la Guía del usuario de IAM. Al generar claves de acceso para un usuario de IAM, asegúrese de ver y guardar de forma segura el par de claves. No puede recuperar la clave de acceso secreta en el futuro. En su lugar, debe generar un nuevo par de claves de acceso.

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

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

IAM roles

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

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

- **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 de usuarios federados:** en lugar de crear un usuario de IAM, puede utilizar identidades existentes de AWS Directory Service, del directorio de usuarios de su empresa o de un proveedor de identidades web. A estas identidades se les llama usuarios federados. AWS asigna una función a un usuario federado cuando se solicita acceso a través de un [proveedor de identidad](#). Para obtener más información acerca de los usuarios federados, consulte [Usuarios federados y roles](#) en la Guía del usuario de IAM.
- **Acceso entre cuentas:** puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puede adjuntar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del usuario de IAM.
- **Acceso entre servicios:** algunos Servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a servicios.
- **Permisos principales:** cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo considera una entidad principal. Las políticas conceden permisos a una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. En este caso, debe tener permisos para realizar ambas acciones. Para ver si una acción requiere acciones dependientes adicionales en una política, consulte [Acciones, recursos y claves de condición de Amazon Elastic Compute Cloud](#) en la Referencia de autorizaciones de servicio.
- **Rol de servicio:** un rol de servicio es un [rol de IAM](#) que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte [Creación de un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.
- **Rol vinculado a servicio:** un rol vinculado a 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 a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- **Aplicaciones que se ejecutan en Amazon EC2:** puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia adjuntado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para obtener más información, consulte [Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2](#) en la Guía del usuario de IAM.

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

Administrar el acceso con políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades de IAM o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. Puede iniciar sesión como usuario raíz o usuario de IAM o puede asumir un rol de IAM. Cuando realiza una solicitud, AWS evalúa las políticas relacionadas basadas en identidad o en recursos. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas

se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte [Información general de políticas JSON](#) en la Guía del usuario de IAM.

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

Cada entidad de IAM (usuario o rol) comienza sin permisos. En otras palabras, de forma predeterminada, los usuarios no pueden hacer nada, ni siquiera cambiar sus propias contraseñas. Para conceder permiso a un usuario para hacer algo, el administrador debe adjuntarle una política de permisos. O bien el administrador puede agregar al usuario a un grupo que tenga los permisos necesarios. Cuando el administrador concede permisos a un grupo, todos los usuarios de ese grupo obtienen los permisos.

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

Políticas basadas en identidad

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar 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 bajo 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 identidad pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas por AWS y las políticas administradas por el cliente. Para obtener más información acerca de 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 adjuntan a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se adjunta la política, la política define qué acciones puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe [especificar una entidad principal](#) en una política basada en recursos. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se puede utilizar políticas de IAM administradas por AWS en una política basada en recursos.

Listas de control de acceso (ACL)

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

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

Otros tipos de políticas

AWS admite otros tipos de políticas adicionales menos frecuentes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le otorgan.

- **Límites de permisos:** un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede establecer un límite de permisos para una identidad. Los permisos resultantes son la intersección de las políticas basadas en identidad de la entidad y los límites de sus permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.
- **Políticas de control de servicio (SCP):** las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias Cuentas de AWS que posea su empresa. Si habilita todas las características en una organización, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Las SCP limitan los permisos de las entidades de las cuentas miembro, incluido cada usuario raíz de la Cuenta de AWS. Para obtener más información acerca de Organizations y las SCP, consulte [Funcionamiento de las SCP](#) en la Guía del usuario de AWS Organizations.
- **Políticas de sesión:** las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidad del rol y las políticas de la sesión. Los permisos también pueden proceder de una política basada en recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información, consulte [Políticas de sesión](#) en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información acerca de cómo AWS decide si permitir o no una solicitud cuando hay varios tipos de políticas implicados, consulte [Lógica de evaluación de políticas](#) en la Guía del usuario de IAM.

Cómo funciona Amazon VPC con IAM

Antes de utilizar IAM para administrar el acceso a Amazon VPC, debe conocer qué características de IAM están disponibles con Amazon VPC. Para obtener una perspectiva general sobre cómo funcionan Amazon VPC y otros servicios de AWS con IAM, consulte [Servicios de AWS que funcionan con IAM](#) en la Guía del usuario de IAM.

Contenido

- [Acciones](#) (p. 242)
- [Recursos](#) (p. 242)
- [Claves de condición](#) (p. 243)
- [Políticas basadas en recursos de Amazon VPC](#) (p. 244)
- [Autorización basada en etiquetas](#) (p. 244)
- [IAM roles](#) (p. 244)

Con las políticas basadas en identidad de IAM, puede especificar acciones permitidas o denegadas. Para algunas acciones, puede especificar los recursos y las condiciones en los cuales se permiten o deniegan las acciones. Amazon VPC admite acciones, claves de condiciones y recursos específicos. Para

obtener información sobre todos los elementos que utiliza en una política JSON, consulte [Referencia de los elementos de las políticas JSON de IAM](#) en la Guía del usuario de IAM.

Acciones

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

El elemento `Action` de una política JSON describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos para realizar la operación asociada.

Amazon VPC comparte su espacio de nombres de la API con Amazon EC2. Las acciones de políticas de Amazon VPC utilizan el siguiente prefijo antes de la acción: `ec2:`. Por ejemplo, para conceder a alguien permiso para crear una VPC con la operación de la API `CreateVpc` de Amazon EC2, debe incluir la acción `ec2:CreateVpc` en la política. Las instrucciones de la política deben incluir un elemento `Action` o un elemento `NotAction`.

Para especificar varias acciones en una única instrucción, sepárelas con comas como se muestra en el siguiente ejemplo.

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

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

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

Para consultar una lista de acciones de Amazon VPC, consulte [Acciones, Recursos y Claves de condición para Amazon EC2](#) en la Guía del usuario de IAM.

Recursos

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo 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 `Resource`. Como práctica recomendada, especifique un recurso utilizando el [Nombre de recurso de Amazon \(ARN\)](#). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

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

Important

Actualmente, no todas las acciones de la API de Amazon EC2 admiten permisos de nivel de recurso. Si una acción de la API de Amazon EC2 no admite permisos de nivel de recurso, puede

conceder permisos a los usuarios para que la utilicen, pero tiene que usar un * (asterisco) para el elemento de recurso de la instrucción de la política. Para consultar las acciones para las que puede especificar un ARN para el elemento de recurso, consulte [Acciones definidas por Amazon EC2](#).

El recurso de VPC tiene el ARN que se muestra en el ejemplo siguiente.

```
arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}
```

Para obtener más información acerca del formato de los ARN, consulte [Nombres de recursos de Amazon \(ARN\)](#).

Por ejemplo, para especificar la VPC `vpc-1234567890abcdef0` en su instrucción, utilice el ARN que se muestra en el ejemplo siguiente.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-1234567890abcdef0"
```

Para especificar todas las VPC de una región específica que pertenezcan a una cuenta específica, utilice el comodín (*).

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*"
```

Algunas acciones de Amazon VPC, como las que se utilizan para crear recursos, no se pueden llevar a cabo en un recurso específico. En dichos casos, debe utilizar el carácter comodín (*).

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

En muchas acciones de la API de Amazon EC2 se utilizan varios recursos. Para especificar varios recursos en una única instrucción, separe los ARN con comas.

```
"Resource": [
    "resource1",
    "resource2"
]
```

Para ver una lista de los tipos de recursos de Amazon VPC y los ARN, consulte [Recursos definidos por Amazon EC2](#) en la Guía del usuario de IAM.

Claves de condición

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

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

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

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre

de usuario de IAM. Para obtener más información, consulte [Elementos de la política de IAM: variables y etiquetas](#) en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS, consulte [Claves de contexto de condición globales de AWS](#) en la Guía del usuario de IAM.

Amazon VPC define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para ver todas las claves de condición globales de AWS, consulte [Claves de contexto de condición globales de AWS](#) en la Guía del usuario de IAM.

Todas las acciones de Amazon EC2 admiten las claves de condición `aws:RequestedRegion` y `ec2:Region`. Para obtener más información, consulte [Ejemplo: Restricción del acceso a una región específica](#).

Para consultar una lista de claves de condición de Amazon VPC, consulte [Claves de condición para Amazon EC2](#) en la Guía del usuario de IAM. Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte [Acciones definidas por Amazon EC2](#).

Políticas basadas en recursos de Amazon VPC

Las políticas basadas en recursos son documentos de políticas JSON que especifican qué acciones puede realizar una entidad principal especificada en el recurso de Amazon VPC y en qué condiciones.

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 basada en recursos](#). Añadir a una política basada en recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando el principal y el recurso se encuentran en cuentas de AWS diferentes, también debe conceder a la entidad principal permiso para obtener acceso al recurso. Conceda permiso asociando a la entidad una política basada en identidades. Sin embargo, si la política basada en recursos concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del usuario de IAM.

Autorización basada en etiquetas

Puede asociar etiquetas a los recursos de Amazon VPC o transferirlas en una solicitud. 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 `ec2:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`. Para obtener más información, consulte [Permisos de nivel de recursos para el etiquetado](#) en la Guía del usuario de Amazon EC2.

Para consultar un ejemplo de política basada en la identidad para limitar el acceso a un recurso en función de las etiquetas de ese recurso, consulte [Lanzar instancias en una VPC específica \(p. 251\)](#).

IAM roles

Un [rol de IAM](#) es una entidad de la cuenta de AWS que dispone de permisos específicos.

Utilizar credenciales temporales

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen mediante una llamada a operaciones de la API de AWS STS, como [AssumeRole](#) o [GetFederationToken](#).

Amazon VPC admite el uso de credenciales temporales.

Roles vinculados a servicios

Los [roles vinculados a servicios](#) permiten a los servicios de AWS obtener acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Las [gateways de tránsito](#) admiten roles vinculados a servicios.

Roles de servicio

Esta característica permite que un servicio asuma un [rol de servicio](#) en su nombre. Este rol permite que el servicio obtenga acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles de servicio aparecen en su cuenta de IAM y son propiedad de la cuenta. Esto significa que un administrador de IAM puede cambiar los permisos de este rol. Sin embargo, hacerlo podría deteriorar la funcionalidad del servicio.

Amazon VPC admite roles de servicio para registros de flujo. Al crear un registro de flujo, debe elegir un rol que permita al servicio de registros de flujo acceder a CloudWatch Logs. Para obtener más información, consulte [Roles de IAM para publicar registros de flujo en CloudWatch Logs \(p. 211\)](#).

Ejemplos de políticas de Amazon VPC

De forma predeterminada, los usuarios y roles de IAM no tienen permiso para crear ni modificar los recursos de VPC. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS CLI, o la API de AWS. Un administrador de IAM debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. El administrador debe adjuntar esas políticas a los usuarios o grupos de IAM que necesiten esos permisos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM con estos documentos de políticas JSON de ejemplo, consulte [Creación de políticas en la pestaña JSON](#) en la Guía del usuario de IAM.

Contenido

- [Prácticas recomendadas relativas a políticas \(p. 245\)](#)
- [Utilizar la consola de Amazon VPC \(p. 246\)](#)
- [Crear una VPC con una subred pública \(p. 247\)](#)
- [Modificar y eliminar recursos de VPC \(p. 248\)](#)
- [Administrar grupos de seguridad \(p. 248\)](#)
- [Administración de reglas de grupos de seguridad \(p. 249\)](#)
- [Lanzar instancias en una subred específica \(p. 250\)](#)
- [Lanzar instancias en una VPC específica \(p. 251\)](#)
- [Ejemplos de políticas de Amazon VPC adicionales \(p. 251\)](#)

Prácticas recomendadas relativas a políticas

Las políticas basadas en identidad son muy eficaces. Determinan si alguien puede crear, acceder o eliminar los recursos de Amazon VPC de la cuenta. Estas acciones pueden generar costes adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidad:

- Comenzar a utilizar políticas administradas por AWS: para comenzar a utilizar Amazon VPC rápidamente, utilice las políticas administradas por AWS para proporcionar los permisos necesarios a

los empleados. Estas políticas ya están disponibles en su cuenta y las mantiene y actualiza AWS. Para obtener más información, consulte [Introducción sobre el uso de permisos con políticas administradas por AWS](#) en la Guía del usuario de IAM.

- Conceder privilegios mínimos: al crear políticas personalizadas, conceda solo los permisos necesarios para llevar a cabo una tarea. Comience con un conjunto mínimo de permisos y conceda permisos adicionales según sea necesario. Por lo general, es más seguro que comenzar con permisos que son demasiado tolerantes e intentar hacerlos más estrictos más adelante. Para obtener más información, consulte [Conceder privilegios mínimos](#) en la Guía del usuario de IAM.
- Habilitar la MFA para operaciones confidenciales: para mayor seguridad, obligue a los usuarios de IAM a utilizar la autenticación multifactor (MFA) para acceder a recursos u operaciones de API confidenciales. Para obtener más información, consulte [Uso de la autenticación multifactor \(MFA\) en AWS](#) en la Guía del usuario de IAM.
- Utilizar condiciones de política para mayor seguridad: en la medida en que sea práctico, defina las condiciones en las que las políticas basadas en identidad permitan el acceso a un recurso. Por ejemplo, puede escribir condiciones para especificar un rango de direcciones IP permitidas desde el que debe proceder una solicitud. También puede escribir condiciones para permitir solicitudes solo en un intervalo de hora o fecha especificado o para solicitar el uso de SSL o MFA. Para obtener más información, consulte [Elementos de la política JSON de IAM: condición](#) en la Guía del usuario de IAM.

Utilizar la consola de Amazon VPC

Para acceder a la consola de Amazon VPC, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle mostrar y consultar los detalles sobre los recursos de Amazon VPC en la cuenta de AWS. Si crea una política basada en identidad que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles de IAM) que tengan esa política.

La siguiente política concede permiso de usuario para enumerar los recursos de la consola de VPC, pero no para crearlos, actualizarlos ni eliminarlos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAddresses",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeClassicLinkInstances",
        "ec2:DescribeClientVpnEndpoints",
        "ec2:DescribeCustomerGateways",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeEgressOnlyInternetGateways",
        "ec2:DescribeFlowLogs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeManagedPrefixLists",
        "ec2:DescribeMovingAddresses",
        "ec2:DescribeNatGateways",
        "ec2:DescribeNetworkAcls",
        "ec2:DescribeNetworkInterfaceAttribute",
        "ec2:DescribeNetworkInterfacePermissions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribePrefixLists",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroupReferences",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeStaleSecurityGroups",
```

```
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeTrafficMirrorFilters",
        "ec2:DescribeTrafficMirrorSessions",
        "ec2:DescribeTrafficMirrorTargets",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeTransitGatewayVpcAttachments",
        "ec2:DescribeTransitGatewayRouteTables",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeVpcClassicLink",
        "ec2:DescribeVpcClassicLinkDnsSupport",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeVpcEndpointConnectionNotifications",
        "ec2:DescribeVpcEndpointConnections",
        "ec2:DescribeVpcEndpointServiceConfigurations",
        "ec2:DescribeVpcEndpointServicePermissions",
        "ec2:DescribeVpcEndpointServices",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribeVpnConnections",
        "ec2:DescribeVpnGateways",
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries"
    ],
    "Resource": "*"
}
]
```

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, para dichos usuarios, permita únicamente el acceso a las acciones que coincidan con la operación de API que tienen que realizar.

Crear una VPC con una subred pública

El siguiente ejemplo permite a los usuarios crear VPC, subredes, tablas de ruteo y gateways de Internet. Los usuarios también pueden adjuntar una gateway de Internet a una VPC y crear rutas en las tablas de ruteo. La acción `ec2:ModifyVpcAttribute` permite a los usuarios habilitar los nombres de host de DNS para la VPC, para que cada instancia lanzada en una VPC reciba un nombre de host de DNS.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:CreateVpc",
      "ec2:CreateSubnet",
      "ec2:DescribeAvailabilityZones",
      "ec2:CreateRouteTable",
      "ec2:CreateRoute",
      "ec2:CreateInternetGateway",
      "ec2:AttachInternetGateway",
      "ec2:AssociateRouteTable",
      "ec2:ModifyVpcAttribute"
    ],
    "Resource": "*"
  }]
}
```

La política anterior también permite a los usuarios crear una VPC mediante la primera opción de configuración del asistente de VPC de la consola de Amazon VPC. Para ver el asistente de VPC, los

usuarios también deben tener permiso para utilizar `ec2:DescribeVpcEndpointServices`. Esto garantiza que la sección de puntos de enlace de la VPC del asistente de VPC se cargue correctamente.

Modificar y eliminar recursos de VPC

Es posible que desee controlar los recursos de VPC que los usuarios pueden modificar o eliminar. Por ejemplo, la siguiente política permite a los usuarios utilizar y eliminar tablas de ruteo con la etiqueta `Purpose=Test`. La política también especifica que los usuarios solo pueden eliminar gateways de Internet con la etiqueta `Purpose=Test`. Los usuarios no pueden utilizar tablas de ruteo ni gateways de Internet que no tengan esta etiqueta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:DeleteInternetGateway",
      "Resource": "arn:aws:ec2:*:*:internet-gateway/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Test"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteRouteTable",
        "ec2:CreateRoute",
        "ec2:ReplaceRoute",
        "ec2>DeleteRoute"
      ],
      "Resource": "arn:aws:ec2:*:*:route-table/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Purpose": "Test"
        }
      }
    }
  ]
}
```

Administrar grupos de seguridad

Mediante la siguiente política, se permite ver cualquier regla de grupo de seguridad y cualquier grupo de seguridad. Con la segunda instrucción, se permite a los usuarios eliminar cualquier grupo de seguridad con la etiqueta `Stack=test` y administrar las reglas de entrada y salida de cualquier grupo de seguridad con la etiqueta `Stack=test`. La tercera instrucción requiere que los usuarios etiqueten cualquier grupo de seguridad que creen con la etiqueta `Stack=Test`. Mediante la cuarta instrucción, se permite a los usuarios crear etiquetas cuando crean un grupo de seguridad.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSecurityGroupRules",
      "ec2:DescribeVpcs"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:*:*:security-group/*",
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/Stack": "test"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:*:*:security-group/*",
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/Stack": "Test"
      }
    }
  }
]
```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
        "ec2:ModifySecurityGroupRules",
        "ec2>DeleteSecurityGroup"
      ],
      "Resource": "arn:aws:ec2:*:*:security-group/*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/Stack": "test"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup"
      ],
      "Resource": "arn:aws:ec2:*:*:security-group/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Stack": "test"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["Stack"]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:*:*:security-group/*",
      "Condition": {
        "StringEquals": {
          "ec2:CreateAction" : "CreateSecurityGroup"
        }
      }
    }
  ]
}

```

Para permitir que los usuarios cambien el grupo de seguridad asociado a una instancia, añada la acción `ec2:ModifyInstanceAttribute` a la política.

Para permitir que los usuarios cambien los grupos de seguridad por una interfaz de red, agregue la acción `ec2:ModifyNetworkInterfaceAttribute` a la política.

Administración de reglas de grupos de seguridad

Mediante la siguiente política, se concede a los usuarios permiso para ver todos los grupos de seguridad y las reglas de los grupos de seguridad, así como para agregar y quitar reglas de entrada y salida para los grupos de seguridad de una VPC específica, y modificar las descripciones de la regla de una VPC específica. En la primera instrucción, se utiliza la clave de condición `ec2:vpc` a fin de obtener permisos para una VPC específica.

Con la segunda instrucción, se concede a los usuarios permisos para describir todos los grupos de seguridad, reglas de grupos de seguridad y etiquetas. Esto permite a los usuarios ver las reglas de los grupos de seguridad para modificarlas.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
      "ec2:ModifySecurityGroupRules"
    ],
    "Resource": "arn:aws:ec2:region:account-id:security-group/*",
    "Condition": {
      "ArnEquals": {
        "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSecurityGroupRules",
      "ec2:DescribeTags"
    ],
    "Resource": "*"
  }
]
```

Lanzar instancias en una subred específica

La siguiente política concede a los usuarios permiso para lanzar instancias en una subred específica, así como para utilizar un grupo de seguridad determinado en la solicitud. Esta política se consigue al especificar el ARN de la subred y el ARN del grupo de seguridad. De este modo, si los usuarios intentan lanzar una instancia en una subred distinta o si tratan de utilizar otro grupo de seguridad, se producirá un error en la solicitud (a no ser que otra política o instrucción conceda a los usuarios permiso para realizar tales acciones).

La política también concede permiso para utilizar el recurso de interfaz de red. Al realizar el lanzamiento en una subred, la solicitud `RunInstances` creará una interfaz de red principal de manera predeterminada, por lo que el usuario necesitará permiso para crear este recurso cuando lance la instancia.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:RunInstances",
    "Resource": [
      "arn:aws:ec2:region::image/ami-*",
      "arn:aws:ec2:region:account:instance/*",
      "arn:aws:ec2:region:account:subnet/subnet-id",
      "arn:aws:ec2:region:account:network-interface/*",
      "arn:aws:ec2:region:account:volume/*",
      "arn:aws:ec2:region:account:key-pair/*",
      "arn:aws:ec2:region:account:security-group/sg-id"
    ]
  }
]
```



```
    ]  
  }  
]  
}
```

Lanzar instancias en una VPC específica

La siguiente política concede a los usuarios permiso para lanzar instancias en cualquier subred de una VPC específica. Esto se consigue al aplicar en la política una clave de condición (`ec2:vpc`) para el recurso de la subred.

La política también concede a los usuarios permiso para lanzar instancias utilizando solo AMI que tengan la etiqueta `"department=dev"`.

```
{  
  "Version": "2012-10-17",  
  "Statement": [{  
    "Effect": "Allow",  
    "Action": "ec2:RunInstances",  
    "Resource": "arn:aws:ec2:region:account-id:subnet/*",  
    "Condition": {  
      "ArnEquals": {  
        "ec2:vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"  
      }  
    }  
  },  
  {  
    "Effect": "Allow",  
    "Action": "ec2:RunInstances",  
    "Resource": "arn:aws:ec2:region::image/ami-*",  
    "Condition": {  
      "StringEquals": {  
        "ec2:ResourceTag/department": "dev"  
      }  
    }  
  },  
  {  
    "Effect": "Allow",  
    "Action": "ec2:RunInstances",  
    "Resource": [  
      "arn:aws:ec2:region:account:instance/*",  
      "arn:aws:ec2:region:account:volume/*",  
      "arn:aws:ec2:region:account:network-interface/*",  
      "arn:aws:ec2:region:account:key-pair/*",  
      "arn:aws:ec2:region:account:security-group/*"  
    ]  
  }  
]  
}
```

Ejemplos de políticas de Amazon VPC adicionales

Puede encontrar otras políticas de IAM de ejemplo relacionadas con Amazon VPC en la siguiente documentación:

- [ClassicLink](#)
- [Listas de prefijos administradas \(p. 71\)](#)
- [Replicación de tráfico](#)
- [Transit gateways](#)

- [Puntos de enlace de la VPC y servicios de puntos de enlace de la VPC](#)
- [Políticas de punto de enlace de la VPC](#)
- [Interconexión con VPC](#)
- [AWS Wavelength](#)

Solucionar problemas de identidad y acceso de Amazon VPC

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que es posible que surjan cuando se trabaja con Amazon VPC e IAM.

Problemas

- [No tengo autorización para realizar una acción en Amazon VPC \(p. 252\)](#)
- [No tengo autorización para realizar la operación iam:PassRole \(p. 252\)](#)
- [Quiero ver mis claves de acceso \(p. 253\)](#)
- [Soy administrador y deseo permitir que otros accedan a Amazon VPC \(p. 253\)](#)
- [Quiero permitir que personas ajenas a mi cuenta de AWS accedan a mis recursos de Amazon VPC. \(p. 253\)](#)

No tengo autorización para realizar una acción en Amazon VPC

Si la AWS Management Console le indica que no está autorizado para llevar a cabo una acción, debe ponerse en contacto con su administrador para recibir ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar detalles sobre una subred pero no tiene permisos `ec2:DescribeSubnets`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
ec2:DescribeSubnets on resource: subnet-id
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso a la subred.

No tengo autorización para realizar la operación iam:PassRole

Si recibe un error que indica que no está autorizado para llevar a cabo la acción `iam:PassRole`, debe ponerse en contacto con su administrador para recibir ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña. Pida a la persona que actualice las políticas de forma que pueda transferir un rol a Amazon VPC.

Los Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al 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 Amazon VPC. Sin embargo, la acción requiere que el servicio cuente con permisos otorgados por 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, Mary pide a su administrador que actualice sus políticas de forma que pueda realizar la acción `iam:PassRole`.

Quiero ver mis claves de acceso

Después de crear sus claves de acceso de usuario de IAM, puede ver su ID de clave de acceso en cualquier momento. Sin embargo, no puede volver a ver su clave de acceso secreta. Si pierde la clave de acceso secreta, debe crear un nuevo par de claves de acceso.

Las claves de acceso se componen de dos partes: un ID de clave de acceso (por ejemplo, `AKIAIOSFODNN7EXAMPLE`) y una clave de acceso secreta (por ejemplo, `wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY`). El ID de clave de acceso y la clave de acceso secreta se utilizan juntos, como un nombre de usuario y contraseña, para autenticar sus solicitudes. Administre sus claves de acceso con el mismo nivel de seguridad que para el nombre de usuario y la contraseña.

Important

No proporcione las claves de acceso a terceros, ni siquiera para que le ayuden a [buscar el ID de usuario canónico](#). Si lo hace, podría conceder a otra persona acceso permanente a su cuenta.

Cuando cree un par de claves de acceso, se le pide que guarde el ID de clave de acceso y la clave de acceso secreta en un lugar seguro. La clave de acceso secreta solo está disponible en el momento de su creación. Si pierde la clave de acceso secreta, debe agregar nuevas claves de acceso a su usuario de IAM. Puede tener un máximo de dos claves de acceso. Si ya cuenta con dos, debe eliminar un par de claves antes de crear uno nuevo. Para consultar las instrucciones, consulte [Administración de claves de acceso](#) en la Guía del usuario de IAM.

Soy administrador y deseo permitir que otros accedan a Amazon VPC

Para permitir que otros accedan a Amazon VPC, debe crear una entidad de IAM (usuario o rol) para la persona o aplicación que necesita acceso. Esta persona utilizará las credenciales de la entidad para acceder a AWS. A continuación, debe asociar una política a la entidad que les conceda los permisos correctos en Amazon VPC.

Para comenzar de inmediato, consulte [Creación del primer grupo y usuario delegado de IAM](#) en la Guía del usuario de IAM.

Quiero permitir que personas ajenas a mi cuenta de AWS accedan a mis recursos de Amazon VPC.

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para saber si Amazon VPC admite estas características, consulte [Cómo funciona Amazon VPC con IAM](#) (p. 241).
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte [Proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario](#) en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos a Cuentas de AWS de terceros, consulte [Proporcionar acceso a Cuentas de AWS que son propiedad de terceros](#) en la Guía del usuario de IAM.

- Para obtener información sobre cómo proporcionar acceso mediante una identidad federada, consulte [Proporcionar acceso a usuarios autenticados externamente \(identidad federada\)](#) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte [Cómo los roles de IAM difieren de las políticas basadas en recursos](#) en la Guía del usuario de IAM.

AWS Políticas administradas por para Amazon Virtual Private Cloud

Para agregar permisos a usuarios, grupos y roles, es más fácil utilizar las políticas administradas por AWS que escribirlas uno mismo. Se necesita tiempo y experiencia para [crear políticas de IAM administradas por el cliente](#) que proporcionen a su equipo solo los permisos necesarios. Para comenzar a hacerlo con rapidez, puede utilizar nuestras políticas administradas por AWS. Estas políticas cubren casos de uso comunes y están disponibles en su cuenta de AWS. Para obtener más información sobre las políticas administradas por AWS, consulte [Políticas administradas por AWS](#) en la Guía del usuario de IAM.

Los servicios de AWS mantienen y actualizan las políticas administradas por AWS. No puede cambiar los permisos en las políticas administradas por AWS. En ocasiones, los servicios agregan permisos adicionales a una política administrada por AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada por AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no quitan permisos de una política administrada por AWS, por lo que las actualizaciones de políticas no deteriorarán los permisos existentes.

Además, AWS admite políticas administradas para funciones de trabajo que abarcan varios servicios. Por ejemplo, la política administrada por `ReadOnlyAccessAWS` proporciona acceso de solo lectura a todos los servicios y los recursos de AWS. Cuando un servicio lanza una nueva característica, AWS agrega permisos de solo lectura para las operaciones y los recursos nuevos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte [Políticas administradas por AWS para funciones de trabajo](#) en la Guía del usuario de IAM.

AWS Política administrada por : `AmazonVPCFullAccess`

Puede adjuntar la política `AmazonVPCFullAccess` a las identidades de IAM. Esta política otorga permisos que brindan acceso completo a Amazon VPC.

Para ver los permisos de esta política, consulte [AmazonVPCFullAccess](#) en la AWS Management Console.

AWS Política administrada por : `AmazonVPCReadOnlyAccess`

Puede adjuntar la política `AmazonVPCReadOnlyAccess` a las identidades de IAM. Esta política otorga permisos que brindan acceso de solo lectura a Amazon VPC.

Para ver los permisos de esta política, consulte [AmazonVPCReadOnlyAccess](#) en la AWS Management Console.

Actualizaciones de Amazon VPC en las políticas administradas por AWS

Es posible consultar los detalles sobre las actualizaciones de las políticas administradas por AWS para Amazon VPC debido a que este servicio comenzó a realizar el seguimiento de estos cambios en marzo de 2021.

Cambio	Descripción	Fecha
the section called “AmazonVPCReadOnlyAccess” (p. 254) : actualización de una política existente	Se agregó la acción <code>DescribeSecurityGroupRules</code> , que permite a un usuario o rol de IAM ver las reglas de los grupos de seguridad .	2 de agosto de 2021
the section called “AmazonVPCFullAccess” (p. 254) : actualización de una política existente	Se agregaron las acciones <code>DescribeSecurityGroupRules</code> y <code>ModifySecurityGroupRules</code> , que permiten a un usuario o rol de IAM ver y modificar las reglas de los grupos de seguridad .	2 de agosto de 2021
the section called “AmazonVPCFullAccess” (p. 254) : actualización de una política existente	Se agregaron acciones para las gateways de operador, los grupos IPv6, las gateways locales y las tablas de enrutamiento de gateways locales.	23 de junio de 2021
the section called “AmazonVPCReadOnlyAccess” (p. 254) : actualización de una política existente	Se agregaron acciones para las gateways de operador, los grupos IPv6, las gateways locales y las tablas de enrutamiento de gateways locales.	23 de junio de 2021

Controlar el tráfico hacia los recursos mediante grupos de seguridad

Un grupo de seguridad actúa como firewall virtual, lo que controla el tráfico al que se permite llegar y dejar los recursos a los que está asociado. Por ejemplo, después de asociar un grupo de seguridad a una instancia de EC2, controla el tráfico de entrada y salida de la instancia.

Al crear una VPC, incluye un grupo de seguridad predeterminado. Puede crear grupos de seguridad adicionales para cada VPC. Puede asociar un grupo de seguridad solo a los recursos de la VPC para la que se creó.

Para cada grupo de seguridad, puede agregar reglas que controlan el tráfico en función de los protocolos y números de puerto. Hay conjuntos de reglas independientes para el tráfico de entrada y el tráfico de salida.

Puede configurar ACL de red con reglas similares a sus grupos de seguridad para añadir una capa de seguridad adicional a su VPC. Para obtener más información acerca de las diferencias entre los grupos de seguridad y las ACL de red, consulte [Comparar grupos de seguridad y ACL de red \(p. 234\)](#).

Contenido

- [Conceptos básicos de los grupos de seguridad \(p. 256\)](#)
- [Grupos de seguridad predeterminados para las VPC \(p. 256\)](#)
- [Reglas del grupo de seguridad \(p. 257\)](#)
- [Trabajar con grupos de seguridad \(p. 259\)](#)

- [Trabajar con reglas de grupos de seguridad \(p. 261\)](#)
- [Administrar de manera centralizada los grupos de seguridad de VPC mediante AWS Firewall Manager \(p. 264\)](#)

Conceptos básicos de los grupos de seguridad

A continuación, se describen las características de los grupos de seguridad:

- Al crear un grupo de seguridad, debe darle un nombre y una descripción. Se aplican las siguientes reglas:
 - El nombre de un grupo de seguridad debe ser único dentro de la VPC.
 - Los nombres y las descripciones pueden tener una longitud máxima de 255 caracteres.
 - Los nombres y las descripciones solo pueden contener los siguientes caracteres: a-z, A-Z, 0-9, espacios y `._-:/()#,@[]+=&:{}!$*`.
 - Cuando el nombre contiene espacios finales, los recortamos. Por ejemplo, si introduce el nombre "Grupo de seguridad de prueba ", se guardará como "Grupo de seguridad de prueba".
 - El nombre del grupo de seguridad no puede comenzar con `sg-`.
- Los grupos de seguridad son grupos con estado. Por ejemplo, si envía una solicitud desde una instancia, se permite el tráfico de respuesta de dicha solicitud para conectar la instancia independientemente de las reglas del grupo de seguridad de entrada. Se permiten las respuestas al tráfico de entrada para dejar la instancia, independientemente de las reglas de salida.
- Se ha establecido una cuota del número de grupos de seguridad que puede crear por cada VPC, al igual que el número de reglas que puede añadir a cada grupo de seguridad y el número de grupos de seguridad que puede asociar a una interfaz de red. Para obtener más información, consulte [Cuotas de Amazon VPC \(p. 378\)](#).

A continuación, se describen las características de las reglas de los grupos de seguridad:

- Puede especificar reglas de permiso, pero no reglas de denegación.
- Cuando se crea un grupo de seguridad, este carece de reglas de entrada. Por lo tanto, no se permitirá el tráfico de entrada hasta que no agregue reglas de entrada al grupo de seguridad.
- La primera vez que crea un grupo de seguridad, este tiene una regla de salida que permite todo el tráfico de salida procedente del recurso. Es posible quitar esta regla y añadir reglas saliente que permitan solo el tráfico saliente específico. Si el grupo de seguridad no tiene reglas de entrada, no se permitirá el tráfico de salida.
- Cuando asocia varios grupos de seguridad a un recurso, las reglas de cada grupo de seguridad se agregan para formar un solo conjunto de reglas utilizadas para determinar si se permite el acceso.
- Cuando se agregan, actualizan o eliminan reglas, los cambios se aplican automáticamente a todos los recursos asociados al grupo de seguridad. El efecto de algunos cambios en las reglas puede depender de cómo se realiza el seguimiento del tráfico. Para obtener más información, consulte [Seguimiento de la conexión](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
- Cuando usted crea una regla de grupo de seguridad, AWS le asigna un ID único. Puede utilizar el ID de una regla cuando utilice la API o la CLI para modificarla o eliminarla.

Grupos de seguridad predeterminados para las VPC

Las VPC predeterminadas y las VPC que cree incluyen un grupo de seguridad predeterminado. Con algunos recursos, si no se asocia un grupo de seguridad al crear el recurso, se asociará el grupo de seguridad predeterminado. Por ejemplo, si no especifica ningún grupo de seguridad al lanzar una instancia de EC2, se asociará el grupo de seguridad predeterminado.

Puede cambiar las reglas de un grupo de seguridad predeterminado. El grupo de seguridad predeterminado no se puede eliminar. Si intenta eliminar el grupo de seguridad predeterminado, aparece el error siguiente: `Client.CannotDelete`.

La tabla siguiente describe las reglas predeterminadas del grupo de seguridad predeterminado.

Inbound			
Fuente	Protocolo	Rango de puerto	Descripción
El ID del grupo de seguridad (su propio ID de recurso)	Todos	Todos	Permite el tráfico de entrada de los recursos asignados al mismo grupo de seguridad.
Outbound			
Destino	Protocolo	Rango de puerto	Descripción
0.0.0.0/0	Todos	Todos	Permite todo el tráfico IPv4 saliente.
::/0	All	All	Allows all outbound IPv6 traffic. This rule is added only if your VPC has an associated IPv6 CIDR block.

Reglas del grupo de seguridad

Las reglas de un grupo de seguridad controlan el tráfico de entrada que puede llegar a los recursos asociados al grupo de seguridad. Las reglas también controlan el tráfico saliente que puede salir de ellos.

Puede añadir o quitar reglas de un grupo de seguridad (este proceso también se conoce como autorización o revocación del acceso entrante o saliente). Las reglas se aplican al tráfico entrante (entrada) o saliente (salida). Puede conceder acceso a un rango de CIDR específico o a otro grupo de seguridad de su VPC o de una VPC del mismo nivel (requiere interconexión de VPC).

Especifique lo siguiente para cada regla:

- Protocolo: el protocolo que se permite. Los protocolos más habituales son 6 (TCP), 17 (UDP) y 1 (ICMP).
- Rango de puertos: para TCP, UDP o un protocolo personalizado, el rango de puertos que se permite. Puede especificar un solo número de puerto (por ejemplo, 22), o bien un rango de números de puertos (por ejemplo, 7000–8000).
- Tipo y código ICMP: para ICMP, el tipo y el código ICMP. Por ejemplo, utilice el tipo 8 para la Echo Request de ICMP o el tipo 128 para la Echo Request de ICMPv6.
- Origen o destino: el origen (reglas de entrada) o el destino (reglas de salida) del tráfico que se va a permitir. Especifique uno de los siguientes valores:
 - Una única dirección IPv4. Debe utilizar la longitud del prefijo /32. Por ejemplo, 203.0.113.1/32.
 - Una única dirección IPv6. Debe utilizar la longitud del prefijo /128. Por ejemplo, 2001:db8:1234:1a00::123/128.
 - Un rango de direcciones IPv4 en notación de bloque de CIDR. Por ejemplo, 203.0.113.0/24.
 - Un rango de direcciones IPv6 en notación de bloque de CIDR. Por ejemplo, 2001:db8:1234:1a00::/64.

- El ID de una lista de prefijos. Por ejemplo, p1-1234abc1234abc123. Para obtener más información, consulte [Agrupar bloques de CIDR mediante listas de prefijos \(p. 70\)](#).
- Identificador de un grupo de seguridad (referido aquí como el grupo de seguridad especificado). Por ejemplo, el grupo de seguridad actual, un grupo de seguridad de la misma VPC o un grupo de seguridad para una VPC interconectada. Esto permite el tráfico en función de las direcciones IP privadas de los recursos asociados al grupo de seguridad especificado. Esto no agrega reglas del grupo de seguridad especificado al grupo de seguridad actual. †
- (Opcional) Descripción: puede añadir una descripción a la regla, que puede ayudarle a identificarla más adelante. Una descripción puede tener una longitud máxima de 255 caracteres. Los caracteres permitidos incluyen a-z, A-Z, 0-9, espacios y . _ - / () # , @ [] + = ; { } ! \$ * .

† Si configura rutas para reenviar el tráfico entre dos instancias en subredes diferentes a través de un dispositivo middlebox, debe asegurarse de que los grupos de seguridad de ambas instancias permitan que el tráfico fluya entre las instancias. El grupo de seguridad de cada instancia debe hacer referencia a la dirección IP privada de la otra instancia, o al rango CIDR de la subred que contiene la otra instancia, como fuente. Si hace referencia al grupo de seguridad de la otra instancia como fuente, esto no permite que el tráfico fluya entre las instancias.

Reglas de ejemplo

Por lo general, las reglas que agregue a un grupo de seguridad dependerá del propósito de este. La tabla siguiente describe reglas de ejemplo de un grupo de seguridad asociado a servidores web. Los servidores web pueden recibir tráfico HTTP y HTTPS de todas las direcciones IPv4 e IPv6 y enviar el tráfico SQL o MySQL a los servidores de la base de datos.

Inbound			
Fuente	Protocolo	Rango de puerto	Descripción
0.0.0.0/0	TCP	80	Permite el acceso HTTP de entrada desde todas las direcciones IPv4
::/0	TCP	80	Allows inbound HTTP access from all IPv6 addresses
0.0.0.0/0	TCP	443	Permite el acceso HTTPS de entrada desde todas las direcciones IPv4
::/0	TCP	443	Allows inbound HTTPS access from all IPv6 addresses
Rango de direcciones IPv4 públicas de su red	TCP	22	Permite el acceso SSH de entrada desde las direcciones IP IPv4 de su red.
Rango de direcciones IPv4 públicas de su red	TCP	3389	Permite el acceso RDP de entrada desde las direcciones IP IPv4 de su red.
Outbound			

Destino	Protocolo	Rango de puerto	Descripción
ID del grupo de seguridad para los servidores de la base de datos de Microsoft SQL Server	TCP	1433	Permite el acceso de Microsoft SQL Server de salida
ID del grupo de seguridad para los servidores de la base de datos MySQL	TCP	3306	Permite el acceso de MySQL de salida

El servidor de la base de datos necesitará un conjunto de reglas diferente. Por ejemplo, en lugar del tráfico HTTP y HTTPS entrante, puede añadir una regla que permita el acceso de MySQL o Microsoft SQL Server entrante. Para ver ejemplos, consulte [Seguridad \(p. 336\)](#). Para obtener más información acerca de los grupos de seguridad para instancias de base de datos de Amazon RDS, consulte [Control de acceso con grupos de seguridad](#) en la Guía del usuario de Amazon RDS.

Para ver otros ejemplos, consulte [Referencia de reglas de grupos de seguridad](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Reglas antiguas de los grupos de seguridad

Si su VPC tiene una conexión de emparejamiento de VPC con otra VPC, o si utiliza una VPC compartida con otra cuenta, la regla del grupo de seguridad puede hacer referencia a otro grupo de seguridad de la VPC del mismo nivel. Esto permite que los recursos asociados al grupo de seguridad al que se hace referencia y los asociados al grupo de seguridad que hace la referencia se comuniquen entre sí.

Si se elimina el grupo de seguridad de la VPC compartida o si se elimina la conexión de emparejamiento de VPC, la regla del grupo de seguridad se marca como obsoleta. Las reglas obsoletas de los grupos de seguridad se pueden eliminar de la misma manera que cualquier otra regla del grupo de seguridad. Para obtener más información, consulte [Trabajo con reglas de grupo de seguridad obsoletas](#) en la Guía de interconexión de Amazon VPC.

Trabajar con grupos de seguridad

Las siguientes tareas muestran cómo usar grupos de seguridad con la consola de Amazon VPC.

Permisos necesarios

- [Administrar grupos de seguridad \(p. 248\)](#)

Tareas

- [Crear un grupo de seguridad \(p. 259\)](#)
- [Ver los grupos de seguridad \(p. 260\)](#)
- [Etiquetar los grupos de seguridad \(p. 261\)](#)
- [Eliminación de un grupo de seguridad \(p. 261\)](#)

Crear un grupo de seguridad

De forma predeterminada, los grupos de seguridad nuevos comienzan con una única regla de salida que permite que todo el tráfico salga del recurso. Debe añadir reglas para permitir el tráfico entrante o restringir el tráfico saliente.

El grupo de seguridad solo se puede utilizar en la VPC para la que se creó.

Para obtener información sobre los permisos necesarios para crear grupos de seguridad y administrar las reglas de los grupos de seguridad, consulte [Administrar grupos de seguridad \(p. 248\)](#) y [Administración de reglas de grupos de seguridad \(p. 249\)](#).

Para crear un grupo de seguridad con la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Elija Create Security Group (Crear grupo de seguridad).
4. Ingrese un nombre y una descripción para el grupo de seguridad. No puede cambiar el nombre ni la descripción de un grupo de seguridad después de crearlo.
5. En VPC, elija la VPC.
6. Puede agregar reglas de grupo de seguridad ahora o más adelante. Para obtener más información, consulte [Agregar reglas a un grupo de seguridad \(p. 262\)](#).
7. Puede agregar etiquetas ahora o más adelante. Para agregar una etiqueta, elija Add new tag (Agregar nueva etiqueta) y, a continuación, ingrese la clave y el valor de la etiqueta.
8. Elija Create Security Group (Crear grupo de seguridad).

Para crear un grupo de seguridad con la línea de comandos

- [create-security-group](#) (AWS CLI)
- [New-EC2SecurityGroup](#) (AWS Tools for Windows PowerShell)

Ver los grupos de seguridad

Puede ver información acerca de sus grupos de seguridad de la siguiente manera.

Para obtener más información sobre los permisos necesarios para visualizar los grupos de seguridad, consulte [Administrar grupos de seguridad \(p. 248\)](#).

Para ver los grupos de seguridad mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Los grupos de seguridad aparecen en la lista. Para ver los detalles de un grupo de seguridad específico, incluidas sus reglas de entrada y salida, elija el grupo de seguridad.

Para ver los grupos de seguridad mediante la línea de comandos

- [describe-security-groups](#) y [describe-security-group-rules](#) (AWS CLI)
- [Get-EC2SecurityGroup](#) y [Get-EC2SecurityGroupRules](#) (AWS Tools for Windows PowerShell)

Para ver todos los grupos de seguridad en las regiones

Abra la consola de Amazon EC2 Global View en <https://console.aws.amazon.com/ec2globalview/home>.

Para obtener más información acerca del uso de Amazon EC2 Global View, consulte [Enumerar y filtrar recursos mediante Amazon EC2 Global View](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Etiquetar los grupos de seguridad

Añada etiquetas a sus recursos para organizarlos e identificarlos mejor, por ejemplo, por objetivo, propietario o entorno. Puede agregar etiquetas a sus grupos de seguridad. Las claves de las etiquetas deben ser únicas para cada grupo de seguridad. Si agrega una etiqueta con una clave que ya está asociada a la regla, se actualiza el valor de esa etiqueta.

Para etiquetar un grupo de seguridad mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Seleccione la casilla de verificación del grupo de seguridad.
4. Elija Actions (Acciones) y, a continuación, Manage tags (Administrar etiquetas).
5. La página Manage tags (Administrar etiquetas) muestra las etiquetas que están asignadas al grupo de seguridad. Para agregar una etiqueta, elija Add tag (Agregar etiqueta) e ingrese la clave y el valor de la etiqueta. Para eliminar una etiqueta, elija Remove (Eliminar) junto a la etiqueta que desee eliminar.
6. Elija Save changes.

Para etiquetar un grupo de seguridad mediante la línea de comandos

- [create-tags](#) (AWS CLI)
- [New-EC2Tag](#) (AWS Tools for Windows PowerShell)

Eliminación de un grupo de seguridad

Puede eliminar un grupo de seguridad solo si no está asociado a ninguna instancia. El grupo de seguridad predeterminado no se puede eliminar.

Si está utilizando la consola, puede eliminar más de un grupo de seguridad a la vez. Si utiliza la línea de comandos o la API, solo podrá eliminar un grupo de seguridad a la vez.

Para eliminar un grupo de seguridad con la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Seleccione uno o más grupos de seguridad y elija Actions (Acciones) y Delete security groups (Eliminar grupos de seguridad).
4. Cuando se le pida confirmación, ingrese **delete** y elija Delete (Eliminar).

Para eliminar un grupo de seguridad con la línea de comandos

- [delete-security-group](#) (AWS CLI)
- [Remove-EC2SecurityGroup](#) (AWS Tools for Windows PowerShell)

Trabajar con reglas de grupos de seguridad

Las siguientes tareas muestran cómo usar reglas de grupos de seguridad con la consola de Amazon VPC.

Permisos necesarios

- [Administración de reglas de grupos de seguridad \(p. 249\)](#)

Tareas

- [Agregar reglas a un grupo de seguridad \(p. 262\)](#)
- [Actualizar reglas de los grupos de seguridad \(p. 263\)](#)
- [Etiquete las reglas de los grupos de seguridad \(p. 263\)](#)
- [Eliminar las reglas de un grupo de seguridad \(p. 264\)](#)

Agregar reglas a un grupo de seguridad

Al agregar una regla a un grupo de seguridad, la nueva regla se aplica automáticamente a cualquier recurso asociado al grupo de seguridad.

Si tiene una interconexión de VPC, podrá hacer referencia a grupos de seguridad de la VPC del mismo nivel como origen o destino en sus reglas de grupo de seguridad. Para obtener más información, consulte [Actualizar los grupos de seguridad para que hagan referencia a grupos de seguridad de VPC del mismo nivel](#) en la Guía de interconexión de Amazon VPC.

Para obtener más información sobre los permisos necesarios para administrar las reglas de los grupos de seguridad, consulte [Administración de reglas de grupos de seguridad \(p. 249\)](#).

Para agregar una regla a través de la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Seleccione el grupo de seguridad.
4. Elija Actions (Acciones), Edit inbound rules (Editar reglas de entrada) o Actions (Acciones), Edit outbound rules (Editar reglas de salida).
5. Para cada regla, elija Add Rule (Agregar regla) y realice lo siguiente.
 - a. En Type (Tipo), elija el tipo de protocolo que desea permitir.
 - Para TCP o UDP, debe ingresar el rango de puertos que va a permitir.
 - Para el protocolo ICMP personalizado, debe elegir el nombre del tipo de ICMP en Protocol (Protocolo) y, si se aplica, el nombre del código en Port Range (Rango de puertos).
 - Si elige cualquier otro tipo, el protocolo y el rango de puertos se configurarán de forma automática.
 - b. Para Source (Origen) (reglas de entrada) o Destination (Destino) (reglas de salida), realice alguna de las siguientes acciones para permitir el tráfico:
 - Elija Custom (Personalizado) y, a continuación, ingrese una dirección IP en notación CIDR, un bloque de CIDR, otro grupo de seguridad o una lista de prefijos.
 - Elija Anywhere (Cualquier lugar) para permitir el tráfico de cualquier dirección IP (reglas de entrada) o para permitir que el tráfico llegue a todas las direcciones IP (reglas de salida). Esto agrega automáticamente una regla para el bloque de CIDR IPv4 0.0.0.0/0.

Si el grupo de seguridad está en una VPC habilitada para IPv6, esto agregará automáticamente una regla para el bloque de CIDR IPv6 ::/0.

En el caso de las reglas de entrada, esta opción es aceptable para un periodo corto en un entorno de prueba, pero no es seguro en los entornos de producción. En entornos de producción, autorice el acceso a una dirección IP específica o a un rango de direcciones IP.

 - Elija My IP (Mi IP) para permitir solo el tráfico entrante (reglas de entrada) o saliente (reglas de salida) de la dirección IPv4 pública de su computadora local.
 - c. En Description (Descripción), especifique una breve descripción de la regla.

6. Seleccione Save rules (Guardar reglas).

Para añadir una regla a un grupo de seguridad con la línea de comandos

- [authorize-security-group-ingress](#) y [authorize-security-group-egress](#) (AWS CLI)
- [Grant-EC2SecurityGroupIngress](#) y [Grant-EC2SecurityGroupEgress](#) (AWS Tools for Windows PowerShell)

Actualizar reglas de los grupos de seguridad

Cuando actualiza una regla, esta se aplica automáticamente a todos los recursos asociados al grupo de seguridad.

Para obtener más información sobre los permisos necesarios para administrar las reglas de los grupos de seguridad, consulte [Administración de reglas de grupos de seguridad](#) (p. 249).

Para actualizar una regla a través de la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Seleccione el grupo de seguridad.
4. Elija Actions (Acciones), Edit inbound rules (Editar reglas de entrada) o Actions (Acciones), Edit outbound rules (Editar reglas de salida).
5. Actualice la regla según sea necesario.
6. Seleccione Save rules (Guardar reglas).

Para actualizar la descripción de una regla de grupo de seguridad con la línea de comandos

- [modify-security-group-rules](#), [update-security-group-rule-descriptions-ingress](#) y [update-security-group-rule-descriptions-egress](#) (AWS CLI)
- [Update-EC2SecurityGroupRuleIngressDescription](#) y [Update-EC2SecurityGroupRuleEgressDescription](#) (AWS Tools for Windows PowerShell)

Etiquete las reglas de los grupos de seguridad

Añada etiquetas a sus recursos para organizarlos e identificarlos mejor, por ejemplo, por objetivo, propietario o entorno. Puede agregar etiquetas a las reglas de los grupos de seguridad. Las claves de las etiquetas deben ser únicas para cada regla de grupo de seguridad. Si agrega una etiqueta con una clave que ya está asociada a la regla del grupo de seguridad, se actualizará el valor de esa etiqueta.

Para etiquetar una regla mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Seleccione el grupo de seguridad.
4. En la pestaña Inbound rules (Reglas de entrada) o Outbound rules (Reglas de salida), seleccione la casilla de verificación correspondiente a la regla y, luego, elija Manage tags (Administrar etiquetas).
5. La página Manage tags (Administrar etiquetas) muestra las etiquetas asignadas a la regla. Para agregar una etiqueta, elija Add tag (Agregar etiqueta) e ingrese la clave y el valor de la etiqueta. Para eliminar una etiqueta, elija Remove (Eliminar) junto a la etiqueta que desee eliminar.
6. Elija Save changes.

Para etiquetar una regla mediante la línea de comandos

- [create-tags](#) (AWS CLI)
- [New-EC2Tag](#) (AWS Tools for Windows PowerShell)

Eliminar las reglas de un grupo de seguridad

Al eliminar una regla de un grupo de seguridad, el cambio se aplica de forma automática a toda instancia asociada al grupo de seguridad.

Para eliminar una regla del grupo de seguridad desde la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Seleccione el grupo de seguridad.
4. Seleccione Actions (Acciones) y, a continuación, elija Edit inbound rules (Editar reglas de entrada) para eliminar una regla de entrada o Edit outbound rules (Editar reglas de salida) para eliminar una regla de salida.
5. Presione el botón Delete (Eliminar), que se encuentra junto a la regla que desea eliminar.
6. Seleccione Save rules (Guardar reglas).

Para eliminar una regla de un grupo de seguridad mediante la línea de comandos

- [revoke-security-group-ingress](#) y [revoke-security-group-egress](#)(AWS CLI)
- [Revoke-EC2SecurityGroupIngress](#) y [Revoke-EC2SecurityGroupEgress](#) (AWS Tools for Windows PowerShell)

Administrar de manera centralizada los grupos de seguridad de VPC mediante AWS Firewall Manager

AWS Firewall Manager simplifica las tareas de administración y mantenimiento de los grupos de seguridad de la VPC en varias cuentas y recursos. Con Firewall Manager, puede configurar y auditar los grupos de seguridad de su organización desde una única cuenta de administrador central. Firewall Manager aplica automáticamente las reglas y las protecciones en todas las cuentas y recursos, incluso cuando se agregan recursos nuevos. Firewall Manager es especialmente útil cuando se desea proteger a toda la organización o si se agregan con frecuencia nuevos recursos que se desea proteger desde una cuenta de administrador central.

Puede utilizar Firewall Manager para administrar de forma centralizada grupos de seguridad de las siguientes maneras:

- Configurar grupos de seguridad de referencia común en toda la organización: puede utilizar una política de grupo de seguridad común para proporcionar una asociación controlada centralmente de grupos de seguridad con cuentas y recursos de toda la organización. Especifique dónde y cómo aplicar la política en su organización.
- Auditar grupos de seguridad existentes en la organización: puede utilizar una política de grupos de seguridad de auditoría para comprobar las reglas existentes que están en uso en los grupos de seguridad de la organización. Puede definir el alcance de la política para auditar todas las cuentas, cuentas específicas o recursos etiquetados dentro de la organización. Firewall Manager detecta automáticamente nuevas cuentas y recursos y los audita. Puede crear reglas de auditoría para establecer límites sobre qué reglas de grupo de seguridad permitir o no permitir dentro de la organización y para comprobar si hay grupos de seguridad no utilizados o redundantes.

- Obtener informes sobre recursos no conformes y remediarlo: puede obtener informes y alertas de recursos no conformes para sus políticas de referencia y de auditoría. También puede establecer flujos de trabajo de corrección automática para corregir cualquier recurso no compatible que Firewall Manager detecte.

Para obtener más información acerca del uso de Firewall Manager para administrar los grupos de seguridad, consulte los siguientes temas de la Guía para desarrolladores de AWS WAF:

- [AWS Firewall Manager Requisitos previos de](#)
- [Introducción a las políticas de grupos de seguridad de Amazon VPC de AWS Firewall Manager](#)
- [Cómo funcionan las políticas de grupos de seguridad en AWS Firewall Manager](#)
- [Casos de uso de políticas de grupos de seguridad](#)

Resiliencia en Amazon Virtual Private Cloud

La infraestructura global de AWS se compone de regiones y zonas de disponibilidad de AWS. Las regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes de baja latencia y con un alto nivel de rendimiento y redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las zonas de disponibilidad y las regiones de AWS, consulte [Infraestructura global de AWS](#).

Además de la infraestructura global de AWS, Amazon VPC ofrece varias características que le ayudan con sus necesidades de resiliencia y copia de seguridad de los datos.

- [Opciones de conectividad de Amazon VPC a Amazon VPC](#)
- [Opciones de conectividad de red a Amazon VPC](#)

Validación de conformidad para Amazon Virtual Private Cloud

Audidores externos evalúan la seguridad y la conformidad de los Servicios de AWS como parte de varios programas de conformidad de AWS, como SOC, PCI, FedRAMP e HIPAA.

Para saber si Amazon VPC u otros Servicios de AWS están incluidos en el ámbito de programas de conformidad específicos, consulte [Servicios de AWS en el ámbito del programa de conformidad](#). Para obtener información general, consulte [Programas de conformidad de AWS](#).

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#).

Su responsabilidad de conformidad al utilizar Servicios de AWS se determina en función de la sensibilidad de los datos, los objetivos de cumplimiento de su empresa y la legislación y los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- [Guías de inicio rápido de seguridad y conformidad](#): en estas guías de implementación, se analizan consideraciones de arquitectura y se proporcionan los pasos para implementar entornos de base de referencia AWS que se centren en la seguridad y conformidad.

- [Documento técnico sobre arquitectura para seguridad y conformidad de HIPAA](#): en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones aptas para HIPAA.

Note

No todos los Servicios de AWS son aptos para HIPAA. Para obtener más información, consulte la [Referencia de servicios aptos para HIPAA](#).

- [Recursos de conformidad de AWS](#): este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- [Evaluación de recursos con reglas](#) en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- [AWS Security Hub](#): este Servicio de AWS proporciona una vista integral de su estado de seguridad en AWS que lo ayuda a verificar la conformidad con los estándares y las prácticas recomendadas del sector de seguridad.
- [AWS Audit Manager](#): este Servicio de AWS le ayuda a auditar continuamente el uso de AWS con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

Configuración y análisis de vulnerabilidades en Amazon Virtual Private Cloud

La configuración y los controles de TI son una responsabilidad compartida entre AWS y usted, nuestro cliente. Para obtener más información, consulte el [modelo de responsabilidad compartida](#) de AWS. Además del modelo de responsabilidad compartida, los usuarios de VPC deben tener en cuenta lo siguiente:

- Es responsabilidad del cliente colocar parches a sus aplicaciones cliente con las dependencias relevantes del lado del cliente.
- Los clientes deben considerar la posibilidad de realizar pruebas de penetración para gateways NAT e instancias EC2 (consulte [Pruebas de penetración](#)/).

Prácticas recomendadas de seguridad de la VPC

Las siguientes prácticas recomendadas son directrices generales y no suponen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

Las siguientes son prácticas recomendadas generales:

- Utilice varias implementaciones de zonas de disponibilidad para disfrutar de una alta disponibilidad.
- Utilice grupos de seguridad y ACL de red. Para obtener más información, consulte [Controlar el tráfico hacia los recursos mediante grupos de seguridad \(p. 255\)](#) y [Controlar el tráfico hacia las subredes utilizando las ACL de red \(p. 120\)](#).
- Utilice políticas de IAM para controlar el acceso.
- Utilice Amazon CloudWatch para monitorear los componentes de VPC y las conexiones de VPN.
- Use registros de flujo de la VPC para capturar información acerca del tráfico IP entrante y saliente de las interfaces de red en su VPC. Para obtener más información, consulte [Registro del tráfico de IP con registros de flujo de la VPC \(p. 197\)](#).

Recursos adicionales

- Administre el acceso a los recursos y las API de AWS mediante identidad federada, usuarios de IAM y roles de IAM. Defina políticas y procedimientos de administración de credenciales para crear, distribuir, rotar y revocar credenciales de acceso de AWS. Para obtener más información, consulte [Prácticas recomendadas de IAM](#) en la Guía del usuario de IAM.
- Para obtener respuestas a las preguntas frecuentes sobre seguridad de VPC, consulte [Preguntas frecuentes de Amazon VPC](#).

Tutoriales

En los siguientes tutoriales, aprenderá a crear VPC mediante el uso de tutoriales paso a paso basados en casos de uso.

Contenido

- [Tutoriales sobre el uso de la AWS CLI \(p. 268\)](#)
- [Tutoriales sobre el uso de AWS Management Console \(p. 291\)](#)

Tutoriales sobre el uso de la AWS CLI

En los siguientes tutoriales, se explica cómo crear VPC mediante la AWS CLI.

Contenido

- [Crear subredes y una VPC habilitada para IPv4 mediante la AWS CLI \(p. 268\)](#)
- [Para crear subredes y una VPC de doble pila mediante la AWS CLI \(p. 273\)](#)
- [Crear una VPC con IPv6 habilitado y subredes con solo IPv6 mediante la AWS CLI \(p. 282\)](#)

Crear subredes y una VPC habilitada para IPv4 mediante la AWS CLI

El siguiente ejemplo utiliza comandos de AWS CLI para crear una VPC no predeterminada con un bloque de CIDR de IPv4, y una subred privada y una pública en la VPC. Tras haber creado la VPC y las subredes, puede lanzar una instancia en la subred pública y conectarse a esta. Para comenzar, primero debe instalar y configurar la AWS CLI. Para obtener más información, consulte [Instalación de la AWS CLI](#).

Crearé los siguientes recursos de AWS:

- Una VPC
- Dos subredes
- Una gateway de Internet
- Una tabla de enrutamiento
- Una instancia EC2.

Tareas

- [Paso 1: Crear una VPC y subredes \(p. 268\)](#)
- [Paso 2: Hacer pública una subred \(p. 269\)](#)
- [Paso 3: Lanzar una instancia en su subred \(p. 271\)](#)
- [Paso 4: Limpieza \(p. 272\)](#)

Paso 1: Crear una VPC y subredes

El primer paso es crear una VPC y dos subredes. Este ejemplo utiliza el bloque de CIDR 10.0.0.0/16 para la VPC, pero puede elegir un bloque de CIDR distinto. Para obtener más información, consulte [Ajuste de tamaño de la VPC \(p. 16\)](#).

Para crear una VPC y las subredes utilizando la AWS CLI

1. Cree una VPC con un bloque de CIDR 10.0.0.0/16 mediante el siguiente comando [create-vpc](#).

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --query Vpc.VpcId --output text
```

El comando devuelve el ID de la nueva VPC. A continuación, se muestra un ejemplo.

```
vpc-2f09a348
```

2. Utilizando el ID de VPC del paso anterior, cree una subred con un bloque de CIDR 10.0.1.0/24 utilizando el siguiente comando [create-subnet](#).

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.1.0/24
```

3. Cree una segunda subred en su VPC con un bloque de CIDR 10.0.0.0/24.

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.0.0/24
```

Paso 2: Hacer pública una subred

Una vez que cree la VPC y las subredes, puede hacer que una de las subredes sea pública; para ello, adjunte una gateway de Internet a su VPC, cree una tabla de enrutamiento personalizada y configure el enrutamiento de la subred a la gateway de Internet.

Para convertir su subred en una subred pública

1. Cree una gateway de Internet mediante el siguiente comando [create-internet-gateway](#).

```
aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --output text
```

El comando devuelve el ID de la nueva gateway de Internet. A continuación, se muestra un ejemplo.

```
igw-1ff7a07b
```

2. Con el ID del paso anterior, adjunte la gateway de Internet a su VPC mediante el siguiente comando [attach-internet-gateway](#).

```
aws ec2 attach-internet-gateway --vpc-id vpc-2f09a348 --internet-gateway-id igw-1ff7a07b
```

3. Cree una tabla de enrutamiento personalizada para la VPC mediante el siguiente comando [create-route-table](#).

```
aws ec2 create-route-table --vpc-id vpc-2f09a348 --query RouteTable.RouteTableId --output text
```

El comando devuelve el ID de la nueva tabla de enrutamiento. A continuación, se muestra un ejemplo.

```
rtb-c1c8faa6
```

4. Cree una ruta en la tabla de enrutamiento que apunte todo el tráfico (0.0.0.0/0) a la gateway de Internet utilizando el siguiente comando [create-route](#).

```
aws ec2 create-route --route-table-id rtb-c1c8faa6 --destination-cidr-block 0.0.0.0/0  
--gateway-id igw-1ff7a07b
```

5. (Opcional) Para confirmar que la ruta se ha creado y está activa, puede describir la tabla de enrutamiento mediante el siguiente comando [describe-route-tables](#).

```
aws ec2 describe-route-tables --route-table-id rtb-c1c8faa6
```

```
{  
  "RouteTables": [  
    {  
      "Associations": [],  
      "RouteTableId": "rtb-c1c8faa6",  
      "VpcId": "vpc-2f09a348",  
      "PropagatingVgws": [],  
      "Tags": [],  
      "Routes": [  
        {  
          "GatewayId": "local",  
          "DestinationCidrBlock": "10.0.0.0/16",  
          "State": "active",  
          "Origin": "CreateRouteTable"  
        },  
        {  
          "GatewayId": "igw-1ff7a07b",  
          "DestinationCidrBlock": "0.0.0.0/0",  
          "State": "active",  
          "Origin": "CreateRoute"  
        }  
      ]  
    }  
  ]  
}
```

6. La tabla de ruteo no está asociada actualmente a ninguna subred. Debe asociarla a una subred de su VPC para que el tráfico de esa subred se dirccione a la gateway de Internet. Utilice el siguiente comando [describe-subnets](#) para obtener los ID de subred. La opción `--filter` restringe las subredes solo a su nueva VPC, y la opción `--query` devuelve solo los ID de la subred y sus bloques de CIDR.

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-2f09a348" --query  
"Subnets[*].{ID:SubnetId,CIDR:CidrBlock}"
```

```
[  
  {  
    "CIDR": "10.0.1.0/24",  
    "ID": "subnet-b46032ec"  
  },  
  {  
    "CIDR": "10.0.0.0/24",  
    "ID": "subnet-a46032fc"  
  }  
]
```

7. Puede elegir qué subred asociar a la tabla de enrutamiento personalizada, por ejemplo, `subnet-b46032ec` y asociarlo usando el comando [associate-route-table](#). Esta subred es su subred pública.

```
aws ec2 associate-route-table --subnet-id subnet-b46032ec --route-table-id rtb-  
c1c8faa6
```

8. (Opcional) Puede modificar el comportamiento de la dirección IP pública de su subred para que una instancia lanzada en la subred reciba automáticamente una dirección IP pública utilizando el siguiente comando [modify-subnet-attribute](#). En caso contrario, asocie una dirección IP elástica a su instancia después del lanzamiento, para que sea accesible desde Internet.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-b46032ec --map-public-ip-on-launch
```

Paso 3: Lanzar una instancia en su subred

Para comprobar que la subred es pública y que las instancias de la subred son accesibles desde Internet, lance una instancia en la subred pública y conéctese a ella. En primer lugar, debe crear un grupo de seguridad que asociar a su instancia, así como un par de claves para conectar a su instancia. Para obtener más información acerca de los grupos de seguridad, consulte [Controlar el tráfico hacia los recursos mediante grupos de seguridad \(p. 255\)](#). Para obtener más información sobre pares de claves, consulte [Pares de claves de Amazon EC2](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Para lanzar una instancia y conectarse a esta en su subred pública

1. Cree un par de claves denominado y utilice la opción `--query` y la opción de texto `--output` para transferir su clave privada directamente a un archivo con extensión `.pem`.

```
aws ec2 create-key-pair --key-name MyKeyPair --query "KeyMaterial" --output text  
> MyKeyPair.pem
```

En este ejemplo, se lanza una instancia de Amazon Linux. Si va a usar un cliente SSH en un sistema operativo Linux o Mac OS X para conectarse a su instancia, utilice el comando a continuación para establecer los permisos de su archivo de clave privada de manera que solo usted pueda leerlo.

```
chmod 400 MyKeyPair.pem
```

2. Cree un grupo de seguridad en su VPC mediante el comando [create-security-group](#).

```
aws ec2 create-security-group --group-name SSHAccess --description "Security group for SSH access" --vpc-id vpc-2f09a348
```

```
{  
  "GroupId": "sg-e1fb8c9a"  
}
```

Agregue una regla que permita obtener acceso a SSH desde cualquier lugar mediante el comando [authorize-security-group-ingress](#).

```
aws ec2 authorize-security-group-ingress --group-id sg-e1fb8c9a --protocol tcp --  
port 22 --cidr 0.0.0.0/0
```

Note

Si utiliza `0.0.0.0/0`, permitirá que todas las direcciones IPv4 tengan acceso a su instancia mediante SSH. Esto es aceptable para este breve ejercicio, pero, en la producción, autorice solo una dirección IP específica o un rango de direcciones.

3. Lance una instancia en su subred pública, utilizando el grupo de seguridad y el par de claves que ha creado. En la salida, anote el ID de su instancia.

```
aws ec2 run-instances --image-id ami-a4827dc9 --count 1 --instance-type t2.micro --key-name MyKeyPair --security-group-ids sg-e1fb8c9a --subnet-id subnet-b46032ec
```

Note

En este ejemplo, la AMI es una AMI de Amazon Linux de la región EE. UU. Este (Norte de Virginia). Si se encuentra en una región diferente, necesitará el ID de la AMI para una AMI adecuada en su región. Para obtener más información, consulte [Búsqueda de una AMI de Linux](#) en la guía del usuario de instancias de Linux de Amazon EC2.

4. Su instancia debe tener el estado `running` para poder conectarse a ella. Utilice el siguiente comando para describir el estado y la dirección IP de la instancia.

```
aws ec2 describe-instances --instance-id i-0146854b7443af453 --query "Reservations[*].Instances[*].{State:State.Name,Address:PublicIpAddress}"
```

A continuación, se muestra un ejemplo del resultado.

```
[
  [
    {
      "State": "running",
      "Address": "52.87.168.235"
    }
  ]
]
```

5. Si su instancia se encuentra en estado de ejecución, puede conectarse a ella utilizando un cliente SSH en un equipo Linux o Mac OS X con el siguiente comando:

```
ssh -i "MyKeyPair.pem" ec2-user@52.87.168.235
```

Si se conecta desde un equipo Windows, utilice las siguientes instrucciones: [Conexión a la instancia de Linux desde Windows utilizando PuTTY](#).

Paso 4: Limpieza

Una vez haya verificado que puede conectarse a su instancia, puede terminarla si ya no la necesita. Para ello, utilice el comando `terminate-instances`. Para eliminar los otros recursos que ha creado en este ejemplo, utilice los siguientes comandos según el orden enumerado:

1. Eliminación de su grupo de seguridad:

```
aws ec2 delete-security-group --group-id sg-e1fb8c9a
```

2. Eliminación de sus subredes:

```
aws ec2 delete-subnet --subnet-id subnet-b46032ec
```

```
aws ec2 delete-subnet --subnet-id subnet-a46032fc
```

3. Eliminación de su tabla de ruteo personalizada:

```
aws ec2 delete-route-table --route-table-id rtb-c1c8faa6
```

4. Separación de la gateway de Internet de la VPC:

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-1ff7a07b --vpc-id vpc-2f09a348
```

5. Eliminación de su gateway de Internet:

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-1ff7a07b
```

6. Eliminación de su VPC:

```
aws ec2 delete-vpc --vpc-id vpc-2f09a348
```

Para crear subredes y una VPC de doble pila mediante la AWS CLI

En el siguiente ejemplo, se utilizan comandos de la AWS CLI para crear una VPC no determinada con un bloque de CIDR de IPv6, una subred pública y una subred privada solo con acceso de salida a Internet. Tras haber creado la VPC y las subredes, puede lanzar una instancia en la subred pública y conectarse a esta. Puede lanzar una instancia en su subred privada y verificar que se puede conectar a Internet. Para comenzar, primero debe instalar y configurar la AWS CLI. Para obtener más información, consulte [Instalación de la AWS CLI](#).

Creará los siguientes recursos de AWS:

- Una VPC
- Dos subredes
- Una gateway de Internet
- Una tabla de enrutamiento
- Una instancia EC2.

Tareas

- [Paso 1: Crear una VPC y subredes \(p. 273\)](#)
- [Paso 2: Configurar una subred pública \(p. 274\)](#)
- [Paso 3: Configurar una subred privada de solo salida \(p. 276\)](#)
- [Paso 4: Modificar el comportamiento de las direcciones IPv6 de las subredes \(p. 277\)](#)
- [Paso 5: Lanzar una instancia en su subred pública \(p. 277\)](#)
- [Paso 6: Lanzar una instancia en su subred privada \(p. 279\)](#)
- [Paso 7: Limpieza \(p. 281\)](#)

Paso 1: Crear una VPC y subredes

El primer paso es crear una VPC y dos subredes. Este ejemplo utiliza el bloque de CIDR IPv4 10.0.0.0/16 para la VPC, pero puede elegir un bloque de CIDR distinto. Para obtener más información, consulte [Ajuste de tamaño de la VPC \(p. 16\)](#).

Para crear una VPC y las subredes utilizando la AWS CLI

1. Cree una VPC con un bloque de CIDR 10.0.0.0/16 y asocie un bloque de CIDR IPv6 a la VPC.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --amazon-provided-ipv6-cidr-block
```

En el documento de salida devuelto, busque y anote el ID de la VPC.

```
{
  "Vpc": {
    "VpcId": "vpc-2f09a348",
    ...
  }
}
```

2. Describa su VPC para obtener el bloque de CIDR IPv6 asociado a la VPC.

```
aws ec2 describe-vpcs --vpc-id vpc-2f09a348
```

```
{
  "Vpcs": [
    {
      ...
      "Ipv6CidrBlockAssociationSet": [
        {
          "Ipv6CidrBlock": "2001:db8:1234:1a00::/56",
          "AssociationId": "vpc-cidr-assoc-17a5407e",
          "Ipv6CidrBlockState": {
            "State": "ASSOCIATED"
          }
        }
      ],
      ...
    }
  ]
}
```

3. Cree una subred con un bloque de CIDR IPv4 10.0.0.0/24 y un bloque de CIDR IPv6 2001:db8:1234:1a00::/64 (de los rangos devueltos en el paso anterior).

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.0.0/24 --ipv6-cidr-block 2001:db8:1234:1a00::/64
```

4. Cree una segunda subred en su VPC con un bloque de CIDR IPv4 10.0.1.0/24 y un bloque de CIDR IPv6 2001:db8:1234:1a01::/64.

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --cidr-block 10.0.1.0/24 --ipv6-cidr-block 2001:db8:1234:1a01::/64
```

Paso 2: Configurar una subred pública

Una vez que cree la VPC y las subredes, puede hacer que una de las subredes sea pública; para ello, adjunte una gateway de Internet a su VPC, cree una tabla de enrutamiento personalizada y configure el enrutamiento de la subred a la gateway de Internet. En este ejemplo, se crea una tabla de enrutamiento que dirige todo el tráfico IPv4 e IPv6 a una gateway de Internet.

Para convertir su subred en una subred pública

1. Cree una gateway de Internet.

```
aws ec2 create-internet-gateway
```

Tome nota del ID de la gateway de Internet que aparece en el documento de salida que se devuelve.

```
{
```



```
"InternetGateway": {  
  ...  
  "InternetGatewayId": "igw-1ff7a07b",  
  ...  
}
```

2. Con el ID del paso anterior, adjunte la gateway de Internet a la VPC.

```
aws ec2 attach-internet-gateway --vpc-id vpc-2f09a348 --internet-gateway-  
id igw-1ff7a07b
```

3. Cree una tabla de ruteo personalizada para su VPC.

```
aws ec2 create-route-table --vpc-id vpc-2f09a348
```

En el documento de salida devuelto, busque y anote el ID de la tabla de ruteo.

```
{  
  "RouteTable": {  
    ...  
    "RouteTableId": "rtb-c1c8faa6",  
    ...  
  }  
}
```

4. Cree una ruta en la tabla de enrutamiento que apunte todo el tráfico IPv6 (:: /0) a la gateway de Internet.

```
aws ec2 create-route --route-table-id rtb-c1c8faa6 --destination-ipv6-cidr-block ::/0  
--gateway-id igw-1ff7a07b
```

Note

Si su intención es utilizar la subred pública también para el tráfico IPv4, debe agregar otra ruta para el tráfico 0.0.0.0/0 que apunte a la gateway de Internet.

5. Para asegurarse de que su ruta se ha creado y está activa, puede describir la tabla de ruteo y ver los resultados.

```
aws ec2 describe-route-tables --route-table-id rtb-c1c8faa6
```

```
{  
  "RouteTables": [  
    {  
      "Associations": [],  
      "RouteTableId": "rtb-c1c8faa6",  
      "VpcId": "vpc-2f09a348",  
      "PropagatingVgws": [],  
      "Tags": [],  
      "Routes": [  
        {  
          "GatewayId": "local",  
          "DestinationCidrBlock": "10.0.0.0/16",  
          "State": "active",  
          "Origin": "CreateRouteTable"  
        },  
        {  
          "GatewayId": "local",  
          "Origin": "CreateRouteTable",  
          ...  
        }  
      ]  
    }  
  ]  
}
```

```
        "State": "active",
        "DestinationIpv6CidrBlock": "2001:db8:1234:1a00::/56"
      },
      {
        "GatewayId": "igw-1ff7a07b",
        "Origin": "CreateRoute",
        "State": "active",
        "DestinationIpv6CidrBlock": ":::/0"
      }
    ]
  }
}
```

6. La tabla de ruteo no está asociada actualmente a ninguna subred. Asíciela a una subred de su VPC para que el tráfico de esa subred se dirija a la gateway de Internet. En primer lugar, describa sus subredes para obtener sus ID. Puede utilizar la opción `--filter` para devolver las subredes solo a su nueva VPC, y la opción `--query` para devolver solo los ID de la subred y sus bloques de CIDR IPv4 e IPv6.

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-2f09a348" --query
  "Subnets[*].
  {ID:SubnetId,IPv4CIDR:CidrBlock,IPv6CIDR:Ipv6CidrBlockAssociationSet[*].Ipv6CidrBlock}"
```

```
[
  {
    "IPv6CIDR": [
      "2001:db8:1234:1a00::/64"
    ],
    "ID": "subnet-b46032ec",
    "IPv4CIDR": "10.0.0.0/24"
  },
  {
    "IPv6CIDR": [
      "2001:db8:1234:1a01::/64"
    ],
    "ID": "subnet-a46032fc",
    "IPv4CIDR": "10.0.1.0/24"
  }
]
```

7. Puede elegir qué subred asociar a la tabla de ruteo personalizada, por ejemplo, `subnet-b46032ec`. Esta subred será su subred pública.

```
aws ec2 associate-route-table --subnet-id subnet-b46032ec --route-table-id rtb-
c1c8faa6
```

Paso 3: Configurar una subred privada de solo salida

Puede configurar la segunda subred en su VPC para que sea una subred privada de solo salida IPv6. Las instancias que se lancen en esta subred podrán acceder a Internet a través de IPv6 (por ejemplo, para obtener actualizaciones de software) mediante una gateway de Internet de solo salida, pero los hosts de Internet no podrán acceder a sus instancias.

Para convertir su subred en una subred privada de solo salida

1. Cree una gateway de Internet de solo salida para su VPC. En el documento de salida devuelto, busque y anote el ID de la gateway.

```
aws ec2 create-egress-only-internet-gateway --vpc-id vpc-2f09a348
```

```
{
  "EgressOnlyInternetGateway": {
    "EgressOnlyInternetGatewayId": "eigw-015e0e244e24dfe8a",
    "Attachments": [
      {
        "State": "attached",
        "VpcId": "vpc-2f09a348"
      }
    ]
  }
}
```

2. Cree una tabla de ruteo personalizada para su VPC. En el documento de salida devuelto, busque y anote el ID de la tabla de ruteo.

```
aws ec2 create-route-table --vpc-id vpc-2f09a348
```

3. Cree una ruta en la tabla de ruteo que apunte todo el tráfico IPv6 (: : /0) a la gateway de Internet de solo salida.

```
aws ec2 create-route --route-table-id rtb-abc123ab --destination-ipv6-cidr-block ::/0  
--egress-only-internet-gateway-id eigw-015e0e244e24dfe8a
```

4. Asocie la tabla de ruteo a la segunda subred en su VPC (describió las subredes en la sección anterior). Esta subred será su subred privada con acceso a Internet IPv6 de solo salida.

```
aws ec2 associate-route-table --subnet-id subnet-a46032fc --route-table-id rtb-abc123ab
```

Paso 4: Modificar el comportamiento de las direcciones IPv6 de las subredes

Puede modificar el comportamiento de las direcciones IP de sus subredes para que las instancias lanzadas en las subredes reciban automáticamente direcciones IPv6. Al lanzar una instancia en la subred, se asigna una dirección IPv6 única del rango de la subred a la interfaz de red principal (eth0) de la instancia.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-b46032ec --assign-ipv6-address-on-creation
```

```
aws ec2 modify-subnet-attribute --subnet-id subnet-a46032fc --assign-ipv6-address-on-creation
```

Paso 5: Lanzar una instancia en su subred pública

Para comprobar si su subred pública es efectivamente pública y si las instancias de la subred son accesibles desde Internet, lance una instancia en su subred pública y conéctese a ella. En primer lugar, debe crear un grupo de seguridad que asociar a su instancia, así como un par de claves para conectar a su instancia. Para obtener más información acerca de los grupos de seguridad, consulte [Controlar el tráfico hacia los recursos mediante grupos de seguridad \(p. 255\)](#). Para obtener más información sobre pares de claves, consulte [Pares de claves de Amazon EC2](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Para lanzar una instancia y conectarse a esta en su subred pública

1. Cree un par de claves denominado y utilice la opción `--query` y la opción de texto `--output` para transferir su clave privada directamente a un archivo con extensión `.pem`.

```
aws ec2 create-key-pair --key-name MyKeyPair --query "KeyMaterial" --output text  
> MyKeyPair.pem
```

En este ejemplo, lance una instancia de Amazon Linux. Si va a usar un cliente SSH en un sistema operativo Linux o OS X para conectarse a su instancia, utilice el comando a continuación para establecer los permisos de su archivo de clave privada de manera que solo usted pueda leerlo.

```
chmod 400 MyKeyPair.pem
```

2. Cree un grupo de seguridad para la VPC mediante el comando `create-security-group`.

```
aws ec2 create-security-group --group-name SSHAccess --description "Security group for SSH access" --vpc-id vpc-2f09a348
```

```
{  
  "GroupId": "sg-e1fb8c9a"  
}
```

Agregue una regla que permita obtener acceso a SSH desde cualquier dirección IPv6 mediante el comando `authorize-security-group-ingress`. Tenga en cuenta que la siguiente sintaxis solo funciona en Linux y macOS. Para obtener información sobre la sintaxis que funciona en Windows, consulte la sección de [ejemplos](#) en la Referencia de los comandos de la AWS CLI.

```
aws ec2 authorize-security-group-ingress --group-id sg-e1fb8c9a --ip-permissions  
'[{"IpProtocol": "tcp", "FromPort": 22, "ToPort": 22, "Ipv6Ranges": [{"CidrIpv6":  
"::/0"}]}]'
```

Note

Si utiliza `::/0`, permitirá que todas las direcciones IPv6 tengan acceso a su instancia mediante SSH. Esto es aceptable para este breve ejercicio, pero, en la producción, autorice solo una dirección IP específica o un rango de direcciones para obtener acceso a su instancia.

3. Lance una instancia en su subred pública, utilizando el grupo de seguridad y el par de claves que ha creado. En la salida, anote el ID de su instancia.

```
aws ec2 run-instances --image-id ami-0de53d8956e8dcf80 --count 1 --instance-  
type t2.micro --key-name MyKeyPair --security-group-ids sg-e1fb8c9a --subnet-id subnet-  
b46032ec
```

Note

En este ejemplo, la AMI es una AMI de Amazon Linux de la región EE. UU. Este (Norte de Virginia). Si se encuentra en una región diferente, necesita el ID de la AMI para una AMI adecuada en su región. Para obtener más información, consulte [Buscar una AMI de Linux](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

4. Su instancia debe tener el estado `running` para poder conectarse a ella. Describa su instancia y confirme su estado, y tome nota de su dirección IPv6.

```
aws ec2 describe-instances --instance-id i-0146854b7443af453
```

A continuación, se muestra un ejemplo del resultado.

```
{
  "Reservations": [
    {
      ...
      "Instances": [
        {
          ...
          "State": {
            "Code": 16,
            "Name": "running"
          },
          ...
          "NetworkInterfaces": {
            "Ipv6Addresses": {
              "Ipv6Address": "2001:db8:1234:1a00::123"
            }
          }
          ...
        }
      ]
    }
  ]
}
```

5. Si su instancia se encuentra en estado de ejecución, puede conectarse a ella utilizando un cliente SSH en un equipo Linux u OS X con el siguiente comando. Su equipo local debe tener una dirección IPv6 configurada.

```
ssh -i "MyKeyPair.pem" ec2-user@2001:db8:1234:1a00::123
```

Si se conecta desde un equipo Windows, utilice las siguientes instrucciones: [Conexión a la instancia de Linux desde Windows utilizando PuTTY](#).

Paso 6: Lanzar una instancia en su subred privada

Para probar si las instancias de su subred privada de solo salida pueden acceder a Internet, lance una instancia en su subred privada y conéctese a ella mediante una instancia de bastión en su subred pública (puede utilizar la instancia que ha lanzado en la sección anterior). En primer lugar, debe crear un grupo de seguridad para la instancia. El grupo de seguridad debe tener una regla que permita a su instancia de bastión conectarse mediante SSH, así como una regla que admita el comando ping6 (tráfico ICMPv6) para verificar que la instancia no es accesible desde Internet.

1. Cree un grupo de seguridad en su VPC mediante el comando [create-security-group](#).

```
aws ec2 create-security-group --group-name SSHAccessRestricted --description "Security group for SSH access from bastion" --vpc-id vpc-2f09a348
```

Agregue una regla que permita el acceso SSH entrante desde la dirección IPv6 de la instancia en su subred pública y una regla que permita todo el tráfico ICMPv6 mediante el comando [authorize-security-group-ingress](#). Tenga en cuenta que la siguiente sintaxis solo funciona en Linux y macOS. Para obtener información sobre la sintaxis que funciona en Windows, consulte la sección de [ejemplos](#) en la Referencia de los comandos de la AWS CLI.

```
{
  "GroupId": "sg-aabb1122"
}
```

```
aws ec2 authorize-security-group-ingress --group-id sg-aabb1122 --ip-permissions
'[{"IpProtocol": "tcp", "FromPort": 22, "ToPort": 22, "Ipv6Ranges": [{"CidrIpv6":
"2001:db8:1234:1a00::123/128"}]}]'
```

```
aws ec2 authorize-security-group-ingress --group-id sg-aabb1122 --ip-permissions
'[{"IpProtocol": "58", "FromPort": -1, "ToPort": -1, "Ipv6Ranges": [{"CidrIpv6":
":::/0"}]}]'
```

2. Lance una instancia en su subred privada, utilizando el grupo de seguridad que ha creado y el mismo par de claves que utilizó para lanzar la instancia en la subred pública.

```
aws ec2 run-instances --image-id ami-a4827dc9 --count 1 --instance-type t2.micro --key-
name MyKeyPair --security-group-ids sg-aabb1122 --subnet-id subnet-a46032fc
```

Utilice el comando `describe-instances` para verificar si su instancia se está ejecutando y obtener su dirección IPv6.

3. Configure el reenvío de agentes SSH en su equipo local y, a continuación, conéctese a instancia en la subred pública.

Para Linux, utilice los siguientes comandos:

```
ssh-add MyKeyPair.pem
ssh -A ec2-user@2001:db8:1234:1a00::123
```

Para OS X, utilice los siguientes comandos:

```
ssh-add -K MyKeyPair.pem
ssh -A ec2-user@2001:db8:1234:1a00::123
```

Para Windows, utilice las siguientes instrucciones: [Para configurar el reenvío de agentes SSH para Windows \(PuTTY\)](#) (p. 164). Conéctese a la instancia de la subred pública utilizando su dirección IPv6.

4. Desde su instancia en la subred pública (la instancia de bastión), conéctese a su instancia en la subred privada utilizando su dirección IPv6:

```
ssh ec2-user@2001:db8:1234:1a01::456
```

5. Desde su instancia privada, compruebe que puede conectarse a Internet ejecutando el comando `ping6` para un sitio web que tenga ICMP habilitado; por ejemplo:

```
ping6 -n ietf.org
```

```
PING ietf.org(2001:1900:3001:11::2c) 56 data bytes
64 bytes from 2001:1900:3001:11::2c: icmp_seq=1 ttl=46 time=73.9 ms
64 bytes from 2001:1900:3001:11::2c: icmp_seq=2 ttl=46 time=73.8 ms
64 bytes from 2001:1900:3001:11::2c: icmp_seq=3 ttl=46 time=73.9 ms
...
```

6. Para comprobar que los hosts de Internet no pueden acceder a su instancia en la subred privada, utilice el comando `ping6` desde un equipo que esté habilitado para IPv6. Debería obtener una

respuesta de tiempo de espera. Si obtiene una respuesta válida, quiere decir que la instancia es accesible desde Internet: compruebe la tabla de enrutamiento asociada con la subred privada y verifique que no tiene una ruta para el tráfico IPv6 a una gateway de Internet.

```
ping6 2001:db8:1234:1a01::456
```

Paso 7: Limpieza

Después de haber verificado que se puede conectar a su instancia en la subred pública y que su instancia en la subred privada puede acceder a Internet, puede terminar las instancias si ya no las necesita. Para ello, utilice el comando `terminate-instances`. Para eliminar los otros recursos que ha creado en este ejemplo, utilice los siguientes comandos según el orden enumerado:

1. Eliminación de sus grupos de seguridad:

```
aws ec2 delete-security-group --group-id sg-e1fb8c9a
```

```
aws ec2 delete-security-group --group-id sg-aabb1122
```

2. Eliminación de sus subredes:

```
aws ec2 delete-subnet --subnet-id subnet-b46032ec
```

```
aws ec2 delete-subnet --subnet-id subnet-a46032fc
```

3. Eliminación de sus tablas de ruteo personalizadas:

```
aws ec2 delete-route-table --route-table-id rtb-c1c8faa6
```

```
aws ec2 delete-route-table --route-table-id rtb-abc123ab
```

4. Separación de la gateway de Internet de la VPC:

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-1ff7a07b --vpc-id vpc-2f09a348
```

5. Eliminación de su gateway de Internet:

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-1ff7a07b
```

6. Eliminación de su gateway de Internet de solo salida:

```
aws ec2 delete-egress-only-internet-gateway --egress-only-internet-gateway-id eigw-015e0e244e24dfe8a
```

7. Eliminación de su VPC:

```
aws ec2 delete-vpc --vpc-id vpc-2f09a348
```

Crear una VPC con IPv6 habilitado y subredes con solo IPv6 mediante la AWS CLI

En el siguiente ejemplo, se utilizan comandos de la AWS CLI para crear una VPC no predeterminada con un bloque de CIDR de IPv6, una subred pública solo de IPv6 y una subred privada solo de IPv6 únicamente con acceso de salida a Internet. Tras haber creado la VPC y las subredes, puede lanzar una instancia en la subred pública y conectarse a esta. Puede lanzar una instancia en su subred privada y verificar que se puede conectar a Internet. Para comenzar, primero debe instalar y configurar la AWS CLI. Para obtener más información, consulte [Instalación de la AWS CLI](#).

Crearé los siguientes recursos de AWS:

- Una VPC
- Dos subredes
- Una gateway de Internet
- Una tabla de enrutamiento
- Una instancia EC2.

Tareas

- [Paso 1: Crear una VPC y subredes \(p. 282\)](#)
- [Paso 2: Configurar una subred pública \(p. 283\)](#)
- [Paso 3: Configurar una subred privada de solo salida \(p. 285\)](#)
- [Paso 4: Modificar las subredes \(p. 286\)](#)
- [Paso 5: Lanzar una instancia en su subred pública \(p. 286\)](#)
- [Paso 6: Lanzar una instancia en su subred privada \(p. 288\)](#)
- [Paso 7: Limpieza \(p. 290\)](#)

Paso 1: Crear una VPC y subredes

El primer paso es crear una VPC. Debe definir un bloque de CIDR de IPv4 para la VPC, si bien en este ejemplo nos centramos principalmente en IPv6. Este ejemplo utiliza el bloque de CIDR IPv4 10.0.0.0/16 para la VPC, pero puede elegir un bloque de CIDR distinto. Para obtener más información, consulte [Ajuste de tamaño de la VPC \(p. 16\)](#).

Para crear una VPC y las subredes utilizando la AWS CLI

1. Cree una VPC con un bloque de CIDR 10.0.0.0/16 y asocie un bloque de CIDR IPv6 a la VPC.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --amazon-provided-ipv6-cidr-block
```

En el documento de salida devuelto, busque y anote el ID de la VPC.

```
{
  "Vpc": {
    "VpcId": "vpc-2f09a348",
    ...
  }
}
```

2. Describa su VPC para obtener el bloque de CIDR IPv6 asociado a la VPC.


```
aws ec2 describe-vpcs --vpc-id vpc-2f09a348
```

```
{
  "Vpcs": [
    {
      ...
      "Ipv6CidrBlockAssociationSet": [
        {
          "Ipv6CidrBlock": "2001:db8:1234:1a00::/56",
          "AssociationId": "vpc-cidr-assoc-17a5407e",
          "Ipv6CidrBlockState": {
            "State": "ASSOCIATED"
          }
        }
      ],
      ...
    }
  ]
}
```

3. Cree una subred solo de IPv6 en su VPC con un bloque de CIDR de IPv6 2001:db8:1234:1a00::/64 (a partir de los rangos devueltos en el paso anterior). Para obtener más información acerca de la opción solo IPv6, consulte [the section called “Crear una subred en la VPC” \(p. 64\)](#) o bien [create-subnet](#) en la Referencia de comandos de AWS CLI.

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --ipv6-cidr-block 2001:db8:1234:1a00::/64 --ipv6-native
```

4. Cree una segunda subred solo de IPv6 en su VPC con un bloque de CIDR de IPv6 2001:db8:1234:1a01::/64.

```
aws ec2 create-subnet --vpc-id vpc-2f09a348 --ipv6-cidr-block 2001:db8:1234:1a01::/64 --ipv6-native
```

Paso 2: Configurar una subred pública

Una vez que cree la VPC y las subredes, puede hacer que una de las subredes de IPv6 sea pública; para ello, adjunte una gateway de Internet a su VPC, cree una tabla de enrutamiento personalizada y configure el enrutamiento de la subred a la gateway de Internet. En este ejemplo, se crea una tabla de enrutamiento que dirige todo el tráfico IPv6 a una gateway de Internet.

Para convertir su subred en una subred pública

1. Cree una gateway de Internet.

```
aws ec2 create-internet-gateway
```

Tome nota del ID de la gateway de Internet que aparece en el documento de salida que se devuelve.

```
{
  "InternetGateway": {
    ...
    "InternetGatewayId": "igw-1ff7a07b",
    ...
  }
}
```

2. Con el ID del paso anterior, adjunte la gateway de Internet a la VPC.

```
aws ec2 attach-internet-gateway --vpc-id vpc-2f09a348 --internet-gateway-id igw-1ff7a07b
```

3. Cree una tabla de ruteo personalizada para su VPC.

```
aws ec2 create-route-table --vpc-id vpc-2f09a348
```

En el documento de salida devuelto, busque y anote el ID de la tabla de ruteo.

```
{
  "RouteTable": {
    ...
    "RouteTableId": "rtb-c1c8faa6",
    ...
  }
}
```

4. Cree una ruta en la tabla de enrutamiento que apunte todo el tráfico IPv6 (::/0) a la gateway de Internet.

```
aws ec2 create-route --route-table-id rtb-c1c8faa6 --destination-ipv6-cidr-block ::/0 --gateway-id igw-1ff7a07b
```

5. Para asegurarse de que su ruta se ha creado y está activa, puede describir la tabla de ruteo y ver los resultados.

```
aws ec2 describe-route-tables --route-table-id rtb-c1c8faa6
```

```
{
  "RouteTables": [
    {
      "Associations": [],
      "RouteTableId": "rtb-c1c8faa6",
      "VpcId": "vpc-2f09a348",
      "PropagatingVgws": [],
      "Tags": [],
      "Routes": [
        {
          "GatewayId": "local",
          "DestinationCidrBlock": "10.0.0.0/16",
          "State": "active",
          "Origin": "CreateRouteTable"
        },
        {
          "GatewayId": "local",
          "Origin": "CreateRouteTable",
          "State": "active",
          "DestinationIpv6CidrBlock": "2001:db8:1234:1a00::/56"
        },
        {
          "GatewayId": "igw-1ff7a07b",
          "Origin": "CreateRoute",
          "State": "active",
          "DestinationIpv6CidrBlock": "::/0"
        }
      ]
    }
  ]
}
```

6. La tabla de ruteo no está asociada actualmente a ninguna subred. Asóciela a una subred de su VPC para que el tráfico de esa subred se dirija a la gateway de Internet. En primer lugar, describa sus subredes para obtener sus ID. Puede utilizar la opción `--filter` para devolver las subredes solo a su nueva VPC, y la opción `--query` para devolver solo los ID de la subred y sus bloques de CIDR de IPv6.

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-2f09a348" --query "Subnets[*].{ID:SubnetId,IPv6CIDR:Ipv6CidrBlockAssociationSet[*].Ipv6CidrBlock}"
```

```
[
  {
    "ID": "subnet-b46032ec",
    "IPv6CIDR": [
      "2001:db8:1234:1a01::/64"
    ],
    "ID": "subnet-a46032fc",
    "IPv6CIDR": [
      "2001:db8:1234:1a01::/64"
    ]
  }
]
```

7. Puede elegir qué subred asociar a la tabla de ruteo personalizada, por ejemplo, `subnet-b46032ec`. Esta subred será su subred pública.

```
aws ec2 associate-route-table --subnet-id subnet-b46032ec --route-table-id rtb-c1c8faa6
```

Paso 3: Configurar una subred privada de solo salida

Puede configurar la segunda subred en su VPC para que sea una subred privada de solo salida IPv6. Las instancias que se lancen en esta subred podrán acceder a Internet a través de IPv6 (por ejemplo, para obtener actualizaciones de software) mediante una gateway de Internet de solo salida, pero los hosts de Internet no podrán acceder a sus instancias.

Para convertir su subred en una subred privada de solo salida

1. Cree una gateway de Internet de solo salida para su VPC. En el documento de salida devuelto, busque y anote el ID de la gateway.

```
aws ec2 create-egress-only-internet-gateway --vpc-id vpc-2f09a348
```

```
{
  "EgressOnlyInternetGateway": {
    "EgressOnlyInternetGatewayId": "eigw-015e0e244e24dfe8a",
    "Attachments": [
      {
        "State": "attached",
        "VpcId": "vpc-2f09a348"
      }
    ]
  }
}
```

2. Cree una tabla de ruteo personalizada para su VPC. En el documento de salida devuelto, busque y anote el ID de la tabla de ruteo.

```
aws ec2 create-route-table --vpc-id vpc-2f09a348
```

3. Cree una ruta en la tabla de ruteo que apunte todo el tráfico IPv6 (: : /0) a la gateway de Internet de solo salida.

```
aws ec2 create-route --route-table-id rtb-abc123ab --destination-ipv6-cidr-block ::/0  
--egress-only-internet-gateway-id eigw-015e0e244e24dfe8a
```

4. Asocie la tabla de ruteo a la segunda subred en su VPC (describió las subredes en la sección anterior). Esta subred será su subred privada con acceso a Internet IPv6 de solo salida.

```
aws ec2 associate-route-table --subnet-id subnet-a46032fc --route-table-id rtb-abc123ab
```

Paso 4: Modificar las subredes

Una vez que haya creado las subredes, puede modificar lo siguiente:

- Puede modificar el comportamiento de las direcciones IP de sus subredes para que las instancias lanzadas en las subredes reciban automáticamente direcciones IPv6. Entonces, al lanzar una instancia en la subred, se asigna una dirección IPv6 única del rango de la subred a la interfaz de red principal (eth0) de la instancia.
- Configuración de nombre basado en recursos (RBN) para la subred y las instancias lanzadas en la subred. Para obtener más información sobre RBN, consulte [Tipos de nombres de host de instancias de Amazon EC2](#) en la Guía del usuario de Amazon EC2. Para obtener más información sobre las opciones de RBN utilizadas en esta sección, consulte [modify-subnet-attribute](#) en la Referencia de los comandos de AWS CLI o [Modificación de las configuraciones de RBN](#) en la Guía del usuario de Amazon EC2.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-b46032ec --assign-ipv6-address-on-  
creation --private-dns-hostname-type-on-launch resource-name --enable-resource-name-dns-  
aaaa-record-on-launch --enable-resource-name-dns-a-record-on-launch
```

```
aws ec2 modify-subnet-attribute --subnet-id subnet-a46032fc --assign-ipv6-address-on-  
creation --private-dns-hostname-type-on-launch resource-name --enable-resource-name-dns-  
aaaa-record-on-launch --enable-resource-name-dns-a-record-on-launch
```

Paso 5: Lanzar una instancia en su subred pública

Para comprobar si su subred pública es efectivamente pública y si las instancias de la subred son accesibles desde Internet, lance una instancia en su subred pública y conéctese a ella. En primer lugar, debe crear un grupo de seguridad que asociar a su instancia, así como un par de claves para conectar a su instancia. Para obtener más información acerca de los grupos de seguridad, consulte [Controlar el tráfico hacia los recursos mediante grupos de seguridad \(p. 255\)](#). Para obtener más información sobre pares de claves, consulte [Pares de claves de Amazon EC2](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Para obtener más información sobre las opciones disponibles cuando ejecuta una instancia, consulte [run-instances](#) en la Referencia de los comandos de AWS CLI o [Lanzar una instancia con el asistente de lanzamiento de instancias](#) en la Guía del usuario de Amazon EC2.

Para lanzar una instancia y conectarse a esta en su subred pública

1. Cree un par de claves denominado y utilice la opción `--query` y la opción de texto `--output` para transferir su clave privada directamente a un archivo con extensión `.pem`.

```
aws ec2 create-key-pair --key-name MyKeyPair --query "KeyMaterial" --output text  
> MyKeyPair.pem
```

En este ejemplo, lance una instancia de Amazon Linux. Si va a usar un cliente SSH en un sistema operativo Linux o OS X para conectarse a su instancia, utilice el comando a continuación para establecer los permisos de su archivo de clave privada de manera que solo usted pueda leerlo.

```
chmod 400 MyKeyPair.pem
```

2. Cree un grupo de seguridad para la VPC mediante el comando [create-security-group](#).

```
aws ec2 create-security-group --group-name SSHAccess --description "Security group for SSH access" --vpc-id vpc-2f09a348
```

```
{  
  "GroupId": "sg-e1fb8c9a"  
}
```

Agregue una regla que permita obtener acceso a SSH desde cualquier dirección IPv6 mediante el comando [authorize-security-group-ingress](#). Tenga en cuenta que la siguiente sintaxis solo funciona en Linux y macOS. Para obtener información sobre la sintaxis que funciona en Windows, consulte la sección de [ejemplos](#) en la Referencia de los comandos de la AWS CLI.

```
aws ec2 authorize-security-group-ingress --group-id sg-e1fb8c9a --ip-permissions  
'[{"IpProtocol": "tcp", "FromPort": 22, "ToPort": 22, "Ipv6Ranges": [{"CidrIpv6":  
"::/0"}]}]'
```

Note

Si utiliza `::/0`, permitirá que todas las direcciones IPv6 tengan acceso a su instancia mediante SSH. Esto es aceptable para este breve ejercicio, pero, en la producción, autorice solo una dirección IP específica o un rango de direcciones para obtener acceso a su instancia.

3. Lance una instancia EC2 solo IPv6 en su subred pública mediante el grupo de seguridad y el par de claves que ha creado. Para lanzar una instancia EC2 solo IPv6, debe utilizar [Instancias EC2 integradas en el sistema Nitro](#). Para obtener más información, consulte [Servidor DNS de Amazon](#) (p. 42). En la salida, anote el ID de su instancia.

```
aws ec2 run-instances --image-id ami-0de53d8956e8dcf80 --count 1 --instance-  
type t3.micro --key-name MyKeyPair --security-group-ids sg-e1fb8c9a --subnet-id subnet-  
b46032ec
```

Note

En este ejemplo, la AMI es una AMI de Amazon Linux de la región EE. UU. Este (Norte de Virginia). Si se encuentra en una región diferente, necesita el ID de la AMI para una AMI adecuada en su región. Para obtener más información, consulte [Buscar una AMI de Linux](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

4. Su instancia debe tener el estado `running` para poder conectarse a ella. Describa su instancia y confirme su estado, y tome nota de su dirección IPv6.

```
aws ec2 describe-instances --instance-id i-0146854b7443af453
```

A continuación, se muestra un ejemplo del resultado.

```
{
  "Reservations": [
    {
      ...
      "Instances": [
        {
          ...
          "State": {
            "Code": 16,
            "Name": "running"
          },
          ...
          "NetworkInterfaces": {
            "Ipv6Addresses": {
              "Ipv6Address": "2001:db8:1234:1a00::123"
            }
          },
          ...
        }
      ]
    }
  ]
}
```

5. Si su instancia se encuentra en estado de ejecución, puede conectarse a ella utilizando un cliente SSH en un equipo Linux u OS X con el siguiente comando. Su equipo local debe tener una dirección IPv6 configurada.

```
ssh -i "MyKeyPair.pem" ec2-user@2001:db8:1234:1a00::123
```

Si se conecta desde un equipo Windows, utilice las siguientes instrucciones: [Conexión a la instancia de Linux desde Windows utilizando PuTTY](#).

Paso 6: Lanzar una instancia en su subred privada

Para probar si las instancias de su subred privada de solo salida pueden acceder a Internet, lance una instancia en su subred privada y conéctese a ella mediante una instancia de bastión en su subred pública (puede utilizar la instancia que ha lanzado en la sección anterior). En primer lugar, debe crear un grupo de seguridad para la instancia. El grupo de seguridad debe tener una regla que permita a su instancia de bastión conectarse mediante SSH, así como una regla que admita el comando `ping6` (tráfico ICMPv6) para verificar que la instancia no es accesible desde Internet.

1. Cree un grupo de seguridad en su VPC mediante el comando `create-security-group`.

```
aws ec2 create-security-group --group-name SSHAccessRestricted --description "Security group for SSH access from bastion" --vpc-id vpc-2f09a348
```

Agregue una regla que permita el acceso SSH entrante desde la dirección IPv6 de la instancia en su subred pública y una regla que permita todo el tráfico ICMPv6 mediante el comando `authorize-security-group-ingress`. Tenga en cuenta que la siguiente sintaxis solo funciona en Linux y macOS. Para obtener información sobre la sintaxis que funciona en Windows, consulte la sección de [ejemplos](#) en la Referencia de los comandos de la AWS CLI.

```
{
  "GroupId": "sg-aabb1122"
```

```
}
```

```
aws ec2 authorize-security-group-ingress --group-id sg-aabb1122 --ip-permissions  
'[{"IpProtocol": "tcp", "FromPort": 22, "ToPort": 22, "Ipv6Ranges": [{"CidrIpv6":  
"2001:db8:1234:1a00::123/128"}]}]'
```

```
aws ec2 authorize-security-group-ingress --group-id sg-aabb1122 --ip-permissions  
'[{"IpProtocol": "58", "FromPort": -1, "ToPort": -1, "Ipv6Ranges": [{"CidrIpv6":  
 "::/0"}]}]'
```

2. Lance una instancia solo IPv6 en su subred privada mediante el grupo de seguridad que ha creado y el mismo par de claves que utilizó para lanzar la instancia en la subred pública. Para lanzar una instancia EC2 solo IPv6, debe utilizar [Instancias EC2 integradas en el sistema Nitro](#).

```
aws ec2 run-instances --image-id ami-a4827dc9 --count 1 --instance-type t3.micro --key-  
name MyKeyPair --security-group-ids sg-aabb1122 --subnet-id subnet-a46032fc
```

Utilice el comando `describe-instances` para verificar si su instancia se está ejecutando y obtener su dirección IPv6.

3. Configure el reenvío de agentes SSH en su equipo local y, a continuación, conéctese a instancia en la subred pública.

Para Linux, utilice los siguientes comandos:

```
ssh-add MyKeyPair.pem  
ssh -A ec2-user@2001:db8:1234:1a00::123
```

Para OS X, utilice los siguientes comandos:

```
ssh-add -K MyKeyPair.pem  
ssh -A ec2-user@2001:db8:1234:1a00::123
```

Para Windows, utilice las siguientes instrucciones: [Para configurar el reenvío de agentes SSH para Windows \(PuTTY\)](#) (p. 164). Conéctese a la instancia de la subred pública utilizando su dirección IPv6.

4. Desde su instancia en la subred pública (la instancia de bastión), conéctese a su instancia en la subred privada utilizando su dirección IPv6:

```
ssh ec2-user@2001:db8:1234:1a01::456
```

5. Desde su instancia privada, compruebe que puede conectarse a Internet ejecutando el comando `ping6` para un sitio web que tenga ICMP habilitado; por ejemplo:

```
ping6 -n ietf.org
```

```
PING ietf.org(2001:1900:3001:11::2c) 56 data bytes  
64 bytes from 2001:1900:3001:11::2c: icmp_seq=1 ttl=46 time=73.9 ms  
64 bytes from 2001:1900:3001:11::2c: icmp_seq=2 ttl=46 time=73.8 ms  
64 bytes from 2001:1900:3001:11::2c: icmp_seq=3 ttl=46 time=73.9 ms  
...
```

6. Para comprobar que los hosts de Internet no pueden acceder a su instancia en la subred privada, utilice el comando `ping6` desde un equipo que esté habilitado para IPv6. Debería obtener una respuesta de tiempo de espera. Si obtiene una respuesta válida, quiere decir que la instancia es

accesible desde Internet: compruebe la tabla de enrutamiento asociada con la subred privada y verifique que no tiene una ruta para el tráfico IPv6 a una gateway de Internet.

```
ping6 2001:db8:1234:1a01::456
```

Paso 7: Limpieza

Después de haber verificado que se puede conectar a su instancia en la subred pública y que su instancia en la subred privada puede acceder a Internet, puede terminar las instancias si ya no las necesita. Para ello, utilice el comando [terminate-instances](#). Para eliminar los otros recursos que ha creado en este ejemplo, utilice los siguientes comandos según el orden enumerado:

1. Eliminación de sus grupos de seguridad:

```
aws ec2 delete-security-group --group-id sg-e1fb8c9a
```

```
aws ec2 delete-security-group --group-id sg-aabb1122
```

2. Eliminación de sus subredes:

```
aws ec2 delete-subnet --subnet-id subnet-b46032ec
```

```
aws ec2 delete-subnet --subnet-id subnet-a46032fc
```

3. Eliminación de sus tablas de ruteo personalizadas:

```
aws ec2 delete-route-table --route-table-id rtb-c1c8faa6
```

```
aws ec2 delete-route-table --route-table-id rtb-abc123ab
```

4. Separación de la gateway de Internet de la VPC:

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-1ff7a07b --vpc-id vpc-2f09a348
```

5. Eliminación de su gateway de Internet:

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-1ff7a07b
```

6. Eliminación de su gateway de Internet de solo salida:

```
aws ec2 delete-egress-only-internet-gateway --egress-only-internet-gateway-id eigw-015e0e244e24dfe8a
```

7. Eliminación de su VPC:

```
aws ec2 delete-vpc --vpc-id vpc-2f09a348
```


Tutoriales sobre el uso de AWS Management Console

En los siguientes tutoriales, aprenderá a crear VPC mediante la AWS Management Console en Amazon Virtual Private Cloud.

Contenido

- [Crear VPC con el asistente \(p. 291\)](#)
- [Migrar VPC existentes de IPv4 a IPv6 \(p. 360\)](#)

Crear VPC con el asistente

En los siguientes tutoriales, aprenderá a crear VPC mediante el uso del asistente en Amazon Virtual Private Cloud.

Contenido

- [VPC que admite las direcciones IPv6 \(p. 291\)](#)
- [VPC con una única subred pública \(p. 296\)](#)
- [VPC con subredes privadas y públicas \(NAT\) \(p. 307\)](#)
- [VPC con subredes públicas y privadas y acceso de AWS Site-to-Site VPN \(p. 330\)](#)
- [VPC solo con una subred privada y acceso de AWS Site-to-Site VPN \(p. 353\)](#)

VPC que admite las direcciones IPv6

En los siguientes pasos se describe cómo crear una VPC no predeterminada que admita direcciones IPv6.

Para completar este ejercicio, realice lo siguiente:

- Crear una VPC no predeterminada con un bloque de CIDR IPv6 y una única subred pública. Las subredes le permiten agrupar instancias en función de sus necesidades operativas y de seguridad. Una subred pública es una subred que tiene acceso a Internet a través de una gateway de Internet.
- Cree un grupo de seguridad para su instancia que permita el tráfico solo a través de puertos específicos.
- Lance una instancia Amazon EC2 en la subred y asocie una dirección IPv6 con la instancia durante el lanzamiento. Las direcciones IPv6 son únicas de forma global y permiten que su instancia se comuniquen con Internet.
- Puede solicitar un bloque de CIDR IPv6 para la VPC. Cuando selecciona esta opción, puede establecer el grupo de bordes de red, que es la ubicación desde la que anunciamos el bloque de CIDR IPv6. Si se establece el grupo de bordes de red, el bloque de CIDR queda restringido a este grupo.

Para obtener más información acerca de las direcciones IPv4 e IPv6, consulte [Direcciones IP en la VPC](#).

Si desea utilizar una zona local para la VPC, cree una VPC y, a continuación, cree una subred en la zona local. Para obtener más información, consulte [the section called "Creación de una VPC" \(p. 21\)](#) y [the section called "Crear una subred en la VPC" \(p. 64\)](#).

Tareas

- [Paso 1: Creación de la VPC \(p. 292\)](#)
- [Paso 2: Crear un grupo de seguridad \(p. 294\)](#)
- [Paso 3: Lanzar una instancia \(p. 295\)](#)

Paso 1: Creación de la VPC

En este paso, se utiliza el asistente de Amazon VPC en la consola de Amazon VPC para crear una VPC. Por defecto, el asistente ejecuta los siguientes pasos por usted:

- Crea una VPC con un bloque de CIDR IPv4 /16 y asocia un bloque de CIDR IPv6 /56 a la VPC. Para obtener más información, consulte [La VPC](#). El tamaño del bloque de CIDR IPv6 es fijo (/56) y el rango de direcciones IPv6 se asigna automáticamente desde el grupo de direcciones IPv6 de Amazon (no es posible seleccionar el rango manualmente).
- Asocia una gateway de Internet con la VPC. Para obtener más información acerca de las gateways de Internet, consulte [Gateways de Internet](#).
- Crea una subred con un bloque de CIDR IPv4 /24 y un bloque de CIDR IPv6 /64 en la VPC. El tamaño del bloque de CIDR IPv6 es fijo (/64).
- Crea una tabla de enrutamiento personalizada y la asocia con su subred para que el tráfico pueda fluir entre la subred y la gateway de Internet. Para obtener más información acerca de las tablas de enrutamiento, consulte [Tablas de enrutamiento](#).
- Asocia un bloque de CIDR IPv6 proporcionado por Amazon a un grupo de bordes de red. Para obtener más información, consulte [the section called “Ampliar los recursos de VPC a Local Zones” \(p. 53\)](#).

Note

Este ejercicio aborda el primer escenario del asistente para la creación de VPC. Para obtener información acerca de los demás escenarios, consulte [the section called “Crear VPC con el asistente” \(p. 291\)](#).

Para crear una VPC en la zona de disponibilidad predeterminada

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En la barra de navegación, en la parte superior derecha, anote la región en la que va a crear la VPC. Asegúrese de continuar trabajando en la misma región en el resto del ejercicio, ya que no podrá lanzar una instancia en su VPC desde una región distinta. Para obtener más información, consulte [Regiones y zonas de disponibilidad](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
3. En el panel de navegación, elija VPC dashboard (Panel de VPC) y elija Launch VPC Wizard (Lanzar asistente de VPC).

Note

No elija Your VPCs (Sus VPC) en el panel de navegación, ya que no podrá obtener acceso al asistente para la creación de VPC con el botón Create VPC (Crear VPC) de esta página.

4. Elija la opción para la configuración que desea implementar, por ejemplo VPC with a Single Public Subnet (VPC con una única subred pública), y elija Select (Seleccionar)
5. En la página de configuración, escriba un nombre para su VPC en VPC name como, por ejemplo, my-vpc, y escriba un nombre para la subred en Subnet name. Esto le ayudará a identificar la VPC y la subred en la consola de Amazon VPC después de crearlas.
6. En IPv4 CIDR block, puede dejar los valores predeterminados (10.0.0.0/16) o especificar valores propios. Para obtener más información, consulte [Tamaño de la VPC](#).

En IPv6 CIDR block, elija Amazon-provided IPv6 CIDR block.

7. En Public subnet's IPv4 CIDR, puede dejar los valores predeterminados o especificar valores propios. En Public subnet's IPv6 CIDR, elija Specify a custom IPv6 CIDR. Puede dejar la pareja de valores hexadecimales predeterminados para la subred IPv6 (00).
8. Deje el resto de opciones de configuración predeterminadas de la página y elija Create VPC.
9. En una ventana de estado se muestra el trabajo en curso. Cuando haya terminado el trabajo, elija OK para cerrar la ventana de estado.
10. La página Your VPCs muestra la VPC predeterminada y la VPC que acaba de crear.

Para crear una VPC en una zona local

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En la barra de navegación, en la parte superior derecha, anote la región en la que va a crear la VPC. Asegúrese de continuar trabajando en la misma región en el resto del ejercicio, ya que no podrá lanzar una instancia en su VPC desde una región distinta. Para obtener más información, consulte [Regiones y zonas](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
3. En el panel de navegación, elija VPC dashboard (Panel de VPC) y elija Launch VPC Wizard (Lanzar asistente de VPC).

Note

No elija Your VPCs (Sus VPC) en el panel de navegación, ya que no podrá obtener acceso al asistente para la creación de VPC con el botón Create VPC (Crear VPC) de esta página.

4. Elija la opción para la configuración que desea implementar, por ejemplo VPC with a Single Public Subnet (VPC con una única subred pública), y elija Select (Seleccionar).
5. En la página de configuración, escriba un nombre para su VPC en VPC name como, por ejemplo, my-vpc, y escriba un nombre para la subred en Subnet name. Esto le ayudará a identificar la VPC y la subred en la consola de Amazon VPC después de crearlas.
6. En IPv4 CIDR block (Bloque de CIDR), especifique el bloque de CIDR. Para obtener más información, consulte [Tamaño de la VPC](#).
7. En IPv6 CIDR block, elija Amazon-provided IPv6 CIDR block.
8. Deje el resto de opciones de configuración predeterminadas de la página y elija Create VPC.
9. En una ventana de estado se muestra el trabajo en curso. Cuando haya terminado el trabajo, elija OK para cerrar la ventana de estado.
10. La página Your VPCs muestra la VPC predeterminada y la VPC que acaba de crear.

Ver información de sus VPC

Una vez creada la VPC, podrá ver información acerca de la subred, la gateway a Internet y las tablas de ruteo. La VPC que ha creado tiene dos tablas de enrutamiento: una tabla de enrutamiento principal que todas las VPC tienen de forma predeterminada y una tabla de enrutamiento personalizada que creó el asistente. La tabla de ruteo personalizada se asocia a su subred, lo que significa que las rutas de dicha tabla determina el modo en que fluye el tráfico de la subred. Si añade una nueva subred a su VPC, utiliza la tabla de ruteo principal de forma predeterminada.

Para ver la información de sus VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs (Sus VPC). Anote el nombre y el ID de la VPC que creó (consulte las columnas Name y VPC ID). Esta información se utiliza más adelante para identificar los componentes asociados a su VPC.

Cuando utiliza Local Zones, la entrada IPv6 (Grupo de bordes de red) indica el grupo de bordes de red de la VPC (por ejemplo:), us-west-2-lax-1).

3. En el panel de navegación, elija Subnets. La consola muestra la subred que se creó cuando creó su VPC. Puede identificar la subred por su nombre mediante la columna Name, o bien puede utilizar la información de VPC que obtuvo en el paso anterior y consultar la columna VPC.
4. En el panel de navegación, elija Internet Gateways (Gateways de Internet). Encontrará la gateway de Internet asociada con su VPC consultando la columna VPC, que muestra el ID y el nombre de la VPC (si corresponde).
5. En el panel de navegación, elija Route Tables. La VPC tiene asociadas dos tablas de ruteo. Seleccione la tabla de ruteo personalizada (la columna Main muestra el valor No) y, a continuación, elija la pestaña Routes para mostrar la información de ruta en el panel de detalles:

- Las primeras dos filas de la tabla son las rutas locales que permiten que las instancias de la VPC se comuniquen mediante IPv4 e IPv6. Estas rutas no se pueden quitar.
 - En la siguiente fila se muestra la ruta que el asistente de Amazon VPC ha agregado para habilitar el flujo del tráfico con destino a una dirección IPv4 externa a la VPC (0.0.0.0/0) desde la subred a la gateway de Internet.
 - La siguiente fila muestra la ruta que permite el flujo del tráfico con destino a una dirección IPv6 externa a la VPC (:::0) desde la subred a la gateway a Internet.
6. Seleccione la tabla de ruteo principal. Esta tabla de ruteo principal solamente tiene una ruta local.

Paso 2: Crear un grupo de seguridad

Un grupo de seguridad actúa como un firewall virtual para controlar el tráfico a las instancias que tiene asociadas. Para utilizar un grupo de seguridad, añada las reglas entrantes que controlan el tráfico entrante a la instancia y las reglas salientes que controlan el tráfico saliente desde su instancia. Para asociar un grupo de seguridad a una instancia, especifique el grupo de seguridad al lanzar la instancia.

La VPC incluye un grupo de seguridad predeterminado. Las instancias no asociadas a ningún otro grupo de seguridad durante el lanzamiento se asociarán al grupo de seguridad predeterminado. En este ejercicio, creará un nuevo grupo de seguridad, `WebServerSG`, y especificará dicho grupo de seguridad al lanzar una instancia en su VPC.

Crear el grupo de seguridad de `WebServerSG`

Puede crear su grupo de seguridad mediante la consola de Amazon VPC.

Para crear el grupo de seguridad `WebServerSG` y añadir reglas

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, seleccione Security Groups, Create Security Group.
3. En Group name, escriba `WebServerSG` como nombre del grupo de seguridad y proporcione una descripción. De manera opcional, puede utilizar el campo Name tag para crear una etiqueta para el grupo de seguridad con una clave de Name y un valor especificado.
4. Seleccione el ID de su VPC del menú VPC y elija Yes, Create.
5. Seleccione el grupo de seguridad `WebServerSG` que acaba de crear (podrá ver su nombre en la columna Group Name).
6. En la pestaña Inbound Rules, elija Edit y use el procedimiento siguiente para añadir reglas para el tráfico entrante:
 - a. En Type (Tipo), elija HTTP e ingrese :::0 en el campo Source (Origen).
 - b. Elija Add another rule (Agregar otra regla), en Type (Tipo) elija HTTPS y, a continuación, ingrese :::0 en el campo Source (Origen).
 - c. Elija Add another rule. Si va a lanzar una instancia de Linux, elija SSH en Type, o bien, si va a lanzar una instancia de Windows, elija RDP. Escriba el rango de direcciones IPv6 públicas de la red en el campo Source. Si no conoce este rango de direcciones, puede utilizar :::0 para este ejercicio.

Important

Si utiliza :::0, todas las direcciones IPv6 podrán obtener acceso a su instancia mediante SSH o RDP. Esto es aceptable para este pequeño ejercicio, pero constituye una práctica peligrosa en entornos de producción. En entornos de producción, debe autorizar el acceso a su instancia únicamente a una dirección IP o a un rango de direcciones IP específico.

- d. Seleccione Save.

Paso 3: Lanzar una instancia

Cuando se lanza una instancia EC2 en una VPC, debe especificar la subred en la que desea lanzar la instancia. En este caso, lanzará una instancia en la subred pública de la VPC que ha creado. Utilice el asistente de lanzamiento de Amazon EC2 en la consola de Amazon EC2 para lanzar la instancia. No todas las opciones del asistente de lanzamiento de Amazon EC2 se detallan aquí. Para obtener más información, consulte [Lanzamiento de una instancia](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Para asegurarse de que su instancia esté disponible desde Internet, asigne una dirección IPv6 desde el rango de subred a la instancia durante el lanzamiento. Esto garantiza que su instancia se pueda comunicar con Internet a través de IPv6.

Para lanzar una instancia EC2 en una VPC

Antes de lanzar la instancia EC2 en la VPC, configure la subred de la VPC para que asigne automáticamente direcciones IP IPv6. Para obtener más información, consulte [the section called "Modificar el atributo de direcciones IPv6 de su subred"](#) (p. 67).

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En la barra de navegación, en la parte superior derecha, asegúrese de seleccionar la misma región en la que creó su VPC y su grupo de seguridad.
3. En el panel, elija Launch Instance (Lanzar instancia).
4. En la primera página del asistente, elija la AMI que va a utilizar. Para este ejercicio, se recomienda elegir una AMI de Amazon Linux o una AMI de Windows.
5. En la página Choose an Instance Type, puede seleccionar la configuración de hardware y el tamaño de la instancia que se va a lanzar. De forma predeterminada, el asistente selecciona el primer tipo de instancia disponible en función de la AMI que ha seleccionado. Puede dejar la selección predeterminada y elegir Next: Configure Instance Details.
6. En la página Configure Instance Details, seleccione la VPC que creó en la lista Network y seleccione la subred desde la lista Subnet.
7. En Auto-assign IPv6 IP (Asignar automáticamente IP IPv6), elija Enable (Habilitar).
8. Deje el resto de los valores predeterminados y omita las páginas siguientes del asistente hasta llegar a la página Add Tags.
9. En la página Add Tags, podrá asignar a su instancia la etiqueta Name. Por ejemplo, Name=MyWebServer. Esto le ayudará a identificar la instancia en la consola de Amazon EC2 después de que la haya lanzado. Elija Next: Configure Security Group cuando haya terminado.
10. En la página Configure Security Group, el asistente define automáticamente el grupo de seguridad x del asistente de lanzamiento para que pueda conectarse a la instancia. En su lugar, elija la opción Select an existing security group, seleccione el grupo WebServerSG que creó previamente y, a continuación, elija Review and Launch.
11. En la página Review Instance Launch, compruebe los detalles de la instancia y elija Launch.
12. En el cuadro de diálogo Select an existing key pair or create a new key pair (Seleccionar par de claves existentes o crear nuevo par de claves), puede elegir un par de claves existente o crear uno nuevo. Si decide crear un nuevo par de claves, asegúrese de descargar el archivo y almacenarlo en una ubicación segura. Necesitará el contenido de la clave privada para conectarse a la instancia después de lanzarla.

Para lanzar la instancia, active la casilla de verificación de confirmación y elija Launch Instances.

13. En la página de confirmación, elija View Instances para ver su instancia en la página Instances. Seleccione su instancia y consulte sus detalles en la pestaña Description. El campo Private IPs muestra la dirección IPv4 privada asignada a su instancia desde el rango de direcciones IPv4 de su subred. El campo IPv6 IPs muestra la dirección IPv6 privada asignada a su instancia desde el rango de direcciones IPv6 de su subred.

Es posible conectarse a su instancia a través de su dirección IPv6 desde su red doméstica mediante SSH o a través del Escritorio remoto. El equipo local debe tener una dirección IPv6 y estar configurado para usar IPv6. Para obtener más información acerca de cómo conectarse a una instancia de Linux, consulte [Conexión a una instancia de Linux](#) en la Guía del usuario de Amazon EC2 para instancias de Linux. Para obtener más información acerca de cómo conectarse a una instancia de Windows, consulte [Conectarse a la instancia de Windows mediante RDP](#) en la Guía del usuario de Amazon EC2 para instancias de Windows.

Note

Si también desea que se pueda obtener acceso a su instancia a través de una dirección IPv4 mediante Internet, SSH o RDP, debe asociar una dirección IP elástica (dirección IPv4 pública estática) a su instancia y ajustar las reglas del grupo de seguridad para permitir el acceso mediante IPv4. Para obtener más información, consulte [Introducción a Amazon VPC \(p. 10\)](#).

VPC con una única subred pública

La configuración de este escenario incluye una nube virtual privada (VPC) con una única subred y un puerto de enlace a Internet para permitir la comunicación a través de Internet. Se recomienda esta configuración si necesita ejecutar aplicaciones web públicas y de una sola capa como, por ejemplo, blogs o sitios web sencillos.

Si lo desea, este escenario también se puede configurar para IPv6: puede utilizar el asistente de VPC para crear una VPC y una subred con los bloques de CIDR IPv6 asociados. Las instancias lanzadas en la subred pública podrán recibir direcciones IPv6 y comunicarse a través de IPv6. Para obtener más información acerca de las direcciones IPv4 e IPv6, consulte [Direccionamiento IP \(p. 4\)](#).

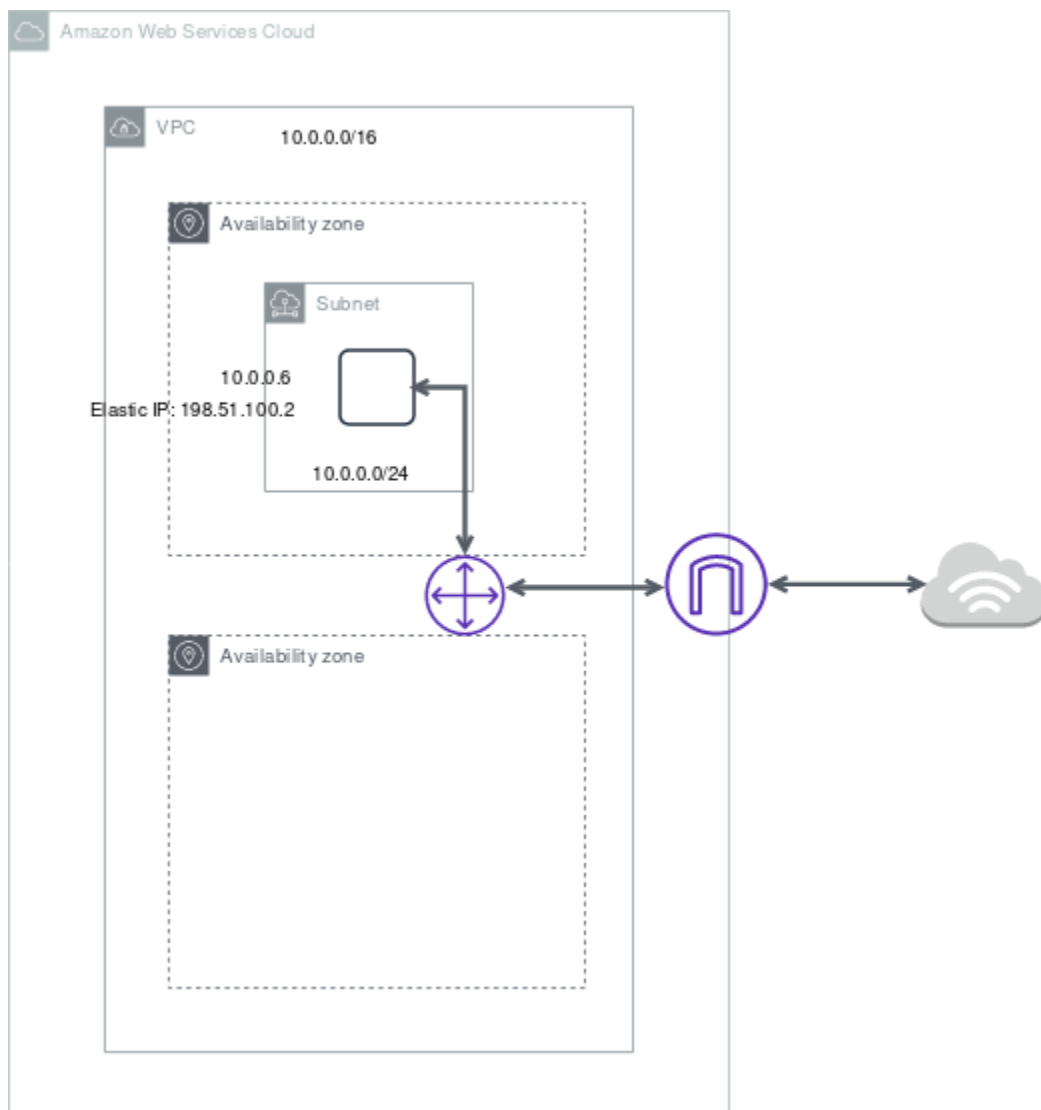
Para obtener información acerca de cómo administrar el software de instancias EC2, consulte [Administración de software en la instancia de Linux](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Contenido

- [Información general \(p. 296\)](#)
- [Direccionamiento \(p. 299\)](#)
- [Seguridad \(p. 300\)](#)

Información general

El siguiente diagrama muestra los componentes clave de la configuración de este escenario.



Note

Si ha completado [Introducción a Amazon VPC \(p. 10\)](#), ya ha implementado este escenario con el asistente de VPC de la consola de Amazon VPC.

La configuración de este escenario incluye lo siguiente:

- Nube virtual privada (VPC) con bloque de CIDR IPv4 de tamaño /16 (ejemplo: 10.0.0.0/16). Esto proporciona 65 536 direcciones IPv4 privadas.
- Subred con bloque de CIDR IPv4 de tamaño /24 (ejemplo: 10.0.0.0/24). Esto proporciona 256 direcciones IPv4 privadas.
- Un gateway de Internet. Esto conecta la VPC a Internet y a otros servicios de AWS.
- Instancia con dirección IPv4 privada en el rango de subred (ejemplo: 10.0.0.6), que permite que la instancia se comuniquen con otras instancias de la VPC y con una dirección IPv4 elástica (ejemplo: 198.51.100.2), que es una dirección IPv4 pública que permite a la instancia el acceso a Internet y que se pueda acceder a esta desde Internet.
- Una tabla de ruteo personalizada asociada a la subred. Las entradas de la tabla de ruteo permiten a las instancias de la subred utilizar IPv4 para comunicarse con las demás instancias de la VPC y para

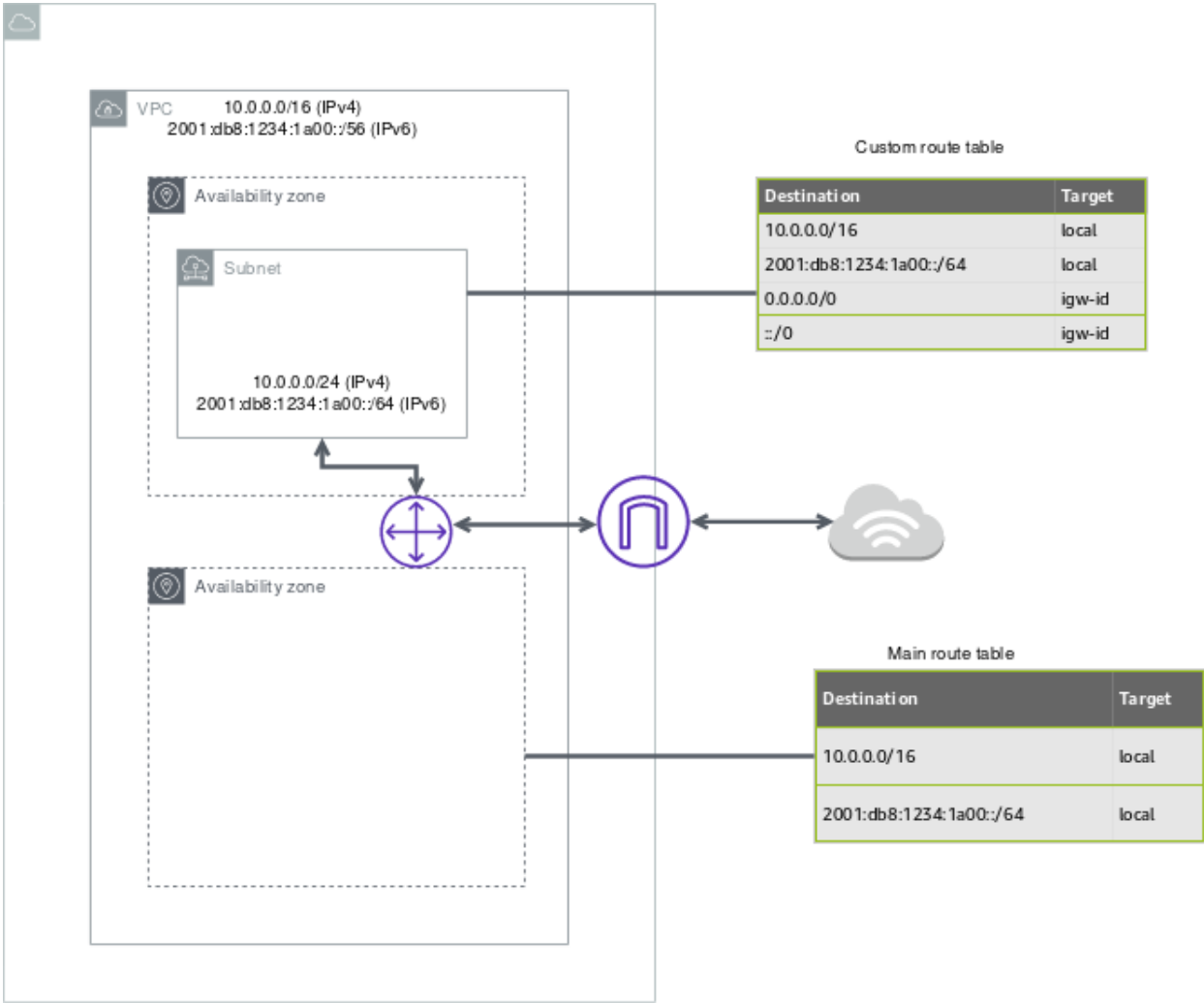
comunicarse directamente a través de internet. La subred asociada a la tabla de ruteo con ruta al puerto de enlace a Internet se conoce como subred pública.

Para obtener más información, consulte . [Subredes \(p. 60\)](#). Para obtener más información acerca de las gateways de Internet, consulte [Conexión a Internet mediante una puerta de enlace de Internet \(p. 142\)](#).

Información general de IPv6

Opcionalmente, puede habilitar IPv6 para este escenario. Además de los componentes mostrados arriba, la configuración incluye lo siguiente:

- Un bloque de CIDR IPv6 de tamaño /56 asociado a la VPC (por ejemplo: 2001:db8:1234:1a00::/56). Amazon asigna automáticamente el CIDR; no podrá elegir el rango por sí mismo.
- Un bloque de CIDR IPv6 de tamaño /64 asociado a la subred pública (por ejemplo: 2001:db8:1234:1a00::/64). Puede elegir el rango de su subred en el rango asignado a la VPC. No es posible elegir el tamaño del bloque de CIDR IPv6 de la subred.
- Una dirección IPv6 asignada a la instancia desde el rango de subred (ejemplo: 2001:db8:1234:1a00::123).
- Entradas de la tabla personalizada que permiten a las instancias de la VPC utilizar IPv6 para comunicarse entre sí y directamente a través de internet.



Direccionamiento

Su VPC tiene un router implícito (tal como se muestra en el diagrama de configuración anterior). En este escenario, el asistente para la creación de VPC crea una tabla de ruteo personalizada que direcciona todo el tráfico con destino a una dirección externa a la VPC a la gateway de Internet para, a continuación, asociar dicha tabla de ruteo a la subred.

La siguiente tabla muestra la tabla de ruteo para el ejemplo del diagrama de configuración anterior. La primera fila es la entrada predeterminada para el direccionamiento IPv4 local de la VPC. Esta entrada permite a las instancias de esta VPC comunicarse entre sí. La segunda entrada dirige el resto del tráfico de la subred IPv4 a la gateway de internet (por ejemplo, igw-1a2b3c4d).

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	igw-id

Direccionamiento de IPv6

Si asocia un bloque de CIDR IPv6 con su VPC y su subred, su tabla de ruteo debe incluir rutas separadas para el tráfico IPv6. La tabla siguiente muestra la tabla de ruteo personalizada para este escenario si elige habilitar la comunicación IPv6 en su VPC. La segunda fila es la ruta predeterminada que se añade automáticamente para el direccionamiento local en la VPC a través de IPv6. La cuarta entrada direcciona todo el resto del tráfico de la subred IPv6 a la gateway de internet.

Destino	Objetivo
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	igw-id
::/0	igw-id

Seguridad

AWS proporciona dos características que puede utilizar para aumentar la seguridad de la VPC: los grupos de seguridad y las ACL de red. Los grupos de seguridad controlan el tráfico de entrada y salida de las instancias, mientras que las ACL de red controlan el tráfico de entrada y salida de las subredes. En la mayoría de los casos, los grupos de seguridad se ajustarán a sus necesidades. No obstante, puede usar también las ACL de red si desea agregar un nivel de seguridad adicional en la VPC. Para obtener más información, consulte [Privacidad del tráfico entre redes en Amazon VPC \(p. 233\)](#).

Para este escenario, se utiliza un grupo de seguridad, pero no una ACL de red. Si desea utilizar una ACL de red, consulte [Reglas de ACL de red recomendadas para una VPC con una única subred pública \(p. 302\)](#).

La VPC incluye un [grupo de seguridad predeterminado \(p. 256\)](#). Una instancia que se lanza en la VPC se asocia automáticamente al grupo de seguridad predeterminado si no especifica ningún grupo de seguridad predeterminado durante el lanzamiento. Puede añadir reglas concretas al grupo de seguridad predeterminado; sin embargo, es posible que las reglas no sean aptas para otras instancias que lance en la VPC. En su lugar, se recomienda crear un grupo de seguridad personalizado para su servidor web.

Para este escenario, cree un grupo de seguridad denominado `WebServerSG`. Cuando cree un grupo de seguridad, este tendrá una regla entrante sencilla que permite el tráfico saliente procedente de las instancias. Debe modificar las reglas para permitir el tráfico entrante y restringir el tráfico saliente según sea necesario. Este grupo de seguridad se especifica al lanzar las instancias en la VPC.

A continuación se describen las reglas y salientes para el tráfico IPv4 del grupo de seguridad `WebServerSG`.

Entrada			
Fuente	Protocolo	Rango de puerto	Comentarios
0.0.0.0/0	TCP	80	Permite el acceso HTTP entrante a los servidores web desde cualquier dirección IPv4.
0.0.0.0/0	TCP	443	Permite el acceso HTTPS entrante a los servidores web desde cualquier dirección IPv4

Rango de direcciones IPv4 públicas de su red	TCP	22	(Instancias de Linux) Permite el acceso SSH entrante desde su red a través de IPv4. Puede obtener la dirección IPv4 pública de su equipo local usando un servicio como, por ejemplo, http://checkip.amazonaws.com o https://checkip.amazonaws.com . Si se conecta a través de un ISP o protegido por su firewall sin una dirección IP estática, deberá encontrar el rango de direcciones IP utilizadas por los equipos cliente.
Rango de direcciones IPv4 públicas de su red	TCP	3389	(Instancias de Windows) Permite el acceso RDP entrante desde su red a través de IPv4.
The security group ID (sg-xxxxxxx)	All	All	(Optional) Allow inbound traffic from other instances associated with this security group. This rule is automatically added to the default security group for the VPC; for any custom security group you create, you must manually add the rule to allow this type of communication.
Saliente (opcional)			
Destino	Protocolo	Rango de puerto	Comentarios
0.0.0.0/0	All	All	Default rule to allow all outbound access to any IPv4 address. If you want your web server to initiate outbound traffic, for example, to get software updates, you can keep the default outbound rule. Otherwise, you can remove this rule.

Reglas de grupo de seguridad para IPv6

Si asocia un bloque de CIDR IPv6 a su VPC y su subred, debe añadir reglas separadas a su grupo de seguridad para controlar el tráfico IPv6 entrante y saliente de su instancia de servidor web. En este escenario, el servidor web podrá recibir todo el tráfico de internet a través de IPv6, así como el tráfico SSH o RDP de su red local a través de IPv6.

A continuación se detallan las reglas específicas de IPv6 para el grupo de seguridad WebServerSG (adicionales a las reglas descritas anteriormente).

Entrada			
Fuente	Protocolo	Rango de puerto	Comentarios
::/0	TCP	80	Permite el acceso HTTP entrante a los servidores web desde cualquier dirección IPv6.
::/0	TCP	443	Permite el acceso HTTPS entrante a los servidores web desde cualquier dirección IPv6.
Rango de direcciones IPv6 de su red	TCP	22	(Instancias de Linux) Permite el acceso SSH entrante desde su red a través de IPv6.
Rango de direcciones IPv6 de su red	TCP	3389	(Instancias de Windows) Permite el acceso RDP entrante desde su red a través de IPv6.
Saliente (opcional)			
Destino	Protocolo	Rango de puerto	Comentarios
::/0	All	All	Default rule to allow all outbound access to any IPv6 address. If you want your web server to initiate outbound traffic, for example, to get software updates, you can keep the default outbound rule. Otherwise, you can remove this rule.

Reglas de ACL de red recomendadas para una VPC con una única subred pública

La tabla siguiente muestra las reglas que recomendamos. Las reglas bloquean todo el tráfico excepto el explícitamente necesario.

Inbound					
Regla n.º	IP de origen	Protocolo	Puerto	Permitir/ Denegar	Comentarios

100	0.0.0.0/0	TCP	80	PERMITIR	Permite el tráfico HTTP entrante de cualquier dirección IPv4.
110	0.0.0.0/0	TCP	443	PERMITIR	Permite el tráfico HTTPS entrante de cualquier dirección IPv4.
120	Rango de direcciones IPv4 públicas de la red doméstica	TCP	22	PERMITIR	Permite el tráfico SSH entrante de su red doméstica (a través de la gateway de Internet).
130	Rango de direcciones IPv4 públicas de la red doméstica	TCP	3389	PERMITIR	Permite el tráfico RDP entrante de su red doméstica (a través de la gateway de Internet).
140	0.0.0.0/0	TCP	32768-65535	PERMITIR	<p>Permite el tráfico de retorno entrante de hosts de Internet que responden a las solicitudes que se originan en la subred.</p> <p>Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133).</p>

*	0.0.0.0/0	Todos	Todos	DENEGAR	Deniega todo el tráfico IPv4 entrante no controlado por ninguna regla precedente (no modificable).
Outbound					
Regla n.º	IP destino	Protocolo	Puerto	Permitir/ Denegar	Comentarios
100	0.0.0.0/0	TCP	80	PERMITIR	Permite el tráfico HTTP saliente de la subred a Internet.
110	0.0.0.0/0	TCP	443	PERMITIR	Permite el tráfico HTTPS saliente de la subred a Internet.
120	0.0.0.0/0	TCP	32768-65535	PERMITIR	Permite las respuestas salientes a clientes de Internet (por ejemplo, al ofrecer páginas web a usuarios que visitan los servidores web de la subred). Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133) .

*	0.0.0.0/0	Todos	Todos	DENEGAR	Deniega todo el tráfico IPv4 saliente no controlado por ninguna regla precedente (no modificable).
---	-----------	-------	-------	---------	--

Reglas de ACL de red recomendadas para IPv6

Si implementó la compatibilidad con el tráfico IPv6 y creó una VPC y una subred con bloques de CIDR IPv6 asociados, deberá añadir reglas separadas a las ACL de red para controlar el tráfico IPv6 entrante y saliente.

A continuación se detallan las reglas específicas de tráfico IPv6 para las ACL de red (adicionales a las reglas anteriores).

Inbound					
Regla n.º	IP de origen	Protocolo	Puerto	Permitir/Denegar	Comentarios
150	::/0	TCP	80	PERMITIR	Permite el tráfico HTTP entrante de cualquier dirección IPv6.
160	::/0	TCP	443	PERMITIR	Permite el tráfico HTTPS entrante de cualquier dirección IPv6.
170	Rango de direcciones IPv6 de la red doméstica	TCP	22	PERMITIR	Permite el tráfico SSH entrante de su red doméstica (a través de la gateway de Internet).
180	Rango de direcciones IPv6 de la red doméstica	TCP	3389	PERMITIR	Permite el tráfico RDP entrante de su red doméstica (a través de la gateway de Internet).
190	::/0	TCP	32768-65535	PERMITIR	Permite el tráfico de retorno entrante de hosts de Internet que responden a

					las solicitudes que se originan en la subred.
					Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133).
*	::/0	Todos	Todos	DENEGAR	Deniega todo el tráfico IPv6 entrante no controlado por ninguna regla precedente (no modificable).
Outbound					
Regla n.º	IP destino	Protocolo	Puerto	Permitir/ Denegar	Comentarios
130	::/0	TCP	80	PERMITIR	Permite el tráfico HTTP saliente de la subred a Internet.
140	::/0	TCP	443	PERMITIR	Permite el tráfico HTTPS saliente de la subred a Internet.

150	::/0	TCP	32768-65535	PERMITIR	<p>Permite las respuestas salientes a clientes de Internet (por ejemplo, al ofrecer páginas web a usuarios que visitan los servidores web de la subred).</p> <p>Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133).</p>
*	::/0	Todos	Todos	DENEGAR	Deniega todo el tráfico IPv6 saliente no controlado por ninguna regla precedente (no modificable).

VPC con subredes privadas y públicas (NAT)

La configuración de este escenario incluye una nube virtual privada (VPC) con una subred pública y una subred privada. Este escenario se recomienda si desea ejecutar una aplicación web pública y, a la vez, mantener los servidores back-end a los que no se puede obtener acceso de forma pública. Un ejemplo común es un sitio web multinivel, con los servidores web en una subred pública y los servidores de base de datos en una subred privada. Puede configurar la seguridad y el direccionamiento para que los servidores web se puedan comunicar con los servidores de base de datos.

Las instancias de la subred pública pueden enviar tráfico de salida directamente a Internet, mientras que las instancias en la subred privada no pueden. En cambio, las instancias de la subred privada pueden obtener acceso a Internet mediante una gateway de traducción de direcciones de red (NAT) que reside en la subred pública. Los servidores de base de datos pueden conectarse a Internet para las actualizaciones de software a través de la gateway NAT, pero Internet no puede establecer conexiones con los servidores de base de datos.

Si lo desea, este escenario también se puede configurar para IPv6: puede utilizar el asistente de VPC para crear una VPC y subredes con los bloques de CIDR IPv6 asociados. Las instancias lanzadas en las subredes podrán recibir direcciones IPv6 y comunicarse a través de IPv6. Las instancias de la subred

privada pueden utilizar una gateway de Internet de solo salida para conectarse a Internet a través de IPv6, pero Internet no puede establecer conexiones con las instancias privadas a través de IPv6. Para obtener más información acerca de las direcciones IPv4 e IPv6, consulte [Direccionamiento IP](#) (p. 4).

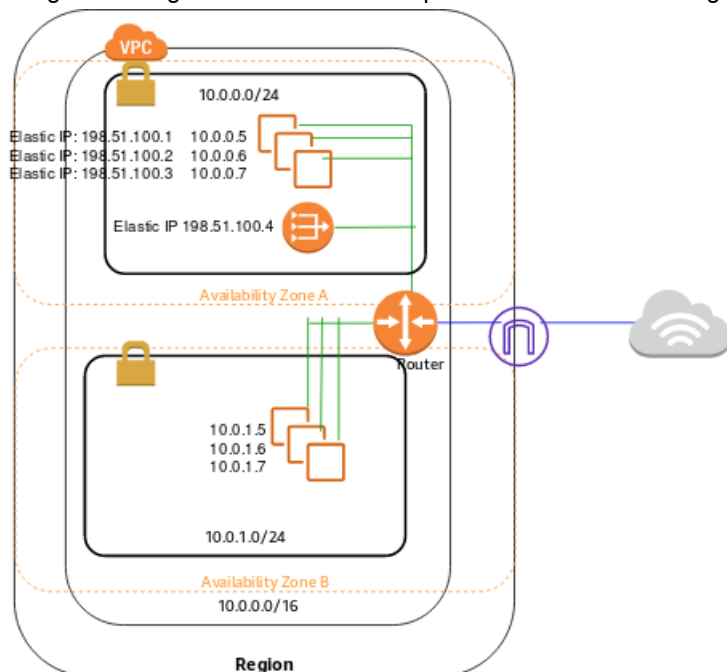
Para obtener información acerca de cómo administrar el software de instancias EC2, consulte [Administración de software en la instancia de Linux](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Contenido

- [Información general](#) (p. 308)
- [Direccionamiento](#) (p. 311)
- [Seguridad](#) (p. 312)
- [Implementar el escenario 2](#) (p. 316)
- [Reglas ACL de red recomendadas para una VPC con subredes públicas y privadas \(NAT\)](#) (p. 316)

Información general

El siguiente diagrama muestra los componentes clave de la configuración de este escenario.



La configuración de este escenario incluye lo siguiente:

- Una VPC con bloque de CIDR IPv4 de tamaño /16 (ejemplo: 10.0.0.0/16). Esto proporciona 65 536 direcciones IPv4 privadas.
- Una subred pública con bloque de CIDR IPv4 de tamaño /24 (ejemplo: 10.0.0.0/24). Esto proporciona 256 direcciones IPv4 privadas. Una subred pública es una subred asociada a la tabla de ruteo con ruta a la gateway de internet.
- Una subred privada con bloque de CIDR IPv4 de tamaño /24 (ejemplo: 10.0.1.0/24). Esto proporciona 256 direcciones IPv4 privadas.
- Un gateway de Internet. Esto conecta la VPC a Internet y a otros servicios de AWS.
- Instancias con direcciones IPv4 privadas en el rango de la subred (ejemplos: 10.0.0.5, 10.0.1.5). Esto les permite comunicarse entre sí y con otras instancias en la VPC.

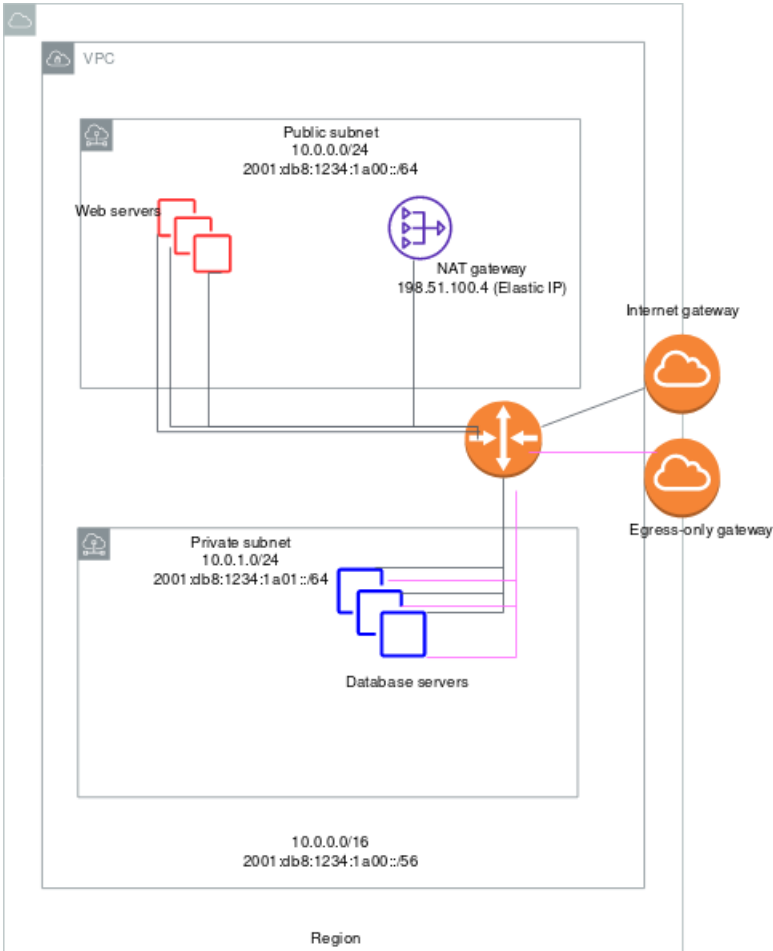
- Instancias en la subred pública con direcciones IPv4 elásticas (por ejemplo: 198.51.100.1), que son direcciones IPv4 públicas que lo habilitan para llegar a ellas desde Internet. Las instancias pueden tener direcciones IP públicas asignadas en el lanzamiento en lugar de direcciones IP elásticas. Las instancias de la subred privada son servidores backend que no necesitan aceptar el tráfico entrante de Internet y, por lo tanto, no tienen direcciones IP públicas; sin embargo, pueden enviar solicitudes a Internet mediante la gateway NAT (consulte la siguiente viñeta).
- Una gateway NAT con su propia dirección IPv4 elástica. Las instancias de la subred privada pueden enviar solicitudes a Internet mediante la gateway NAT través de IPv4 (por ejemplo, para actualizaciones de software).
- Una tabla de ruteo personalizada asociada a la subred pública. Esta tabla de enrutamiento contiene una entrada que lo habilita para que las instancias de la subred se comuniquen con otras instancias de la VPC a través de IPv4 y una entrada que permite que las instancias de la subred se comuniquen directamente con Internet a través de IPv4.
- La tabla de ruteo principal asociada a una subred privada. La tabla de enrutamiento contiene una entrada que lo habilita para que las instancias de la subred se comuniquen con otras instancias de la VPC a través de IPv4 y una entrada que permite que las instancias de la subred se comuniquen con Internet mediante la gateway NAT a través de IPv4.

Para obtener más información, consulte [Subredes \(p. 60\)](#). Para obtener más información acerca de las gateways de Internet, consulte [Conexión a Internet mediante una puerta de enlace de Internet \(p. 142\)](#). Para obtener más información acerca de las gateways NAT, consulte [Gateways NAT \(p. 157\)](#).

Información general de IPv6

Opcionalmente, puede habilitar IPv6 para este escenario. Además de los componentes mostrados arriba, la configuración incluye lo siguiente:

- Un bloque de CIDR IPv6 de tamaño /56 asociado a la VPC (por ejemplo: 2001:db8:1234:1a00::/56). Amazon asigna automáticamente el CIDR; no podrá elegir el rango por sí mismo.
- Un bloque de CIDR IPv6 de tamaño /64 asociado a la subred pública (por ejemplo: 2001:db8:1234:1a00::/64). Puede elegir el rango de su subred en el rango asignado a la VPC. No es posible elegir el tamaño del bloque de CIDR IPv6 de la VPC.
- Un bloque de CIDR IPv6 de tamaño /64 asociado a la subred privada (por ejemplo: 2001:db8:1234:1a01::/64). Puede elegir el rango de su subred en el rango asignado a la VPC. No es posible elegir el tamaño del bloque de CIDR IPv6 de la subred.
- Las direcciones IPv6 asignadas a las instancias desde el rango de subred (ejemplo: 2001:db8:1234:1a00::1a).
- Una gateway de Internet de solo salida. Utilice la gateway a fin de gestionar solicitudes a Internet desde instancias de la subred privada a través de IPv6 (por ejemplo, para actualizaciones de software). Se requiere una gateway de Internet de solo salida si desea que las instancias de la subred privada puedan iniciar la comunicación con Internet a través de IPv6. Para obtener más información, consulte [Habilitar el tráfico IPv6 saliente mediante una puerta de enlace de Internet de solo salida \(p. 153\)](#).
- Entradas de la tabla personalizada que permiten a las instancias de la subred pública utilizar IPv6 para comunicarse entre sí y directamente a través de Internet.
- Las entradas de tabla de enrutamiento en la tabla de enrutamiento principal que permiten que las instancias de la subred privada utilicen IPv6 con el fin de comunicarse entre sí, así como para comunicarse con Internet a través de una gateway de Internet de solo salida.



Los servidores web de la subred pública tienen las siguientes direcciones.

Servidor	Dirección IPv4	Dirección IP elástica	Dirección IPv6
1	10.0.0.5	198.51.100.1	2001:db8:1234:1a00::1a
2	10.0.0.6	198.51.100.2	2001:db8:1234:1a00::2b
3	10.0.0.7	198.51.100.3	2001:db8:1234:1a00::3c

Los servidores de base de datos de la subred privada tienen las siguientes direcciones.

Servidor	Dirección IPv4	Dirección IPv6
1	10.0.1.5	2001:db8:1234:1a01::1a
2	10.0.1.6	2001:db8:1234:1a01::2b
3	10.0.1.7	2001:db8:1234:1a01::3c

Direccionamiento

En este escenario, el asistente de VPC actualiza la tabla de ruteo principal utilizada con la subred privada, y crea una tabla de ruteo personalizada y la asocia a la subred pública.

En este caso, todo el tráfico de las subredes que esté vinculado a AWS (por ejemplo, a los puntos de enlace de Amazon EC2 o Amazon S3) pasará a través de la puerta de enlace de Internet. Los servidores de base de datos de la subred privada no pueden recibir tráfico de Internet directamente porque no tienen direcciones IP elásticas. Sin embargo, los servidores de base de datos pueden enviar y recibir tráfico de Internet a través del dispositivo NAT en la subred pública.

Las subredes adicionales que cree utilizarán la tabla de ruteo principal de forma predeterminada, lo que significa que son subredes privadas de forma predeterminada. Si desea hacer una subred pública, siempre puede cambiar la tabla de ruteo con la que esté asociada.

Las siguientes tablas describen las tablas de ruteo para este escenario.

Tabla de enrutamiento principal

La tabla de enrutamiento principal está asociada a una subred privada. La primera fila es la entrada predeterminada para el direccionamiento local de la VPC. Esta entrada permite a las instancias de la VPC comunicarse entre sí. La segunda entrada envía el resto del tráfico de la subred a la gateway NAT (por ejemplo, nat-12345678901234567).

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	nat-gateway-id

Tabla de enrutamiento personalizada

La tabla de enrutamiento personalizada está asociada a la subred pública. La primera fila es la entrada predeterminada para el direccionamiento local de la VPC. Esta entrada permite a las instancias de esta VPC comunicarse entre sí. La segunda entrada direcciona el resto del tráfico de la subred a Internet a través de la gateway de Internet (por ejemplo, igw-1a2b3d4d).

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	igw-id

Direccionamiento de IPv6

Si asocia un bloque de CIDR IPv6 con su VPC y sus subredes, sus tablas de ruteo deben incluir rutas separadas para el tráfico IPv6. Las tablas siguientes muestran las tablas de ruteo personalizadas para este escenario si elige habilitar la comunicación IPv6 en su VPC.

Tabla de enrutamiento principal

La segunda fila es la ruta predeterminada que se añade automáticamente para el direccionamiento local en la VPC a través de IPv6. La cuarta entrada direcciona todo el resto del tráfico de la subred IPv6 a la gateway de Internet de solo salida.

Destino	Objetivo
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	nat-gateway-id
::/0	egress-only-igw-id

Tabla de enrutamiento personalizada

La segunda fila es la ruta predeterminada que se añade automáticamente para el direccionamiento local en la VPC a través de IPv6. La cuarta entrada direcciona todo el resto del tráfico de la subred IPv6 a la gateway de internet.

Destino	Objetivo
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	igw-id
::/0	igw-id

Seguridad

AWS proporciona dos características que puede utilizar para aumentar la seguridad de la VPC: los grupos de seguridad y las ACL de red. Los grupos de seguridad controlan el tráfico de entrada y salida de las instancias, mientras que las ACL de red controlan el tráfico de entrada y salida de las subredes. En la mayoría de los casos, los grupos de seguridad se ajustarán a sus necesidades. No obstante, puede usar también las ACL de red si desea agregar un nivel de seguridad adicional en la VPC. Para obtener más información, consulte [Privacidad del tráfico entre redes en Amazon VPC \(p. 233\)](#).

Para el escenario 2, utilizará los grupos de seguridad, pero no las ACL de red. Si desea utilizar una ACL de red, consulte [Reglas ACL de red recomendadas para una VPC con subredes públicas y privadas \(NAT\) \(p. 316\)](#).

La VPC incluye un [grupo de seguridad predeterminado \(p. 256\)](#). Una instancia que se lanza en la VPC se asocia automáticamente al grupo de seguridad predeterminado si no especifica ningún grupo de seguridad predeterminado durante el lanzamiento. Para este escenario, recomendamos crear los siguientes grupos de seguridad en lugar de utilizar el grupo de seguridad predeterminado:

- WebServerSG: especifique este grupo de seguridad al lanzar los servidores web en la subred pública.
- DBServerSG: especifique este grupo de seguridad al lanzar los servidores de base de datos en la subred privada.

Las instancias asignadas a un grupo de seguridad pueden estar en distintas subredes. Sin embargo, en este escenario, cada grupo de seguridad corresponde al tipo de función que desempeña una instancia, y cada función requiere que una instancia esté en una subred determinada. Por lo tanto, en este escenario, todas las instancias asignadas a un grupo de seguridad estarán en la misma subred.

La siguiente tabla describe las reglas recomendadas para el grupo de seguridad WebServerSG, que permiten a los servidores web recibir el tráfico de internet, así como el tráfico SSH y RDP procedente de su

red. Los servidores web también pueden iniciar solicitudes de lectura y escritura en los servidores de bases de datos de la subred privada, así como enviar tráfico a Internet; por ejemplo, para obtener actualizaciones de software. Puesto que el servidor web no inicia ninguna otra comunicación saliente, se ha quitado la regla saliente predeterminada.

Note

Estas recomendaciones incluyen tanto acceso a SSH como a RDP, así como acceso a Microsoft SQL Server y a MySQL. En su caso, puede que solo necesite reglas para Linux (SSH y MySQL) o Windows (RDP y Microsoft SQL Server).

WebServerSG: reglas recomendadas

Entrada			
Fuente	Protocolo	Rango de puerto	Comentarios
0.0.0.0/0	TCP	80	Permite el acceso HTTP entrante a los servidores web desde cualquier dirección IPv4.
0.0.0.0/0	TCP	443	Permite el acceso HTTPS entrante a los servidores web desde cualquier dirección IPv4.
Rango de direcciones IPv4 públicas de su red doméstica	TCP	22	Permite el acceso SSH entrante a las instancias de Linux desde la red doméstica (a través de la gateway de Internet). Puede obtener la dirección IPv4 pública de su equipo local usando un servicio como, por ejemplo, http://checkip.amazonaws.com o https://checkip.amazonaws.com . Si se conecta a través de un ISP o protegido por su firewall sin una dirección IP estática, deberá encontrar el rango de direcciones IP utilizadas por los equipos cliente.
Rango de direcciones IPv4 públicas de su red doméstica	TCP	3389	Permite el acceso RDP entrante a las instancias de Windows desde la red doméstica (a través de la gateway de Internet).
Salida			
Destino	Protocolo	Rango de puerto	Comentarios

ID del grupo de seguridad DBServerSG	TCP	1433	Permite el acceso saliente de Microsoft SQL Server a los servidores de base de datos asignados al grupo de seguridad DBServerSG.
ID del grupo de seguridad DBServerSG	TCP	3306	Permite el acceso saliente de MySQL a los servidores de base de datos asignados al grupo de seguridad DBServerSG.
0.0.0.0/0	TCP	80	Permite el acceso HTTP saliente a cualquier dirección IPv4.
0.0.0.0/0	TCP	443	Permite el acceso HTTPS saliente a cualquier dirección IPv4.

La siguiente tabla describe las reglas recomendadas para el grupo de seguridad DBServerSG, que permiten las solicitudes de las bases de datos de lectura o escritura procedentes de los servidores web. Los servidores de base de datos también pueden iniciar el tráfico vinculado a Internet (la tabla de enrutamiento envía ese tráfico a la gateway NAT, que lo reenvía a Internet a través de la gateway de Internet).

DBServerSG: reglas recomendadas

Entrada			
Fuente	Protocolo	Rango de puerto	Comentarios
ID del grupo de seguridad WebServerSG	TCP	1433	Permite el acceso entrante de Microsoft SQL Server desde los servidores web asociados al grupo de seguridad WebServerSG.
ID del grupo de seguridad WebServerSG	TCP	3306	Permite el acceso entrante del servidor MySQL desde los servidores web asociados al grupo de seguridad WebServerSG.
Salida			
Destino	Protocolo	Rango de puerto	Comentarios
0.0.0.0/0	TCP	80	Permite el acceso saliente de HTTP a Internet a través de

0.0.0.0/0	TCP	443	IPv4 (por ejemplo, para actualizaciones de software). Permite el acceso saliente de HTTPS a Internet a través de IPv4 (por ejemplo, para actualizaciones de software).
-----------	-----	-----	---

(Opcional) El grupo de seguridad predeterminado de una VPC tiene reglas que permiten, de forma automática, que las instancias asignadas se comuniquen entre sí. Para permitir ese tipo de comunicación para un grupo de seguridad personalizado, debe añadir las siguientes reglas:

Entrada			
Fuente	Protocolo	Rango de puerto	Comentarios
El ID del grupo de seguridad	Todos	Todos	Permite el tráfico entrante desde otras instancias asignadas a este grupo de seguridad.
Salida			
Destino	Protocolo	Rango de puerto	Comentarios
The ID of the security group	All	All	Allow outbound traffic to other instances assigned to this security group.

(Opcional) Si lanza un host bastión en su subred pública para utilizarlo como proxy para tráfico SSH o RDP desde su red doméstica a su subred privada, añada una regla al grupo de seguridad DBServerSG que permita tráfico SSH o RDP de entrada desde la instancia bastión o su grupo de seguridad asociado.

Reglas de grupo de seguridad para IPv6

Si asocia un bloque de CIDR IPv6 a su VPC y sus subredes, debe añadir reglas separadas a sus grupos de seguridad WebServerSG y DBServerSG para controlar el tráfico IPv6 entrante y saliente de sus instancias. En este escenario, los servidores web podrán recibir todo el tráfico de internet a través de IPv6, así como el tráfico SSH o RDP de su red local a través de IPv6. Asimismo, pueden iniciar tráfico IPv6 saliente a internet. Los servidores de base de datos pueden iniciar tráfico IPv6 saliente a Internet.

A continuación se detallan las reglas específicas de IPv6 para el grupo de seguridad WebServerSG (adicionales a las reglas descritas anteriormente).

Entrada			
Fuente	Protocolo	Rango de puerto	Comentarios
::/0	TCP	80	Permite el acceso HTTP entrante a los servidores web desde cualquier dirección IPv6.

::/0	TCP	443	Permite el acceso HTTPS entrante a los servidores web desde cualquier dirección IPv6.
Rango de direcciones IPv6 de su red	TCP	22	(Instancias de Linux) Permite el acceso SSH entrante desde su red a través de IPv6.
Rango de direcciones IPv6 de su red	TCP	3389	(Instancias de Windows) Permite el acceso RDP entrante desde su red a través de IPv6.
Salida			
Destino	Protocolo	Rango de puerto	Comentarios
::/0	TCP	HTTP	Allow outbound HTTP access to any IPv6 address.
::/0	TCP	HTTPS	Allow outbound HTTPS access to any IPv6 address.

A continuación se detallan las reglas específicas de IPv6 para el grupo de seguridad DBServerSG (adicionales a las reglas descritas anteriormente).

Salida			
Destino	Protocolo	Rango de puerto	Comentarios
::/0	TCP	80	Permite el acceso HTTP saliente a cualquier dirección IPv6.
::/0	TCP	443	Permite el acceso HTTPS saliente a cualquier dirección IPv6.

Implementar el escenario 2

Puede utilizar el asistente de VPC para crear la VPC, las subredes, la gateway NAT y, opcionalmente, una gateway de Internet de solo salida. Debe especificar una dirección IP elástica para su gateway NAT; si no tiene una, debe asignar primero una a su cuenta. Si desea utilizar una dirección IP elástica existente, asegúrese de que no esté actualmente asociada a otra instancia o interfaz de red. La gateway NAT se creará automáticamente en la subred pública de su VPC.

Reglas ACL de red recomendadas para una VPC con subredes públicas y privadas (NAT)

Para este escenario, dispondrá de una ACL de red para la subred pública y una ACL de red distinta para la subred privada. La tabla siguiente muestra las reglas que recomendamos para cada ACL. Las reglas bloquean todo el tráfico excepto el explícitamente necesario. Estas reglas imitan en gran medida las reglas del grupo de seguridad para el escenario.

Reglas de ACL para la subred pública

Inbound					
Regla n.º	IP de origen	Protocolo	Puerto	Permitir/ Denegar	Comentarios
100	0.0.0.0/0	TCP	80	PERMITIR	Permite el tráfico HTTP entrante de cualquier dirección IPv4.
110	0.0.0.0/0	TCP	443	PERMITIR	Permite el tráfico HTTPS entrante de cualquier dirección IPv4.
120	Rango de direcciones IP públicas de la red doméstica	TCP	22	PERMITIR	Permite el tráfico SSH entrante de su red doméstica (a través de la gateway de Internet).
130	Rango de direcciones IP públicas de la red doméstica	TCP	3389	PERMITIR	Permite el tráfico RDP entrante de su red doméstica (a través de la gateway de Internet).
140	0.0.0.0/0	TCP	1024 - 65535	PERMITIR	<p>Permite el tráfico de retorno entrante de hosts de Internet que responden a las solicitudes que se originan en la subred.</p> <p>Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración,</p>

Outbound	*	0.0.0.0/0	Todos	Todos	DENEGAR	consulte Puertos efimeros (p. 133) . Deniega todo el tráfico IPv4 entrante no controlado por ninguna regla precedente (no modificable).
	Regla n.º	IP destino	Protocolo	Puerto	Permitir/ Denegar	Comentarios
	100	0.0.0.0/0	TCP	80	PERMITIR	Permite el tráfico HTTP saliente de la subred a Internet.
	110	0.0.0.0/0	TCP	443	PERMITIR	Permite el tráfico HTTPS saliente de la subred a Internet.

120	10.0.1.0/24	TCP	1433	PERMITIR	<p>Permite el acceso de MS SQL saliente a los servidores de bases de datos de la subred privada.</p> <p>Este número de puerto se proporciona solo como ejemplo. Otros ejemplos incluyen el número de puerto 3306 para el acceso de MySQL/Aurora, el número 5432 para el acceso de PostgreSQL, el número 5439 para el acceso de Amazon Redshift o el número 1521 para el acceso de Oracle.</p>
-----	-------------	-----	------	----------	---

140	0.0.0.0/0	TCP	32768-65535	PERMITIR	<p>Permite las respuestas salientes a clientes de Internet (por ejemplo, al ofrecer páginas web a usuarios que visitan los servidores web de la subred).</p> <p>Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133).</p>
150	10.0.1.0/24	TCP	22	PERMITIR	Permite el acceso SSH saliente a las instancias de su subred privada (desde un bastión SSH, si es su caso).
*	0.0.0.0/0	Todos	Todos	DENEGAR	Deniega todo el tráfico IPv4 saliente no controlado por ninguna regla precedente (no modificable).

Reglas de ACL para la subred privada

Inbound					
Regla n.º	IP de origen	Protocolo	Puerto	Permitir/Denegar	Comentarios
100	10.0.0.0/24	TCP	1433	PERMITIR	Permite a los servidores web de la subred

					<p>pública realizar operaciones de lectura y escritura en servidores de MS SQL de la subred privada.</p> <p>Este número de puerto se proporciona solo como ejemplo. Otros ejemplos incluyen el número de puerto 3306 para el acceso de MySQL/Aurora, el número 5432 para el acceso de PostgreSQL, el número 5439 para el acceso de Amazon Redshift o el número 1521 para el acceso de Oracle.</p>
120	10.0.0.0/24	TCP	22	PERMITIR	Permite el tráfico SSH entrante de un bastión SSH en la subred pública (si es su caso).
130	10.0.0.0/24	TCP	3389	PERMITIR	Permite el tráfico RDP entrante de una gateway de Microsoft Terminal Services en la subred pública.

140	0.0.0.0/0	TCP	1024 - 65535	PERMITIR	<p>Permite el tráfico de retorno entrante del dispositivo NAT de la subred pública de solicitudes que se originan en la subred privada.</p> <p>Para obtener información acerca de la especificación de los puertos efímeros correctos, consulte la nota importante que se proporciona al principio de este tema.</p>
*	0.0.0.0/0	Todos	Todos	DENEGAR	Deniega todo el tráfico IPv4 entrante no controlado por ninguna regla precedente (no modificable).
Outbound					
Regla n.º	IP destino	Protocolo	Puerto	Permitir/ Denegar	Comentarios
100	0.0.0.0/0	TCP	80	PERMITIR	Permite el tráfico HTTP saliente de la subred a Internet.
110	0.0.0.0/0	TCP	443	PERMITIR	Permite el tráfico HTTPS saliente de la subred a Internet.

120	10.0.0.0/24	TCP	32768-65535	PERMITIR	<p>Permite las respuestas salientes a la subred pública (por ejemplo, respuestas a servidores web de la subred pública que se comunican con servidores de bases de datos de la subred privada).</p> <p>Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133).</p>
*	0.0.0.0/0	Todos	Todos	DENEGAR	Deniega todo el tráfico IPv4 saliente no controlado por ninguna regla precedente (no modificable).

Reglas de ACL de red recomendadas para IPv6

Si implementó la compatibilidad con el tráfico IPv6 y creó una VPC y subredes con bloques de CIDR IPv6 asociados, deberá añadir reglas separadas a las ACL de red para controlar el tráfico IPv6 entrante y saliente.

A continuación se detallan las reglas específicas de tráfico IPv6 para las ACL de red (adicionales a las reglas descritas anteriormente).

Reglas de ACL para la subred pública

Inbound					
Regla n.º	IP de origen	Protocolo	Puerto	Permitir/ Denegar	Comentarios

150	::/0	TCP	80	PERMITIR	Permite el tráfico HTTP entrante de cualquier dirección IPv6.
160	::/0	TCP	443	PERMITIR	Permite el tráfico HTTPS entrante de cualquier dirección IPv6.
170	Rango de direcciones IPv6 de la red doméstica	TCP	22	PERMITIR	Permite el tráfico SSH entrante a través de IPv6 de su red doméstica (a través de la gateway de Internet).
180	Rango de direcciones IPv6 de la red doméstica	TCP	3389	PERMITIR	Permite el tráfico RDP entrante a través de IPv6 de su red doméstica (a través de la gateway de Internet).

190	::/0	TCP	1024 - 65535	PERMITIR	<p>Permite el tráfico de retorno entrante de hosts de Internet que responden a las solicitudes que se originan en la subred.</p> <p>Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133).</p>
*	::/0	Todos	Todos	DENEGAR	Deniega todo el tráfico IPv6 entrante no controlado por ninguna regla precedente (no modificable).
Outbound					
Regla n.º	IP destino	Protocolo	Puerto	Permitir/ Denegar	Comentarios
160	::/0	TCP	80	PERMITIR	Permite el tráfico HTTP saliente de la subred a Internet.
170	::/0	TCP	443	PERMITIR	Permite el tráfico HTTPS saliente de la subred a Internet.

180	2001:db8:1234:1a::64	1433	PERMITIR	<p>Permite el acceso de MS SQL saliente a los servidores de bases de datos de la subred privada.</p> <p>Este número de puerto se proporciona solo como ejemplo. Otros ejemplos incluyen el número de puerto 3306 para el acceso de MySQL/Aurora, el número 5432 para el acceso de PostgreSQL, el número 5439 para el acceso de Amazon Redshift o el número 1521 para el acceso de Oracle.</p>
-----	----------------------	------	----------	---

200	::/0	TCP	32768-65535	PERMITIR	<p>Permite las respuestas salientes a clientes de Internet (por ejemplo, al ofrecer páginas web a usuarios que visitan los servidores web de la subred).</p> <p>Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133).</p>
210	2001:db8:1234:1a::/64	TCP	22	PERMITIR	Permite el acceso SSH saliente a las instancias de su subred privada (desde un bastión SSH, si es su caso).
*	::/0	Todos	Todos	DENEGAR	Deniega todo el tráfico IPv6 saliente no controlado por ninguna regla precedente (no modificable).

Reglas de ACL para la subred privada

Inbound					
Regla n.º	IP de origen	Protocolo	Puerto	Permitir/Denegar	Comentarios
150	2001:db8:1234:1a::/64	TCP	1433	PERMITIR	Permite a los servidores web de la subred

					<p>pública realizar operaciones de lectura y escritura en servidores de MS SQL de la subred privada.</p> <p>Este número de puerto se proporciona solo como ejemplo. Otros ejemplos incluyen el número de puerto 3306 para el acceso de MySQL/Aurora, el número 5432 para el acceso de PostgreSQL, el número 5439 para el acceso de Amazon Redshift o el número 1521 para el acceso de Oracle.</p>
170	2001:db8:1234:1a::64	22	PERMITIR		Permite el tráfico SSH entrante de un bastión SSH en la subred pública (si procede).
180	2001:db8:1234:1a::64	3389	PERMITIR		Permite el tráfico RDP entrante de una gateway de Microsoft Terminal Services en la subred pública, si procede.

190	::/0	TCP	1024 - 65535	PERMITIR	<p>Permite el tráfico de retorno entrante de la gateway de Internet de solo salida de solicitudes que se originan en la subred privada.</p> <p>Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133).</p>
*	::/0	Todos	Todos	DENEGAR	Deniega todo el tráfico IPv6 entrante no controlado por ninguna regla precedente (no modificable).
Outbound					
Regla n.º	IP destino	Protocolo	Puerto	Permitir/Denegar	Comentarios
130	::/0	TCP	80	PERMITIR	Permite el tráfico HTTP saliente de la subred a Internet.
140	::/0	TCP	443	PERMITIR	Permite el tráfico HTTPS saliente de la subred a Internet.

150	2001:db8:1234:1a00::64	32768-65535	PERMITIR	Permite las respuestas salientes a la subred pública (por ejemplo, respuestas a servidores web de la subred pública que se comunican con servidores de bases de datos de la subred privada).
				Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133) .
*	::/0	Todos	Todos	DENEGAR
				Deniega todo el tráfico IPv6 saliente no controlado por ninguna regla precedente (no modificable).

VPC con subredes públicas y privadas y acceso de AWS Site-to-Site VPN

La configuración de este escenario incluye una nube virtual privada (VPC) con una subred pública y una subred privada, así como una gateway privada virtual para habilitar la comunicación con su propia red a través de un túnel de VPN IPsec. Este escenario es recomendable si desea llevar su red a la nube y obtener acceso directo a internet desde la VPC. Este escenario le permite ejecutar una aplicación multinivel con un front-end web escalable en una subred pública, así como alojar sus datos en una subred privada conectada a su red mediante una conexión de AWS Site-to-Site VPN de IPsec.

Si lo desea, este escenario también se puede configurar para IPv6: puede utilizar el asistente de VPC para crear una VPC y subredes con los bloques de CIDR IPv6 asociados. Las instancias lanzadas en las subredes pueden recibir direcciones IPv6. No se admite la comunicación IPv6 mediante una conexión de VPN de sitio a sitio en una gateway privada virtual; no obstante, las instancias de la VPC se pueden comunicar entre sí mediante IPv6 y las instancias de la subred pública se pueden comunicar a través de

Internet mediante IPv6. Para obtener más información acerca de las direcciones IPv4 e IPv6, consulte [Direccionamiento IP](#) (p. 4).

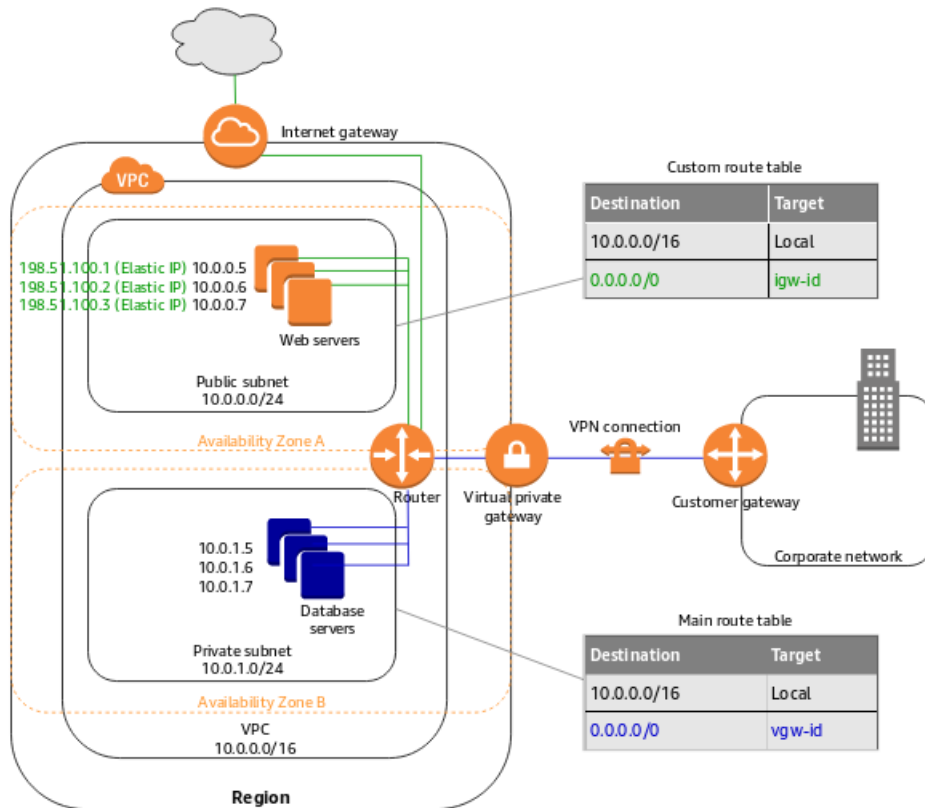
Para obtener información acerca de cómo administrar el software de instancias EC2, consulte [Administración de software en la instancia de Linux](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Contenido

- [Información general](#) (p. 331)
- [Direccionamiento](#) (p. 334)
- [Seguridad](#) (p. 336)
- [Implementar el escenario 3](#) (p. 340)
- [Reglas ACL recomendadas para una VPC con subredes públicas y privadas y acceso de AWS Site-to-Site VPN](#) (p. 340)

Información general

El siguiente diagrama muestra los componentes clave de la configuración de este escenario.



Important

Para este caso, consulte [Su dispositivo de puerta de enlace de cliente](#) en la Guía del usuario de AWS Site-to-Site VPN para obtener información acerca de cómo configurar el dispositivo de puerta de enlace de cliente en el lado de la conexión de Site-to-Site VPN.

La configuración de este escenario incluye lo siguiente:

- Una nube virtual privada (VPC) con CIDR IPv4 de tamaño /16 (ejemplo: 10.0.0.0/16). Esto proporciona 65 536 direcciones IPv4 privadas.

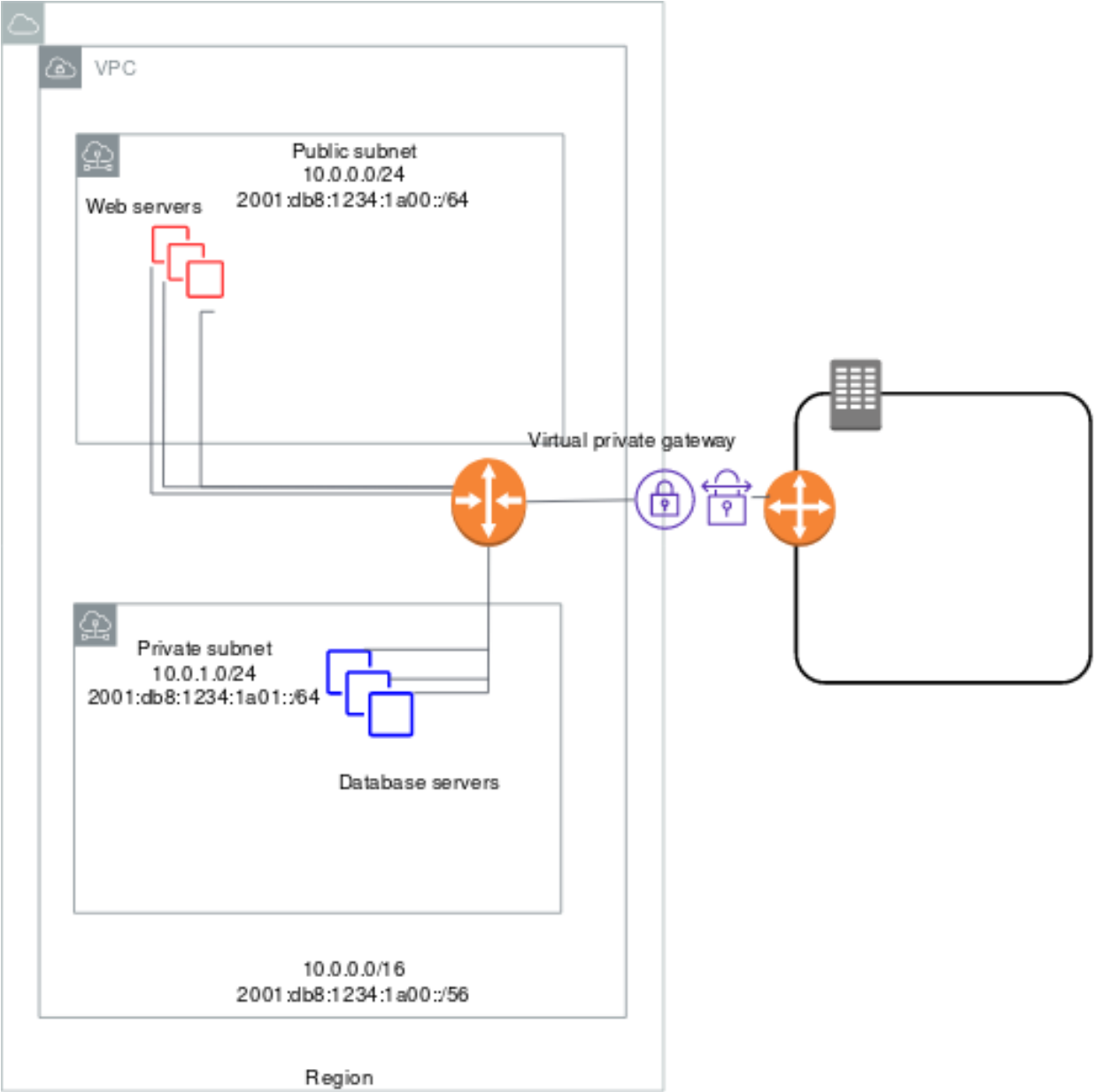
- Una subred pública con CIDR IPv4 de tamaño /24 (ejemplo: 10.0.0.0/24). Esto proporciona 256 direcciones IPv4 privadas. Una subred pública es una subred asociada a la tabla de ruteo con ruta a la gateway de internet.
- Una subred de solo VPN con CIDR IPv4 de tamaño /24 (ejemplo: 10.0.1.0/24). Esto proporciona 256 direcciones IPv4 privadas.
- Un gateway de Internet. Esto conecta la VPC a Internet y a otros productos de AWS.
- Una conexión de VPN de sitio a sitio entre la VPC y la red. La conexión de VPN de sitio a sitio consta de una gateway privada virtual ubicada en el lado de Amazon de la conexión de VPN de sitio a sitio y una gateway de cliente ubicada en su lado de la conexión de VPN de sitio a sitio.
- Instancias con direcciones IPv4 privadas en el rango de la subred (por ejemplo: 10.0.0.5 y 10.0.1.5), lo que permite que las instancias se comuniquen entre sí y con otras instancias de la VPC.
- Instancias en la subred pública con direcciones IP elásticas (por ejemplo: 198.51.100.1), que son direcciones IPv4 públicas que les permiten estar accesibles desde internet. Las instancias pueden tener direcciones IPv4 públicas asignadas en el lanzamiento en lugar de direcciones IP elásticas. Las instancias de la subred de solo VPN son servidores back-end que no necesitan aceptar el tráfico entrante de internet, pero pueden enviar y recibir tráfico desde su red.
- Una tabla de ruteo personalizada asociada a la subred pública. Esta tabla de ruteo contiene una entrada que permite que las instancias de la subred se comuniquen con otras instancias de la VPC, y una entrada que permite que las instancias de la subred se comuniquen directamente con internet.
- La tabla de ruteo principal asociada a una subred de solo VPN. La tabla de ruteo contiene una entrada que permite que las instancias de la subred se comuniquen con otras instancias de la VPC, y una entrada que permite que las instancias de la subred se comuniquen directamente con su red.

Para obtener más información, consulte [Subredes \(p. 60\)](#). Para obtener más información acerca de las gateways de Internet, consulte [Conexión a Internet mediante una puerta de enlace de Internet \(p. 142\)](#). Para obtener más información sobre su conexión de AWS Site-to-Site VPN, consulte la [Guía del usuario de AWS Site-to-Site VPN](#).

Información general de IPv6

Opcionalmente, puede habilitar IPv6 para este escenario. Además de los componentes mostrados arriba, la configuración incluye lo siguiente:

- Un bloque de CIDR IPv6 de tamaño /56 asociado a la VPC (por ejemplo: 2001:db8:1234:1a00::/56). AWS asigna automáticamente el CIDR; no podrá elegir el rango por sí mismo.
- Un bloque de CIDR IPv6 de tamaño /64 asociado a la subred pública (por ejemplo: 2001:db8:1234:1a00::/64). Puede elegir el rango de su subred en el rango asignado a la VPC. No es posible elegir el tamaño del CIDR IPv6.
- Un bloque de CIDR IPv6 de tamaño /64 asociado a la subred de solo VPN (por ejemplo: 2001:db8:1234:1a01::/64). Puede elegir el rango de su subred en el rango asignado a la VPC. No es posible elegir el tamaño del CIDR IPv6.
- Las direcciones IPv6 asignadas a las instancias desde el rango de subred (ejemplo: 2001:db8:1234:1a00::1a).
- Entradas de la tabla personalizada que permiten a las instancias de la subred pública utilizar IPv6 para comunicarse entre sí y directamente a través de internet.
- Una entrada de la tabla de ruteo en la tabla de ruteo principal que permite a las instancias de la subred de solo VPN utilizar IPv6 para comunicarse entre sí.



Los servidores web de la subred pública tienen las siguientes direcciones.

Servidor	Dirección IPv4	Dirección IP elástica	Dirección IPv6
1	10.0.0.5	198.51.100.1	2001:db8:1234:1a00::1a
2	10.0.0.6	198.51.100.2	2001:db8:1234:1a00::2b
3	10.0.0.7	198.51.100.3	2001:db8:1234:1a00::3c

Los servidores de base de datos de la subred privada tienen las siguientes direcciones.

Servidor	Dirección IPv4	Dirección IPv6
1	10.0.1.5	2001:db8:1234:1a01::1a
2	10.0.1.6	2001:db8:1234:1a01::2b
3	10.0.1.7	2001:db8:1234:1a01::3c

Direccionamiento

Su VPC tiene un router implícito (tal como se muestra en el diagrama de configuración de este escenario). En este escenario, el asistente de VPC actualiza la tabla de ruteo principal utilizada con la subred de solo VPN, y crea una tabla de ruteo personalizada y la asocia a la subred pública.

Las instancias de la subred de solo VPN no pueden acceder a internet directamente; el tráfico vinculado a internet debe atravesar primero la gateway privada virtual a su red, donde el tráfico está sujeto al firewall y a las políticas de seguridad corporativas. Si las instancias envían tráfico vinculado a AWS (por ejemplo, solicitudes a las API de Amazon S3 o Amazon EC2), las solicitudes deben pasar por la puerta de enlace virtual privada hacia la red y, luego, salir a Internet antes de llegar a AWS.

Tip

El tráfico de su red que vaya a la dirección IP elástica de una instancia en la subred pública pasará por internet, y no por la gateway privada virtual. En su lugar, puede configurar una ruta y reglas de grupo que permitan que el tráfico llegue desde su red a través de la gateway privada virtual a la subred pública.

La conexión de VPN de sitio a sitio se configura como una conexión de VPN de sitio a sitio enrutada estáticamente o como una conexión de VPN de sitio a sitio enrutada dinámicamente (mediante BGP). Si selecciona el enrutamiento estático, se le pedirá que escriba manualmente el prefijo IP para la red cuando cree la conexión de VPN de sitio a sitio. Si selecciona el direccionamiento dinámico, el prefijo IP se anunciará automáticamente a la gateway privada virtual para su VPC mediante BGP.

Las siguientes tablas describen las tablas de ruteo para este escenario.

Tabla de enrutamiento principal

La primera fila es la entrada predeterminada para el direccionamiento local de la VPC. Esta entrada permite a las instancias de la VPC comunicarse entre sí mediante IPv4. La segunda fila direcciona el resto del tráfico de la subred IPv4 desde la subred privada a su red a través de la gateway privada virtual (por ejemplo, vgw-1a2b3c4d).

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	vgw-id

Tabla de enrutamiento personalizada

La primera fila es la entrada predeterminada para el direccionamiento local de la VPC. Esta entrada permite a las instancias de la VPC comunicarse entre sí. La segunda fila dirige el resto del tráfico de la subred IPv4 desde la subred pública hasta internet a través de la gateway de internet (por ejemplo, igw-1a2b3c4d).

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	igw-id

Enrutamiento alternativo

De forma alternativa, si desea que las instancias de la subred privada obtengan acceso a internet, puede crear una instancia o una gateway de conversión de dirección de red (NAT) en la subred pública, y configurar el direccionamiento para que el tráfico vinculado a internet para la subred vaya al dispositivo NAT. Esto permitirá a las instancias de la subred de solo VPN enviar solicitudes a través de la gateway de internet (por ejemplo, para actualizaciones de software).

Para obtener más información acerca de cómo configurar un dispositivo NAT manualmente, consulte [Conexión a Internet u otras redes mediante dispositivos NAT \(p. 156\)](#). Para obtener más información acerca de la utilización del asistente de VPC para configurar un dispositivo NAT, consulte [VPC con subredes privadas y públicas \(NAT\) \(p. 307\)](#).

Para permitir que el tráfico vinculado a internet de la subred privada se dirija al dispositivo NAT, debe actualizar la tabla de ruteo principal de la siguiente forma.

La primera fila es la entrada predeterminada para el direccionamiento local de la VPC. La segunda entrada enruta el tráfico de subred enlazado a su propia red local (cliente) a la gateway privada virtual. En este ejemplo, suponga que el intervalo de direcciones IP de la red local es 172.16.0.0/12. La tercera fila envía el resto del tráfico de la subred a una gateway NAT.

Destino	Objetivo
10.0.0.0/16	local
172.16.0.0/12	vgw-id
0.0.0.0/0	nat-gateway-id

Direccionamiento de IPv6

Si asocia un bloque de CIDR IPv6 con su VPC y sus subredes, sus tablas de ruteo deben incluir rutas separadas para el tráfico IPv6. Las tablas siguientes muestran las tablas de ruteo personalizadas para este escenario si elige habilitar la comunicación IPv6 en su VPC.

Tabla de enrutamiento principal

La segunda fila es la ruta predeterminada que se añade automáticamente para el direccionamiento local en la VPC a través de IPv6.

Destino	Objetivo
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	vgw-id

Tabla de enrutamiento personalizada

La segunda fila es la ruta predeterminada que se añade automáticamente para el direccionamiento local en la VPC a través de IPv6. La cuarta entrada direcciona todo el resto del tráfico de la subred IPv6 a la gateway de internet.

Destino	Objetivo
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	igw-id
::/0	igw-id

Seguridad

AWS proporciona dos características que puede utilizar para aumentar la seguridad de la VPC: los grupos de seguridad y las ACL de red. Los grupos de seguridad controlan el tráfico de entrada y salida de las instancias, mientras que las ACL de red controlan el tráfico de entrada y salida de las subredes. En la mayoría de los casos, los grupos de seguridad se ajustarán a sus necesidades. No obstante, puede usar también las ACL de red si desea agregar un nivel de seguridad adicional en la VPC. Para obtener más información, consulte [Privacidad del tráfico entre redes en Amazon VPC](#) (p. 233).

Para el escenario 3, utilizará los grupos de seguridad, pero no las ACL de red. Si desea utilizar una ACL de red, consulte [Reglas ACL recomendadas para una VPC con subredes públicas y privadas y acceso de AWS Site-to-Site VPN](#) (p. 340).

La VPC incluye un [grupo de seguridad predeterminado](#) (p. 256). Una instancia que se lanza en la VPC se asocia automáticamente al grupo de seguridad predeterminado si no especifica ningún grupo de seguridad predeterminado durante el lanzamiento. Para este escenario, recomendamos crear los siguientes grupos de seguridad en lugar de utilizar el grupo de seguridad predeterminado:

- WebServerSG: especifique este grupo de seguridad al lanzar servidores web en la subred pública.
- DBServerSG: especifique este grupo de seguridad al lanzar servidores de base de datos en la subred de solo VPN.

Las instancias asignadas a un grupo de seguridad pueden estar en distintas subredes. Sin embargo, en este escenario, cada grupo de seguridad corresponde al tipo de función que desempeña una instancia, y cada función requiere que una instancia esté en una subred determinada. Por lo tanto, en este escenario, todas las instancias asignadas a un grupo de seguridad estarán en la misma subred.

La siguiente tabla describe las reglas recomendadas para el grupo de seguridad WebServerSG, que permiten a los servidores web recibir el tráfico de internet, así como el tráfico SSH y RDP procedente de su red. Los servidores web también pueden iniciar solicitudes de lectura y escritura en los servidores de bases de datos de la subred de solo VPN, así como enviar tráfico a internet; por ejemplo, para obtener actualizaciones de software. Puesto que el servidor web no inicia ninguna otra comunicación saliente, se ha quitado la regla saliente predeterminada.

Note

El grupo incluye tanto acceso a SSH como a RDP, así como acceso a Microsoft SQL Server y a MySQL. En su caso, puede que solo necesite reglas para Linux (SSH y MySQL) o Windows (RDP y Microsoft SQL Server).

WebServerSG: reglas recomendadas

Entrada

Fuente	Protocolo	Rango de puertos	Comentarios
0.0.0.0/0	TCP	80	Permite el acceso HTTP entrante a los servidores web desde cualquier dirección IPv4.
0.0.0.0/0	TCP	443	Permite el acceso HTTPS entrante a los servidores web desde cualquier dirección IPv4.
Rango de direcciones IP públicas de su red	TCP	22	Permite el acceso SSH entrante a las instancias de Linux desde la red (a través de la gateway de internet).
Rango de direcciones IP públicas de su red	TCP	3389	Permite el acceso RDP entrante a las instancias de Windows desde la red (a través de la gateway de internet).
Salida			
ID del grupo de seguridad DBServerSG	TCP	1433	Permite el acceso saliente de Microsoft SQL Server a los servidores de base de datos asignados a DBServerSG.
ID del grupo de seguridad DBServerSG	TCP	3306	Permite el acceso saliente de MySQL a los servidores de base de datos asignados a DBServerSG.
0.0.0.0/0	TCP	80	Permite el acceso HTTP saliente a internet.
0.0.0.0/0	TCP	443	Permite el acceso HTTPS saliente a internet.

La siguiente tabla describe las reglas recomendadas para el grupo de seguridad DBServerSG, que permiten las solicitudes de lectura y escritura de Microsoft SQL Server y MySQL desde servidores web, así como el tráfico SSH y RDP desde su red. Los servidores de base de datos también pueden iniciar tráfico vinculado a internet (sus tablas de ruteo envían ese tráfico a través de la gateway privada virtual).

DBServerSG: reglas recomendadas

Entrada			
Fuente	Protocolo	Rango de puerto	Comentarios

ID del grupo de seguridad WebServerSG	TCP	1433	Permite el acceso entrante de Microsoft SQL Server desde los servidores web asociados al grupo de seguridad WebServerSG.
ID del grupo de seguridad WebServerSG	TCP	3306	Permite el acceso entrante del servidor MySQL desde los servidores web asociados al grupo de seguridad WebServerSG.
Rango de direcciones IPv4 de su red	TCP	22	Permite el tráfico SSH entrante a las instancias de Linux desde la red (a través de la gateway privada virtual).
Rango de direcciones IPv4 de su red	TCP	3389	Permite el tráfico RDP entrante a las instancias de Windows desde la red (a través de la gateway privada virtual).
Salida			
Destino	Protocolo	Rango de puerto	Comentarios
0.0.0.0/0	TCP	80	Permite el acceso saliente de HTTP IPv4 a internet (por ejemplo, para actualizaciones de software) a través de la gateway privada virtual.
0.0.0.0/0	TCP	443	Permite el acceso saliente de HTTPS IPv4 a internet (por ejemplo, para actualizaciones de software) a través de la gateway privada virtual.

(Opcional) El grupo de seguridad predeterminado de una VPC tiene reglas que permiten, de forma automática, que las instancias asignadas se comuniquen entre sí. Para permitir ese tipo de comunicación para un grupo de seguridad personalizado, debe añadir las siguientes reglas:

Entrada			
Fuente	Protocolo	Rango de puerto	Comentarios
El ID del grupo de seguridad	Todos	Todos	Permite el tráfico entrante desde otras instancias asignadas

Salida			a este grupo de seguridad.
Destino	Protocolo	Rango de puerto	Comentarios
The ID of the security group	All	All	Allow outbound traffic to other instances assigned to this security group.

Reglas de grupo de seguridad para IPv6

Si asocia un bloque de CIDR IPv6 a su VPC y sus subredes, debe añadir reglas separadas a sus grupos de seguridad WebServerSG y DBServerSG para controlar el tráfico IPv6 entrante y saliente de sus instancias. En este escenario, los servidores web podrán recibir todo el tráfico de internet a través de IPv6, así como el tráfico SSH o RDP de su red local a través de IPv6. Asimismo, pueden iniciar tráfico IPv6 saliente a internet. Los servidores de base de datos no pueden iniciar el tráfico IPv6 saliente a internet, por lo que no necesitan reglas de grupos de seguridad adicionales.

A continuación se detallan las reglas específicas de IPv6 para el grupo de seguridad WebServerSG (adicionales a las reglas descritas anteriormente).

Entrada			
Fuente	Protocolo	Rango de puerto	Comentarios
::/0	TCP	80	Permite el acceso HTTP entrante a los servidores web desde cualquier dirección IPv6.
::/0	TCP	443	Permite el acceso HTTPS entrante a los servidores web desde cualquier dirección IPv6.
Rango de direcciones IPv6 de su red	TCP	22	(Instancias de Linux) Permite el acceso SSH entrante desde su red a través de IPv6.
Rango de direcciones IPv6 de su red	TCP	3389	(Instancias de Windows) Permite el acceso RDP entrante desde su red a través de IPv6.
Salida			
Destino	Protocolo	Rango de puerto	Comentarios
::/0	TCP	HTTP	Allow outbound HTTP access to any IPv6 address.
::/0	TCP	HTTPS	Allow outbound HTTPS access to any IPv6 address.

Implementar el escenario 3

Para implementar el escenario 3, obtenga información acerca de su gateway de cliente y cree la VPC con el asistente de VPC. El asistente de VPC crea una conexión de VPN de sitio a sitio por usted con una gateway de cliente y una gateway privada virtual.

Estos procedimientos incluyen pasos opcionales para habilitar y configurar la comunicación IPv6 para su VPC. Si no desea utilizar IPv6 en su VPC, no tiene que realizar estos pasos.

Para preparar su gateway de cliente

1. Determine el dispositivo que utilizará como su dispositivo de gateway del cliente. Para obtener más información, consulte [Su dispositivo de puerta de enlace de cliente](#) en la Guía del usuario de AWS Site-to-Site VPN.
2. Obtenga la dirección IP enrutable de internet para la interfaz externa del dispositivo de gateway del cliente. La dirección debe ser estática, y puede encontrarse detrás de un dispositivo que realice la conversión de las direcciones de red (NAT).
3. Si desea crear una conexión de VPN de sitio a sitio enrutada estáticamente, obtenga la lista de intervalos IP internos (en la notación CIDR) que se deberían anunciar en la conexión de VPN de sitio a sitio a la gateway privada virtual. Para obtener más información, consulte [Tablas de ruteo y prioridad de las rutas de VPN](#) en la Guía del usuario de AWS Site-to-Site VPN.

Para obtener información acerca de cómo utilizar el asistente de VPC con IPv4, consulte [Introducción](#) (p. 10).

Para obtener información acerca de cómo utilizar el asistente de VPC con IPv6, consulte [the section called "VPC que admite las direcciones IPv6"](#) (p. 291).

Reglas ACL recomendadas para una VPC con subredes públicas y privadas y acceso de AWS Site-to-Site VPN

Para este escenario, dispondrá de una ACL de red para la subred pública y una ACL de red distinta para la subred de solo VPN. La tabla siguiente muestra las reglas que recomendamos para cada ACL. Las reglas bloquean todo el tráfico excepto el explícitamente necesario.

Reglas de ACL para la subred pública

Inbound					
Regla n.º	IP de origen	Protocolo	Puerto	Permitir/ Denegar	Comentarios
100	0.0.0.0/0	TCP	80	PERMITIR	Permite el tráfico HTTP entrante a los servidores web desde cualquier dirección IPv4.
110	0.0.0.0/0	TCP	443	PERMITIR	Permite el tráfico HTTPS entrante a los servidores web desde cualquier dirección IPv4.

120	Rango de direcciones IPv4 públicas de la red doméstica	TCP	22	PERMITIR	Permite el tráfico SSH entrante a los servidores web desde su red doméstica (a través de la gateway de Internet).
130	Rango de direcciones IPv4 públicas de la red doméstica	TCP	3389	PERMITIR	Permite el tráfico RDP entrante a los servidores web desde su red doméstica (a través de la gateway de Internet).
140	0.0.0.0/0	TCP	32768-65535	PERMITIR	Permite el tráfico de retorno entrante de hosts de Internet que responden a las solicitudes que se originan en la subred. Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133) .
*	0.0.0.0/0	Todos	Todos	DENEGAR	Deniega todo el tráfico IPv4 entrante no controlado por ninguna regla precedente (no modificable).
Outbound					

Regla n.º	IP destino	Protocolo	Puerto	Permitir/ Denegar	Comentarios
100	0.0.0.0/0	TCP	80	PERMITIR	Permite el tráfico HTTP saliente de la subred a Internet.
110	0.0.0.0/0	TCP	443	PERMITIR	Permite el tráfico HTTPS saliente de la subred a Internet.
120	10.0.1.0/24	TCP	1433	PERMITIR	<p>Permite el acceso de MS SQL saliente a los servidores de bases de datos de la subred de solo VPN.</p> <p>Este número de puerto se proporciona solo como ejemplo. Otros ejemplos incluyen el número de puerto 3306 para el acceso de MySQL/Aurora, el número 5432 para el acceso de PostgreSQL, el número 5439 para el acceso de Amazon Redshift o el número 1521 para el acceso de Oracle.</p>

140	0.0.0.0/0	TCP	32768-65535	PERMITIR	<p>Permite las respuestas IPv4 salientes a clientes de Internet (por ejemplo, al ofrecer páginas web a usuarios que visitan los servidores web de la subred).</p> <p>Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133).</p>
*	0.0.0.0/0	Todos	Todos	DENEGAR	Deniega todo el tráfico saliente no controlado por ninguna regla precedente (no modificable).

Configuración de ACL para la subred de solo VPN

Inbound					
Regla n.º	IP de origen	Protocolo	Puerto	Permitir/Denegar	Comentarios
100	10.0.0.0/24	TCP	1433	PERMITIR	Permite a los servidores web de la subred pública realizar operaciones de lectura y escritura en servidores de MS SQL de la subred de solo VPN.

					Este número de puerto se proporciona solo como ejemplo. Otros ejemplos incluyen el número de puerto 3306 para el acceso de MySQL/Aurora, el número 5432 para el acceso de PostgreSQL, el número 5439 para el acceso de Amazon Redshift o el número 1521 para el acceso de Oracle.
120	Rango de direcciones IPv4 privadas de la red doméstica	TCP	22	PERMITIR	Permite el tráfico SSH entrante de la red doméstica (a través de la gateway privada virtual).
130	Rango de direcciones IPv4 privadas de la red doméstica	TCP	3389	PERMITIR	Permite el tráfico RDP entrante de la red doméstica (a través de la gateway privada virtual).

140	Rango de direcciones IP privadas de la red doméstica	TCP	32768-65535	PERMITIR	<p>Permite el tráfico de retorno entrante de clientes de la red doméstica (a través de la gateway privada virtual).</p> <p>Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133).</p>
*	0.0.0.0/0	Todos	Todos	DENEGAR	Deniega todo el tráfico entrante no controlado por ninguna regla precedente (no modificable).
Outbound					
Regla n.º	IP destino	Protocolo	Puerto	Permitir/ Denegar	Comentarios

100	Rango de direcciones IP privadas de la red doméstica	Todos	Todos	PERMITIR	Permite todo el tráfico saliente de la subred a su red doméstica (a través de la gateway privada virtual). Esta regla también abarca la regla 120. Sin embargo, puede hacer que esta regla sea más restrictiva si usa un número de puerto y un tipo de protocolo específico. Si opta por hacer que esta regla sea más restrictiva, deberá incluir la regla 120 en el ACL de red para asegurarse de que no se bloqueen las respuestas salientes.
-----	--	-------	-------	----------	---

110	10.0.0.0/24	TCP	32768-65535	PERMITIR	<p>Permite las respuestas salientes a los servidores web de la subred pública.</p> <p>Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133).</p>
120	Rango de direcciones IP privadas de la red doméstica	TCP	32768-65535	PERMITIR	<p>Permite las respuestas salientes a clientes de la red doméstica (a través de la gateway privada virtual).</p> <p>Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133).</p>
*	0.0.0.0/0	Todos	Todos	DENEGAR	<p>Deniega todo el tráfico saliente no controlado por ninguna regla precedente (no modificable).</p>

Reglas de ACL de red recomendadas para IPv6

Si implementó la compatibilidad con el tráfico IPv6 y creó una VPC y subredes con bloques de CIDR IPv6 asociados, deberá añadir reglas separadas a las ACL de red para controlar el tráfico IPv6 entrante y saliente.

A continuación se detallan las reglas específicas de tráfico IPv6 para las ACL de red (adicionales a las reglas descritas anteriormente).

Reglas de ACL para la subred pública

Inbound					
Regla n.º	IP de origen	Protocolo	Puerto	Permitir/ Denegar	Comentarios
150	::/0	TCP	80	PERMITIR	Permite el tráfico HTTP entrante de cualquier dirección IPv6.
160	::/0	TCP	443	PERMITIR	Permite el tráfico HTTPS entrante de cualquier dirección IPv6.
170	Rango de direcciones IPv6 de la red doméstica	TCP	22	PERMITIR	Permite el tráfico SSH entrante a través de IPv6 de su red doméstica (a través de la gateway de Internet).
180	Rango de direcciones IPv6 de la red doméstica	TCP	3389	PERMITIR	Permite el tráfico RDP entrante a través de IPv6 de su red doméstica (a través de la gateway de Internet).
190	::/0	TCP	1024 - 65535	PERMITIR	Permite el tráfico de retorno entrante de hosts de Internet que responden a las solicitudes que se originan en la subred.

					Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133).
*	::/0	Todos	Todos	DENEGAR	Deniega todo el tráfico IPv6 entrante no controlado por ninguna regla precedente (no modificable).
Outbound					
Regla n.º	IP destino	Protocolo	Puerto	Permitir/ Denegar	Comentarios
150	::/0	TCP	80	PERMITIR	Permite el tráfico HTTP saliente de la subred a Internet.
160	::/0	TCP	443	PERMITIR	Permite el tráfico HTTPS saliente de la subred a Internet.

170	2001:db8:1234:1a00::64	1433	PERMITIR	<p>Permite el acceso de MS SQL saliente a los servidores de bases de datos de la subred privada.</p> <p>Este número de puerto se proporciona solo como ejemplo. Otros ejemplos incluyen el número de puerto 3306 para el acceso de MySQL/Aurora, el número 5432 para el acceso de PostgreSQL, el número 5439 para el acceso de Amazon Redshift o el número 1521 para el acceso de Oracle.</p>
-----	------------------------	------	----------	---

190	::/0	TCP	32768-65535	PERMITIR	<p>Permite las respuestas salientes a clientes de Internet (por ejemplo, al ofrecer páginas web a usuarios que visitan los servidores web de la subred).</p> <p>Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133).</p>
*	::/0	Todos	Todos	DENEGAR	<p>Deniega todo el tráfico IPv6 saliente no controlado por ninguna regla precedente (no modificable).</p>

Reglas de ACL para la subred de solo VPN

Inbound					
Regla n.º	IP de origen	Protocolo	Puerto	Permitir/Denegar	Comentarios
150	2001:db8:1234:1a::/64	TCP	1433	PERMITIR	<p>Permite a los servidores web de la subred pública realizar operaciones de lectura y escritura en servidores de MS SQL de la subred privada.</p> <p>Este número de puerto se</p>

					proporciona solo como ejemplo. Otros ejemplos incluyen el número de puerto 3306 para el acceso de MySQL/Aurora, el número 5432 para el acceso de PostgreSQL, el número 5439 para el acceso de Amazon Redshift o el número 1521 para el acceso de Oracle.
*	::/0	Todos	Todos	DENEGAR	Deniega todo el tráfico IPv6 entrante no controlado por ninguna regla precedente (no modificable).
Outbound					
Regla n.º	IP destino	Protocolo	Puerto	Permitir/ Denegar	Comentarios

130	2001:db8:1234:1a00::64	32768-65535	PERMITIR	Permite las respuestas salientes a la subred pública (por ejemplo, respuestas a servidores web de la subred pública que se comunican con servidores de bases de datos de la subred privada).
				Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133) .
*	::/0	Todos	Todos	DENEGAR
				Deniega todo el tráfico IPv6 saliente no controlado por ninguna regla precedente (no modificable).

VPC solo con una subred privada y acceso de AWS Site-to-Site VPN

La configuración de este escenario incluye una nube virtual privada (VPC) con una única subred privada y una gateway privada virtual para habilitar la comunicación con su propia red a través de un túnel de VPN IPsec. En este caso, no hay ninguna gateway de Internet para habilitar la comunicación a través de Internet. Se recomienda este escenario si desea ampliar la red a [la nube](#) utilizando la infraestructura de Amazon sin exponer su red a Internet.

Si lo desea, este escenario también se puede configurar para IPv6: puede utilizar el asistente de VPC para crear una VPC y una subred con los bloques de CIDR IPv6 asociados. Las instancias lanzadas en la subred pueden recibir direcciones IPv6. No se admite la comunicación IPv6 a través de una conexión de AWS Site-to-Site VPN en una puerta de enlace virtual privada; no obstante, las instancias de la VPC pueden comunicarse entre sí mediante IPv6. Para obtener más información acerca de las direcciones IPv4 e IPv6, consulte [Direccionamiento IP \(p. 4\)](#).

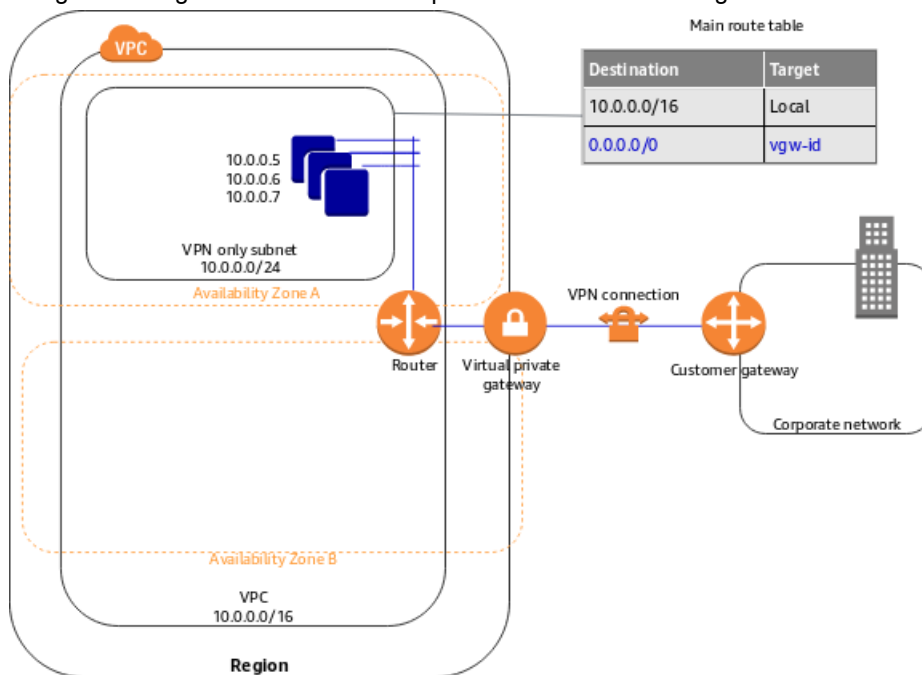
Para obtener información acerca de cómo administrar el software de instancias EC2, consulte [Administración de software en la instancia de Linux](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Contenido

- [Información general](#) (p. 354)
- [Direccionamiento](#) (p. 355)
- [Seguridad](#) (p. 356)

Información general

El siguiente diagrama muestra los componentes clave de la configuración de este escenario.



Important

Para este escenario, consulte [El dispositivo de gateway de cliente](#) para configurar el dispositivo de gateway de cliente en su lado de la conexión de VPN de sitio a sitio.

La configuración de este escenario incluye lo siguiente:

- Una nube virtual privada (VPC) con CIDR de tamaño /16 (ejemplo: 10.0.0.0/16). Esto proporciona 65 536 direcciones IP privadas.
- Una subred de solo VPN con CIDR de tamaño /24 (ejemplo: 10.0.0.0/24). Esto proporciona 256 direcciones IP privadas.
- Una conexión de VPN de sitio a sitio entre la VPC y la red. La conexión de VPN de sitio a sitio consta de una gateway privada virtual ubicada en el lado de Amazon de la conexión de VPN de sitio a sitio y una gateway de cliente ubicada en su lado de la conexión de VPN de sitio a sitio.
- Instancias con direcciones IP privadas en el rango de la subred (por ejemplo: 10.0.0.5, 10.0.0.6 y 10.0.0.7), lo que permite que las instancias se comuniquen entre sí y con otras instancias de la VPC.
- La tabla de ruteo principal contiene una ruta que permite a las instancias de la subred comunicarse exclusivamente con otras instancias de la VPC. La propagación de rutas está habilitada, por lo que hay una ruta que permite que las instancias de la subred se comuniquen directamente con la red que aparece como una ruta propagada en la tabla de ruteo principal.

Para obtener más información, consulte [Subredes](#) (p. 60). Para obtener más información acerca de la conexión VPN de sitio a sitio, consulte la [Guía del usuario de AWS Site-to-Site VPN](#). Para obtener más información acerca de cómo configurar un dispositivo de gateway de cliente, consulte [El dispositivo de gateway de cliente](#).

Información general de IPv6

Opcionalmente, puede habilitar IPv6 para este escenario. Además de los componentes mostrados arriba, la configuración incluye lo siguiente:

- Un bloque de CIDR IPv6 de tamaño /56 asociado a la VPC (por ejemplo: 2001:db8:1234:1a00::/56). AWS asigna automáticamente el CIDR; no podrá elegir el rango por sí mismo.
- Un bloque de CIDR IPv6 de tamaño /64 asociado a la subred de solo VPN (por ejemplo: 2001:db8:1234:1a00::/64). Puede elegir el rango de su subred en el rango asignado a la VPC. No es posible elegir el tamaño del CIDR IPv6.
- Las direcciones IPv6 asignadas a las instancias desde el rango de subred (ejemplo: 2001:db8:1234:1a00::1a).
- Una entrada de la tabla de ruteo principal que permite a las instancias de la subred privada utilizar IPv6 para comunicarse entre sí.

Direccionamiento

Su VPC tiene un router implícito (tal como se muestra en el diagrama de configuración de este escenario). En este escenario, el asistente para la creación de VPC crea una tabla de ruteo que direcciona todo el tráfico con destino a una dirección externa a la VPC a la conexión de AWS Site-to-Site VPN para, a continuación, asociar la tabla de ruteo a la subred.

A continuación se describe la tabla de ruteo para este escenario. La primera fila es la entrada predeterminada para el direccionamiento local de la VPC. Esta entrada permite a las instancias de esta VPC comunicarse entre sí. La segunda entrada direcciona el resto del tráfico de la subred a la gateway privada virtual (por ejemplo, vgw-1a2b3c4d).

Destino	Objetivo
10.0.0.0/16	local
0.0.0.0/0	vgw-id

La conexión de AWS Site-to-Site VPN se configura como una conexión de Site-to-Site VPN dirigida estáticamente o como una conexión de Site-to-Site VPN dirigida dinámicamente (mediante BGP). Si selecciona el enrutamiento estático, se le pedirá que escriba manualmente el prefijo IP para la red cuando cree la conexión de VPN de sitio a sitio. Si selecciona el direccionamiento dinámico, el prefijo IP se anuncia automáticamente a su VPC a través de BGP.

Las instancias de su VPC no pueden acceder a Internet directamente; el tráfico vinculado a Internet debe atravesar primero la gateway privada virtual correspondiente a su red, donde el tráfico está sujeto a su firewall y a las políticas de seguridad corporativas. Si las instancias envían tráfico vinculado a AWS (por ejemplo, solicitudes a Amazon S3 o Amazon EC2), las solicitudes deben pasar por la puerta de enlace virtual privada a su red y, luego, a Internet antes de llegar a AWS.

Direccionamiento de IPv6

Si asocia un bloque de CIDR IPv6 con su VPC y sus subredes, su tabla de ruteo incluirá rutas separadas para el tráfico IPv6. A continuación se describe la tabla de ruteo personalizada para este escenario. La

segunda fila es la ruta predeterminada que se añade automáticamente para el direccionamiento local en la VPC a través de IPv6.

Destino	Objetivo
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	vgw-id

Seguridad

AWS proporciona dos características que puede utilizar para aumentar la seguridad de la VPC: los grupos de seguridad y las ACL de red. Los grupos de seguridad controlan el tráfico de entrada y salida de las instancias, mientras que las ACL de red controlan el tráfico de entrada y salida de las subredes. En la mayoría de los casos, los grupos de seguridad se ajustarán a sus necesidades. No obstante, puede usar también las ACL de red si desea agregar un nivel de seguridad adicional en la VPC. Para obtener más información, consulte [Privacidad del tráfico entre redes en Amazon VPC](#) (p. 233).

Para el escenario 4, utilizará el grupo de seguridad predeterminado de su VPC, pero no una ACL de red. Si desea utilizar una ACL de red, consulte [Reglas ACL de la red recomendadas para una VPC con una subred privada solamente y acceso a AWS Site-to-Site VPN](#) (p. 357).

Su VPC incluye un grupo de seguridad predeterminado cuya configuración inicial deniega todo el tráfico entrante y permite todo el tráfico saliente y todo el tráfico entre las instancias asignadas al grupo de seguridad. Para este escenario, se recomienda añadir reglas entrantes al grupo de seguridad predeterminado para permitir el tráfico SSH (Linux) y el tráfico de Escritorio remoto (Windows) desde su red.

Important

El grupo de seguridad predeterminado permite, de forma automática, que las instancias asignadas se comuniquen entre sí. Por tanto, no tiene que añadir ninguna regla para permitir esto. Si utiliza un grupo de seguridad diferente, debe añadir una regla que lo permita.

La siguiente tabla describe las reglas entrantes que debería añadir al grupo de seguridad predeterminado para su VPC.

Grupo de seguridad predeterminado: reglas recomendadas

Entrada			
Fuente	Protocolo	Rango de puertos	Comentarios
Rango de direcciones IPv4 privadas de su red	TCP	22	(Instancias de Linux) Permite el tráfico SSH entrante desde su red.
Rango de direcciones IPv4 privadas de su red	TCP	3389	(Instancias de Windows) Permite el tráfico RDP entrante desde su red.

Reglas de grupo de seguridad para IPv6

Si asocia un bloque de CIDR IPv6 a su VPC y sus subredes, debe añadir reglas separadas a su grupo de seguridad para controlar el tráfico IPv6 entrante y saliente de sus instancias. En este escenario, los

servidores de bases de datos no están disponibles a través de la conexión de VPN de sitio a sitio mediante IPv6; por lo tanto, no son necesarias reglas de grupos de seguridad adicionales.

Reglas ACL de la red recomendadas para una VPC con una subred privada solamente y acceso a AWS Site-to-Site VPN

La tabla siguiente muestra las reglas que recomendamos. Las reglas bloquean todo el tráfico excepto el explícitamente necesario.

Inbound					
Regla n.º	IP de origen	Protocolo	Puerto	Permitir/ Denegar	Comentarios
100	Rango de direcciones IP privadas de la red doméstica	TCP	22	PERMITIR	Permite el tráfico SSH entrante a la subred desde su red doméstica.
110	Rango de direcciones IP privadas de la red doméstica	TCP	3389	PERMITIR	Permite el tráfico RDP entrante a la subred desde su red doméstica.
120	Rango de direcciones IP privadas de la red doméstica	TCP	32768-65535	PERMITIR	Permite el tráfico de retorno entrante desde solicitudes que se originan en la subred. Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133) .
*	0.0.0.0/0	Todos	Todos	DENEGAR	Deniega todo el tráfico entrante no controlado por ninguna regla

					precedente (no modificable).
Outbound					
Regla n.º	IP destino	Protocolo	Puerto	Permitir/ Denegar	Comentarios
100	Rango de direcciones IP privadas de la red doméstica	Todos	Todos	PERMITIR	Permite todo el tráfico saliente desde la subred a su red doméstica. Esta regla también abarca la regla 120. Sin embargo, puede hacer que esta regla sea más restrictiva si usa un número de puerto y un tipo de protocolo específico. Si opta por hacer que esta regla sea más restrictiva, deberá incluir la regla 120 en el ACL de red para asegurarse de que no se bloqueen las respuestas salientes.

120	Rango de direcciones IP privadas de la red doméstica	TCP	32768-65535	PERMITIR	Permite las respuestas salientes a los clientes de la red doméstica. Este rango se proporciona solo como ejemplo. Para obtener información acerca de la elección de los puertos efímeros correctos para su configuración, consulte Puertos efímeros (p. 133) .
*	0.0.0.0/0	Todos	Todos	DENEGAR	Deniega todo el tráfico saliente no controlado por ninguna regla precedente (no modificable).

Reglas de ACL de red recomendadas para IPv6

Si implementó el escenario 4 con compatibilidad con el tráfico IPv6 y creó una VPC y una subred con bloques de CIDR IPv6 asociados, deberá añadir reglas separadas a las ACL de red para controlar el tráfico IPv6 entrante y saliente.

En este escenario, los servidores de bases de datos no están disponibles a través de la comunicación de VPN mediante IPv6, por lo que no son necesarias reglas de ACL de red adicionales. A continuación se describen las reglas predeterminadas que deniegan el tráfico IPv6 hacia la subred y procedente de esta.

Reglas de ACL para la subred de solo VPN

Inbound					
Regla n.º	IP de origen	Protocolo	Puerto	Permitir/ Denegar	Comentarios
*	::/0	Todos	Todos	DENEGAR	Deniega todo el tráfico IPv6 entrante no controlado por ninguna regla precedente (no modificable).
Outbound					

Regla n.º	IP destino	Protocolo	Puerto	Permitir/ Denegar	Comentarios
*	::/0	Todos	Todos	DENEGAR	Deniega todo el tráfico IPv6 saliente no controlado por ninguna regla precedente (no modificable).

Migrar VPC existentes de IPv4 a IPv6

Si tiene una VPC existente que solo admite IPv4 y los recursos de su subred están configurados para utilizar solamente IPv4, puede habilitar la compatibilidad con IPv6 para su VPC y sus recursos. La VPC puede funcionar en modo de pila doble: esto implica que los recursos se pueden comunicar mediante IPv4, IPv6 o ambos. Las comunicaciones IPv4 e IPv6 son independientes.

No puede desactivar la compatibilidad con IPv4 para la VPC y subredes, ya que este es el sistema de direccionamiento IP predeterminado para Amazon VPC y Amazon EC2.

Note

- Actualmente no hay ninguna ruta de migración desde subredes solo de IPv4 a subredes solo de IPv6. Para obtener información sobre la creación de subredes solo de IPv6, consulte [the section called “Crear una subred en la VPC” \(p. 64\)](#).
- En esta sección, se presupone que hay una VPC con subredes públicas y privadas. Para obtener información sobre cómo configurar una nueva VPC para usarla con IPv6, consulte [the section called “Información general de IPv6” \(p. 298\)](#).

La tabla siguiente ofrece información general de los pasos que debe seguir para habilitar su VPC y sus subredes para utilizar IPv6.

Paso	Notas
Paso 1: Asociar un bloque de CIDR IPv6 a su VPC y subredes (p. 364)	Asocie un bloque de CIDR IPv6 proporcionado por Amazon o BYOIP a la VPC y a las subredes.
Paso 2: Actualizar las tablas de enrutamiento (p. 365)	Actualice sus tablas de ruteo para direccionar el tráfico IPv6. Para una subred pública, cree una ruta que dirija todo el tráfico IPv6 desde la subred al puerto de enlace a Internet. Para una subred privada, cree una ruta que dirija todo el tráfico IPv6 entrante desde la subred a un gateway de Internet de solo salida.
Paso 3: Actualizar las reglas del grupo de seguridad (p. 365)	Actualice las reglas de su grupo de seguridad para que incluyan reglas para direcciones IPv6. Esto permite el flujo de tráfico IPv6 entrante y saliente en las instancias. Si ha creado reglas de ACL de red personalizadas para controlar el flujo de tráfico entrante y saliente de su subred, debe incluir reglas para el tráfico IPv6.
Paso 4: Cambiar el tipo de instancia (p. 366)	Si su tipo de instancia no es compatible con IPv6, cambie el tipo de instancia.

Paso	Notas
Paso 5: Asignar direcciones IPv6 a sus instancias (p. 367)	Asigne direcciones IPv6 a sus instancias desde el rango de direcciones IPv6 de su subred.
Paso 6: (opcional) Configurar IPv6 en sus instancias (p. 368)	Si su instancia se ha lanzado desde una AMI que no está configurado para utilizar DHCPv6, deberá configurar manualmente su instancia para reconocer una dirección IPv6 asignada a la instancia.

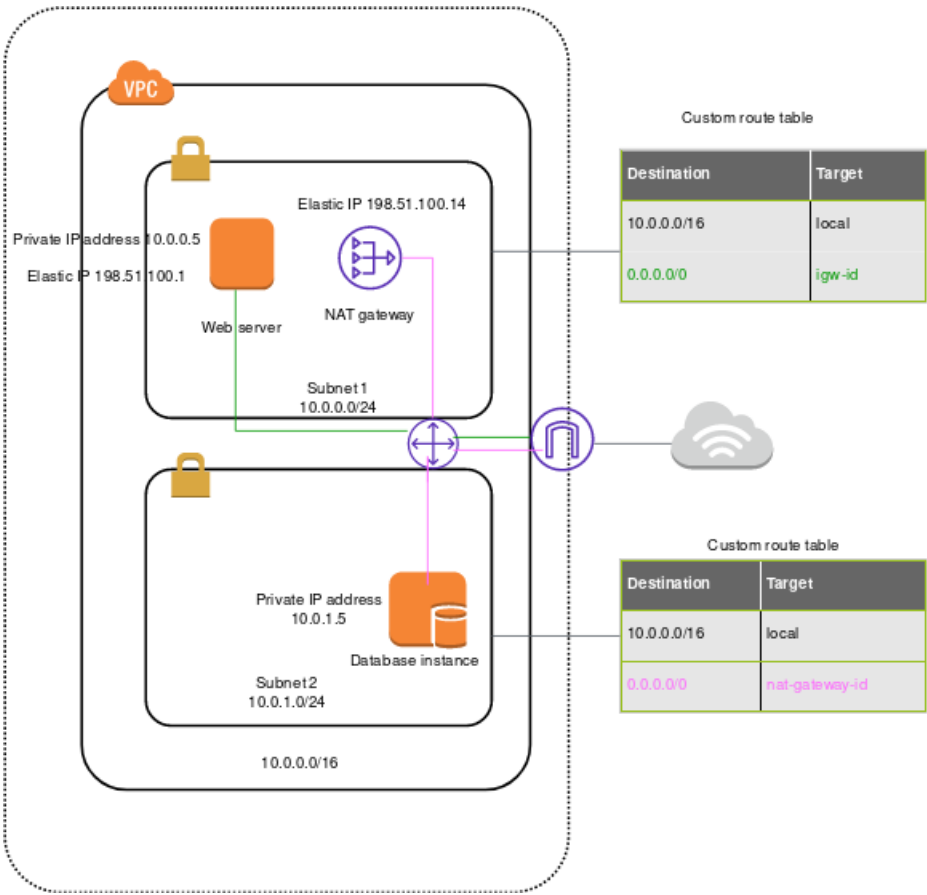
Antes de migrar a la utilización de IPv6, asegúrese de leer las características de las direcciones IPv6 para Amazon VPC: ??? (p. 4).

Contenido

- [Ejemplo: habilitar IPv6 en una VPC con una subred pública y privada \(p. 361\)](#)
- [Paso 1: Asociar un bloque de CIDR IPv6 a su VPC y subredes \(p. 364\)](#)
- [Paso 2: Actualizar las tablas de enrutamiento \(p. 365\)](#)
- [Paso 3: Actualizar las reglas del grupo de seguridad \(p. 365\)](#)
- [Paso 4: Cambiar el tipo de instancia \(p. 366\)](#)
- [Paso 5: Asignar direcciones IPv6 a sus instancias \(p. 367\)](#)
- [Paso 6: \(opcional\) Configurar IPv6 en sus instancias \(p. 368\)](#)

Ejemplo: habilitar IPv6 en una VPC con una subred pública y privada

En este ejemplo, su VPC tiene una subred pública y privada. También dispone de una instancia de base de datos en su subred privada que tiene comunicación saliente a Internet mediante una gateway NAT en su VPC. Asimismo, tiene un servidor web público en su subred pública con acceso a Internet mediante la gateway de Internet. El diagrama siguiente representa la arquitectura de su VPC.



El grupo de seguridad de su servidor web (sg-11aa22bb11aa22bb1) tiene las siguientes reglas entrantes:

Tipo	Protocolo	Rango de puerto	Source	Comentario
Todo el tráfico	Todos	Todos	sg-33cc44dd33cc44dd3	Permite el acceso entrante de todo el tráfico de instancias asociadas al grupo de seguridad sg-33cc44dd33cc44dd3 (instancia de la base de datos).
HTTP	TCP	80	0.0.0.0/0	Permite el tráfico entrante desde Internet mediante HTTP.
HTTPS	TCP	443	0.0.0.0/0	Permite el tráfico entrante desde Internet mediante HTTPS.

Tipo	Protocolo	Rango de puerto	Source	Comentario
SSH	TCP	22	203.0.113.123/32	Permite el acceso SSH entrante desde su equipo local. Por ejemplo, cuando necesita conectarse a su instancia para realizar tareas de administración.

El grupo de seguridad de su instancia de base de datos (`sg-33cc44dd33cc44dd3`) tiene la regla entrante siguiente:

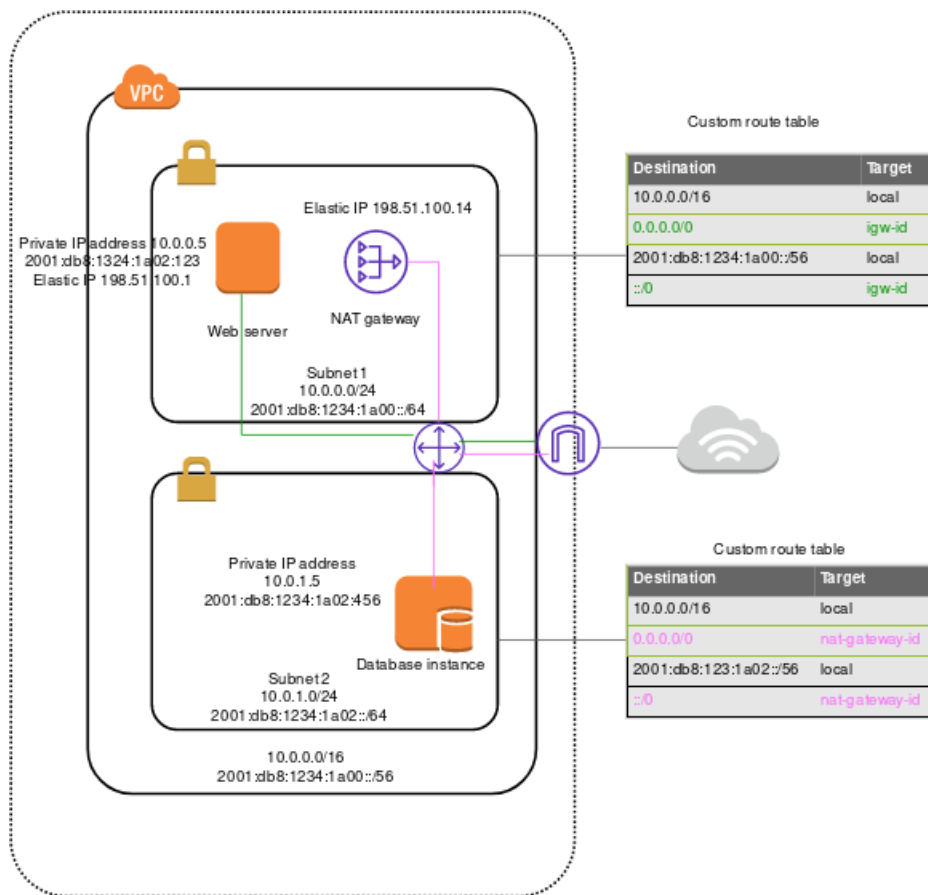
Tipo	Protocolo	Rango de puerto	Source	Comentario
MySQL	TCP	3306	sg-11aa22bb11aa22bb1	Permite el acceso entrante de tráfico MySQL desde instancias asociadas al grupo de seguridad sg-11aa22bb11aa22bb1 (instancia del servidor web).

Ambos grupos de seguridad tienen la regla saliente predeterminada que permite todo el tráfico IPv4 saliente y ninguna otra regla saliente.

El servidor web es un tipo de instancia `t2.medium`. El servidor de la base de datos es del tipo `m3.large`.

Usted desea que su VPC y sus recursos admitan IPv6. Asimismo, desea que puedan funcionar en modo de pila doble. En otras palabras, desea utilizar las direcciones IPv4 e IPv6 entre los recursos de su VPC y los recursos a través de Internet.

Una vez completados los pasos, su VPC tendrá la configuración siguiente.



Paso 1: Asociar un bloque de CIDR IPv6 a su VPC y subredes

Puede asociar un bloque de CIDR IPv6 a su VPC y, a continuación, asociar un bloque de CIDR /64 de dicho rango a cada subred.

Para asociar un bloque de CIDR IPv6 a una VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Your VPCs.
3. Seleccione su VPC, elija Actions, Edit CIDRs.
4. Elija Añadir CIDR IPv6, elija una de las siguientes opciones y, a continuación, elija Select CIDR (Seleccionar CIDR):
 - Amazon-provided IPv6 CIDR block (Bloque de CIDR IPv6 proporcionado por Amazon): solicita un bloque de CIDR IPv6 del grupo de direcciones IPv6 de Amazon. En Network Border Group (Grupo de borde de red), seleccione el grupo desde el que AWS anuncia las direcciones IP.
 - IPv6 CIDR owned by me (CIDR IPv6 de mi propiedad: [BYOIP](#)) asigna un bloque de CIDR IPv6 de su grupo de direcciones IPv6. En Pool (Grupo), elija el grupo de direcciones IPv6 desde el que desea asignar el bloque de CIDR IPv6.

Para asociar un bloque de CIDR IPv6 a una subred

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Subnets.

3. Seleccione su subred, elija Subnet Actions, Edit IPv6 CIDRs.
4. Elija Add IPv6 CIDR. Especifique la pareja de valores hexadecimales para la subred (por ejemplo, 00) y confirme la entrada seleccionando el icono de marca de verificación.
5. Seleccione la opción Close. Repita los pasos para las demás subredes de su VPC.

Para obtener más información, consulte [Ajuste de tamaño de VPC para IPv6 \(p. 20\)](#).

Paso 2: Actualizar las tablas de enrutamiento

Para una subred pública, debe actualizar la tabla de ruteo para habilitar instancias (tales como servidores web) para utilizar el puerto de enlace a Internet para tráfico IPv6.

Para una subred privada, debe actualizar la tabla de ruteo para habilitar instancias (tales como instancias de base de datos) para utilizar una gateway de Internet de solo salida para tráfico IPv6.

Para actualizar la tabla de ruteo para una subred pública

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Route Tables y seleccione la tabla de ruteo asociada a la subred pública.
3. En la pestaña Routes (Rutas), elija Edit routes (Editar rutas).
4. Seleccione Add route (Añadir ruta). Especifique `::/0` en Destination (Destino), seleccione el ID de la puerta de enlace de Internet en Target (Destino) y, a continuación, elija Save (Guardar).

Para actualizar la tabla de ruteo para una subred privada

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. Si usa un dispositivo NAT en su subred privada, no admite el tráfico IPv6. En lugar de ello, cree un puerto de enlace a Internet de solo salida para que su subred privada permita la comunicación saliente a Internet mediante IPv6 y para impedir las comunicaciones entrantes. El puerto de enlace a Internet de solo salida solo admite el tráfico IPv6. Para obtener más información, consulte [Habilitar el tráfico IPv6 saliente mediante una puerta de enlace de Internet de solo salida \(p. 153\)](#).
3. En el panel de navegación, elija Route Tables y seleccione la tabla de ruteo asociada a la subred privada.
4. En la pestaña Routes (Rutas), elija Edit routes (Editar rutas).
5. Seleccione Add route (Añadir ruta). En Destination (Destino), especifique `::/0`. En Target (Destino), seleccione el ID de la puerta de enlace de Internet de solo salida y, a continuación, elija Save changes (Guardar cambios).

Para obtener más información, consulte [Opciones de enrutamiento de ejemplo \(p. 90\)](#).

Paso 3: Actualizar las reglas del grupo de seguridad

Para habilitar sus instancias de modo que puedan enviar y recibir tráfico por IPv6 debe actualizar las reglas del grupo de seguridad para incluir reglas para direcciones IPv6.

Por ejemplo, en el ejemplo anterior, puede actualizar el grupo de seguridad del servidor web (`sg-11aa22bb11aa22bb1`) para agregar reglas que permitan acceso entrante HTTP, HTTPS y SSH desde direcciones IPv6. No es necesario que haga ningún cambio a las reglas entrantes del grupo de seguridad de su base de datos; la regla que permite todas las comunicaciones desde el grupo de seguridad `sg-11aa22bb11aa22bb1` incluye la comunicación IPv6 de manera predeterminada.

Para actualizar las reglas de su grupo de seguridad

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Security Groups y seleccione el grupo de seguridad de su servidor web.
3. En la pestaña Inbound Rules, elija Edit.
4. Para cada regla, elija Add another rule y elija Save cuando haya terminado. Por ejemplo, para agregar una regla que permita todo el tráfico HTTP por IPv6, para Type (Tipo), seleccione HTTP, y para Source (Origen), escriba ::/0.

De forma predeterminada, cuando se asocia un bloque de CIDR IPv6 a su VPC, a los grupos de seguridad se les agrega automáticamente una regla saliente que permite todo el tráfico IPv6. Sin embargo, si ha modificado las reglas salientes originales de su grupo de seguridad, esta regla no se añadirá automáticamente, por lo que deberá añadir las reglas salientes equivalentes para el tráfico IPv6. Para obtener más información, consulte [Controlar el tráfico hacia los recursos mediante grupos de seguridad](#) (p. 255).

Actualizar las reglas de ACL de red

Si asocia un bloque de CIDR IPv6 a su VPC, se añadirán automáticamente reglas a la ACL de red predeterminada para permitir el tráfico IPv6 siempre que no haya modificado las reglas predeterminadas. Si ha modificado la ACL de red predeterminada o si ha creado una ACL de red personalizada con reglas para controlar el flujo de tráfico entrante y saliente de la subred, deberá añadir manualmente las reglas para el tráfico IPv6. Para obtener más información, consulte [Controlar el tráfico hacia las subredes utilizando las ACL de red](#) (p. 120).

Paso 4: Cambiar el tipo de instancia

Todos los tipos de instancia de la generación actual admiten IPv6. Para obtener más información, consulte [Tipos de instancia](#).

Si su tipo de instancia no es compatible con IPv6, deberá cambiar el tamaño de la instancia a un tipo compatible de instancia. En el ejemplo anterior, la instancia de la base de datos es del tipo `m3.large`, que no es compatible con IPv6. Por lo tanto, debe redimensionar la instancia con un tipo de instancia compatible como, por ejemplo, `m4.large`.

Para redimensionar la instancia, tenga en cuenta las limitaciones de compatibilidad. Para obtener más información, consulte [Compatibilidad para cambiar el tamaño de instancias](#) en la Guía del usuario de Amazon EC2 para instancias de Linux. En este escenario, si la instancia de la base de datos se lanzó desde una AMI que utiliza virtualización HVM, podrá redimensionarla al tipo de instancia `m4.large` utilizando el procedimiento siguiente.

Important

Para redimensionar su instancia, debe detenerla. La detención y el inicio de la instancia modifica la dirección IPv4 pública de la instancia, si es que dispone de alguna. Si tiene datos almacenados en volúmenes de almacén de instancias, los datos se borrarán.

Para redimensionar su instancia

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, elija Instances y seleccione la instancia de la base de datos.
3. Elija Actions, Instance State, Stop.
4. En el cuadro de diálogo de confirmación, elija Yes, Stop.

5. Con la instancia aún seleccionada, elija Actions, Instance Settings, Change Instance Type.
6. En Instance Type (Tipo de instancia), elija el nuevo tipo de instancia y luego elija Apply (Aplicar).
7. Para reiniciar la instancia detenida, seleccione la instancia y elija Actions, Instance State, Start. En el cuadro de diálogo de confirmación, elija Yes, Start.

Si su instancia es una AMI con respaldo en el almacenamiento de la instancia, no podrá redimensionar la instancia con el procedimiento anterior. En su lugar, cree una AMI con respaldo en el almacenamiento de la instancia desde su instancia y lance una nueva instancia desde su AMI utilizando un nuevo tipo de instancia. Para obtener más información, consulte [Creación de una AMI de Linux con respaldo en el almacén de instancias](#) en la Guía del usuario de Amazon EC2 para instancias de Linux y [Creación de una AMI de Windows con respaldo en el almacén de instancias](#) en la Guía del usuario de Amazon EC2 para instancias de Windows.

Es posible que no pueda migrar a un nuevo tipo de instancia si hay limitaciones de compatibilidad. Por ejemplo, si su instancia se lanzó desde una AMI que utiliza virtualización de PV, el único tipo de instancia que admite virtualización de PV e IPv6 es el tipo C3. Es posible que este tipo de instancia no se ajuste a sus necesidades. En este caso, es posible que tenga que volver a instalar el software en una AMI HVM básica y lanzar una nueva instancia.

Si lanza una instancia desde una nueva AMI, puede asignar una dirección IPv6 a su instancia durante el lanzamiento.

Paso 5: Asignar direcciones IPv6 a sus instancias

Después de comprobar que el tipo de instancia admite IPv6, puede asignar una dirección IPv6 a la instancia mediante la consola de Amazon EC2. La dirección IPv6 se asigna a la interfaz de red principal (eth0) para la instancia.

Para asignar una dirección IPv6 a su instancia

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. En el panel de navegación, seleccione Instances (Instancias).
3. Seleccione su instancia y elija Actions, Networking, Manage IP Addresses.
4. En IPv6 Addresses, elija Assign new IP. Puede escribir una dirección IPv6 específica del rango de su subred, o bien puede dejar el valor `Auto-Assign` predeterminado para que Amazon elija una dirección por usted.
5. Elija Yes, Update.

También, si lanza una instancia nueva (por ejemplo, si no pudo cambiar el tipo de instancia y creó una nueva AMI en su lugar), podrá asignar una dirección IPv6 durante el lanzamiento.

Para asignar una dirección IPv6 a una instancia durante el lanzamiento

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Seleccione su AMI y un tipo de instancia compatible con IPv6 y elija Next: Configure Instance Details.
3. En la página Configure Instance Details, seleccione una VPC en Network y una subred en Subnet. En Auto-assign IPv6 IP, seleccione Enable.
4. Siga el resto de pasos del asistente para lanzar su instancia.

Puede conectarse a una instancia utilizando su dirección IPv6. Si se conecta desde un equipo local, asegúrese de que el equipo local tiene una dirección IPv6 y que está configurada para usar IPv6. Para obtener más información, consulte [Conexión con la instancia de Linux](#) en la Guía del usuario de Amazon

EC2 para instancias de Linux y [Conexión a instancias de Windows](#) en la Guía del usuario de Amazon EC2 para instancias de Windows.

Paso 6: (opcional) Configurar IPv6 en sus instancias

Si ha lanzado la instancia con Amazon Linux 2016.09.0 o posterior, Windows Server 2008 R2 o posterior o Ubuntu Server 2018 o posterior, la instancia está configurada para IPv6 y no es necesario realizar ningún paso adicional.

Si ha iniciado la instancia desde una AMI diferente, es posible que no esté configurada para IPv6 y DHCPv6, lo que significa que cualquier dirección IPv6 que asigne a la instancia no se reconoce automáticamente en la interfaz de red principal.

Para verificar DHCPv6 en Linux

Utilice el ping6 comando de la siguiente manera.

```
$ ping6 ipv6.google.com
```

Para verificar DHCPv6 en Windows

Utilice el ping comando de la siguiente manera.

```
C:\> ping -6 ipv6.google.com
```

Si la instancia aún no está configurada, puede hacerlo manualmente, como se muestra en los procedimientos siguientes.

Configuración manual, por sistema operativo

- [Amazon Linux \(p. 368\)](#)
- [Ubuntu \(p. 369\)](#)
- [RHEL/CentOS \(p. 371\)](#)
- [Windows \(p. 373\)](#)

Amazon Linux

Para configurar la instancia de Amazon Linux

1. Conecte su instancia utilizando la dirección IPv4 pública de la instancia.
2. Obtenga los paquetes de software más recientes para su instancia:

```
sudo yum update -y
```

3. Con el editor de texto que desee, abra `/etc/sysconfig/network-scripts/ifcfg-eth0` y localice la línea siguiente:

```
IPV6INIT=no
```

Sustituya dicha línea por lo siguiente:

```
IPV6INIT=yes
```

Añada las siguientes dos líneas y guarde sus cambios:

```
DHCPV6C=yes
DHCPV6C_OPTIONS=-nw
```

4. Abra `/etc/sysconfig/network`, quite las líneas siguientes y guarde los cambios:

```
NETWORKING_IPV6=no
IPV6INIT=no
IPV6_ROUTER=no
IPV6_AUTOCONF=no
IPV6FORWARDING=no
IPV6TO4INIT=no
IPV6_CONTROL_RADVD=no
```

5. Abra `/etc/hosts`, sustituya los contenidos por los siguientes y guarde los cambios:

```
127.0.0.1    localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost6 localhost6.localdomain6
```

6. Reinicie su instancia. Vuelva a conectarse a su instancia y utilice el comando `ifconfig` para comprobar que la dirección IPv6 se reconoce en la interfaz de red principal.

Ubuntu

Puede configurar su instancia de Ubuntu para que reconozca de forma dinámica cualquier dirección IPv6 asignada a la interfaz de red. Si su instancia no tiene dirección IPv6, esta configuración hará que el tiempo de inicio de su instancia se amplíe hasta 5 minutos.

Contenido

- [Ubuntu Server 16 \(p. 369\)](#)
- [Ubuntu Server 14 \(p. 370\)](#)
- [Iniciar el cliente DHCPv6 \(p. 371\)](#)

Ubuntu Server 16

Estos pasos deben realizarse como usuario raíz.

Para configurar una instancia de Ubuntu Server 16

1. Conecte su instancia utilizando la dirección IPv4 pública de la instancia.
2. Visualice el contenido del archivo `/etc/network/interfaces.d/50-cloud-init.cfg`:

```
cat /etc/network/interfaces.d/50-cloud-init.cfg
```

```
# This file is generated from information provided by
# the datasource. Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp
```

Compruebe que el dispositivo de red de bucle invertido (lo) esté configurado y anote el nombre de la interfaz de red. En este ejemplo, el nombre de la interfaz de red es `eth0`. Es posible que el nombre varíe en función del tipo de instancia.

3. Cree el archivo `/etc/network/interfaces.d/60-default-with-ipv6.cfg` y añada la línea siguiente. Si es necesario, sustituya `eth0` por el nombre de la interfaz de red que recuperó en el paso anterior.

```
iface eth0 inet6 dhcp
```

4. Reinicie su instancia o la interfaz de red. Para ello, ejecute el comando que se describe a continuación. Si es necesario, sustituya `eth0` por el nombre de su interfaz de red.

```
sudo ifdown eth0 ; sudo ifup eth0
```

5. Vuelva a conectarse a su instancia y utilice el comando `ifconfig` para comprobar que la dirección IPv6 está configurada en la interfaz de red.

Para configurar IPv6 mediante datos de usuario

- Puede lanzar una nueva instancia de Ubuntu y asegurarse de que las direcciones IPv6 asignadas a la instancia se configuren automáticamente en la interfaz de red especificando los datos de usuario siguientes durante el lanzamiento:

```
#!/bin/bash  
echo "iface eth0 inet6 dhcp" >> /etc/network/interfaces.d/60-default-with-ipv6.cfg  
dhclient -6
```

En este caso, no tiene que conectarse a la instancia para configurar la dirección IPv6.

Para obtener más información, consulte [Ejecución de comandos en la instancia de Linux en el lanzamiento](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Ubuntu Server 14

Si va a utilizar Ubuntu Server 14, debe incluir una solución a un [problema conocido](#) que se produce al reiniciar la interfaz de red de pila doble (al reiniciarse, se agota el tiempo de espera y no se puede obtener acceso a la instancia durante dicho periodo).

Estos pasos deben realizarse como usuario raíz.

Para configurar una instancia de Ubuntu Server 14

1. Conecte su instancia utilizando la dirección IPv4 pública de la instancia.
2. Edite el archivo `/etc/network/interfaces.d/eth0.cfg` para que contenga lo siguiente:

```
auto lo  
iface lo inet loopback  
auto eth0  
iface eth0 inet dhcp  
    up dhclient -6 $IFACE
```

3. Reinicie su instancia:

```
sudo reboot
```


4. Vuelva a conectarse a su instancia y utilice el comando `ifconfig` para comprobar que la dirección IPv6 está configurada en la interfaz de red.

Iniciar el cliente DHCPv6

De manera alternativa, para mostrar la dirección IPv6 de la interfaz de red de inmediato sin tener que realizar ninguna configuración adicional, puede iniciar el cliente DHCPv6 de la instancia. Sin embargo, la dirección IPv6 no se mantiene en la interfaz de red tras el reinicio.

Para iniciar el cliente DHCPv6 en Ubuntu

1. Conecte su instancia utilizando la dirección IPv4 pública de la instancia.
2. Inicie el cliente DHCPv6:

```
sudo dhclient -6
```

3. Utilice el comando `ifconfig` para comprobar que la interfaz de red principal reconoce la dirección IPv6.

RHEL/CentOS

RHEL 7.4 y CentOS 7 y versiones posteriores usan [cloud-init](#) para configurar la interfaz de red y generar el `/etc/sysconfig/network-scripts/ifcfg-eth0` archivo. Puede crear un archivo de configuración `cloud-init` personalizado para habilitar DHCPv6, que genera un archivo `ifcfg-eth0` con configuraciones que habilitan DHCPv6 después de cada reinicio.

Note

Un problema conocido hace que, si utiliza RHEL/CentOS 7.4 con la última versión de `cloud-init-0.7.9`, al realizar estos pasos puede que pierda la conectividad con su instancia tras reiniciar. Una alternativa es editar manualmente el archivo `/etc/sysconfig/network-scripts/ifcfg-eth0`.

Para configurar una instancia de RHEL/CentOS mediante `cloud-init`

1. Conecte su instancia utilizando la dirección IPv4 pública de la instancia.
2. Con el editor de texto que desee, cree un archivo personalizado, por ejemplo:

```
/etc/cloud/cloud.cfg.d/99-custom-networking.cfg
```

3. Añada las siguientes líneas al archivo y guarde los cambios:

```
network:
  version: 1
  config:
    - type: physical
      name: eth0
      subnets:
        - type: dhcp
        - type: dhcp6
```

4. Con un editor de texto de su elección, agregue la siguiente línea al archivo específico de la interfaz en `/etc/sysctl.d`. Si deshabilitó la nomenclatura coherente de dispositivos de red, el nombre de la interfaz de red es `ethX` o la interfaz secundaria.

```
net.ipv6.conf.network-interface-name.accept_ra=1
```

En el ejemplo siguiente, la interfaz de red es en5.

```
net.ipv6.conf.en5.accept_ra=1
```

5. Reinicie su instancia.
6. Vuelva a conectarse a su instancia y utilice el comando `ifconfig` para comprobar que la dirección IPv6 está configurada en la interfaz de red.

Alternativamente, puede utilizar el siguiente procedimiento para modificar el `/etc/sysconfig/network-scripts/ifcfg-eth0` archivo directamente. Debe utilizar este método con una versión anterior de RHEL y CentOS que no admitan cloud-init.

Para configurar una instancia de RHEL/CentOS

1. Conecte su instancia utilizando la dirección IPv4 pública de la instancia.
2. Con el editor de texto que desee, abra `/etc/sysconfig/network-scripts/ifcfg-eth0` y localice la línea siguiente:

```
IPV6INIT="no"
```

Sustituya dicha línea por lo siguiente:

```
IPV6INIT="yes"
```

Añada las siguientes dos líneas y guarde sus cambios:

```
DHCPV6C=yes  
NM_CONTROLLED=no
```

3. Abra `/etc/sysconfig/network`, añada o modifique la línea siguiente como se indica a continuación y guarde los cambios:

```
NETWORKING_IPV6=yes
```

4. Reinicie las redes en su instancia ejecutando el comando siguiente:

```
sudo service network restart
```

Puede utilizar el comando `ifconfig` para comprobar que la interfaz de red principal reconoce la dirección IPv6.

Para solucionar problemas de RHEL 6 o CentOS 6

Si reinicia las redes y obtiene un error que indica que no se puede obtener la dirección IPv6, abra `/etc/sysconfig/network-scripts/ifup-eth` y localice la siguiente línea (de forma predeterminada el contenido se encuentra en la línea 327):

```
if /sbin/dhclient "$DHCLIENTARGS"; then
```

Quite las comillas antes y después de `$DHCLIENTARGS` y guarde los cambios. Reinicie las redes en su instancia:

```
sudo service network restart
```

Windows

Utilice los procedimientos siguientes para configurar IPv6 en Windows Server 2003 y Windows Server 2008 SP2.

Para asegurarse de que el sistema prefiere IPv6 frente a IPv4, descargue la corrección Preferir IPv4 acerca de IPv6 en las directivas de prefijo de la siguiente página de soporte de Microsoft: <https://support.microsoft.com/en-us/help/929852/how-to-disable-ipv6-or-its-components-in-windows>.

Para habilitar y configurar IPv6 en Windows Server 2003

1. Obtenga la dirección IPv6 de la instancia mediante el comando [describe-instances](#) de AWS CLI o marcando el campo IPv6 IPs (Direcciones IP IPv6) de la instancia en la consola de Amazon EC2.
2. Conecte su instancia utilizando la dirección IPv4 pública de la instancia.
3. Desde su instancia, elija Inicio, Panel de control, Conexiones de red, Conexión de área local.
4. Elija Propiedades y, a continuación, elija Instalar.
5. Elija Protocolo y Agregar. En la lista Protocolo de red, elija Microsoft TCP/IP versión 6 y, a continuación, elija Aceptar.
6. Abra el símbolo del sistema y el shell de red.

```
netsh
```

7. Cambie al contexto IPv6 de la interfaz.

```
interface ipv6
```

8. Añada la dirección IPv6 a la conexión de área local utilizando el comando siguiente. Sustituya el valor de la dirección IPv6 por la dirección IPv6 para su instancia.

```
add address "Local Area Connection" "ipv6-address"
```

Por ejemplo:

```
add address "Local Area Connection" "2001:db8:1234:1a00:1a01:2b:12:d08b"
```

9. Salga del shell de red.

```
exit
```

10. Utilice el comando `ipconfig` para comprobar que la conexión de área local reconoce la dirección IPv6.

Para habilitar y configurar IPv6 en Windows Server 2008 SP2

1. Obtenga la dirección IPv6 de la instancia mediante el comando [describe-instances](#) de AWS CLI o marcando el campo IPv6 IPs (Direcciones IP IPv6) de la instancia en la consola de Amazon EC2.
2. Conecte su instancia de Windows utilizando la dirección IPv4 pública de la instancia.
3. Elija Inicio, Panel de control.
4. Abra Centro de redes y recursos compartidos y, a continuación, abra Conexiones de red.
5. Haga clic con el botón derecho en Red de área local (para la interfaz de red) y elija Propiedades.
6. Elija la casilla de verificación Protocolo de Internet versión 6 (TCP/IPv6) y elija Aceptar.

7. Vuelva a abrir el cuadro de diálogo de propiedades de Red de área local. Elija Protocolo de Internet versión 6 (TCP/IPv6) y elija Propiedades.
8. Elija Usar la siguiente dirección IPv6: y haga lo siguiente:
 - En Dirección IPV6, escriba la dirección IPv6 que obtuvo en el paso 1.
 - En Longitud del prefijo de subred, escriba 64.
9. Elija Aceptar y cierre el cuadro de diálogo de propiedades.
10. Abra el símbolo del sistema. Utilice el comando `ipconfig` para comprobar que la conexión de área local reconoce la dirección IPv6.

Uso de Amazon VPC con otros Servicios de AWS

Puede utilizar Amazon VPC con otros Servicios de AWS para crear soluciones que satisfagan sus necesidades.

Contenido

- [Conectar la VPC a los servicios mediante AWS PrivateLink \(p. 375\)](#)
- [Filtrado del tráfico de red utilizando el AWS Network Firewall \(p. 376\)](#)
- [Filtrar el tráfico de DNS utilizando Route 53 Resolver DNS Firewall \(p. 377\)](#)

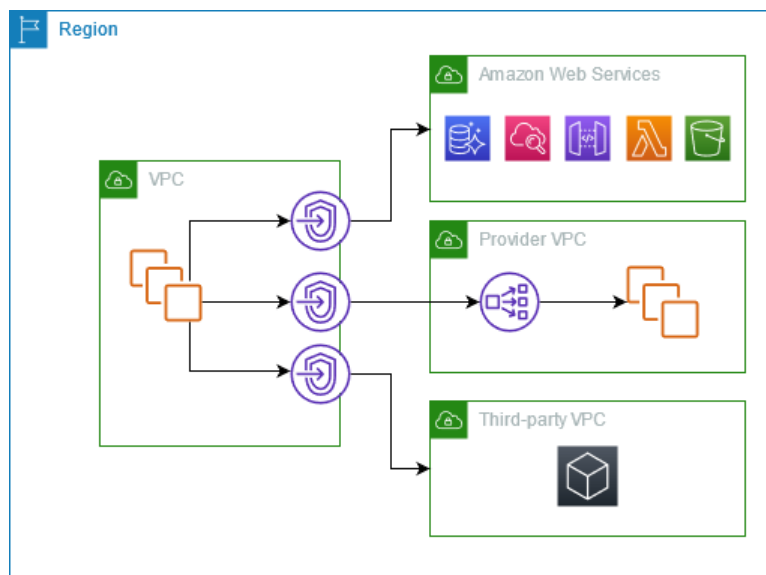
Conectar la VPC a los servicios mediante AWS PrivateLink

AWS PrivateLink establece conectividad privada entre nubes virtuales privadas (VPC) y servicios de Servicios de AWS compatibles alojados por otras Cuentas de AWS y servicios de AWS Marketplace compatibles. Para comunicarse con el servicio no necesita una puerta de enlace de Internet, dispositivo NAT, conexión a AWS Direct Connect ni conexión de AWS Site-to-Site VPN.

Para utilizar AWS PrivateLink, cree un punto de conexión de VPC en la VPC, especificando el nombre del servicio y una subred. De este modo se crea una interfaz de red elástica en la subred que sirve como punto de entrada al tráfico dirigido al servicio.

Puede crear su propio servicio de punto de enlace de la VPC, con tecnología de AWS PrivateLink, y permitir que otros clientes de AWS accedan al servicio.

En el siguiente diagrama, se muestran casos de uso comunes de AWS PrivateLink. La VPC de la izquierda tiene varias instancias de EC2 en una subred privada y tres puntos de conexión de VPC. El punto de conexión de VPC superior se conecta a un Servicio de AWS. El punto de conexión de VPC central se conecta a un servicio alojado por otra Cuenta de AWS (un servicio de punto de conexión de VPC). El punto de conexión de VPC inferior se conecta a un servicio asociado de AWS Marketplace.



Para obtener más información, consulte [AWS PrivateLink](#).

Filtrado del tráfico de red utilizando el AWS Network Firewall

Puede filtrar el tráfico de red en el perímetro de la VPC mediante AWS Network Firewall. Network Firewall es un servicio de detección y prevención de intrusiones con estado, administrado y de firewall de red. Para obtener más información, consulte [AWS Network Firewall Developer Guide](#).

Puede implementar Network Firewall con los siguientes recursos de AWS.

Recurso de Network Firewall	Descripción
Firewall	<p>Un firewall conecta el comportamiento de filtrado del tráfico de red de una política de firewall a la VPC que desea proteger. La configuración del firewall incluye especificaciones para las zonas de disponibilidad y las subredes donde se colocan los puntos de enlace del firewall. También define parámetros de alto nivel, como la configuración de registro del firewall y el etiquetado en el recurso de firewall de AWS.</p> <p>Para obtener más información, consulte Firewall en AWS Network Firewall.</p>
Directiva de firewall	<p>Una política de firewall define el comportamiento de supervisión y protección de un firewall. Los detalles del comportamiento se definen en los grupos de reglas que agregue a la política y en algunas configuraciones predeterminadas de políticas. Para utilizar una política de firewall, debe asociarla a uno o varios firewalls.</p> <p>Para obtener más información, consulte Políticas de firewall en AWS Network Firewall.</p>
Grupo de reglas	<p>Un grupo de reglas es un conjunto reutilizable de criterios para inspeccionar y gestionar el tráfico de red. Agregue uno o varios grupos de reglas a una política de firewall como parte de la configuración de políticas. Puede definir grupos de reglas sin estado para inspeccionar cada paquete de red de forma aislada. Los grupos de reglas sin estado son similares en comportamiento y uso a las listas de control de acceso (ACL) de red de Amazon VPC. También puede definir grupos de reglas con estado para inspeccionar paquetes en el contexto de su flujo de tráfico. Los grupos de reglas con estado son similares en comportamiento y uso a los grupos de seguridad de Amazon VPC.</p> <p>Para obtener más información, consulte Grupos de reglas en AWS Network Firewall.</p>

También puede utilizar AWS Firewall Manager para configurar y administrar de manera centralizada los recursos de Network Firewall en todas sus cuentas y aplicaciones de AWS Organizations. Puede administrar firewalls para varias cuentas al utilizar una sola cuenta en Firewall Manager. Para obtener más información, consulte [AWS Firewall Manager](#) en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Advanced.

Filtrar el tráfico de DNS utilizando Route 53 Resolver DNS Firewall

Con DNS Firewall, puede definir reglas de filtrado de nombres de dominio en grupos de reglas y asociarlos a las VPC. Puede especificar listas de nombres de dominio que se deban permitir o bloquear, así como personalizar las respuestas a las consultas de DNS que bloquee. Para obtener más información, consulte la [Documentación de DNS Firewall de Route 53 Resolver](#).

Puede implementar DNS Firewall con los siguientes recursos de AWS.

Recurso de DNS Firewall	Descripción
Grupo de reglas de DNS Firewall	<p>Un grupo de reglas de DNS Firewall es una colección, con nombre y reutilizable, de reglas de DNS Firewall para filtrar consultas de DNS. El grupo de reglas se rellena con las reglas de filtrado y, a continuación, se asocia a una o varias VPC de Amazon VPC. Cuando se asocia un grupo de reglas a una VPC, se habilita el filtrado de DNS Firewall en la VPC. A continuación, cuando Resolver recibe una consulta de DNS para una VPC que tiene asociado un grupo de reglas, Resolver pasa la consulta a DNS Firewall para que la filtre.</p> <p>Cada regla del grupo de reglas especifica una lista de dominios y una acción que se debe realizar en relación con las consultas de DNS cuyos dominios coincidan con las especificaciones de dominios de la lista. Las consultas concordantes se pueden permitir o bloquear, o bien emitir una alerta sobre ellas. También se pueden definir respuestas personalizadas para las consultas bloqueadas.</p> <p>Para obtener más información, consulte Grupos de reglas y reglas en DNS Firewall de Route 53 Resolver.</p>
Lista de dominios	<p>Una lista de dominios es un conjunto reutilizable de especificaciones de dominio que se utiliza en una regla de firewall de DNS, dentro de un grupo de reglas.</p> <p>Para obtener más información, consulte Listas de dominios en DNS Firewall de Route 53 Resolver.</p>

También puede utilizar AWS Firewall Manager para configurar y administrar de manera centralizada los recursos de DNS Firewall en todas sus cuentas y organizaciones de AWS Organizations. Puede administrar firewalls para varias cuentas al utilizar una sola cuenta en Firewall Manager. Para obtener más información, consulte [AWS Firewall Manager](#) en la Guía para desarrolladores de AWS WAF, AWS Firewall Manager y AWS Shield Advanced.

Cuotas de Amazon VPC

En las tablas siguientes, se muestran las cuotas, antes llamadas límites, para los recursos de Amazon VPC por región para su cuenta de AWS. A no ser que se indique lo contrario, puede solicitar un aumento de estas cuotas. Para algunas de estas cuotas, puede consultar la cuota actual mediante la página [Limits \(Límites\)](#) de la consola de Amazon EC2.

Si solicita un aumento de cuota que se aplica a cada uno de los recursos, aumente la cuota para todos los recursos de la región.

VPC y subredes

Nombre	Valor predeterminado	Ajustable	Comentarios
VPC por región	5	Sí	Al aumentar esta cuota, aumenta la cuota de gateways de Internet por región en la misma cantidad. Puede aumentar este límite para tener centenas de VPC por región.
Subredes por VPC	200	Sí	
Bloques de CIDR IPv4 por VPC	5	Sí (hasta 50)	Este bloque de CIDR principal y todos los bloques de CIDR secundarios se tienen en cuenta para esta cuota.
Bloques de CIDR IPv6 por VPC	1	No	

DNS

Cada instancia EC2 puede enviar 1024 paquetes por segundo por interface de red hacia Route 53 Resolver (en concreto, la dirección .2, como 10.0.0.2 y 169.254.169.253). Esta cuota no puede incrementarse. El número de consultas de DNS por segundo que Route 53 Resolver admite varía según el tipo de consulta, el tamaño de respuesta y el protocolo en uso. Para obtener más información y recomendaciones para una arquitectura de DNS escalable, consulte la guía técnica de AWS [Hybrid DNS with Active Directory](#) (DNS híbrido con Active Directory).

Direcciones IP elásticas (IPv4)

Nombre	Valor predeterminado	Ajustable	Comentarios
Direcciones IP elásticas por región	5	Sí	Esta cuota se aplica a las VPC de cuentas de AWS individuales y a las VPC compartidas.

Gateways

Nombre	Valor predeterminado	Ajustable	Comentarios
Gateways de Internet de solo salida por región	5	Sí	Para aumentar esta cuota, aumente la cuota de las VPC por región. Solo puede adjuntar una gateway de Internet de solo salida a una VPC a la vez.
Gateways de Internet por región	5	Sí	Para aumentar esta cuota, aumente la cuota de las VPC por región. Solo puede adjuntar una gateway de Internet a una VPC a la vez.
Gateways NAT por zona de disponibilidad	5	Sí	Cuando se calculan las cuotas, las gateways NAT en estado <code>pending</code> , <code>active</code> o <code>deleting</code> se tienen en cuenta.
Gateways de operador por VPC	1	No	

Listas de prefijos administradas por el cliente

Note

Si bien las cuotas predeterminadas para las listas de prefijos administradas por los clientes son ajustables, no se pueden ajustar las cuotas mediante la consola de Service Quotas. Debe ponerse en contacto con el Centro de soporte de AWS como se describe en [AWS Service Quotas](#) en la Referencia general de AWS.

Nombre	Valor predeterminado	Ajustable	Comentarios
Listas de prefijos por región	100	Sí	
Versiones por lista de prefijos	1 000	Sí	Si una lista de prefijos tiene 1000 versiones almacenadas y usted agrega una nueva versión, se quita la más antigua para que la nueva versión se pueda agregar.
Número máximo de entradas por lista de prefijos	1 000	Sí	La cuota predeterminada para las listas de prefijos administradas por el cliente es 10, a menos que se modifique el tamaño de la lista de prefijos. Puede cambiar el tamaño hasta 1000. Para obtener más información, consulte Cambiar una lista de prefijos (p. 74) . Cuando se hace referencia a una lista de prefijos de un recurso, el número máximo de entradas de las listas de prefijos cuenta respecto de la cuota correspondiente al número de entradas del recurso. Por ejemplo, si crea una lista de

Nombre	Valor predeterminado	Ajustable	Comentarios
			prefijos con un máximo de 20 entradas y hace referencia a esa lista de prefijos en una regla de un grupo de seguridad, cuenta como 20 reglas de grupos de seguridad.
Referencias a una lista de prefijos por tipo de recurso	5 000	Sí	Esta cuota se aplica por el tipo de recurso que puede hacer referencia a una lista de prefijos. Por ejemplo, puede tener 5000 referencias a una lista de prefijos en todos los grupos de seguridad más 5000 referencias a una lista de prefijos en todas las tablas de enrutamiento de la subred. Si comparte una lista de prefijos con otras cuentas de AWS, las referencias de las otras cuentas a su lista de prefijos cuentan para esta cuota.

ACL de red

Nombre	Valor predeterminado	Ajustable	Comentarios
ACL de red por VPC	200	Sí	Puede asociar una ACL de red de una o varias subredes de una VPC.
Reglas por ACL de red	20	Sí	<p>Esta es la cuota unidireccional para una ACL de red única. Esta cuota se aplica de manera individual para las reglas IPv4 e IPv6. Por ejemplo, puede tener 20 reglas entrantes para el tráfico IPv4 y 20 reglas entrantes para el tráfico IPv6. Esta cuota incluye las reglas de denegación predeterminada (número de regla 32767 para IPv4 y 32768 para IPv6 o un asterisco * en la consola de Amazon VPC).</p> <p>Esta cuota puede aumentarse hasta un máximo de 40; sin embargo, el desempeño de la red puede verse afectado debido al aumento de la carga de trabajo para procesar las reglas adicionales.</p>

Interfaces de red

Nombre	Valor predeterminado	Ajustable	Comentarios
Interfaces de red por instancia	Varía según el	No	Para obtener más información, consulte Interfaces de red por tipo de instancias .

Nombre	Valor predeterminado	Ajustable	Comentarios
	tipo de instancias		
Interfaces de red por región	5 000	Sí	Esta cuota se aplica a las VPC de cuentas de AWS individuales y a las VPC compartidas.

Tablas de ruteo

Nombre	Valor predeterminado	Ajustable	Comentarios
Tablas de rutas por VPC	200	Sí	La tabla de ruteo principal cuenta para esta cuota.
Rutas por tabla de rutas (rutas no propagadas)	50	Sí	Puede aumentar esta cuota a un máximo de 1000; no obstante, el rendimiento de la red podría verse afectado. Esta cuota se aplica de forma independiente para las rutas IPv4 e IPv6. Si tiene más de 125 rutas, para conseguir un mejor rendimiento, le recomendamos que pague las llamadas para describir las tablas de ruteo.
Rutas anunciadas de BGP por tabla de rutas (rutas propagadas)	100	No	Si necesita más prefijos, anuncie una ruta predeterminada.

Grupos de seguridad

Nombre	Valor predeterminado	Ajustable	Comentarios
Grupos de seguridad de VPC por región	2.500	Sí	Esta cuota se aplica a las VPC de cuentas de AWS individuales y a las VPC compartidas. Si aumenta esta cuota a más de 5000 grupos de seguridad en una región, para alcanzar un mejor rendimiento, le recomendamos que pague las llamadas para describir los grupos de seguridad.
Reglas entrantes o salientes por grupo de seguridad	60	Sí	Puede tener 60 reglas entrantes y 60 salientes por grupo de seguridad (lo que suma un total de 120 reglas). Esta cuota se aplica de manera individual para las

Nombre	Valor predeterminado	Ajustable	Comentarios
			reglas IPv4 e IPv6. Por ejemplo, un grupo de seguridad puede tener 60 reglas entrantes para el tráfico IPv4 y 60 reglas entrantes para el tráfico IPv6. Se aplica un cambio de cuota tanto a las reglas de entrada como a las de salida. Esta cuota multiplicada por la cuota para grupos de seguridad por interfaz de red no puede superar el valor de 1000.
Grupos de seguridad por interfaz de red	5	Sí (hasta 16)	Esta cuota multiplicada por la cuota para grupos de seguridad no puede superar el valor de 1000.

Interconexiones de VPC

Nombre	Valor predeterminado	Ajustable	Comentarios
Interconexiones de VPC activas por VPC	50	Sí (hasta 125)	Si aumenta esta cuota, debe aumentar la cantidad de entradas por tabla de enrutamiento en consecuencia.
Solicitudes de interconexión de VPC pendientes	25	Sí	Este es el número de interconexiones de VPC pendientes que ha solicitado desde su cuenta.
Tiempo de caducidad de una solicitud de interconexión de VPC no aceptada	1 semana (168 horas)	No	

Puntos de conexión de la VPC

Nombre	Valor predeterminado	Ajustable	Comentarios
Puntos de enlace de la VPC de tipo gateway por región	20	Sí	No puede haber más de 255 puntos de enlace de gateway por VPC.
Interfaz y puntos de enlace del balanceador de carga de gateway por VPC	50	Sí	Esta es la cuota combinada para el número máximo de puntos de enlace de interfaz y puntos de enlace del balanceador de carga de gateway en una VPC. Para aumentar esta cuota, póngase en contacto con AWS Support.
Tamaño de la política de puntos de enlace de la VPC	20 480 caracteres	No	Esta cuota incluye el espacio en blanco.

Las siguientes reglas de unidad de transmisión máxima (MTU) se aplican al tráfico que pasa a través de un punto de enlace de la 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 del punto de enlace de la VPC. Cuanto mayor sea la MTU, mayor cantidad de datos se podrán transferir en un solo paquete. Un punto de enlace de la VPC admite una MTU de 8500 bytes.
- Se eliminan los paquetes con un tamaño superior a 8500 bytes que llegan al punto de enlace de la VPC.
- El punto de enlace de la VPC no genera el paquete FRAG_NEEDEDICMP, por lo que la Detección de la MTU de la ruta (PMTUD) no es compatible.
- El punto de enlace de la VPC aplica el bloqueo de tamaño máximo de segmento (MSS) a todos los paquetes. Para obtener más información, consulte [RFC879](#).

Uso compartido de VPC

Todas las cuotas de VPC estándar se aplican a una VPC compartida.

Para aumentar esta cuota, contáctese con AWS Support. AWS le recomienda pagar las llamadas a la API `DescribeSecurityGroups` y `DescribeSubnets` antes de solicitar un aumento.

Nombre	Valor predeterminado	Ajustable	Comentarios
Cuentas de participante por VPC	100	Sí	<p>Este es la cantidad de cuentas de participantes distintas con las que se pueden compartir las subredes en una VPC. Esto es según la cuota de VPC y se aplica en todas las subredes compartidas en una VPC. Para aumentar esta cuota, póngase en contacto con AWS Support.</p> <p>Los propietarios de la VPC pueden ver las interfaces de red y los grupos de seguridad asociados a los recursos de los participantes.</p>
Subredes que se pueden compartir con una cuenta	100	Sí	Esta es la cantidad máxima de subredes que se pueden compartir con una cuenta de AWS.

Limitación controlada de API de Amazon EC2

Para obtener información sobre la limitación controlada de Amazon EC2, consulte [Limitación controlada de solicitudes de la API](#) en la Referencia de la API de Amazon EC2.

Recursos de cuotas adicionales

Para obtener más información, consulte los siguientes:

- [Cuotas de Transit Gateway](#) en Amazon VPC Transit Gateways.

- [Cuotas de AWS Client VPN](#) en la Guía del administrador de AWS Client VPN
- [Cuotas de Site-to-Site VPN](#) en la Guía del usuario de AWS Site-to-Site VPN
- [Cuotas de AWS Direct Connect](#) en la Guía del usuario de AWS Direct Connect

Historial de revisión

En la siguiente tabla se describen los cambios importantes en cada versión de la Guía del usuario de Amazon VPC y la Guía de interconexión de Amazon VPC.

update-history-change	update-history-description	update-history-date
Reorganización (p. 385)	Reorganización general de esta Guía del usuario de Amazon Virtual Private Cloud.	2 de enero de 2022
Gateway NAT de IPv6 a IPv4	La gateway NAT admite la traducción de direcciones de red de IPv6 a IPv4, y se la conoce popularmente como NAT64.	24 de noviembre de 2021
Subredes solo IPv6 en VPC	Puede crear subredes solo IPv6 en las que puede lanzar instancias EC2 solo IPv6.	23 de noviembre de 2021
Opciones de entrega de registros de flujo de la VPC a Amazon S3 (p. 385)	Puede especificar el formato de archivo de registro de Apache Parquet, las particiones por hora y los prefijos de S3 compatibles con Hive.	13 de octubre de 2021
Amazon EC2 Global View	Amazon EC2 Global View permite ver VPC, subredes, instancias, grupos de seguridad y volúmenes en varias regiones de AWS en una sola consola.	1 de septiembre de 2021
Rutas más específicas (p. 385)	Puede agregar una ruta a sus tablas de enrutamiento que sea más específica que la ruta local. Puede utilizar rutas más específicas para redirigir el tráfico entre subredes dentro de una VPC (tráfico Este-Oeste) a un dispositivo de middlebox. Puede establecer el destino de una ruta para que coincida con un bloque de CIDR IPv4 o IPv6 de una subred en su VPC.	30 de agosto de 2021
Compatibilidad con el etiquetado y los ID de recursos para las reglas de los grupos de seguridad (p. 385)	Puede consultar las reglas de los grupos de seguridad mediante el ID del recurso. También puede agregar etiquetas a las reglas de los grupos de seguridad.	7 de julio de 2021
Gateways NAT privadas (p. 385)	Puede utilizar una gateway NAT privada para la comunicación privada de solo salida entre las VPC o entre una VPC y la red en las instalaciones.	10 de junio de 2021

Gateways de operador	Cree gateways de operador para permitir el tráfico entrante desde una red de operador en una ubicación específica y a fin de permitir el tráfico saliente a la red del operador y a Internet.	6 de agosto de 2020
Etiqueta al crear (p. 385)	Puede añadir etiquetas al crear una conexión de emparejamiento de VPC y una tabla de enrutamiento.	20 de julio de 2020
Etiqueta al crear (p. 385)	Puede agregar etiquetas al crear una VPC, opciones DHCP, gateway de Internet, gateway de solo salida, ACL de red y grupo de seguridad.	30 de junio de 2020
Listas de prefijos administradas	Puede crear y administrar un conjunto de bloques CIDR en la lista de prefijos.	29 de junio de 2020
Mejoras de logs de flujo	Hay nuevos campos de registro de flujo disponibles y puede especificar un formato personalizado para los registros de flujo que se publican en CloudWatch Logs.	4 de mayo de 2020
Compatibilidad del etiquetado para los registros de flujo	Puede agregar etiquetas a los registros de flujo.	16 de marzo de 2020
Etiqueta al crear una gateway NAT	Puede agregar una etiqueta al crear una gateway NAT.	9 de marzo de 2020
Intervalo máximo de agregación para registros de flujo	Puede especificar el período máximo de tiempo durante el cual se captura un flujo y se agrega a un registro de flujo.	4 de febrero de 2020
Configuración del grupo de bordes de red	Puede configurar grupos de bordes de red para las VPC desde la Amazon Virtual Private Cloud Console.	22 de enero de 2020
Nombre de DNS privado	Ahora puede obtener acceso a los servicios basados en AWS PrivateLink de forma privada desde su VPC mediante nombres DNS privados.	6 de enero de 2020
Tablas de ruteo de gateway	Puede asociar una tabla de ruteo a una gateway y dirigir el tráfico entrante de la VPC a una interfaz de red específica en su VPC.	3 de diciembre de 2019

Mejoras de logs de flujo	Puede especificar un formato personalizado para su log de flujo y elegir qué campos devolver en los registros de logs de flujo.	11 de septiembre de 2019
Interconexión entre regiones	La resolución de nombres de host DNS se admite para las interconexiones de VPC entre regiones en la región Asia-Pacífico (Hong Kong).	26 de agosto de 2019
Uso compartido de VPC	Puede compartir las subredes que se encuentren en la misma VPC con varias cuentas de la misma organización de AWS.	27 de noviembre de 2018
Interconexión entre regiones	Puede crear una interconexión de VPC entre VPC de distintas regiones de AWS.	29 de noviembre de 2017
Crear subred predeterminada	Si una zona de disponibilidad no tienen una subred predeterminada, puede crearla.	9 de noviembre de 2017
Compatibilidad de etiquetado para las gateways NAT	Puede etiquetar su gateway NAT.	7 de septiembre de 2017
Métricas de Amazon CloudWatch para gateways NAT	Puede consultar métricas de CloudWatch para la gateway NAT.	7 de septiembre de 2017
Descripciones de regla de grupo de seguridad	Puede agregar descripciones a sus reglas de grupo de seguridad.	31 de agosto de 2017
Bloques de CIDR IPv4 secundarios para su VPC	Puede agregar varios bloques de CIDR IPv4 a su VPC.	29 de agosto de 2017
Recuperar las direcciones IP elásticas	Si libera una dirección IP elástica, es posible que pueda recuperarla.	11 de agosto de 2017
Crear una VPC predeterminada	Puede crear una VPC predeterminada si elimina la VPC predeterminada existente.	27 de julio de 2017
Compatibilidad con IPv	Puede asociar un bloque de CIDR IPv6 a su VPC y asignar direcciones IPv6 a los recursos de su VPC.	1 de diciembre de 2016
Soporte para la resolución de DNS para rangos de direcciones IP distintos de RFC (p. 385)	Ahora, el servidor DNS de Amazon puede resolver nombres de host DNS privados en direcciones IP privadas para todos los espacios de direcciones.	24 de octubre de 2016

Soporte para la resolución de DNS para la interconexión de VPC	Puede habilitar una VPC local para resolver nombres de host DNS públicos en direcciones IP privadas al consultar desde instancias en la VPC del mismo nivel.	28 de julio de 2016
Reglas antiguas de los grupos de seguridad	Puede identificar si se está haciendo referencia a su grupo de seguridad en las reglas de un grupo de seguridad de una VPC del mismo nivel, y puede identificar las reglas antiguas del grupo de seguridad.	12 de mayo de 2016
Uso de ClassicLink a través de una interconexión de VPC	Puede modificar su interconexión de VPC para permitir que las instancias locales vinculadas de EC2-Classic se comuniquen con las instancias de una VPC del mismo nivel y viceversa.	26 de abril de 2016
Gateways NAT	Puede crear una gateway NAT en una subred pública y habilitar las instancias en una subred privada para iniciar el tráfico saliente a Internet u otros servicios de AWS.	17 de diciembre de 2015
Logs de flujo de VPC	Puede crear un log de flujo para capturar información acerca del tráfico IP entrante y saliente de las interfaces de red de su VPC.	10 de junio de 2015
ClassicLink	ClassicLink le permite vincular su instancia EC2-Classic a una VPC de su cuenta. Puede asociar los grupos de seguridad de VPC a la instancia de EC2-Classic, para hacer posible la comunicación entre su instancia de EC2-Classic y las instancias de su VPC que usan direcciones IP privadas.	7 de enero de 2015
Utilización de zonas hospedadas privadas	Puede acceder a los recursos de la VPC utilizando nombres de dominio DNS personalizados que defina en una zona alojada privada en Route 53.	5 de noviembre de 2014
Modificación de un atributo de asignación de direcciones IP públicas de una subred	Puede modificar el atributo de asignación de direcciones IP públicas de su subred para identificar si las instancias lanzadas en esa subred deberían recibir una dirección IP pública.	21 de junio de 2014

Interconexión con VPC	También puede crear una interconexión VPC entre dos VPC, que permitirá a las instancias de las dos VPC comunicarse entre sí utilizando direcciones IP privadas.	24 de marzo de 2014
Asignación de una dirección IP pública	Puede asignar una dirección IP pública a una instancia durante el lanzamiento.	20 de agosto de 2013
Habilitación de nombres de host DNS y deshabilitación de resolución DNS	Puede modificar los valores predeterminados de la VPC y deshabilitar la resolución DNS y habilitar los nombres de host DNS.	11 de marzo de 2013
VPC en todas partes (p. 385)	Se ha agregado compatibilidad con la VPC en cinco regiones de AWS, las VPC en varias zonas de disponibilidad, varias VPC por cuenta de AWS y varias conexiones de VPN por VPC.	3 de agosto de 2011
Instancias dedicadas (p. 385)	Las instancias dedicadas son instancias Amazon EC2 lanzadas en su VPC que se ejecutan en hardware dedicado a un solo cliente.	27 de marzo de 2011