aws

Guía del usuario

Amazon Virtual Private Cloud



Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Virtual Private Cloud: Guía del usuario

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

¿Qué es Amazon VPC? ... 1
Características ... 1
Introducción a Amazon VPC ... 3
Trabajo con VPC de Amazon ... 3
Precios de Amazon VPC ... 3
Cómo funciona Amazon VPC ... 6
VPC y subredes ... 7
VPC predeterminadas y no predeterminadas ... 7
Tablas de ruteo ... 8
Acceder a Internet ... 8
Acceder a una red corporativa o doméstica ... 9
Conectar VPC y redes ... 10
AWSRed global privada de ... 10
Planificación de su VPC ... 11
Cómo crear una Cuenta de AWS ... 11
Cómo crear una Cuenta de AWS ... 11
Verificar permisos ... 11
Determine los rangos de direcciones IP ... 11
Seleccione las zonas de disponibilidad ... 12
Planifique la conectividad a Internet ... 12
Cree su VPC ... 13
Implementar la aplicación ... 13
Direccionamiento IP ... 15
Direcciones IPv4 privadas ... 16
Direcciones IPv4 públicas ... 17
Direcciones IPv6 ... 18
Direcciones IPv6 públicas ... 19
Direcciones IPv6 privadas ... 20
Utilizar sus propias direcciones IP ... 21
Utilice IP Address Manager (IPAM) de Amazon VPC ... 22
Bloques de CIDR de VPC ... 22
Bloques de CIDR de VPC IPv4 ... 22
Administración de bloques de CIDR de IPv4 para una VPC ... 24
Restricciones de asociación de bloques de CIDR IPv4 ... 26

Bloques de CIDR de VPC IPv6 29
Bloques de CIDR de subred 29
Ajuste de tamaño de subredes para direcciones IPv4 30
Ajuste de tamaño de subredes para direcciones IPv6 31
Comparar IPv4 e IPv6 32
Listas de prefijos administradas 33
Conceptos y reglas de las listas de prefijos 34
Administración de identidades y accesos para listas de prefijos 35
Listas de prefijos administradas por el cliente 36
AWSListas de prefijos administradas por 47
Optimización de la administración de la infraestructura AWS con listas de prefijos 50
Rangos de direcciones IP de AWS 52
Descargar 53
Control de salida 53
Fuente de geolocalización 54
Buscar los rangos de direcciones 54
Sintaxis 61
Suscribirse a las notificaciones de 66
Compatibilidad con IPv6 para su VPC 68
Adición de la compatibilidad de IPv6 con su VPC 69
Ejemplo de VPC de doble pila 74
Compatibilidad con IPv6 en AWS 76
Servicios compatibles con IPv6 76
Compatibilidad adicional con IPv6 91
Más información 92
Nubes virtuales privadas 93
Conceptos básicos sobre VPC 94
Rango de direcciones IP de una VPC 94
Diagrama de una VPC 94
Recursos de la VPC 95
Opciones de configuración de la VPC 96
VPC predeterminadas 98
Componentes de VPC predeterminados 98
Subredes predeterminadas 101
Utilización de su VPC y subredes predetermiandas 102
Creación de una VPC 106

Creación de una VPC y otros recursos de la VPC ... 106
Crear una sola VPC ... 108
Creación de una VPC mediante la AWS CLI ... 111
Visualización de los recursos de su VPC ... 115
Adición o eliminación de un bloque de CIDR ... 117
Conjunto de opciones de DHCP ... 120
¿Qué es DHCP? ... 120
Conceptos de conjuntos de opciones de DHCP ... 121
Trabajar con los conjuntos de opciones de DHCP ... 125
Atributos DNS ... 129
Descripción de Amazon DNS ... 130
Consultar los nombres de host DNS de su instancia EC2 ... 136
Ver y actualizar los atributos de DNS de su VPC ... 137
Uso de direcciones de red ... 138
Superar las cuotas de NAU ... 139
Cómo se calcula el NAU ... 139
Ejemplos de NAU ... 140
Intercambio de una subred de VPC ... 143
Requisitos previos para las subredes compartidas ... 143
Utilización de las subredes compartidas ... 144
Facturación y medición para el propietario y los participantes ... 147
Responsabilidades y permisos para propietarios y participantes ... 147
AWSRecursos de y subredes de VPC compartidas ... 151
Ampliar una VPC a otras zonas ... 152
Subredes en AWS Local Zones ... 153
Subredes en AWS Wavelength ... 159
Subredes en AWS Outposts ... 162
Eliminar su VPC ... 163
Eliminación mediante la consola ... 164
Eliminación mediante la CLI ... 165
Generar IaC a partir de las acciones de la consola ... 166
Subredes ... 168
Conceptos básicos sobre subredes ... 168
Rango de direcciones IP de una subred ... 168
Tipos de subred ... 169
Diagrama de la subred ... 170

Enrutar la subred ... 170
Configuración de subredes ... 170
Seguridad de la subred ... 171
Crear una subred ... 172
Adición o eliminación de un bloque de CIDR de IPv6 en su subred ... 174
Modificación de los atributos de las direcciones IP de sus subredes ... 174
Reservas de CIDR de subred ... 176
Trabaje con reservas de CIDR de subred mediante la consola ... 177
Trabajar con reservas de CIDR de subred mediante la AWS CLI ... 177
Tablas de enrutamiento ... 178
Conceptos de las tablas de enrutamiento ... 179
Tablas de enrutamiento de subred ... 181
Tablas de ruteo de puerta de enlace ... 189
Prioridad de la ruta ... 192
Opciones de enrutamiento de ejemplo ... 194
Creación de una tabla de enrutamiento y rutas ... 210
Administración de las tablas de enrutamiento de subred ... 212
Sustituir la tabla de enrutamiento principal ... 216
Asociación de una tabla de enrutamiento con una puerta de enlace ... 217
Reemplazar o restaurar el destino de una ruta local ... 218
Enrutamiento avanzado ... 219
Solución de problemas de accesibilidad ... 269
Asistente de enrutamiento de Middlebox ... 269
Requisitos previos del asistente de enrutamiento de Middlebox ... 270
Redirección del tráfico de VPC a un dispositivo de seguridad ... 270
Consideraciones del asistente de enrutamiento de Middlebox ... 273
Escenarios de Middlebox ... 273
Eliminar una subred ... 284
Conectar la VPC ... 285
Gateways de Internet ... 287
Conceptos básicos de la puerta de enlace de Internet ... 287
Cree un puerta de enlace de Internet ... 290
Eliminar un puerta de enlace de Internet ... 293
Gateways de Internet de solo salida ... 294
Conceptos básicos de las gateways de Internet de solo salida ... 295
Adición de acceso a Internet de solo salida en una subred ... 296

Dispositivos NAT ... 299
Gateways NAT ... 300
Instancias de NAT ... 356
Comparación de los dispositivos NAT ... 368
Direcciones IP elásticas ... 371
Conceptos y reglas de direcciones IP elásticas ... 372
Introducción a las direcciones IP elásticas ... 374
AWS Transit Gateway ... 383
AWS Virtual Private Network ... 384
Interconexiones de VPC ... 386
Supervisión ... 388
Logs de flujo de VPC ... 389
Conceptos básicos de logs de flujo ... 390
Registros de log de flujo ... 394
Ejemplos de registros de log de flujo ... 413
Limitaciones de los logs de flujo ... 424
Precios ... 429
Trabajo con registros de flujo ... 429
Publicar en CloudWatch Logs ... 432
Publicar en Amazon S3 ... 441
Publicar en Amazon Data Firehose ... 450
Realizar consultas mediante Athena ... 459
Administración de identidades y accesos en los registros de flujo de VPC ... 464
Solucionar problemas ... 472
Métricas de CloudWatch ... 477
Dimensiones y métricas de NAU ... 477
Habilitación o deshabilitación de la supervisión del NAU ... 480
Ejemplo de alarma de CloudWatch para NAU ... 481
Informes de facturación y de uso ... 482
Administración de direcciones IP ... 483
Puntos de conexión de VPC ... 483
Puertas de enlace de tránsito ... 484
Análisis de redes ... 485
Replicación de tráfico ... 485
VPC Lattice ... 486
Recursos entre cuentas/regiones ... 487

Descripción de la red de VPC ... 487
Ubicación geográfica ... 489
Subredes ... 490
La conectividad de red ... 491
Controles de seguridad ... 496
Administración del tráfico ... 498
Recursos relacionados ... 501
Seguridad ... 502
Protección de datos ... 503
Privacidad del tráfico entre redes ... 504
Aplicación del cifrado del tráfico en tránsito en VPC ... 505
Modos de control de cifrado ... 505
Supervisión del estado de cifrado de los flujos de tráfico ... 506
Exclusiones de Controles de cifrado de VPC ... 507
Flujo de trabajo de implementación ... 508
Estados de Controles de cifrado de VPC ... 509
AWSSoporte y compatibilidad con servicios de ... 509
Precios ... 3
AWS CLIReferencia de comandos de ... 515
Recursos adicionales ... 516
Identity and Access Management ... 516
Público ... 516
Autenticarse con identidades ... 517
Administrar el acceso con políticas ... 518
Cómo funciona Amazon VPC con IAM ... 520
Ejemplos de políticas ... 525
Solucionar problemas ... 538
AWSPolíticas administradas por ... 540
Cómo utilizar roles vinculados a servicios ... 544
Seguridad de la infraestructura ... 549
Aislamiento de red ... 550
Controlar el tráfico de red ... 550
Comparar grupos de seguridad y ACL de red ... 551
Grupos de seguridad ... 552
Conceptos básicos de los grupos de seguridad ... 554
Ejemplo de grupo de seguridad ... 555

Reglas del grupo de seguridad ... 556
Grupos de seguridad predeterminados ... 562
Crear un grupo de seguridad ... 564
Configuración de reglas de grupos de seguridad ... 566
Eliminación de un grupo de seguridad ... 568
Asociación de grupos de seguridad a varias VPC ... 569
Compartir grupos de seguridad con AWS Organizations ... 572
ACL de red ... 578
Conceptos básicos de la ACL de red ... 579
Reglas de ACL de red ... 581
ACL de red predeterminada ... 582
ACL de red personalizada ... 584
Detección de la MTU de la ruta ... 590
Crear una ACL de red ... 590
Administración de las asociaciones de ACL de red ... 594
Eliminación de una ACL de red ... 597
Ejemplo: controlar el acceso a las instancias de una subred ... 598
Resiliencia ... 602
Validación de cumplimiento ... 603
Bloqueo de acceso público de las VPC y subredes ... 604
Conceptos básicos del BPA de la VPC ... 605
Evaluación del impacto y monitoreo del BPA de la VPC ... 611
Ejemplo avanzado ... 616
Prácticas recomendadas ... 670
Uso con otros servicios ... 672
AWS PrivateLink ... 673
AWS Network Firewall ... 674
DNS Firewall de Route 53 Resolver ... 676
Analizador de accesibilidad ... 677
Ejemplos ... 679
Entorno de prueba ... 680
Descripción general ... 680
1. Creación de la VPC ... 683
2. Implementar la aplicación ... 684
3. Pruebe la configuración ... 684
4. Limpieza ... 684

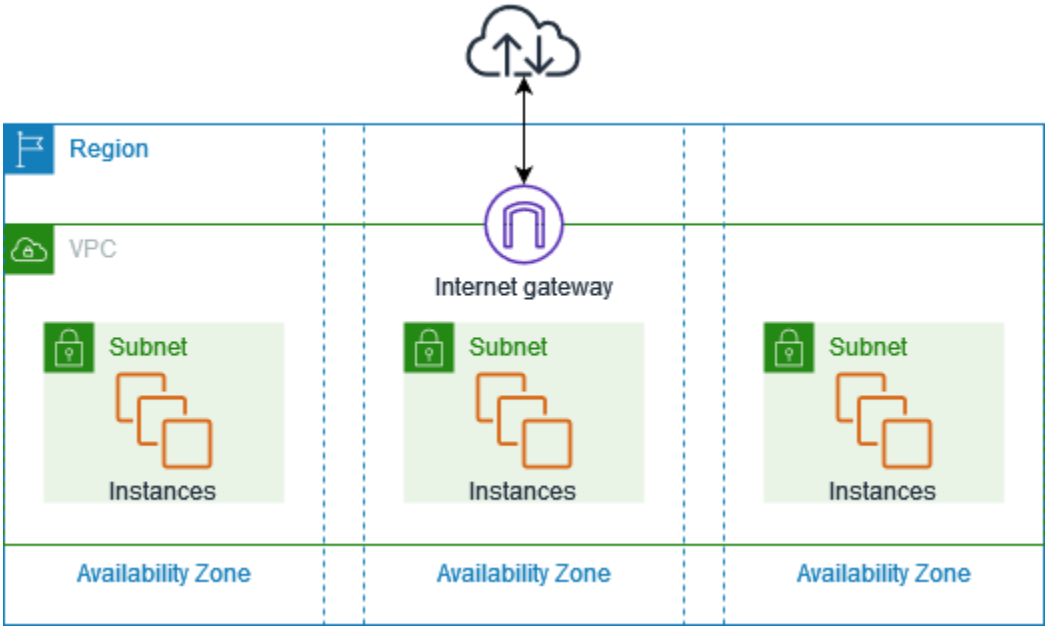
Servidores web y de bases de datos 684
Descripción general 685
1. Creación de la VPC 689
2. Implementar la aplicación 691
3. Pruebe la configuración 691
4. Limpieza 691
Servidores privados 692
Descripción general 692
1. Creación de la VPC 695
2. Implementar la aplicación 696
3. Pruebe la configuración 697
4. Limpieza 697
Tutoriales 698
Introducción a Amazon VPC mediante la AWS CLI 698
Requisitos previos 699
Creación de una VPC 699
Creación de subredes 700
Configuración de la conectividad a Internet 702
Creación de una puerta de enlace NAT 703
Configuración de los ajustes de la subred 704
Creación de grupos de seguridad 705
Verificación de la configuración VPC 706
Implementación de las instancias de EC2 707
Solución de problemas 234
Eliminar recursos 710
Paso a la producción 712
Siguientes pasos 713
Creación de una VPC con subredes privadas y puertas de enlace NAT mediante la AWS CLI . 713
Requisitos previos 699
Creación de las VPC y las subredes 715
Creación y configuración de la conectividad a Internet 717
Creación de puertas de enlace NAT 719
Creación de un punto de conexión de VPC para Amazon S3 720
Configuración de grupos de seguridad 721
Creación de una plantilla de lanzamiento para instancias de EC2 722
Creación de un equilibrador de carga y un grupo de destino 723

Creación de un grupo de escalado automático ... 725
Pruebe la configuración ... 725
Eliminar recursos ... 710
Pasos a seguir a continuación ... 713
Cuotas ... 729
VPC y subredes ... 729
DNS ... 730
Direcciones IP elásticas ... 730
Puertas de enlace ... 731
Listas de prefijos administradas por el cliente ... 731
ACL de red ... 733
Interfaces de red ... 733
Tablas de enrutamiento ... 734
Servidores de enrutamiento ... 735
Grupos de seguridad ... 737
Uso compartido de subredes de VPC ... 738
Uso de direcciones de red ... 739
Limitación controlada de API de Amazon EC2 ... 739
Recursos de cuotas adicionales ... 739
Historial de revisión ... 741

¿Qué es Amazon VPC?

Con Amazon Virtual Private Cloud (Amazon VPC), puede lanzar recursos de AWS en una red virtual aislada de manera lógica 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.

En el siguiente diagrama se muestra una VPC de ejemplo. La VPC tiene una subred en cada zona de disponibilidad de la región, instancias de EC2 en cada subred y una puerta de enlace de Internet para permitir la comunicación entre los recursos en su VPC y la Internet.



Para obtener más información, consulte Amazon Virtual Private Cloud (Amazon VPC).

Características

Las siguientes funciones lo ayudan a configurar una VPC para proporcionar la conectividad que necesitan sus aplicaciones:

Nubes virtuales privadas (VPC)

Una VPC es una red virtual prácticamente idéntica a una red tradicional que podría operar en su propio centro de datos. Una vez creada una VPC, podrá agregar las subredes.

Subredes

Una subred es un rango de direcciones IP en su VPC. Una subred debe residir en una sola zona de disponibilidad. Después de agregar subredes, puede implementar recursos de AWS de su VPC.

Direccionamiento IP

Puede asignar direcciones IP, IPv4 y IPv6, a las VPC y las subredes. También puede incorporar sus direcciones IPv4 públicas y GUA IPv6 a AWS y asignarlas a los recursos de su VPC, como las instancias de EC2, las puertas de enlace NAT y los equilibradores de carga de red.

Enrutamiento

Use las tablas de enrutamiento para determinar dónde se dirige el tráfico de red de su subred o puerta de enlace.

Puertas de enlace y puntos de conexión

Una puerta de enlace conecta su VPC a otra red. Por ejemplo, use una puerta de enlace de Internet para conectar la VPC a Internet. Use un punto de conexión de VPC para conectarse a Servicios de AWS de forma privada, sin el uso de una puerta de enlace de Internet o un dispositivo NAT.

Conexiones de emparejamiento

Use una conexión de emparejamiento de VPC para enrutar el tráfico entre los recursos de dos VPC.

Replicación de tráfico

Copie el tráfico de red desde las interfaces de red y envíelo a dispositivos de seguridad y monitoreo para una inspección profunda de paquetes.

Puertas de enlace de tránsito

Use una puerta de enlace de tránsito, que actúa como un concentrador central, para enrutar el tráfico entre sus VPC, las conexiones de VPN y las conexiones de Direct Connect.

Logs de flujo de VPC

Los registros de flujo capturan información acerca del tráfico IP entrante y saliente de las interfaces de red en su VPC.

Conexiones de VPN

Conecte sus VPC a las redes en las instalaciones mediante AWS Virtual Private Network (Site-to-Site VPN).

Introducción a Amazon VPC

Su Cuenta de AWS incluye una VPC predeterminada en cada Región de AWS. Las VPC predeterminadas se configuran de manera que pueda comenzar a lanzar instancias de EC2 y conectarse a ellas de inmediato. Para obtener más información, consulte Planificación de su VPC.

Puede optar por crear VPC adicionales con las subredes, las direcciones IP, las puertas de enlace y el enrutamiento que necesite. Para obtener más información, consulte the section called “Creación de una VPC”.

Trabajo con VPC de Amazon

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

- Consola de administración de AWS — 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. Sin embargo, se aplican cargos por algunos componentes de la VPC, como las puertas de enlace de NAT, el Administrador de direcciones IP, la replicación

de tráfico, el Analizador de accesibilidad y el Analizador de acceso a la red. Para obtener más información, consulte Precios de Amazon VPC.

Casi todos los recursos que inicie en la nube privada virtual (VPC) brindan una dirección IP para la conectividad. La mayoría de los recursos en la VPC utilizan direcciones IPv4 privadas. No obstante, los recursos que necesitan un acceso directo a Internet con IPv4 utilizan direcciones IPv4 públicas.

Amazon VPC le permite lanzar servicios administrados, como Elastic Load Balancing, Amazon RDS y Amazon EMR, sin necesidad de configurar previamente la VPC. Para hacerlo, utiliza la VPC predeterminada de su cuenta, si tiene una. Se cobrarán las direcciones IPv4 públicas proporcionadas a su cuenta por el servicio administrado. Estos cargos se asociarán al servicio de Amazon VPC en su AWS Cost and Usage Report.

Precios de direcciones IPv4 públicas

Una dirección IPv4 pública es una dirección IPv4 que se puede enrutar desde Internet. Se necesita una dirección IPv4 pública para poder acceder directamente a un recurso desde Internet a través de IPv4.

Si ya es usuario del nivel gratuito de AWS o es un usuario nuevo, obtendrá 750 horas de uso de direcciones IPv4 públicas sin cargo alguno con el servicio EC2. Si no utiliza el servicio EC2 en el nivel gratuito de AWS, se cobrará a las direcciones IPv4 públicas. Para obtener información específica sobre los precios, consulte la pestaña Dirección IPv4 pública en Precios de Amazon VPC.

Las direcciones IPv4 privadas (RFC 1918) no se cobran. Para obtener más información sobre cómo se cobran las direcciones IPv4 públicas por las VPC compartidas, consulte Facturación y medición para el propietario y los participantes.

Las direcciones IPv4 públicas pueden ser de alguno de los siguientes tipos:

- Direcciones IP elásticas (EIP): direcciones IPv4 públicas y estáticas proporcionadas por Amazon que puede asociar a una instancia de EC2, una interfaz de red elástica o un recurso de AWS.
- Direcciones IPv4 públicas de EC2: direcciones IPv4 públicas que Amazon ha asignado a una instancia de EC2 (si la instancia de EC2 se lanza en una subred predeterminada o si la instancia se lanza en una subred configurada para asignar automáticamente una dirección IPv4 pública).
- Direcciones BYOIPv4: direcciones IPv4 públicas en el rango de direcciones IPv4 que ha llevado a AWS mediante Traiga sus propias direcciones IP (BYOIP).

- Direcciones IPv4 administradas por un servicio: direcciones IPv4 públicas aprovisionadas automáticamente en recursos de AWS y administrada por un servicio de AWS. Por ejemplo, las direcciones IPv4 públicas en Amazon ECS, Amazon RDS o Amazon WorkSpaces.

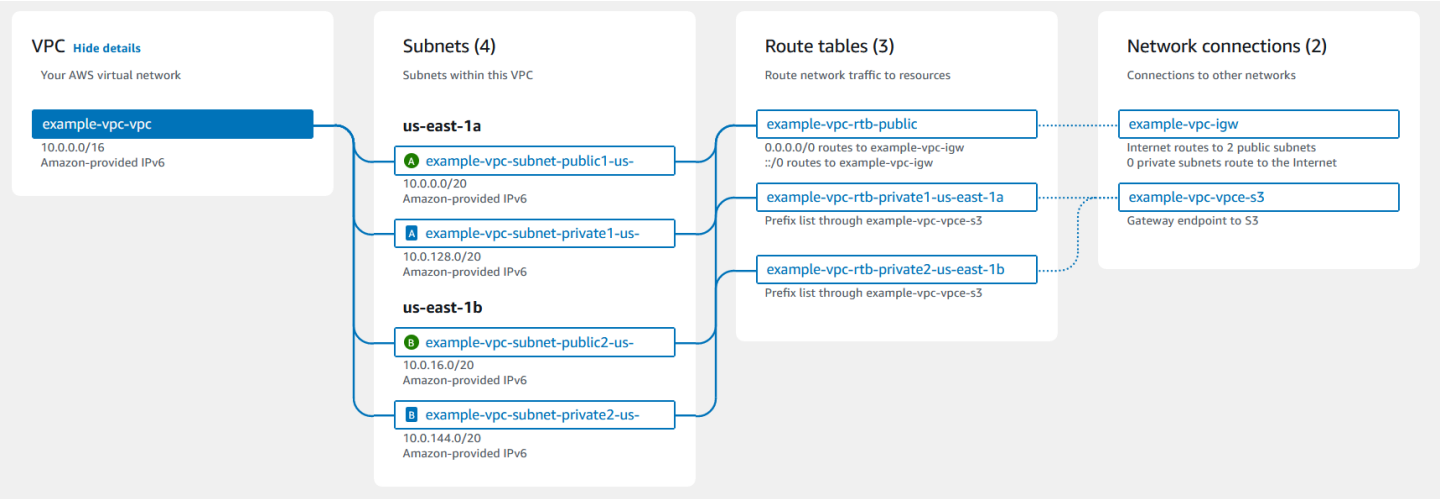
En la siguiente lista se muestran los servicios de AWS más comunes que pueden utilizar direcciones IPv4 públicas.

- Amazon WorkSpaces Applications
- AWS Client VPN
- AWS Database Migration Service
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EKS
- Amazon EMR
- Servidores de Amazon GameLift (Amazon GameLift Servers)
- AWS Global Accelerator
- AWS Mainframe Modernization
- Transmisión administrada de Amazon para Apache Kafka
- Amazon MQ
- Amazon RDS
- Amazon Redshift
- AWS Site-to-Site VPN
- Puerta de enlace NAT de Amazon VPC
- Amazon WorkSpaces
- Elastic Load Balancing

Cómo funciona Amazon VPC

Con Amazon Virtual Private Cloud (Amazon VPC), puede lanzar recursos de AWS en una red virtual aislada de manera lógica 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.

A continuación, se observa una representación visual de una VPC y sus recursos desde el panel Vista previa que se muestra cuando se crea una VPC mediante la Consola de administración de AWS. En una VPC existente, puede acceder a esta visualización en la pestaña Mapa de recursos. En el siguiente ejemplo se muestran los recursos que se seleccionan inicialmente en la página Crear VPC cuando se elige crear la VPC y otros recursos de red. Esta VPC está configurada con un bloque de CIDR de IPv4 y un bloque de CIDR de IPv6 proporcionado por Amazon, subredes en dos zonas de disponibilidad, tres tablas de enrutamiento, una puerta de enlace de Internet y un punto de conexión de puerta de enlace. Dado que seleccionamos la puerta de enlace de Internet, la visualización indica que el tráfico de las subredes públicas se enruta a Internet porque la tabla de enrutamiento correspondiente envía el tráfico a la puerta de enlace de Internet.



Conceptos

- VPC y subredes
- VPC predeterminadas y no predeterminadas
- Tablas de ruteo
- Acceder a Internet
- Acceder a una red corporativa o doméstica

- Conectar VPC y redes
- AWSRed global privada de

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 especificar un intervalo de direcciones IP para la VPC, añadir subredes, añadir puertas de enlace y asociar grupos de seguridad.

Una subred es un rango de direcciones IP en su VPC. Lanza recursos de AWS, como instancias de Amazon EC2, en las subredes. Puede conectar una subred a Internet, a otras VPC y a sus propios centros de datos, y dirigir el tráfico hacia y desde las subredes mediante tablas de enrutamiento.

Más información

- Direccionamiento IP
- Nubes virtuales privadas
- Subredes

VPC predeterminadas y no predeterminadas

Si la cuenta se creó después del 4 de diciembre de 2013, incluye una VPC predeterminada en cada región. Una VPC predeterminada está configurada y lista para utilizar. Por ejemplo, tiene una subred predeterminada en cada zona de disponibilidad de la región, una puerta de enlace de Internet conectada, una ruta de la tabla de enrutamiento principal que envía todo el tráfico a la puerta de enlace de Internet y una configuración de DNS que automáticamente aisgna nombres de host de DNS a las instancias de EC2 con direcciones IP públicas y habilita la resolución de DNS mediante el servidor de DNS proporcionado por Amazon (consulte Atributos DNS para la VPC). Por lo tanto, una instancia de EC2 que se lanza en una subred predeterminada tiene acceso automáticamente a Internet. Si tiene una VPC predeterminada en una región y no especifica una subred al lanzar una instancia de EC2 en esa región, elegimos una de las subredes predeterminadas y lanzaremos la instancia en esa subred.

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

- the section called “VPC predeterminadas”
- the section called “Creación de una VPC”

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 enrutamiento particular. De lo contrario, la subred se asocia de forma implícita con la tabla de enrutamiento principal.

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

Más información

- Configurar tablas de enrutamiento

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 puerta de enlace de Internet. Una puerta de enlace 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 puerta de enlace 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 puerta de enlace de Internet. De manera alternativa, las instancias podrán iniciar conexiones salientes a Internet mediante IPv6 a través de un puerta de enlace 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

- Activación del acceso a Internet de una VPC con una puerta de enlace de Internet
- Habilitar el tráfico IPv6 saliente mediante una puerta de enlace de Internet de solo salida
- Conexión a Internet u otras redes mediante dispositivos NAT

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 puerta de enlace 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
- Puertas de enlace de tránsito de Amazon VPC

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 puerta de enlace de tránsito y utilizarla para interconectar las VPC y las redes locales. La puerta de enlace de tránsito actúa como un enrutador virtual regional para el tráfico que fluye entre sus asociaciones, que puede incluir VPC, conexiones de VPN, puerta de enlaces de Direct Connect e interconexiones de puerta de enlaces de tránsito.

Más información

- Amazon VPC Peering Guide
- Puertas de enlace de tránsito de Amazon VPC

AWSRed 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.

Los paquetes que se originan en la red de AWS con un destino en la red de AWS permanecen en la red global de AWS, excepto el tráfico con destino u origen en las regiones de China de AWS y la región de la nube soberana europea de AWS. Esto es así tanto si el destino es una dirección IP privada como si es una dirección IP pública. Por ejemplo, si las instancias de EC2 de dos VPC se comunican mediante direcciones IP públicas, el tráfico permanece en la red global privada. El destino puede estar en la misma zona de disponibilidad, en una zona de disponibilidad diferente en la misma región o en una región diferente.

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 %.

Planificación de su VPC

Complete las siguientes tareas y prepárese para crear y conectar sus VPC. Cuando termine, estará listo para implementar su aplicación en AWS.

Tareas

- Cómo crear una Cuenta de AWS
- Verificar permisos
- Determine los rangos de direcciones IP
- Seleccione las zonas de disponibilidad
- Planifique la conectividad a Internet
- Cree su VPC
- Implementar la aplicación

Cómo crear una Cuenta de AWS

Cómo crear una Cuenta de AWS

Para empezar a utilizar AWS, necesita una Cuenta de AWS. Para obtener más información sobre cómo crear una Cuenta de AWS, consulte la sección Introducción a una Cuenta de AWS en la Guía de referencia de AWS Account Management.

Verificar permisos

Antes de poder utilizar Amazon VPC, debe tener los permisos necesarios. Para obtener más información, consulte Identity and Access Management para Amazon VPC y Ejemplos de políticas de Amazon VPC.

Determine los rangos de direcciones IP

Los recursos de su VPC se comunican entre sí y con recursos de Internet mediante direcciones IP. Cuando crea sus VPC y subredes, puede seleccionar los rangos de direcciones IP. Cuando implementa recursos en una subred, como instancias de EC2, reciben las direcciones IP del rango de direcciones IP de la subred. Para obtener más información, consulte Direccionamiento IP.

Cuando elija el tamaño de su VPC, tenga en cuenta cuántas direcciones IP necesitará en las Cuentas de AWS y las VPC. Asegúrese de que los rangos de direcciones IP de sus VPC no se superpongan con los rangos de direcciones IP de su red. Si necesita conectividad entre varias VPC, asegúrese de que las direcciones IP no se superpongan.

El administrador de direcciones IP (IP Address Manager, IPAM) facilita la planificación, el seguimiento y el monitoreo de las direcciones IP de la aplicación. Para obtener más información, consulte la Guía del Administrador de direcciones IP.

Seleccione las zonas de disponibilidad

Una región de AWS es una ubicación física donde se agrupan centros de datos, conocidos como zonas de disponibilidad. Cada zona de disponibilidad cuenta con alimentación, refrigeración y seguridad física independientes, con alimentación, red y conectividad redundantes. Las zonas de disponibilidad de una región están separadas físicamente por una distancia significativa e interconectadas mediante redes de ancho de banda alto y baja latencia. Puede diseñar su aplicación para que se ejecute en varias zonas de disponibilidad y así, lograr más tolerancia a los errores.

Entorno de producción

En un entorno de producción, se recomienda seleccionar como mínimo dos zonas de disponibilidad e implementar los recursos de AWS de manera uniforme en cada zona de disponibilidad activa.

Entorno de desarrollo o pruebas

En un entorno de desarrollo o pruebas, puede optar por ahorrar dinero e implementar los recursos en una sola zona de disponibilidad.

Planifique la conectividad a Internet

Planifique dividir cada VPC en subredes en función de los requisitos de conectividad. Por ejemplo:

- Si tiene servidores web que recibirán tráfico de clientes en Internet, cree una subred para estos servidores en cada zona de disponibilidad.
- Si también tiene servidores web que recibirán tráfico solo de otros servidores de la VPC, cree una subred independiente para estos servidores en cada zona de disponibilidad.
- Si tiene servidores web que recibirán tráfico solo mediante una conexión VPN, cree una subred independiente para estos servidores en cada zona de disponibilidad.

Si la aplicación recibirá tráfico de Internet, la VPC debe tener una puerta de enlace de Internet. La acción de adjuntar una puerta de enlace de Internet a una VPC no habilita de manera automática el acceso a las instancias desde Internet. Además de conectar la puerta de enlace de Internet, debe actualizar la tabla de enrutamiento de la subred con una ruta a la puerta de enlace de Internet. También debe asegurarse de que las instancias tengan direcciones IP públicas y un grupo de seguridad asociado que permita el tráfico desde Internet a través de puertos y protocolos específicos requeridos por su aplicación.

Como alternativa, registre las instancias con un equilibrador de carga expuesto a Internet. El equilibrador de carga recibe el tráfico de los clientes y lo distribuye entre las instancias registradas en una o más zonas de disponibilidad. Para obtener más información, consulte Elastic Load Balancing. Para permitir que las instancias de una subred privada accedan a Internet (por ejemplo, para descargar actualizaciones) sin permitir conexiones entrantes no solicitadas desde Internet, agregue una puerta de enlace de NAT pública en cada zona de disponibilidad activa y actualice la tabla de enrutamiento para enviar el tráfico de Internet a la puerta de enlace de NAT. Para obtener más información, consulte the section called “Acceso a Internet desde una subred privada”.

Cree su VPC

Una vez que haya determinado cuántas VPC y subredes necesita, qué bloques CIDR asignará a las VPC y las subredes, y cómo conectará la VPC a Internet, estará listo para crear su VPC. Si crea la VPC mediante la Consola de administración de AWS e incluye subredes públicas en la configuración, se creará una tabla de enrutamiento para la subred y se agregarán las rutas necesarias para el acceso directo a Internet. Para obtener más información, consulte the section called “Creación de una VPC”.

Implementar la aplicación

Una vez que creó la VPC, puede implementar la aplicación.

Entorno de producción

En un entorno de producción, puede utilizar uno de los siguientes servicios para implementar servidores en varias zonas de disponibilidad, para configurar el escalado a fin de mantener la cantidad mínima de servidores que requiere la aplicación y para registrar los servidores con un equilibrador de carga con tal de distribuir el tráfico de manera uniforme entre los servidores.

- Amazon EC2 Auto Scaling

- Flota de EC
- Amazon Elastic Container Service (Amazon ECS)

Entorno de desarrollo o pruebas

En un entorno de desarrollo o pruebas, puede optar por lanzar una única instancia de EC2. Para obtener más información, consulte Introducción a Amazon EC2 en la Guía del usuario de Amazon EC2.

Direccionamiento IP para VPC y subredes

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

La notación de enrutamiento entre dominios sin clases (CIDR) es una forma de representar una dirección IP y su máscara de red. El formato de estas direcciones es el siguiente:

- Una dirección IPv4 individual es de 32 bits, con 4 grupos de hasta 3 dígitos decimales, 0-255. Por ejemplo, 10.0.1.0.
- Un bloque de CIDR IPv4 tiene una dirección IPv4 seguida de una barra diagonal y un número del 0 al 32. Por ejemplo, 10.0.0.0/16 representa 65 536 direcciones IPv4 desde 10.0.0.0 hasta 10.0.255.255.
- Una dirección IPv6 individual es de 128 bits, con 8 segmentos de hasta 4 dígitos hexadecimales. Por ejemplo, 2001:0db8:85a3:0000:0000:8a2e:0370:7334. No es necesario incluir los ceros iniciales en un segmento. También puede reemplazar los segmentos consecutivos de ceros con dos puntos (::) una vez en una dirección. Por lo tanto, la dirección de ejemplo puede comprimirse como 2001:db8:85a3::8a2e:370:7334.
- Un bloque de CIDR IPv6 tiene una dirección IPv6 que termina con segmentos de cero, y se sustituyen los segmentos de cero por dos puntos, seguidos de una barra diagonal y un número del 0 al 128. Por ejemplo, 2001:db8:1234:1a00::/56 representa 2^72 direcciones IPv6 desde 2001:db8:1234:1a00:0000:0000:0000:0000 hasta 2001:db8:1234:1aff:ffff:ffff:ffff:ffff.

Para obtener más información, consulte ¿Qué es CIDR?

Contenido

- Direcciones IPv4 privadas
- Direcciones IPv4 públicas
- Direcciones IPv6
- Utilizar sus propias direcciones IP
- Utilice IP Address Manager (IPAM) de Amazon VPC
- Bloques de CIDR de VPC
- Bloques de CIDR de subred
- Comparar IPv4 e IPv6

- Consolidación y administración de los bloques de CIDR de red con listas de prefijos administradas
- Rangos de direcciones IP de AWS
- Compatibilidad con IPv6 para su VPC
- Servicios de AWS compatibles con IPv6

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 primaria (por ejemplo, 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.

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.

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 puerta de enlace como, por ejemplo, una puerta de enlace de Internet, una puerta de enlace privada virtual, una conexión de AWS Site-to-Site VPN o Direct Connect.

Nunca anunciamos en Internet el intervalo de direcciones IPv4 de una subred.

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 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).

> **Note**
>
> AWS cobra por todas las direcciones IPv4 públicas, incluidas las direcciones IPv4 públicas asociadas a las instancias en ejecución y las direcciones IP elásticas. Para obtener más información, consulte la pestaña Dirección IPv4 pública en la página Precios de Amazon VPC.

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 Modificación de los atributos de las direcciones IP de sus subredes.
- 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.
- Para anular la asignación de una dirección IP pública de la instancia tras iniciarla, administre las direcciones IP asociadas a una interfaz de red. Para obtener más información, consulte Administrar direcciones IP en la Guía del usuario de Amazon EC2.

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. En casos determinados, se libera la dirección IP pública desde la instancia o se asigna una dirección nueva. Para obtener más información, consulte direcciones IP públicas en la Guía del usuario de Amazon EC2.

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.

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.

Si utiliza el Administrador de direcciones IP (IPAM) de Amazon VPC, puede obtener un bloque contiguo de direcciones IPv4 públicas de AWS y utilizarlo para asignar direcciones IP elásticas secuenciales a los recursos de AWS. El uso de bloques de direcciones IPv4 contiguos puede reducir considerablemente la sobrecarga de administración de las listas de control de acceso de seguridad y simplificar la asignación y el seguimiento de las direcciones IP para las empresas que escalan en AWS. Para obtener más información, consulte Asignación de direcciones IP elásticas secuenciales de un grupo del IPAM en la Guía del usuario del Administrador de direcciones IP de Amazon VPC.

Direcciones IPv6

A medida que Internet sigue creciendo, también crece la necesidad de direcciones IP. El formato más común para las direcciones IP es IPv4. El formato nuevo para las direcciones IP es IPv6, que brinda un espacio de direcciones más grande que IPv4. IPv6 resuelve el problema del agotamiento de direcciones IPv4 y permite conectar más dispositivos a Internet. La transición es gradual, pero a medida que aumente la adopción de IPv6, podrá simplificar sus redes y aprovechar las capacidades avanzadas de IPv6 para mejorar la conectividad, el rendimiento y la seguridad.

Muchos servicios de AWS, como Amazon EC2, Amazon S3 y Amazon CloudFront, ofrecen compatibilidad con doble pila (IPv4 e IPv6) o solo con IPv6, lo que permite asignar direcciones IPv6 a los recursos y acceder a ellos a través del protocolo IPv6. Esto simplifica la configuración y la administración de la red para aquellos clientes que adoptan IPv6.

Otros servicios ofrecen soporte de doble pila limitado o parcial y solo IPv6.

Para obtener más información acerca de los servicios compatibles con IPv6, consulte Servicios de AWS compatibles con IPv6.

Tenga en cuenta que algunas direcciones IPv6 están reservadas por la Internet Engineering Task Force. Para obtener más información acerca de los rangos de direcciones IPv6 reservados, consulte IANA IPv6 Special-Purpose Address Registry y RFC4291.

> **Note**
>
> Tanto el direccionamiento IPv6 público como el privado están disponibles en AWS. AWS define las direcciones IP públicas como las que se anuncian en Internet desde AWS, mientras que las direcciones IP privadas no lo son ni pueden anunciarse en Internet desde AWS.

Contenido

- Direcciones IPv6 públicas
- Direcciones IPv6 privadas

Direcciones IPv6 públicas

Las direcciones IPv6 proporcionadas por Amazon siempre se anuncian en Internet. Son únicas de forma global y, por lo tanto, están disponibles a través de Internet. Es posible controlar si los recursos, como instancias de EC2, están disponibles a través de sus direcciones IPv6 controlando el direccionamiento de sus subredes, o bien utilizando grupos de seguridad y ACL de red.

Estas son algunas de las maneras en las que puede prepararse para usar direcciones IPv6 públicas en sus cargas de trabajo:

- Cree un IPAM con el Administrador de direcciones IP de Amazon VPC y aprovisione un rango de direcciones IPv6 públicas propiedad de Amazon a un conjunto de direcciones de IPAM. Para obtener más información, consulte Crear grupos IPv6 en la Guía de usuario de Amazon VPC IPAM.
- Si tiene un IPAM y es propietario de un rango de direcciones IPv6 público, incorpore una parte o todo el rango de direcciones IPv6 públicas a IPAM y aprovisione el rango de direcciones IPv6 públicas a un conjunto de direcciones IPAM. Para obtener más información, consulte Tutorial: Traer sus direcciones IP a IPAM en la Guía del usuario de Amazon VPC IPAM.
- Si no tiene un IPAM pero es propietario de un intervalo de direcciones IPv6 público, incorpore parte del intervalo de direcciones IPv6 público a AWS. Para obtener más información, consulte Traer sus propias direcciones IP (BYOIP) a Amazon EC2 en la Guía del usuario de Amazon EC2.

Una vez que esté preparado para usar direcciones IPv6 públicas, puede asignar direcciones IPv6 públicas a las instancias (consulte las direcciones IPv6 en la Guía del usuario de Amazon EC2),

puede asignar un bloque CIDR de IPv6 público a su VPC (consulte Adición o eliminación de un bloque de CIDR de su VPC) y asociar el bloque CIDR de IPv6 a sus subredes (consulteModificación de los atributos de las direcciones IP de sus subredes).

Direcciones IPv6 privadas

Las direcciones IPv6 privadas son direcciones IPv6 que no se anuncian ni se pueden anunciar en Internet desde AWS.

Puede usar una dirección IPv6 privada si desea que sus redes privadas admitan IPv6 y no tiene intención de enrutar el tráfico de estas direcciones a Internet. Si desea conectarse a Internet desde un recurso que tenga una dirección IPv6 privada, puede hacerlo, pero para ello debe enrutar el tráfico a través de un recurso de otra subred con una dirección IPv6 pública.

Hay dos tipos de direcciones IPv6 privadas:

- Intervalos ULA de IPv6: direcciones IPv6 tal como se definen en el RFC4193. Estos rangos de direcciones siempre comienzan por “fc” o “fd”, lo que los hace fácilmente identificables. El espacio ULA de IPv6 válido es cualquier espacio inferior a fd00::/8 que no se superponga con el rango reservado de Amazon fd00::/16.
- Intervalos GUA de IPv6: direcciones IPv6 tal como se definen en el RFC3587. La opción de usar rangos GUA de IPv6 como direcciones IPv6 privadas está deshabilitada de forma predeterminada y debe estar habilitada antes de poder usarla. Para obtener más información, consulte Habilitar el aprovisionamiento de CIDR GUA IPv6 privados en la Guía del usuario de IPAM de Amazon VPC.

Tenga en cuenta lo siguiente:

- Las direcciones IPv6 privadas solo están disponibles en el Administrador de direcciones IP (IPAM) de Amazon VPC. El IPAM detecta recursos con direcciones ULA y GUA de IPv6 y supervisa los grupos en busca de espacios de direcciones ULA y GUA de IPv6 superpuestos.
- Cuando utilice rangos GUA de IPv6 privados, requerimos que utilice los rangos GUA de IPv6 de su propiedad.
- Las direcciones IPv6 privadas no se anuncian ni pueden ser anunciadas en Internet por AWS. AWS no permite la salida directa a la Internet pública desde un rango de IPv6 privado, incluso si hay una puerta de enlace de Internet o una puerta de enlace de Internet de solo salida en la VPC. Las direcciones IPv6 privadas se guardan automáticamente en la periferia de la puerta de enlace de Internet, lo que garantiza que no se enruten públicamente.

- AWS reserva las 4 primeras direcciones IPv6 privadas de la subred y la última.
- Los rangos válidos para la ULA de IPv6 privada son de /9 a /60, empezando por fd80::/9.
- Si tiene un rango GUA de IPv6 privado asignado a una VPC, no puede usar el espacio GUA de IPv6 público que se superponga al espacio GUA de IPv6 privado de la misma VPC.
- Se admite la comunicación entre recursos con rangos de direcciones ULA y GUA IPv6 privados (por ejemplo, a través de Direct Connect, emparejamiento de VPC, puerta de enlace de tránsito o conexiones VPN).
- Puede usar direcciones IPv6 privadas con subredes de VPC de doble pila y solo IPv6, equilibradores de carga elásticos y puntos de conexión de AWS Global Accelerator.
- Las direcciones IPv6 privadas son gratuitas.

Estas son algunas de las maneras en las que puede prepararse para usar direcciones IPv6 privadas en sus cargas de trabajo:

- Cree un IPAM con el Administrador de direcciones IP de Amazon VPC y aprovisione un rango IPv6 ULA privado a un conjunto de direcciones de IPAM. Para obtener más información, consulte Crear grupos IPv6 en la Guía de usuario de Amazon VPC IPAM.
- Cree un IPAM con Administrador de direcciones IP de Amazon VPC y aprovisione un rango GUA de IPv6 privado a un conjunto de direcciones de IPAM. La opción de usar rangos GUA de IPv6 como direcciones IPv6 privadas está deshabilitada de forma predeterminada y debe estar habilitada en su IPAM antes de poder usarla. Para obtener más información, consulte Habilitar el aprovisionamiento de CIDR GUA IPv6 privados en la Guía del usuario de IPAM de Amazon VPC.

Una vez que esté preparado para usar direcciones IPv6 privadas, puede asignar un bloque CIDR de IPv6 privado de un grupo de IPAM a su VPC (consulte Adición o eliminación de un bloque de CIDR de su VPC) y asociar el bloque CIDR de IPv6 a sus subredes (consulte Modificación de los atributos de las direcciones IP de sus subredes).

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 de 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.

Utilice IP Address Manager (IPAM) de Amazon VPC

Amazon VPC IP Address Manager (IPAM) es una característica de VPC que facilita la planificación, el seguimiento y el monitoreo de las direcciones IP de las cargas de trabajo de AWS. Puede usar IPAM para asignar los CIDR de direcciones IP a las VPC mediante reglas comerciales específicas.

Para obtener más información acerca de Amazon VPC, consulte ¿Qué es IPAM? en la Guía del usuario de IPAM de Amazon VPC.

Bloques de CIDR de VPC

Las direcciones IP de la nube privada virtual (VPC) se representan mediante la notación de enrutamiento entre dominios sin clases (CIDR). Una VPC debe tener un bloque de CIDR de IPv4 asociado. Opcionalmente, puede asociar bloques de CIDR de IPv4 adicionales y uno o varios bloques de CIDR de IPv6. Para obtener más información, consulte Direccionamiento IP para VPC y subredes.

Contenido

- Bloques de CIDR de VPC IPv4
- Administración de bloques de CIDR de IPv4 para una VPC
- Restricciones de asociación de bloques de CIDR IPv4
- Bloques de CIDR de VPC IPv6

Bloques de CIDR de VPC 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 IPv4 secundarios con la VPC. Para obtener más información, consulte Adición o eliminación de un bloque de CIDR de su VPC.

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)	10.0.0.0/16
172.16.0.0 - 172.31.255.255 (prefijo 172.16/12)	172.31.0.0/16
192.168.0.0 - 192.168.255.255 (prefijo 192.168/16)	192.168.0.0/20

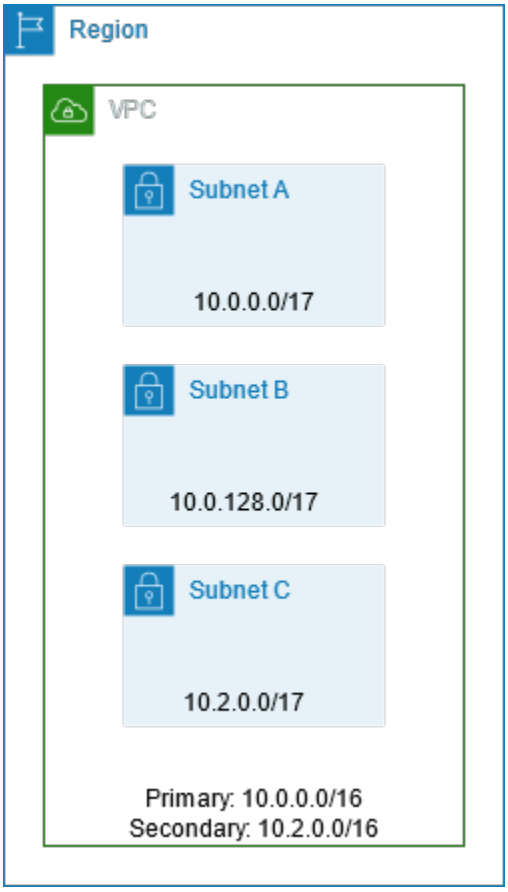
Consideraciones

- No puede especificar los siguientes bloques CIDR para sus VPC:
  - 0.0.0.0/8
  - 127.0.0.0/8 (rango de direcciones de loopback interno del host)
  - 169.254.0.0/16 (rango de direcciones locales del enlace)
  - 224.0.0.0/4 (rango de direcciones de multidifusión)
- Cuando crea una VPC para usarla con un servicio de AWS, debe consultar la documentación de dicho servicio para comprobar si hay requisitos específicos para su configuración.
- Algunos servicios de AWS utilizan el rango de CIDR `172.17.0.0/16`. Los servicios pueden experimentar conflictos de direcciones IP si el rango de dirección IP ya está en uso en la red. Por ejemplo, AWS Cloud9 y Amazon SageMaker AI utilizan `172.17.0.0/16`. Para evitar conflictos, no utilice este rango al crear la VPC. Para obtener más información, consulte No se puede conectar al entorno de EC2 porque Docker utiliza las direcciones IP de VPC en la Guía del usuario de AWS Cloud9.
- Puede crear una VPC con un bloque de CIDR direccionable públicamente externo a los intervalos de direcciones IPv4 privadas especificadas en RFC 1918. Sin embargo, para esta documentación, nos referimos a las direcciones IP privadas como las direcciones IPv4 que se encuentran en el intervalo de CIDR de su VPC.
- 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.
- 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.
- 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.
- 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 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 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 --output text
```

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 una descripción general de las asociaciones permitidas y restringidas para los bloques de CIDR de la VPC existentes. El motivo de las restricciones es que algunos servicios de AWS utilizan funciones multiVPC y multicuenta que requieren bloques de CIDR no conflictivos en el servicio de AWS.

Rango de direcciones IPv4 existentes	Asociaciones restringidas	Asociaciones permitidas
10.0.0.0/8	Bloques de CIDR de otros rangos RFC 1918* (172.16.0.0/12 y 192.168.0.0/16). Si alguno de los bloques de CIDR asociados a la VPC son del rango 10.0.0.0/15 (de 10.0.0.0 a 10.1.255.	Cualquier otro bloque de CIDR no restringido entre una máscara de red /16 y una máscara de red /28 del rango 10.0.0.0/8. Cualquier bloque de CIDR IPv4 direccionable públicamente (no RFC

Rango de direcciones IPv4 existentes	Asociaciones restringidas	Asociaciones permitidas
	255), no puede agregar un bloque de CIDR del rango 10.0.0.0/16 (de 10.0.0.0 a 10.0.255.255). Bloques de CIDR del rango 198.19.0.0/16.	1918) entre una máscara de red /16 y /28, o un bloque de CIDR entre una máscara de red /16 y /28 del rango 100.64.0.0/10.
169.254.0.0/16	Los bloques de CIDR del bloque “enlace local” se reservan tal como se describe en RFC 5735 y no se pueden asignar a las VPC.	
172.16.0.0/12	Bloques de CIDR de otros rangos RFC 1918* (10.0.0.0/8 y 192.168.0.0/16). Bloques de CIDR del rango 172.31.0.0/16. Bloques de CIDR del rango 198.19.0.0/16.	Cualquier otro bloque de CIDR no restringido, entre una máscara de red /16 y una máscara de red /28 del rango 172.16.0.0/12. Cualquier bloque de CIDR IPv4 direccionable públicamente (no RFC 1918) entre una máscara de red /16 y /28, o un bloque de CIDR entre una máscara de red /16 y /28 del rango 100.64.0.0/10.

Rango de direcciones IPv4 existentes	Asociaciones restringidas	Asociaciones permitidas
192.168.0.0/16	Bloques de CIDR de otros rangos RFC 1918* (10.0.0.0/8 y 172.16.0.0/12). Bloques de CIDR del rango 198.19.0.0/16.	Cualquier otro bloque de CIDR entre una máscara de red /16 y una máscara de red /28 del rango 192.168.0.0/16. Cualquier bloque de CIDR IPv4 direccionable públicamente (no RFC 1918) entre una máscara de red /16 y /28, o un bloque de CIDR del rango 100.64.0.0/10 rango entre una máscara de red /16 y /28.
198.19.0.0/16	Bloques de CIDR de los rangos RFC 1918*.	Cualquier bloque de CIDR IPv4 direccionable públicamente (no RFC 1918) entre una máscara de red /16 y /28, o un bloque de CIDR del rango 100.64.0.0/10 rango entre una máscara de red /16 y /28.
Bloque de CIDR direccionable públicamente (no RFC 1918), o un bloque de CIDR del rango 100.64.0.0/10	Bloques de CIDR de los rangos RFC 1918*. Bloques de CIDR del rango 198.19.0.0/16.	Cualquier otro bloque de CIDR IPv4 direccionable públicamente (no RFC 1918) entre una máscara de red /16 y /28, o un bloque de CIDR entre una máscara de red /16 y /28 del rango 100.64.0.0/10. También puede asociar un CIDR a uno de los rangos RFC 1918, pero para hacerlo, debe agregar ese CIDR primero al crear la VPC y luego agregar el CIDR que no sea RFC 1918.

*Los rangos de RFC 1918 son los rangos de direcciones IPv4 privadas que se especifican en RFC 1918.

Bloques de CIDR de VPC IPv6

Puede asociar un único bloque de CIDR de IPv6 cuando crea una VPC nueva o puede asociar hasta cinco bloques de CIDR de IPv6 de `/44` a `/60` en incrementos de `/4`. Puede solicitar un bloque de CIDR IPv6 del grupo de direcciones IPv6 de Amazon. Para obtener más información, consulte Adición o eliminación de un bloque de CIDR de su VPC.

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 cuando cree una nueva subred. Para obtener más información, consulte the section called “Ajuste de tamaño de subredes para direcciones IPv6”.

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`.

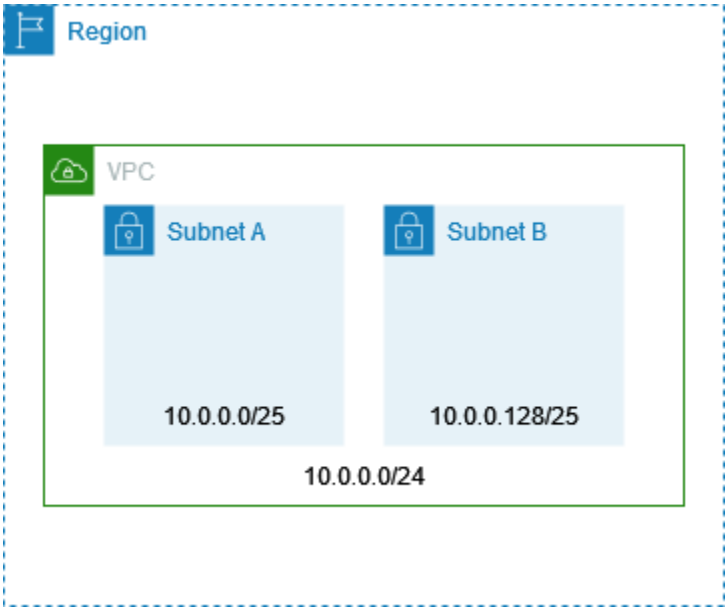
Puede desasociar un bloque de CIDR IPv6 de una VPC. Tras anular la asociación de un bloque de CIDR IPv6 de una VPC, no podrá esperar recibir el mismo CIDR si vuelve a asociar un bloque de CIDR IPv6 a su VPC más adelante.

Bloques de CIDR de subred

Las direcciones IP de las subredes se representan mediante la notación de enrutamiento entre dominios sin clases (CIDR). El bloque de CIDR de una subred puede ser el mismo que el de la VPC (para crear una subred única en la VPC) o un subconjunto del bloque de CIDR para la VPC (para crear varias subredes en la VPC).

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 e IPv6. 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 de IPv4 e IPv6 que debe especificar para las subredes.

Ajuste de tamaño de subredes para direcciones IPv4

El tamaño de bloque de CIDR de IPv4 permitido para una subred oscila entre una máscara de red `/28` y una `/16`. 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.
- 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.

Si incorpora un rango de direcciones IPv4 a AWS utilizando BYOIP, puede usar todas las direcciones IP del rango, incluidas la primera dirección (la dirección de red) y la última dirección (la dirección de transmisión).

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. Las longitudes posibles de las máscaras de red IPv6 oscilan entre `/44` y `/64` en incrementos de `/4`.

Existen herramientas en Internet que pueden servirle de ayuda para calcular y crear bloques de CIDR de subredes IPv6. Puede encontrar 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`: reservada por AWS para el router de la VPC.
- `2001:db8:1234:1a00::2`
- `2001:db8:1234:1a00::3`
- `2001:db8:1234:1a00:ffff:ffff:ffff:ffff`

Además de la dirección IP reservada por AWS para el enrutador de VPC en el ejemplo anterior, las siguientes direcciones IPv6 están reservadas para el enrutador de VPC predeterminado:

- Una dirección IPv6 local de enlace en el rango FE80::/10 generada mediante EUI-64. Para obtener más información sobre las direcciones locales de enlace, consulte Dirección local de enlace.
- La dirección IPv6 local de enlace `FE80:ec2::1`.

Si necesita comunicarse con el enrutador de VPC a través de IPv6, puede configurar sus aplicaciones para que se comuniquen con la dirección que mejor se adapte a sus necesidades.

Comparar IPv4 e IPv6

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

Para obtener una lista de los servicios de AWS que admiten configuraciones de doble pila (IPv4 e IPv6) y configuraciones solo de IPv6, consulte Servicios compatibles con IPv6.

Característica	IPv4	IPv6
Tamaño de la VPC	Hasta 5 CIDR de /16 a /28. Esta cuota se puede ajustar.	Hasta 5 CIDR de /44 a /60 en incrementos de /4. Esta cuota se puede ajustar.
Tamaño de la subred	De /16 a /28.	De /44 a /64 en incrementos de /4.
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.
Acceso a Internet	Requiere una puerta de enlace de Internet.	Requiere una puerta de enlace de Internet. Admite la comunicación solo

Característica	IPv4	IPv6
		de salida mediante una puerta de enlace de Internet solo de salida.
Direcciones IP elásticas	Soportado. Otorga a una instancia de EC2 una dirección IPv4 pública, estática y permanente.	No admitido. Los EIP mantienen estática la dirección IPv4 pública de una instancia al reiniciarla. Las direcciones IPv6 son estáticas de forma predeterminada.
Puerta de enlace de NAT	Soportado. Las instancias en subredes privadas pueden conectarse a Internet utilizando una puerta de enlace NAT pública o a recursos en otras VPC utilizando una puerta de enlace NAT privada.	Soportado. Puede utilizar una puerta de enlace NAT con NAT64 para que las instancias de subredes solo de IPv6 puedan comunicarse con recursos solo de IPv4 dentro de las VPC, entre VPC, en las redes de sus instalaciones o a través de Internet.
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.

Consolidación y administración de los bloques de CIDR de red con listas de prefijos administradas

Una lista de prefijos administrada es un conjunto de uno o más bloques de 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. También puede utilizar listas de prefijos administradas con otras cuentas de AWS mediante Resource Access Manager (RAM).

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
- Administración de identidades y accesos para listas de prefijos
- Listas de prefijos administradas por el cliente
- AWSListas de prefijos administradas por
- Optimización de la administración de la infraestructura AWS con listas de prefijos

Conceptos y reglas de las listas de prefijos

Una lista de prefijos consta de entradas. Cada entrada consta de un bloque de CIDR y, opcionalmente, de una descripción para el bloque de 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 de 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 enrutamiento, se aplican las reglas de prioridad de ruta. Para obtener más información, consulte Prioridad de ruta para listas de prefijos.
- 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.
- Las listas de prefijos administradas por el cliente están disponibles en todas las regiones comerciales de AWS, incluidas las regiones de China y GovCloud (EE. UU.).

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 AWSPeso de una lista de prefijos administrada por.
- 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 no tienen permiso para crear, ver, modificar o eliminar listas de prefijos. Puede crear una política de IAM y asociarla a un rol que permita a los usuarios utilizar 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 Referencia de autorizaciones de servicio.

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.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetManagedPrefixListAssociations",
                "ec2:GetManagedPrefixListEntries",
                "ec2:ModifyManagedPrefixList",
                "ec2:RestoreManagedPrefixListVersion"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012: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.

Listas de prefijos administradas por el cliente

Las listas de prefijos administradas por los clientes permiten definir y mantener los conjuntos propios de rangos de direcciones IP, conocidos como prefijos, dentro de AWS. En vez de codificar estas direcciones IP de forma rígida en varios recursos, puede crear una lista de prefijos centralizada y referenciarla cuando la necesite. Esto no solo simplifica la administración de sus direcciones IP, sino que también promueve la coherencia y la reutilización en todo el entorno de AWS.

Una de las características sobresalientes de las listas de prefijos administradas por los clientes es la posibilidad de compartirlas con otras cuentas de AWS. Cuando concede el acceso a sus listas de prefijos, permite que otros equipos u organizaciones utilicen, en sus recursos propios, las direcciones IP que usted definió. Este enfoque colaborativo fomenta una experiencia en la nube más coherente y eficiente, en la que la administración de direcciones IP se comparte y sincroniza.

En las siguientes secciones, trataremos en profundidad los aspectos prácticos del trabajo con las listas de prefijos administradas por los clientes, lo que incluye una guía detallada para crear, administrar y compartir sus rangos de dirección IP.

> **Note**
>
> Puede automatizar la administración de listas de prefijos mediante Amazon VPC IPAM para sincronizar automáticamente los CIDR en función de las reglas que defina. Esto evita tener que realizar actualizaciones manuales cuando cambia la infraestructura. Para obtener más información, consulte Automatización de las actualizaciones de listas de prefijos con IPAM en la Guía del usuario de Amazon VPC IPAM.

Tareas

- Trabajar con listas de prefijos administradas por el cliente

Trabajar con listas de prefijos administradas por el cliente

En esta sección, se describe cómo trabajar con las listas de prefijos administradas por los clientes.

Contenido

- Crear una lista de prefijos
- Ver las listas de prefijos
- Ver las entradas de una lista de prefijos
- Ver las asociaciones (referencias) de su lista de prefijos
- Modifique una lista de prefijos
- Cambiar una lista de prefijos
- Restaurar una versión anterior de una lista de prefijos
- Eliminar una lista de prefijos
- Intercambio de listas de prefijos administradas por los clientes

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 de 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 ayudarlo 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.

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. Si la lista de prefijos administrada está configurada como destino de resolución de listas de prefijos de IPAM, verá la opción de sincronización de resolución de listas de prefijos de IPAM.

   Elija si desea habilitar o desactivar la sincronización con el solucionador de listas de prefijos de IPAM. Cuando está habilitada, los CIDR de la lista de prefijos se actualizan automáticamente en función de las reglas de selección de CIDR del solucionador asociado. Cuando está desactivada, los CIDR de la lista de prefijos no se actualizan de forma automática. Para obtener más información sobre esta característica, consulte Automatización de las actualizaciones de listas de prefijos con IPAM en la Guía del usuario de Amazon VPC IPAM.

6. 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.
7. 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 hasta 1000. Para obtener más información sobre las cuotas de listas de prefijos administradas por el cliente, consulte Listas de prefijos administradas por el cliente.

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.

Intercambio de listas de prefijos administradas por los clientes

Con AWS Resource Access Manager (AWS RAM), el propietario de una lista de prefijos administrada por el cliente puede compartir la lista de prefijos con lo siguiente:

- 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 sobre AWS RAM, consulte la Guía del usuario de AWS RAM. Para más información, consulte Service Quotas en la Guía del usuario de AWS RAM.

> **Important**
>
> No se aplican cargos adicionales por compartir listas de prefijos.

Contenido

- Permisos de lista de prefijos compartida
- Trabajar con listas de prefijos compartidas

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.

Trabajar con listas de prefijos compartidas

Las listas de prefijos de AWS ofrecen una manera conveniente para administrar y referenciar los rangos de las direcciones IP que utilizan varios productos de AWS. Además de las listas de prefijos administradas por AWS, también puede crear y compartir sus propias listas de prefijos administradas por los clientes con otras cuentas de AWS.

Compartir listas de prefijos puede resultar especialmente útil para las organizaciones con requisitos de red complejos o para las que necesitan coordinar el uso de direcciones IP en varias cargas de trabajo de AWS. Al compartir una lista de prefijos, garantiza una administración coherente de las direcciones IP y simplifica las configuraciones de red de sus colaboradores.

En esta sección, se describe cómo compartir listas de prefijos y cómo identificar y utilizar las listas de prefijos que se compartieron con su cuenta.

Contenido

- Compartir una lista de prefijos
- Dejar de compartir una lista de prefijos compartida
- Identificar una lista de prefijos compartida
- Identificar referencias a una lista de prefijos compartida

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.

> **Important**
>
> - 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.

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

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. 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.

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.

AWSListas de prefijos administradas por

Las listas de prefijos administradas por AWS son conjuntos de rangos de direcciones IP para los servicios de AWS. Amazon Web Services mantiene estas listas de prefijos, las cuales ofrecen una manera de referenciar las direcciones IP que utilizan varias ofertas de AWS. Esto puede resultar particularmente útil al momento de configurar los grupos de seguridad u otros controles de la red dentro de una VPC.

Las listas de prefijos cubren una gran variedad de servicios de AWS, como S3 y DynamoDB, entre muchos otros. Las listas de prefijos administradas aseguran que las configuraciones de red estén actualizadas y tengan debidamente en cuenta las direcciones IP que utilizan los servicios de AWS que usted emplea. Esto puede simplificar las tareas de red y reducir la sobrecarga administrativa que supone la administración manual de las listas de direcciones IP.

Además de las ventajas prácticas, las listas de prefijos administradas también se ajustan a las prácticas recomendadas de seguridad de AWS. Al confiar en la información fiable que brinda AWS sobre la dirección IP, puede minimizar el riesgo de cometer errores en la configuración o la aparición de problemas de conectividad inesperados. Esto puede ser especialmente importante para las aplicaciones esenciales o las cargas de trabajo con requisitos de cumplimiento estrictos.

Contenido

- Listas de prefijos administradas por AWS disponibles
- AWSPeso de una lista de prefijos administrada por
- Utilizar una lista de prefijos administrada por AWS

Listas de prefijos administradas por AWS disponibles

Los siguientes servicios proporcionan listas de prefijos administradas por AWS.

Servicio de AWS	Nombre de una lista de prefijos	Peso
Amazon CloudFront	com.amazonaws.global.cloudfront.origin-facing (IPv4)	55
	com.amazonaws.global.ipv6.cloudfront.origin-facing (IPv6)	
Amazon DynamoDB	com.amazonaws.*region*.dynamodb	1
Amazon EC2 Instance Connect	com.amazonaws.*region*.ec2-instance-connect	2
	com.amazonaws.*region*.ipv6.ec2-instance-connect	2
AWS Ground Station	com.amazonaws.global.groundstation	5
Amazon Route 53	com.amazonaws.*region*.ipv6.route53-healthchecks	25
	com.amazonaws.*region*.route53-healthchecks	25
Amazon S3	com.amazonaws.*region*.s3	1
Amazon S3 Express One Zone	com.amazonaws.*region*.s3express	6
AWS Secrets Manager	com.amazonaws.*region*.secretsmanager-managed-external-secrets	20
Amazon VPC Lattice	com.amazonaws.*region*.vpc-lattice	10
	com.amazonaws.*region*.ipv6.vpc-lattice	10

Para ver las listas de prefijos administradas por AWS 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. En el campo de búsqueda, agregue el filtro ID del propietario: AWS.

Para ver las listas de prefijos administradas por AWS mediante la AWS CLI

Use el comando describe-managed-prefix-lists de la siguiente manera.

```
aws ec2 describe-managed-prefix-lists --filters Name=owner-id,Values=AWS
```

AWSPeso de una lista de prefijos administrada por

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

Por ejemplo, el peso de una lista de prefijos administrados de Amazon CloudFront es 55. Así es como esto afecta a sus cuotas de Amazon VPC:

- Grupos de seguridad: la cuota predeterminada 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.
- Tabla de enrutamiento: la cuota predeterminada 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.

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.

Al igual que con las listas de prefijos administradas por el cliente, puede usar las listas de prefijos administradas por AWS con recursos de AWS como grupos de seguridad y tablas de enrutamiento. Para obtener más información, consulte Optimización de la administración de la infraestructura AWS con listas de prefijos.

Optimización de la administración de la infraestructura AWS con listas de prefijos

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

Recursos

- Grupos de seguridad de la VPC
- Tablas de enrutamiento de subred
- Tablas de enrutamiento de la transit puerta de enlace
- AWS Network FirewallGrupos de reglas de
- Control de acceso a la red de Amazon Managed Grafana
- AWS Outposts bastidor de puertas de enlace locales

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, consulte Grupos de seguridad.

> **Important**
>
> No se puede modificar una regla existente para que utilice una lista de prefijos. Debe crear una regla nueva para utilizar una lista de prefijos.

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 Origen (reglas de entrada) o Destino (reglas de salida), elija Personalizar. A continuación, en el siguiente campo, en Listas de prefijos, elija el ID de 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 enrutamiento de puerta de enlace. Para obtener más información acerca de las tablas de ruteo, consulte Configurar tablas de enrutamiento.

Para hacer referencia a una lista de prefijos en una tabla de enrutamiento 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 enrutamiento.
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 enrutamiento 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 puerta de enlace

Puede especificar una lista de prefijos como destino de una ruta. Para obtener más información, consulte Referencias de listas de prefijos en Transit puerta de enlaces en Amazon VPC.

AWS Network FirewallGrupos de reglas de

Un grupo de reglas AWS Network Firewall es un conjunto reutilizable de criterios para inspeccionar y gestionar el tráfico de red. Si crea grupos de reglas con estado compatibles con Suricata en AWS

Network Firewall, puede hacer referencia a una lista de prefijos del grupo de reglas. Para obtener más información, consulte Referencing Amazon VPC prefix lists (Referencias de listas de prefijos de Amazon VPC) y Creating a stateful rule group (Crear un grupo de reglas con estado) en la AWS Network FirewallGuía para desarrolladores de .

Control de acceso a la red de Amazon Managed Grafana

Puede especificar una o más listas de prefijos como regla de entrada para las solicitudes a los espacios de trabajo de Amazon Managed Grafana. Para obtener más información sobre el control de acceso a la red de los espacios de trabajo de Grafana, incluido cómo hacer referencia a las listas de prefijos, consulte Administración del acceso a la red en la Guía del usuario de Amazon Managed Grafana.

AWS Outposts bastidor de puertas de enlace locales

Cada AWS Outposts bastidor proporciona una puerta de enlace local que le permite conectar los recursos de Outpost con las redes en las instalaciones. Puede agrupar los CIDR que usa con frecuencia en una lista de prefijos y hacer referencia a esta lista como destino de ruta en la tabla de enrutamiento de su puerta de enlace local. Para obtener más información, consulte Administrar las tablas de enrutamiento de puerta de enlace locales en la AWS Outposts Guía del usuario de bastidores.

Rangos de direcciones IP de AWS

AWS publica sus rangos de direcciones IP actuales en formato JSON. Con esta información, puede identificar el tráfico desde AWS. También puede utilizar esta información para permitir o denegar el tráfico hacia algunos servicios hacia o desde algunos Servicios de AWS.

Consideraciones

- Publicamos los rangos de direcciones IP de los servicios que los clientes suelen utilizar para realizar el filtrado de salida. No publicamos los rangos de direcciones IP para todos los servicios.
- Los servicios usan sus rangos de direcciones IP para comunicarse con otros servicios o con la red de un cliente.
- Los rangos de direcciones IP que usted agrega a AWS mediante la incorporación de direcciones IP propias (BYOIP) no se incluyen en el archivo `.json`. Para obtener más información, consulte Anuncie su rango de direcciones mediante AWS la Guía del usuario de Amazon EC2.

Algunos servicios publican sus rangos de direcciones mediante listas de prefijos administrados por AWS. Para obtener más información, consulte the section called “Listas de prefijos administradas por AWS disponibles”.

Contenido

- Descargue el archivo JSON
- Control de salida
- Fuente de geolocalización
- Buscar los rangos de direcciones IP para Servicios de AWS
- Sintaxis del JSON de rango de direcciones IP de AWS
- Notificaciones de rangos de direcciones IP de AWS

Descargue el archivo JSON

Para ver los rangos de direcciones actuales, descargue ip-ranges.json. Para mantener el historial, guarde versiones sucesivas del archivo JSON en su sistema. Para determinar si se han producido cambios desde la última vez que guardó el archivo, consulte la fecha y hora de publicación en el archivo actual y compárelas con la fecha y hora de publicación del último archivo que ha guardado.

El siguiente es un ejemplo del comando curl que guarda el archivo JSON en el directorio actual.

```
curl -O https://ip-ranges.amazonaws.com/ip-ranges.json
```

Si accede a este archivo mediante programación, es responsabilidad suya asegurarse de que la aplicación descargue el archivo correctamente únicamente después de haber comprobado el certificado TLS presentado por el servidor.

Para recibir notificaciones de actualizaciones del archivo JSON, consulte Notificaciones de rangos de direcciones IP de AWS.

Control de salida

Para permitir que los recursos que ha creado con un servicio de AWS solo accedan a otros servicios de AWS, puede usar la información del rango de direcciones IP del archivo ip-ranges.json para realizar el filtrado de salida. Asegúrese de que las reglas del grupo de seguridad permitan el tráfico saliente a los bloques de CIDR de la lista de AMAZON. Hay cuotas para los grupos de seguridad.

Según la cantidad de rangos de direcciones IP en cada región, es posible que necesite varios grupos de seguridad por región.

> **Note**
>
> Algunos productos AWS se basan en EC2 y utilizan el espacio de direcciones IP de EC2. Si bloquea el tráfico al espacio de direcciones IP de EC2, también bloquea el tráfico a estos servicios que no son de EC2.

Fuente de geolocalización

Los rangos de direcciones IP de `ip-ranges.json` son por Región de AWS. Sin embargo, una zona local no se encuentra en la misma ubicación física que su región principal. Los datos de geolocalización publicados en geo-ip-feed.csv representan zonas locales. Los datos siguen el RFC 8805.

Buscar los rangos de direcciones IP para Servicios de AWS

El archivo JSON de rangos de direcciones IP AWS provisto por AWS puede ser un recurso de gran valor para encontrar las direcciones IP de varios servicios de AWS y utilizar dicha información para mejorar la seguridad de red y el control de acceso. Con el análisis de los datos detallados contenidos dentro de este archivo JSON, puede identificar de manera precisa los rangos de direcciones IP asociados con Servicios de AWS y regiones específicos.

Por ejemplo, se pueden utilizar los rangos de direcciones IP para configurar políticas de seguridad de red robustas, al establecer reglas de firewall granulares para permitir o denegar el acceso a determinados recursos de AWS. Esta información también puede resultar útil para varias tareas de AWS Network Firewall. Este nivel de control es crucial para proteger sus aplicaciones y datos y garantizar que solo el tráfico tenga acceso a los necesarios Servicios de AWS. Además, esta inteligencia IP puede garantizar que sus aplicaciones estén configuradas correctamente para comunicarse con los puntos de conexión de AWS correctos, lo que mejora la fiabilidad y el rendimiento generales.

Más allá de las simples reglas de firewall, el archivo `ip-ranges.json` también se puede utilizar para configurar filtros de salida sofisticados en la infraestructura de red. Al comprender los rangos de direcciones IP de destino de los distintos Servicios de AWS, se pueden establecer políticas de enrutamiento o utilizar soluciones avanzadas de seguridad de red para permitir o bloquear de forma

selectiva el tráfico de salida según su destino previsto. Este control de salida es de suma importancia para la mitigación del riesgo de filtración de datos y el acceso sin autorización.

Es importante tener en cuenta que el archivo `ip-ranges.json` se actualiza periódicamente, por lo que es fundamental mantener una copia local actualizada para garantizar que se utiliza la información más precisa y actualizada. Al utilizar continuamente el contenido de este archivo, se puede administrar de manera eficiente el acceso y la seguridad de la red para sus aplicaciones basadas en AWS, lo que refuerza su postura general de seguridad en la nube.

Los siguientes ejemplos pueden ayudarle a filtrar los rangos de direcciones IP de AWS para que coincidan con lo que está buscando. En Linux, puede descargar y utilizar la herramienta jq para analizar una copia local del archivo JSON. AWS Tools for Windows PowerShell incluye un cmdlet, Get-AWSPublicIpAddressRange, que puede usar para analizar este archivo JSON. Para obtener más información, consulte el siguiente blog: Consulta de los rangos de direcciones IP públicas para AWS.

Para obtener el archivo JSON, consulte the section called “Descargar”. Para obtener más información acerca de la sintaxis del archivo JSON, consulte the section called “Sintaxis”.

Ejemplos

- Obtención de la fecha de creación del archivo
- Obtención de las direcciones IP de una región específica
- Obtención de todas las direcciones IPv4
- Obtención de todas las direcciones IPv4 de un servicio específico
- Obtención de todas las direcciones IPv4 de un servicio concreto en una región específica
- Obtención de todas las direcciones IPv6
- Obtención de todas las direcciones IPv6 de un servicio específico
- Obtenga todas las direcciones IP de un grupo fronterizo específico

Obtención de la fecha de creación del archivo

En el siguiente ejemplo se obtiene la fecha de creación de `ip-ranges.json`.

jq

```
$ jq .createDate < ip-ranges.json
```

```
"2024-08-01-17-22-15"
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -OutputPublicationDate

Thursday, August 1, 2024 9:22:35 PM
```

Obtención de las direcciones IP de una región específica

En el siguiente ejemplo, se filtra el archivo JSON para ver las direcciones IP de la región especificada.

jq

```
$ jq '.prefixes[] | select(.region=="us-east-1")' < ip-ranges.json

{
  "ip_prefix": "23.20.0.0/14",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
{
  "ip_prefix": "50.16.0.0/15",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
{
  "ip_prefix": "50.19.0.0/16",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -Region us-east-1
```

```
IpPrefix        Region      NetworkBorderGroup         Service
--------        ------       -------                   -------
23.20.0.0/14    us-east-1    us-east-1                 AMAZON
50.16.0.0/15    us-east-1    us-east-1                 AMAZON
50.19.0.0/16    us-east-1    us-east-1                 AMAZON
...
```

Obtención de todas las direcciones IPv4

En el siguiente ejemplo, se filtra el archivo JSON para las direcciones IPv4.

jq

```
$ jq -r '.prefixes | .[].ip_prefix' < ip-ranges.json

23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.IpAddressFormat -eq "Ipv4"} | select
 IpPrefix

IpPrefix
--------
23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
```

Obtención de todas las direcciones IPv4 de un servicio específico

En el siguiente ejemplo, se filtra el archivo JSON para las direcciones IPv4 del servicio especificado.

jq

```
$ jq -r '.prefixes[] | select(.service=="GLOBALACCELERATOR") | .ip_prefix' < ip-
ranges.json
```

```
13.248.117.0/24
15.197.34.0/23
15.197.36.0/22
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -ServiceKey GLOBALACCELERATOR | where
 {$_.IpAddressFormat -eq "Ipv4"} | select IpPrefix

IpPrefix
--------
13.248.117.0/24
15.197.34.0/23
15.197.36.0/22
...
```

Obtención de todas las direcciones IPv4 de un servicio concreto en una región específica

En el siguiente ejemplo, se filtra el archivo JSON para las direcciones IPv4 del servicio especificado en la región especificada.

jq

```
$ jq -r '.prefixes[] | select(.region=="us-east-1") |
 select(.service=="GLOBALACCELERATOR") | .ip_prefix' < ip-ranges.json

13.248.124.0/24
99.82.166.0/24
99.82.171.0/24
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -Region us-east-1 -ServiceKey GLOBALACCELERATOR
 | where {$_.IpAddressFormat -eq "Ipv4"} | select IpPrefix

IpPrefix
--------
13.248.117.0/24
```

```
99.82.166.0/24
99.82.171.0/24
...
```

Obtención de todas las direcciones IPv6

En el siguiente ejemplo, se filtra el archivo JSON para las direcciones IPv6.

jq

```
$ jq -r '.ipv6_prefixes | .[].ipv6_prefix' < ip-ranges.json

2a05:d07c:2000::/40
2a05:d000:8000::/40
2406:dafe:2000::/40
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.IpAddressFormat -eq "Ipv6"} | select
 IpPrefix

IpPrefix
--------
2a05:d07c:2000::/40
2a05:d000:8000::/40
2406:dafe:2000::/40
...
```

Obtención de todas las direcciones IPv6 de un servicio específico

En el siguiente ejemplo, se filtra el archivo JSON para las direcciones IPv6 del servicio especificado.

jq

```
$ jq -r '.ipv6_prefixes[] | select(.service=="GLOBALACCELERATOR") | .ipv6_prefix' <
 ip-ranges.json

2600:1f01:4874::/47
2600:1f01:4802::/47
2600:1f01:4860::/47
```

```
2600:9000:a800::/40
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -ServiceKey GLOBALACCELERATOR | where
 {$_.IpAddressFormat -eq "Ipv6"} | select IpPrefix

IpPrefix
--------
2600:1f01:4874::/47
2600:1f01:4802::/47
2600:1f01:4860::/47
2600:9000:a800::/40
...
```

Obtenga todas las direcciones IP de un grupo fronterizo específico

En el siguiente ejemplo, se filtra el archivo JSON de todas las direcciones IP del grupo fronterizo especificado.

jq

```
$ jq -r '.prefixes[] | select(.network_border_group=="us-west-2-lax-1")
 | .ip_prefix' < ip-ranges.json
70.224.192.0/18
52.95.230.0/24
15.253.0.0/16
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.NetworkBorderGroup -eq "us-west-2-
lax-1"} | select IpPrefix

IpPrefix
--------
70.224.192.0/18
52.95.230.0/24
15.253.0.0/16
...
```

Sintaxis del JSON de rango de direcciones IP de AWS

AWS publica sus rangos de direcciones IP actuales en formato JSON. Para obtener el archivo JSON, consulte the section called “Descargar”. La sintaxis del archivo JSON es la siguiente.

```
{
  "syncToken": "0123456789",
  "createDate": "yyyy-mm-dd-hh-mm-ss",
  "prefixes": [
    {
      "ip_prefix": "cidr",
      "region": "region",
      "network_border_group": "network_border_group",
      "service": "subset"
    }
  ],
  "ipv6_prefixes": [
    {
      "ipv6_prefix": "cidr",
      "region": "region",
      "network_border_group": "network_border_group",
      "service": "subset"
    }
  ]
}
```

syncToken

La fecha y hora de publicación en formato de tiempo Unix.

Tipo: cadena

Ejemplo: `"syncToken": "1416435608"`

createDate

La fecha y la hora de publicación, en formato UTC AA-MM-DD-hh-mm-ss.

Tipo: cadena

Ejemplo: `"createDate": "2014-11-19-23-29-02"`

prefixes

Prefijos IP para los rangos de direcciones IPv4.

Tipo: Array

ipv6_prefixes

Prefijos IP para los rangos de direcciones IPv6.

Tipo: matriz

ip_prefix

Rango de direcciones IPv4 públicas en notación CIDR. Tenga en cuenta que AWS puede anunciar un prefijo en rangos más específicos. Por ejemplo, el 96.127.0.0/17 del archivo se puede anunciar como 96.127.0.0/21, 96.127.8.0/21, 96.127.32.0/19 y 96.127.64.0/18.

Tipo: cadena

Ejemplo: `"ip_prefix": "198.51.100.2/24"`

ipv6_prefix

Rango de direcciones IPv6 públicas en notación CIDR. Tenga en cuenta que AWS puede anunciar un prefijo en rangos más específicos.

Tipo: cadena

Ejemplo: `"ipv6_prefix": "2001:db8:1234::/64"`

network_border_group

El nombre del grupo de bordes de red, el cual es un conjunto único de zonas de disponibilidad o zonas locales desde las que AWS anuncia las direcciones IP, o `GL0BAL`. El tráfico para los servicios de `GL0BAL` puede atraerse a varias zonas de disponibilidad o zonas locales desde las que AWS anuncia las direcciones IP (o incluso a todas ellas) o también puede originarse desde allí.

Tipo: cadena

Ejemplo: `"network_border_group": "us-west-2-lax-1"`

region

La región de AWS o `GL0BAL`. El tráfico para los servicios de `GL0BAL` puede atraerse a varias regiones de AWS (o incluso a todas ellas) o puede originarse desde allí.

Tipo: cadena

Valores válidos: af-south-1 | ap-east-1 | ap-east-2 | ap-northeast-1 | ap-northeast-2 | ap-northeast-3 | ap-south-1 | ap-south-2 | ap-southeast-1 | ap-southeast-2 | ap-southeast-3 | ap-southeast-4 | ap-southeast-5 | ap-southeast-6 | ap-southeast-7 | ca-central-1 | ca-west-1 | cn-north-1 | cn-northwest-1 | eu-central-1 | eu-central-2 | eu-north-1 | eu-south-1 | eu-south-2 | eu-west-1 | eu-west-2 | eu-west-3 | il-central-1 | mx-central-1 | me-central-1 | me-south-1 | sa-east-1 | us-east-1 | us-east-2 | us-gov-east-1 | us-gov-west-1 | us-west-1 | us-west-2 | GLOBAL

Ejemplo: `"region": "us-east-1"`

servicio

Subconjunto de rangos de direcciones IP. Las direcciones que aparecen enumeradas para API_GATEWAY son solo de salida. Especifique AMAZON para obtener todos los rangos de direcciones IP (lo que significa que cada subconjunto también está en el subconjunto AMAZON). Sin embargo, algunos rangos de direcciones IP solo están en el subconjunto AMAZON (lo que significa que no están disponibles también en otro subconjunto).

Tipo: cadena

Valores válidos: AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | AURORA_DSQL | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CLOUDFRONT_ORIGIN_FACING | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | IVS_LOW_LATENCY | IVS_REALTIME | KINESIS_VIDEO_STREAMS | MEDIA_PACKAGE_V2 | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | WORKSPACES_GATEWAYS

Ejemplo: `"service": "AMAZON"`

Superposiciones de rango

Los rangos de direcciones IP devueltos por cualquier código de servicio también los devuelve el código de servicio AMAZON. Por ejemplo, todos los rangos de direcciones IP devueltos por cualquier código de servicio S3 también los devuelve el código de servicio AMAZON.

Cuando el servicio A usa recursos del servicio B, hay rangos de direcciones IP que devuelven los códigos de servicio tanto para el servicio A como para el servicio B. Sin embargo, estos rangos de direcciones IP los usa exclusivamente el servicio A y no los puede usar el servicio B. Por ejemplo, Amazon S3 usa recursos de Amazon EC2, por lo que hay rangos de direcciones IP que

devuelven los códigos de servicio S3 y EC2. Sin embargo, estos rangos de direcciones IP los utiliza exclusivamente Amazon S3. Por lo tanto, el código de servicio S3 devuelve todos los rangos de direcciones IP que Amazon S3 utiliza exclusivamente. Para identificar los rangos de direcciones IP que Amazon EC2 utiliza exclusivamente, busque los rangos de direcciones IP que devuelve el código de servicio EC2, pero no el código de servicio S3.

Más información

En esta sección, encontrará enlaces a información adicional sobre los distintos códigos de los servicios.

- AMAZON_APPFLOW – rangos de direcciones IP
- AMAZON_CONNECT – configuración de la red
- CHIME_MEETINGS – Configuración de los medios y la señalización
- CLOUDFRONT – ubicaciones y rangos de direcciones IP de servidores de periferia de CloudFront
- DYNAMODB – rangos de direcciones IP
- EC2 – direcciones IPv4 públicas
- EC2_INSTANCE_CONNECT – Requisitos previos de EC2 Instance Connect
- GLOBALACCELERATOR – ubicación y rangos de direcciones IP de servidores de periferia de Global Accelerator
- ROUTE53 – rangos de direcciones IP de servidores de Amazon Route 53
- ROUTE53_HEALTHCHECKS – rangos de direcciones IP de servidores de Amazon Route 53
- ROUTE53_HEALTHCHECKS_PUBLISHING – rangos de direcciones IP de servidores de Amazon Route 53
- WORKSPACES_GATEWAYS – servidores de puerta de enlace PCoIP

Notas de la versión

En la siguiente tabla se describen las actualizaciones de la sintaxis de `ip-ranges.json`. También añadimos nuevos códigos de región con cada lanzamiento de región.

Descripción	Fecha de lanzamiento de la nueva versión
Se ha añadido el código de servicio IVS_LOW_LATENCY .	29 de julio de 2025

Descripción	Fecha de lanzamiento de la nueva versión
Se ha añadido el código de servicio `AURORA_DSQL` .	21 de mayo de 2025
Se ha añadido el código de servicio `IVS_REALTIME` .	11 de junio de 2024
Se ha añadido el código de servicio `MEDIA_PACKAGE_V2` .	9 de mayo de 2023
Se ha añadido el código de servicio `CLOUDFRONT_ORIGIN_FACING` .	12 de octubre de 2021
Se ha añadido el código de servicio `ROUTE53_RESOLVER` .	24 de junio de 2021
Se ha añadido el código de servicio `EBS`.	12 de mayo de 2021
Se ha añadido el código de servicio `KINESIS_VIDEO_STREAMS` .	19 de noviembre de 2020
Se han añadido los códigos de servicio `CHIME_MEETINGS` y `CHIME_VOICECONNECTOR` .	19 de junio de 2020
Se ha añadido el código de servicio `AMAZON_APPFLOW` .	9 de junio de 2020
Añadida compatibilidad con el grupo de bordes de red.	7 de abril de 2020
Se ha añadido el código de servicio `WORKSPACES_GATEWAYS` .	30 de marzo de 2020
Se ha añadido el código de servicio `ROUTE53_HEALTHCHECK_PUBLISHING` .	30 de enero de 2020
Se ha añadido el código de servicio `API_GATEWAY` .	26 de septiembre de 2019

Descripción	Fecha de lanzamiento de la nueva versión
Se ha añadido el código de servicio `EC2_INSTANCE_CONNECT` .	26 de junio de 2019
Se ha añadido el código de servicio `DYNAMODB`.	25 de abril de 2019
Se ha añadido el código de servicio `GLOBALACCELERATOR` .	20 de diciembre de 2018
Se ha añadido el código de servicio `AMAZON_CONNECT` .	20 de junio de 2018
Se ha añadido el código de servicio `CLOUD9`.	20 de junio de 2018
Se ha añadido el código de servicio `CODEBUILD` .	19 de abril de 2018
Se ha añadido el código de servicio `S3`.	28 de febrero de 2017
Se ha añadido compatibilidad con intervalos de direcciones IPv6.	22 de agosto de 2016
Versión inicial	19 de noviembre de 2014

Notificaciones de rangos de direcciones IP de AWS

AWS publica sus rangos de direcciones IP actuales en formato JSON. Siempre que se produce un cambio en los rangos de direcciones IP de AWS, enviamos una notificaciones a los suscriptores del tema de Amazon SNS denominado `AmazonIpSpaceChanged`. Para obtener más información acerca de la sintaxis del archivo JSON, consulte the section called “Sintaxis”.

La carga útil de la notificación contiene información en el formato siguiente.

```
{
  "create-time":"yyyy-mm-ddThh:mm:ss+00:00",
  "synctoken":"0123456789",
  "md5":"6a45316e8bc9463c9e926d5d37836d33",
  "url":"https://ip-ranges.amazonaws.com/ip-ranges.json"
```

```
}
```

create-time

La fecha y hora de creación.

Las notificaciones se pueden entregar de forma desordenada. Por lo tanto, se recomienda comprobar el las marcas de tiempo para saber cuál es el orden correcto.

synctoken

La fecha y hora de publicación en formato de tiempo Unix.

md5

Valor hash criptográfico del archivo `ip-ranges.json` archivo. Puede utilizar este valor para comprobar si el archivo descargado está dañado.

url

Ubicación del archivo `ip-ranges.json`. Para obtener más información, consulte the section called “Descargar”.

Puede suscribirse para recibir notificaciones de la siguiente manera.

Para suscribirse a las notificaciones de los rangos de direcciones IP de AWS

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En la barra de navegación, cambie la región a Este de EE. UU. (Norte de Virginia), si es necesario. Debe seleccionar esta región porque las notificaciones de SNS a las que se va a suscribir se han creado en esa región.
3. En el panel de navegación, seleccione Subscriptions.
4. Seleccione Create subscription.
5. En el cuadro de diálogo Crear suscripción, haga lo siguiente:
   a. En Topic ARN, copie el siguiente Nombre de recurso de Amazon (ARN):

      ```
      arn:aws:sns:us-east-1:806199016981:AmazonIpSpaceChanged
      ```

   b. En Protocol, elija el protocolo que desea utilizar (por ejemplo, `Email`).

c. En Endpoint, escriba el punto de enlace donde desea recibir la notificación (por ejemplo, su dirección de correo electrónico).

d. Elige Crear una suscripción.

6. Nos pondremos en contacto con usted en el punto de enlace especificado y le pediremos que confirme su suscripción. Por ejemplo, si ha especificado una dirección de correo electrónico, recibirá un mensaje de correo electrónico con la línea de asunto `AWS Notification - Subscription Confirmation`. Siga las instrucciones para confirmar la suscripción.

Las notificaciones están sujetas a la disponibilidad del punto de enlace. Por lo tanto, es conveniente revisar el archivo JSON periódicamente para asegurarse de disponer de los últimos rangos. Para obtener más información acerca de la fiabilidad de Amazon SNS, consulte https://aws.amazon.com/sns/faqs/#Reliability.

Si ya no desea recibir estas notificaciones, utilice el siguiente procedimiento para cancelar la suscripción.

Para cancelar la suscripción a las notificaciones de los rangos de direcciones IP de AWS

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. En el panel de navegación, seleccione Subscriptions.
3. Seleccione la casilla de verificación de la suscripción.
4. Elija Actions, Delete subscriptions.
5. Cuando se le pida confirmación, seleccione Eliminar.

Para obtener más información sobre Amazon SNS, consulte la Guía para desarrolladores de Amazon Simple Notification Service.

Compatibilidad con IPv6 para su VPC

Si tiene una VPC existente que solo admite IPv4 y los recursos de su subred están configurados para utilizar solamente IPv4, puede agregar 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.

Consideraciones

- No hay ninguna ruta de migración desde subredes solo de IPv4 a subredes solo de IPv6.
- En este ejemplo, se presupone que hay una VPC existente con subredes públicas y privadas. Para obtener más información sobre cómo crear una VPC nueva para utilizarla con IPv6, consulte the section called “Creación de una VPC”.
- Antes de comenzar a utilizar IPv6, asegúrese de leer las características de las direcciones IPv6 para Amazon VPC: Comparar IPv4 e IPv6.

Contenido

- Adición de la compatibilidad de IPv6 con su VPC
- Ejemplo de configuración de VPC de doble pila

Adición de la compatibilidad de IPv6 con su VPC

La siguiente tabla brinda información general del proceso para habilitar IPv6 para la VPC.

Contenido

- Paso 1: Asociar un bloque de CIDR IPv6 a su VPC y subredes
- Paso 2: Actualizar las tablas de enrutamiento
- Paso 3: Actualizar las reglas del grupo de seguridad
- Paso 4: Asignación de direcciones IPv6 a las instancias

Paso	Notas
Paso 1: Asociar un bloque de CIDR IPv6 a su VPC y subredes	Asocie un bloque de CIDR IPv6 proporcio nado por Amazon o BYOIP a la VPC y a las subredes.
Paso 2: Actualizar las tablas de enrutamiento	Actualice sus tablas de ruteo para direccionar el tráfico IPv6. Para una subred pública, cree una ruta que direccione todo el tráfico IPv6 desde la subred al puerto de enlace a Internet. Para una subred privada, cree una ruta que

Paso	Notas
	direccione 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	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: Asignación de direcciones IPv6 a las instancias	Asigne direcciones IPv6 a sus instancias desde el rango de direcciones IPv6 de su subred.

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 (Sus VPC).
3. Seleccione la VPC.
4. Elija Acciones, Editar CIDR y luego, elija Agregar CIDR de IPv6 nuevo.
5. Seleccione una de las siguientes opciones y luego, elija Seleccionar CIDR:
   - Bloque de CIDR de IPv6 proporcionado por Amazon: utilice un bloque de CIDR de IPv6 del grupo de direcciones IPv6 de Amazon. En Grupo de bordes de red, elija el grupo desde el que AWS anuncia las direcciones IP.
   - Bloque de CIDR de IPv6 asignado por IPAM: utilice un bloque de CIDR de IPv6 de un grupo de IPAM. Elija el grupo de IPAM y el bloque de CIDR de IPv6.
   - CIDR de IPv6 de mi propiedad: utilice un bloque de CIDR de IPv6 de su grupo de direcciones IPv6 (BYOIP). Elija el grupo de direcciones IPv6 y el bloque de CIDR de IPv6.
6. Seleccione Cerrar.

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 (Subredes).
3. Seleccione una subred.
4. Elija Acciones, Editar CIDR de IPv6 y luego, elija Agregar CIDR de IPv6.
5. Edite el bloque de CIDR según sea necesario (por ejemplo, reemplace el `00`).
6. Seleccione Save.
7. Repita este procedimiento para cualquier otra subred de su VPC.

Para obtener más información, consulte Bloques de CIDR de VPC IPv6.

Paso 2: Actualizar las tablas de enrutamiento

Cuando asocia un bloque de CIDR de IPv6 a su VPC, se agrega automáticamente una ruta local a cada tabla de enrutamiento para permitir el tráfico IPv6 dentro de la VPC.

Debe actualizar las tablas de enrutamiento de las subredes públicas para permitir que las instancias (como los servidores web) utilicen la puerta de enlace de Internet para el tráfico IPv6. Además, debe actualizar las tablas de enrutamiento de las subredes privadas para permitir que las instancias (como las instancias de base de datos) utilicen una puerta de enlace de Internet de solo salida para el tráfico IPv6, ya que las puertas de enlace NAT no admiten IPv6.

Para actualizar la tabla de enrutamiento de una subred pública

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Subnets (Subredes). Seleccione la subred pública. En la pestaña Tabla de enrutamiento, elija el ID de la tabla de enrutamiento para abrir la página de detalles de la tabla de enrutamiento.
3. Seleccione la tabla de enrutamiento. En la pestaña Rutas, elija Editar rutas.
4. Seleccione Añadir ruta. En Destino, elija `::/0`. En Objetivo, elija el ID de la puerta de enlace de Internet.
5. Seleccione Save changes (Guardar cambios).

Para actualizar la tabla de enrutamiento de una subred privada

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puertas de enlace de Internet de solo salida. Elija Crear puerta de enlace de Internet de solo salida. Elija su VPC en VPC y luego, elija Crear puerta de enlace 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.
3. En el panel de navegación, elija Subnets (Subredes). Seleccione la subred privada. En la pestaña Tabla de enrutamiento, elija el ID de la tabla de enrutamiento para abrir la página de detalles de la tabla de enrutamiento.
4. Seleccione la tabla de enrutamiento. En la pestaña Rutas, elija Editar rutas.
5. Seleccione Añadir ruta. En Destino, elija `::/0`. En Objetivo, elija el ID de la puerta de enlace de Internet de solo salida.
6. Seleccione Save changes (Guardar cambios).

> **Note**
>
> Una tabla de enrutamiento no puede tener el mismo destino (::/0) apuntando simultáneamente a una puerta de enlace de Internet y a una puerta de enlace de Internet de solo salida. Si recibe un mensaje de error que dice «Existen rutas IPv6 con el siguiente salto como puerta de enlace de Internet» al configurar una puerta de enlace de Internet de solo salida, primero debe eliminar la ruta IPv6 existente a la puerta de enlace de Internet antes de agregar la ruta a la puerta de enlace de Internet de solo salida.

Para obtener más información, consulte Opciones de enrutamiento de ejemplo.

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 realizar ningún cambio en las reglas de entrada del grupo de seguridad de la base de

datos; la regla que permite toda la comunicación de `sg-11aa22bb11aa22bb1` incluye comunicación mediante IPv6.

Para actualizar las reglas de entrada del grupo de seguridad

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Grupos de seguridad y seleccione el grupo de seguridad de su servidor web.
3. En la pestaña Reglas de entrada, elija Editar reglas de entrada.
4. Para cada regla que permita tráfico IPv4, elija Agregar regla y configure la regla para permitir el tráfico IPv6 correspondiente. Por ejemplo, para agregar una regla que permita todo el tráfico HTTP a través de IPv6, elija HTTP en Tipo y elija `::/0` en Origen.
5. Cuando haya terminado de agregar reglas, elija Guardar reglas.

Actualización de las reglas de salida del grupo de seguridad

Cuando asocia un bloque de CIDR de IPv6 a su VPC, se agrega de manera automática una regla de salida a los grupos de seguridad de la VPC para permitir 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.

Actualizar las reglas de ACL de red

Cuando asocia un bloque de CIDR de IPv6 a una VPC, se agregan de manera automática reglas a la ACL de red predeterminada para permitir el tráfico IPv6. Sin embargo, si modificó la ACL de red predeterminada o si creó una ACL de red personalizada, deberá agregar de manera manual las reglas para el tráfico IPv6. Para obtener más información, consulte Agregar y eliminar reglas.

Paso 4: Asignación de direcciones IPv6 a las instancias

Todos los tipos de instancia de la generación actual admiten IPv6. Si el tipo de instancia no es compatible con IPv6, deberá cambiar el tamaño de la instancia a un tipo de instancia compatible antes de asignar una dirección IPv6. El proceso que utilice dependerá de si el tipo de instancia nuevo que elija es compatible con el tipo de instancia actual. Para obtener más información, consulte Cambiar el tipo de instancia en la Guía del usuario de Amazon EC2. Si debe lanzar una instancia desde una AMI nueva para admitir IPv6, puede asignar una dirección IPv6 a su instancia durante el lanzamiento.

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 (por ejemplo, eth0) para la instancia. Para obtener más información, consulte Asignación de una dirección IPv6 a una instancia en la Guía del usuario de Amazon EC2.

Puede conectarse a una instancia utilizando su dirección IPv6. Para obtener más información, consulte Conexión a la instancia de Linux mediante un cliente SSH en la Guía del usuario de Amazon EC2.

Si lanzó la instancia mediante una AMI para una versión actual del sistema operativo, la instancia está configurada para IPv6. Si no puede hacer ping a una dirección IPv6 desde su instancia, consulte la documentación del sistema operativo para configurar IPv6.

Ejemplo de configuración de VPC de doble pila

Con una configuración de doble pila, puede usar tanto direcciones IPv4 e IPv6 para la comunicación entre los recursos de su VPC y los recursos a través de Internet.

El diagrama siguiente representa la arquitectura de su VPC. Su VPC tiene una subred pública y una subred privada. La VPC y las subredes tienen tanto un bloque de CIDR IPv4 como un bloque de CIDR IPv6. Hay una instancia de EC2 en la subred privada que tiene tanto una dirección IPv4 como una dirección IPv6. La instancia puede enviar tráfico IPv4 saliente a Internet mediante una puerta de enlace NAT y tráfico IPv6 saliente a Internet mediante una puerta de enlace de Internet solo de salida.

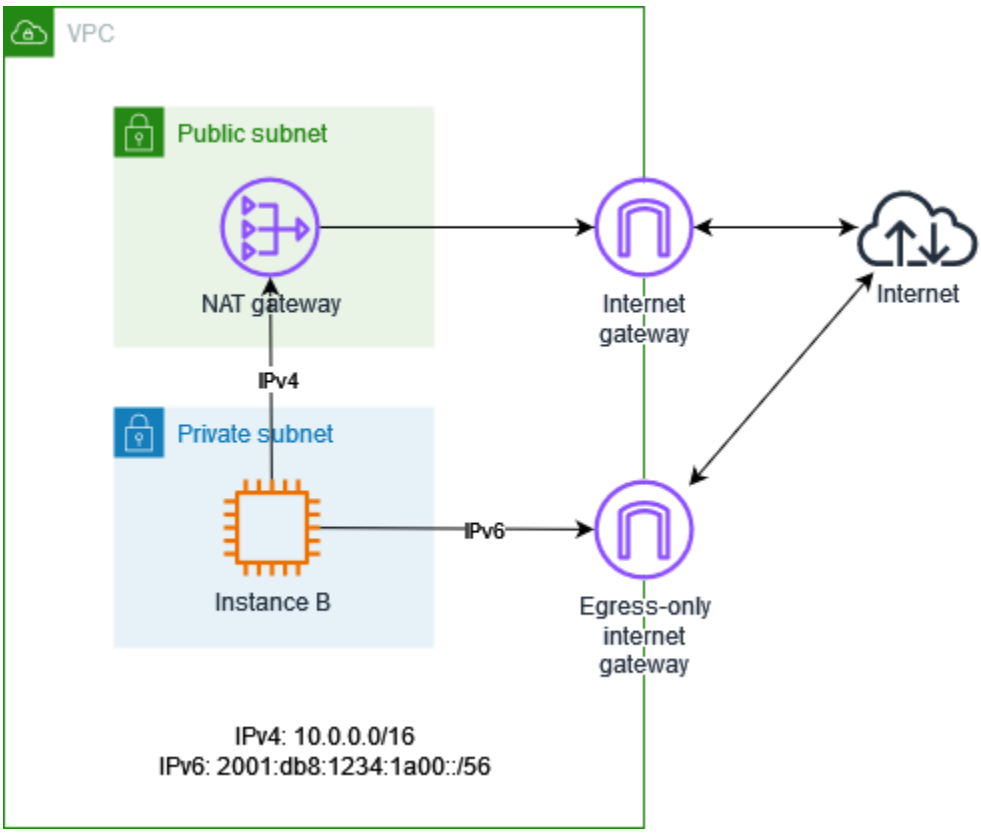


Tabla de enrutamiento para la subred pública

A continuación, se muestra la tabla de enrutamiento para la subred pública. Las dos primeras entradas son las rutas locales. La tercera entrada envía el resto del tráfico de IPv4 a la puerta de enlace de Internet. Tenga en cuenta que la cuarta entrada solo es necesaria si planea lanzar instancias de EC2 con direcciones IPv6 en la subred pública.

Destino	Objetivo
CIDR IPv4 de VPC	local
CIDR IPv6 de VPC	local
0.0.0.0/0	*internet-puerta de enlace -id*
::/0	*internet-puerta de enlace -id*

Tabla de enrutamiento de la subred privada

A continuación, se muestra la tabla de enrutamiento para la subred privada. Las dos primeras entradas son las rutas locales. La tercera entrada envía todo el tráfico de IPv4 a una puerta de enlace NAT. La última entrada envía todo el tráfico de IPv6 a la puerta de enlace de Internet de solo salida.

Destino	Objetivo
CIDR IPv4 de VPC	local
CIDR IPv6 de VPC	local
0.0.0.0/0	*nat-gateway-id*
::/0	*egress-only-gateway-id*

Servicios de AWS compatibles con IPv6

Las computadoras y los dispositivos inteligentes utilizan direcciones IP para comunicarse entre sí a través de Internet y otras redes. A medida que Internet sigue creciendo, también crece la necesidad de direcciones IP. El formato más común para las direcciones IP es IPv4. El formato nuevo para las direcciones IP es IPv6, que brinda un espacio de direcciones más grande que IPv4.

La compatibilidad de los Servicios de AWS con IPv6 incluye la compatibilidad con configuraciones de doble pila (IPv4 e IPv6) o solo de IPv6. Por ejemplo, una nube privada virtual (VPC) es una sección de Nube de AWS aislada de manera lógica en la que se pueden lanzar recursos de AWS. Dentro de una VPC, se pueden crear subredes que sean solo de IPv4, de doble pila o solo de IPv6.

Los Servicios de AWS admiten el acceso mediante puntos de conexión públicos. Algunos Servicios de AWS también admiten el acceso mediante puntos de conexión privados con tecnología de AWS PrivateLink. Los Servicios de AWS pueden admitir IPv6 mediante los puntos de conexión privados, incluso si no admiten IPv6 mediante los puntos de conexión públicos. Los puntos de conexión que admiten IPv6 pueden responder a consultas de DNS con registros AAAA.

Servicios compatibles con IPv6

En la siguiente tabla se enumeran los Servicios de AWS que proporcionan compatibilidad con doble pila, solo con IPv6 y puntos de conexión que admiten IPv6. Esta tabla se actualizará a medida que se

lancen servicios compatibles con IPv6. Para obtener información específica sobre cómo un servicio admite IPv6, consulte la documentación del servicio.

Nombre del servicio	Compatibilidad con doble pila	Compatibilidad solo con IPv6	Puntos de conexión públicos compatibles con IPv6	Puntos de conexión privados compatibles con IPv6 [1]
AWS Amplify	Sí	No	Sí	
Amazon API Gateway	Sí	No	Sí	Sí
AWS App Mesh	Sí	Sí	Sí	No
AWS App Runner	Sí	No	Sí	Sí
AWS AppConfig	Sí	No	Sí	Sí
Application Auto Scaling	No	No	Sí	Sí
AWS Application Discovery Service	Sí	No	Sí	Sí
Controlador de recuperación de aplicaciones (ARC)	Sí	No	Sí	
Amazon WorkSpaces Applications	Sí	No	No	No
AWS AppSync[2]	Parcial	No	Parcial	Sí
Amazon Athena	Sí	No	Sí	Sí
AWS Audit Manager	No	No	Sí	Sí
Amazon Aurora	Sí	No	Sí	No
Amazon Aurora DSQL	No	No	Sí	Sí

Nombre del servicio	Compatibilidad con doble pila	Compatibilidad solo con IPv6	Puntos de conexión públicos compatibles con IPv6	Puntos de conexión privados compatibles con IPv6 [1]
AWS Auto Scaling	No	No	Sí	Sí
Intercambio de datos de AWS B2B	Sí	No	Sí	Sí
AWS Backup	Sí	No	Sí	Sí
AWS Batch	Sí	No	Sí	Sí
Amazon Bedrock	No	No	Sí	Sí
Administración de facturación y costos de AWS Exportación de datos	Sí	No	Sí	Sí
Administración de facturación y costos de AWS Calculadora de precios	Sí	No	Sí	Sí
AWS Billing Conductor	Sí	No	Sí	Sí
AWS Budgets	Sí	No	Sí	
Amazon Braket	Sí	Sí	Sí	Sí
AWS Gestor de certificados	Sí	No	Sí	No
Amazon Chime SDK	Sí	No	Sí	
Amazon Comprehend	Sí	Sí	Sí	Sí

Nombre del servicio	Compatibilidad con doble pila	Compatibilidad solo con IPv6	Puntos de conexión públicos compatibles con IPv6	Puntos de conexión privados compatibles con IPv6 [1]
AWS Clean Rooms	Sí	Sí	Sí	Sí
AWS Clean Rooms ML	Sí	Sí	Sí	Sí
AWS Cloud9	Sí	No	Sí	
API de control de nube de AWS	Sí	No	Sí	Sí
CloudFormation	No	No	Sí	Sí
Amazon CloudFront	Sí	Sí	Sí	
AWS CloudHSM	Sí	No	Sí	Sí
AWS CloudTrail	Sí	No	Sí	Sí
Amazon CloudWatch	Sí	Sí	Sí	Sí
Información de aplicaciones de Amazon CloudWatch	No	No	Sí	Sí
Amazon CloudWatch Internet Monitor	No	No	Sí	Sí
Amazon CloudWatch Logs	Sí	Sí	Sí	Sí
Amazon CloudWatch Observability Access Manager	Sí	Sí	Sí	

Nombre del servicio	Compatibilidad con doble pila	Compatibilidad solo con IPv6	Puntos de conexión públicos compatibles con IPv6	Puntos de conexión privados compatibles con IPv6 [1]
Amazon CloudWatch Synthetics	Sí	No	Sí	Sí
AWS Cloud Map	Sí	Sí	Sí	Sí
WAN en la nube de AWS	Sí	No	Sí	No
AWS CodeArtifact	Sí	No	Sí	Sí
Conexión de perfiles de clientes	Sí	No	Sí	Sí
AWS CodeBuild	No	No	Sí	Sí
AWS CodeCommit	No	No	Sí	Sí
AWS CodeDeploy	No	No	Sí	Sí
AWS Compute Optimizer	No	No	Sí	Sí
Amazon Comprehend Medical	No	No	Sí	Sí
Generador de perfiles de Amazon CodeGuru	Sí	No	Sí	Sí
Amazon Cognito	Sí	No	Sí	
AWS Config	No	No	Sí	Sí
AWS Control Tower	No	No	Sí	Sí

Nombre del servicio	Compatibilidad con doble pila	Compatibilidad solo con IPv6	Puntos de conexión públicos compatibles con IPv6	Puntos de conexión privados compatibles con IPv6 [1]
AWS Cost Explorer	Sí	No	Sí	Sí
Centro de optimización de costes de AWS	Sí	No	Sí	Sí
AWS Data Exchange	No	No	Sí	Sí
Amazon Data Firehose	No	No	Sí	Sí
Administrador de vida útil de datos de Amazon	Sí	No	Sí	Sí
AWS Database Migration Service	Sí	No	No	Sí
AWS DataSync	Sí	Sí	Sí	Sí
Amazon DataZone	No	No	Sí	Sí
AWS Deadline Cloud	Sí	No	Sí	Sí
Amazon Detective	Sí	Sí	Sí	
Direct Connect	Sí	Sí	No	Sí
Directory Service	No	No	Sí	Sí
API directas de Amazon EBS	Sí	No	Sí	Sí
Amazon EC2	Sí	Sí	Sí	No
EC2 Image Builder	Sí	Sí	Sí	Sí
Amazon ECR	Sí	No	Sí	No

Nombre del servicio	Compatibilidad con doble pila	Compatibilidad solo con IPv6	Puntos de conexión públicos compatibles con IPv6	Puntos de conexión privados compatibles con IPv6 [1]
Amazon ECS	Sí	Sí	Sí	Sí
Amazon EFS	Sí	Sí	Sí	Sí
Amazon EKS	Parcial	Parcial	Sí	Sí
Amazon EMR	No	No	Sí	Sí
AWS Elastic Beanstalk	Sí	No	Sí	Sí
AWS Elastic Disaster Recovery	No	No	Sí	Sí
Elastic Load Balancing	Parcial	Parcial	Sí	No
Amazon ElastiCache	Sí	Sí	No	Sí
AWS Elemental MediaConvert	No	No	Sí	Sí
AWS Elemental MediaConnect	Sí	Sí	Sí	Parcial
Mensajes de redes sociales para usuarios finales de AWS	Sí	No	Sí	No
AWS Entity Resolution	Sí	No	Sí	Sí
Amazon EventBridge	No	No	Sí	Sí
AWS Fargate	Sí	No	Sí	Sí
Amazon FSx	No	No	Sí	Sí

Nombre del servicio	Compatibilidad con doble pila	Compatibilidad solo con IPv6	Puntos de conexión públicos compatibles con IPv6	Puntos de conexión privados compatibles con IPv6 [1]
Amazon GameLift Streams	Sí	No	Sí	Sí
AWS Global Accelerator	Sí	No	Sí	
AWS Glue	Sí	No	No	Sí
AWS Glue DataBrew	No	No	Sí	Sí
Amazon Managed Grafana [3]	Sí	No	Sí	Sí
AWS Ground Station [4]	Sí	No	Sí	Sí
Amazon GuardDuty	No	No	Sí	Sí
AWS HealthImaging	No	No	Sí	Sí
AWS HealthLake	No	No	Sí	Sí
AWS HealthOmics	No	No	Sí	Sí
AWS Identity and Access Management (IAM)	Sí	Sí	Sí	No
AWS IAM Access Analyzer	Sí	No	Sí	Sí
AWS IAM Identity Center	Sí	No	Sí	
AWS IAM Roles Anywhere	No	No	Sí	Sí

Nombre del servicio	Compatibilidad con doble pila	Compatibilidad solo con IPv6	Puntos de conexión públicos compatibles con IPv6	Puntos de conexión privados compatibles con IPv6 [1]
Amazon Inspector	Sí	Sí	Sí	Sí
Amazon Interactive Video Service (IVS) [5]	Sí	No	Sí	Sí
AWS IoT Core	Sí	No	Sí	Sí
AWS IoT Device Defender	Sí	No	Sí	No
AWS IoT Device Management	Sí	No	Sí	No
AWS IoT FleetWise	Sí	No	Sí	Sí
AWS IoT Greengrass	Sí	No	Sí	No
AWS IoT SiteWise	Sí	No	Sí	Sí
AWS IoT TwinMaker	Sí	No	Sí	Sí
AWS IoT Wireless	Sí	No	Sí	Sí
Amazon Kendra	No	No	Sí	No
AWS Key Management Service	Sí	Parcial	Sí	Sí
Amazon Keyspaces	Sí	Sí	Sí	Sí
Amazon Keyspaces CDC streams	Sí	Sí	Sí	Sí

Nombre del servicio	Compatibilidad con doble pila	Compatibilidad solo con IPv6	Puntos de conexión públicos compatibles con IPv6	Puntos de conexión privados compatibles con IPv6 [1]
Amazon Kinesis Data Streams	Sí	No	Sí	Sí
AWS Lake Formation	No	No	No	Sí
AWS Lambda	Sí	No	Sí	Sí
AWS Launch Wizard	No	No	Sí	Sí
AWS License Manager	No	No	Sí	Sí
Amazon Lightsail	Sí	Sí	Sí	Sí
Amazon Location Service	No	No	Sí	Sí
Amazon MQ	No	No	Sí	Sí
Amazon MWAA	No	No	Sí	Sí
Amazon Macie	Sí	No	Sí	Sí
AWS Mainframe Modernization	Sí	No	Sí	Sí
Amazon Managed Grafana	No	No	Sí	Sí
Amazon Managed Service para Prometheus	Sí	No	Sí	Sí
Orquestador de AWS Migration Hub	No	No	Sí	Sí

Nombre del servicio	Compatibilidad con doble pila	Compatibilidad solo con IPv6	Puntos de conexión públicos compatibles con IPv6	Puntos de conexión privados compatibles con IPv6 [1]
AWS Network Firewall	Sí	Sí	No	Sí
AWS Network Manager	Sí	No	Sí	No
Amazon OpenSearch Service	Sí	No	Sí	
AWS Organizations	Sí	No	Sí	Sí
AWS Outposts	No	No	Sí	Sí
Amazon Personalize	Sí	No	Sí	Sí
Amazon Pinpoint	Sí	No	Sí	Sí
Amazon Polly	Sí	No	Sí	Sí
Lista de precios de AWS	No	No	Sí	No
AWS Autoridad de certificación privada	Sí	No	Sí	Sí
Conector AWS Privada CA para Active Directory	Sí	No	Sí	Sí
Conector AWS Privada CA para SCEP	Sí	No	Sí	Sí
AWS PrivateLink	Sí	Sí	Sí	
Amazon Q Business	No	No	Sí	No
Amazon RDS	Sí	No	Sí	No

Nombre del servicio	Compatibilidad con doble pila	Compatibilidad solo con IPv6	Puntos de conexión públicos compatibles con IPv6	Puntos de conexión privados compatibles con IPv6 [1]
API de datos de Amazon RDS	No	No	Sí	Sí
Información de rendimiento de Amazon RDS	No	No	Sí	Sí
Amazon Redshift	Sí	No	Sí	
Amazon Rekognition	No	No	Sí	Sí
Papelera de reciclaje	Sí	No	Sí	Sí
AWS re:Post Private	Sí	No	Sí	Sí
AWS Resource Access Manager	Sí	No	Sí	Sí
Explorador de recursos de AWS	Sí	No	Sí	No
Grupos de recursos de AWS	Sí	Sí	Sí	Sí
AWS Resource Groups Tagging API	Sí	Sí	Sí	Sí
Amazon Route 53	Sí	Sí	Sí	Sí
Amazon S3	Sí	No	Sí	No
Amazon S3 en Outposts	No	No	Sí	No
Amazon SageMaker	No	No	Sí	Sí

Nombre del servicio	Compatibilidad con doble pila	Compatibilidad solo con IPv6	Puntos de conexión públicos compatibles con IPv6	Puntos de conexión privados compatibles con IPv6 [1]
AWS Secrets Manager	Sí	No	Sí	Sí
AWS Security Hub	No	No	Sí	Sí
Amazon Security Lake	Sí	No	Sí	Sí
AWS Security Token Service	Sí	No	Sí	Sí
AWS Service Catalog	No	No	Sí	Sí
AWS Shield	Sí	Sí	No	Sí
Amazon Simple Email Service	Sí	No	Sí	Sí
Amazon Simple Notification Service	Sí	No	Sí	Sí
Amazon Simple Queue Service	Sí	No	Sí	Sí
Amazon Simple Workflow Service	Sí	No	Sí	Sí
AWS Site-to-Site VPN	Sí	No	Sí	No
AWS Snow Family	No	No	Sí	
AWS Step Functions	Sí	No	Sí	Sí
AWS Storage Gateway	Sí	Sí	Sí	Sí
AWS Systems Manager	No	No	Sí	Sí

Nombre del servicio	Compatibilidad con doble pila	Compatibilidad solo con IPv6	Puntos de conexión públicos compatibles con IPv6	Puntos de conexión privados compatibles con IPv6 [1]
Administrador de incidentes de AWS Systems Manager	No	No	Sí	Sí
AWS Systems Manager para SAP	No	No	Sí	Sí
Amazon Textract	No	No	Sí	Sí
Amazon Timestream	No	No	Sí	Sí
Amazon Transcribe	Sí	Sí	Sí	Sí
AWS Transfer Family [6]	Sí	No	Sí	Sí
AWS Transit Gateway	Sí	No	Sí	No
Amazon Translate	Sí	Sí	Sí	Sí
AWS Trusted Advisor	No	No	Sí	Sí
AWS User Notifications	No	No	Sí	Sí
Amazon Verified Permissions	Sí	No	Sí	Sí
VMware Cloud enAWS	No	No	Sí	Sí
Amazon VPC	Sí	Sí	Sí	No
Amazon VPC Lattice	No	No	Sí	Sí
AWS WAF	Sí	Sí	No	
AWS WAFV2	No	No	Sí	Sí

Nombre del servicio	Compatibilidad con doble pila	Compatibilidad solo con IPv6	Puntos de conexión públicos compatibles con IPv6	Puntos de conexión privados compatibles con IPv6 [1]
AWS Well-Architected Tool	No	No	Sí	Sí
Amazon WorkMail	No	No	Sí	Sí
Amazon WorkSpaces	Sí	No	Sí	Sí
AWS X-Ray	Sí	No	Sí	Sí

[1] Una celda vacía indica que el servicio no se integra con AWS PrivateLink.

[2] Esta entrada representa la compatibilidad con IPv6 para las operaciones de configuración de AWS AppSync GraphLQL y Event API, a través de la API del AWS AppSync SDK. IPv6 no es compatible con las conexiones de los clientes a las API AWS AppSync GraphQL y Event administradas por el cliente.

[3] Esta entrada representa la compatibilidad con IPv6 para las operaciones de administración del espacio de trabajo de Grafana, como, por ejemplo, actualizar los espacios de trabajo y sus permisos. No se ofrece compatibilidad con IPv6 para las operaciones generales del espacio de trabajo de Grafana, como, por ejemplo, crear y editar paneles o consultar orígenes de datos.

[4] Esta entrada representa la compatibilidad con IPv6 para las operaciones del plano de control de AWS Ground Station, como la llamada a la API AWS Ground Station. El plano de AWS Ground Station datos no admite IPv6, así que asegúrese de que los recursos a los que va a entregar los datos (como las instancias de Amazon EC2) estén accesibles a través de IPv4.

[5] Esta entrada representa la compatibilidad con IPv6 para las operaciones del plano de control de Amazon IVS, como la llamada a un punto de conexión de IVS.

[6] Para obtener más información sobre la compatibilidad con IPv6 en AWS Transfer Family, consulte las limitaciones de IPv6.

Compatibilidad adicional con IPv6

Computación

- Amazon EC2 admite el lanzamiento de instancias basadas en Nitro System en subredes solo de IPv6.
- Amazon EC2 proporciona puntos de conexión IPv6 para el servicio de metadatos de instancias (IMDS) y el Servicio de sincronización temporal de Amazon.

Desarrollo de juegos

- Amazon GameLift Streams admite la transmisión a través de IPv6 en el tiempo de ejecución de Microsoft Windows Server 2022 Base.

Redes y entrega de contenido

- Amazon VPC admite la creación de subredes solo de IPv6.
- Amazon VPC ayuda a los recursos IPv6 de AWS a comunicarse con los recursos IPv4, ya que admite DNS64 en las subredes y NAT64 en las puertas de enlace de NAT.

Seguridad, identidad y conformidad

- Amazon Detective admite direcciones IPv6 en los resultados relacionados con la red y en los perfiles de entidades.
- AWS Identity and Access Management (IAM) es compatible con las direcciones IPv6 en las políticas de identidad de IAM.
- Amazon Macie admite direcciones IPv6 en la información de identificación personal (PII).
- Amazon Security Lake admite direcciones IPv6 en todas las operaciones en las fuentes de registro y los suscriptores.

Administración y gobierno

- Los registros de AWS CloudTrail incluyen información de IPv6 de origen.
- La AWS CLI v2 admite la descarga mediante conexiones IPv6 para clientes que solo utilizan IPv6.

Más información

- IPv6 en AWS
- Dual Stack and IPv6-only Amazon VPC Reference Architectures (PDF)

Configuración de una nube virtual privada

Amazon Virtual Private Cloud (VPC) es un componente fundamental que permite un aprovisionamiento de redes virtuales aisladas lógicamente dentro de la nube de AWS. Al crear su propia VPC, obtiene el control total del entorno de red, incluida la capacidad de definir los rangos de las direcciones IP, las subredes, las tablas de enrutamiento y las opciones de conectividad.

Su cuenta de AWS cuenta con una VPC predeterminada en cada región de AWS. Esta VPC predeterminada tienen ajustes configurados previamente que la convierten en una opción práctica para iniciar recursos de manera rápida. Sin embargo, es posible que, a largo plazo, la VPC predeterminada no siempre se ajuste a sus necesidades de red. Aquí es donde la creación de VPC adicionales puede resultar ventajosa.

La creación de VPC adicionales ofrece varias ventajas en comparación con la VPC predeterminada aprovisionada con cada cuenta nueva de AWS. Con una VPC autoadministrada, puede diseñar la topología de la red para que se ajuste con precisión a sus necesidades específicas, como la implementación de una aplicación de varios niveles, la conexión a los recursos en las instalaciones o la división de las cargas de trabajo por departamento o unidad de negocio.

Además, la creación de varias VPC ofrece una mayor seguridad y aislamiento entre las distintas aplicaciones o unidades de negocio. Cada VPC actúa como una red virtual independiente, lo que le permite aplicar distintas políticas de seguridad, controles de acceso y configuraciones de enrutamiento adaptadas a cada entorno.

En última instancia, el uso de la VPC predeterminada o la creación de una (o más) VPC personalizadas debe basarse en los requisitos específicos de la aplicación, las necesidades de seguridad y los objetivos de escalabilidad a largo plazo. Invertir tiempo en el diseño cuidadoso de la infraestructura de su VPC puede dar sus frutos en forma de una base de red en la nube robusta, segura y adaptable.

Contenido

- Conceptos básicos sobre VPC
- Opciones de configuración de la VPC
- VPC predeterminadas
- Creación de una VPC
- Visualización de los recursos de su VPC

- Adición o eliminación de un bloque de CIDR de su VPC
- Conjuntos de opciones de DHCP en Amazon VPC
- Atributos DNS para la VPC
- Uso de direcciones de red para su VPC
- Intercambio de sus subredes de VPC con otras cuentas
- Ampliar una VPC a una zona local, una zona Wavelength o Outpost
- Eliminar su VPC
- Se puede generar infraestructura como código a partir de las acciones de su consola de VPC con Console-to-Code

Conceptos básicos sobre VPC

Una VPC abarca todas las zonas de disponibilidad de una región. Después de crear la VPC, podrá añadir una o varias subredes en cada zona de disponibilidad. Para obtener más información, consulte Subredes.

Contenido

- Rango de direcciones IP de una VPC
- Diagrama de una VPC
- Recursos de la VPC

Rango de direcciones IP de una VPC

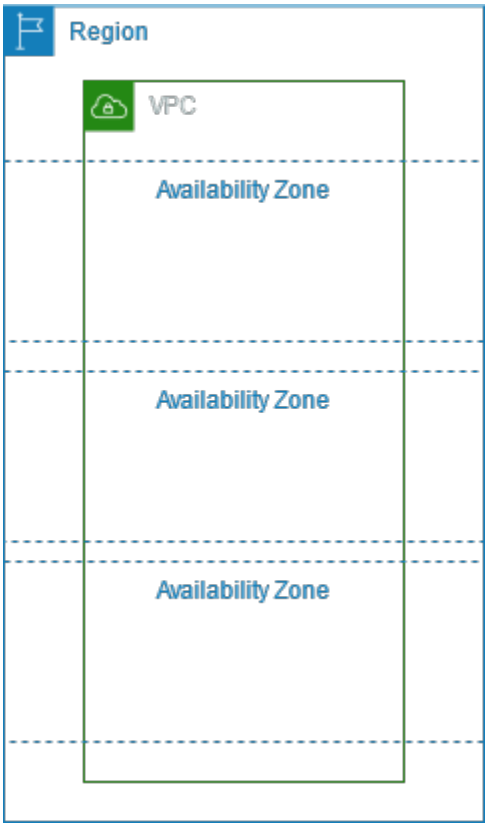
Cuando se crea una VPC, se especifican las direcciones IP de la siguiente manera:

- Solo IPv4: la VPC tiene un bloque de CIDR IPv4 pero no tiene un bloque de CIDR IPv6.
- Doble pila: la VPC tiene un bloque de CIDR IPv4 y un bloque de CIDR IPv6.

Para obtener más información, consulte Direccionamiento IP para VPC y subredes.

Diagrama de una VPC

En el siguiente diagrama se muestra una VPC sin recursos adicionales de VPC. Para ver configuraciones de ejemplo de VPC, consulte Ejemplos.



Recursos de la VPC

Cada VPC incluye automáticamente los siguientes recursos:

- Conjunto de opciones de DHCP predeterminado
- ACL de red predeterminada
- Grupo de seguridad predeterminado
- Tabla de enrutamiento principal

Puede crear los siguientes recursos para su VPC:

- ACL de red
- Tablas de enrutamiento personalizadas
- Grupos de seguridad
- Puerta de enlace de Internet
- Puertas de enlace NAT

Opciones de configuración de la VPC

Cuando se crea una VPC, se pueden especificar las siguientes opciones de configuración.

Zonas de disponibilidad

Centros de datos discretos con alimentación, redes y conectividad redundantes en una región de AWS. Puede utilizar varias zonas de disponibilidad para operar aplicaciones de producción y bases de datos con mayor disponibilidad, tolerancia a errores y escalabilidad de lo que sería posible desde un único centro de datos. Si divide las aplicaciones que se ejecutan en subredes entre zonas de disponibilidad, logrará mejor aislamiento y protección frente a incidencias, como cortes de energía, rayos, tornados o terremotos.

Bloques CIDR

Debe especificar rangos de direcciones IP para la VPC y las subredes. Para obtener más información, consulte Direccionamiento IP para VPC y subredes.

Opciones de DNS

Si necesita nombres de host DNS IPv4 públicos para las instancias de EC2 lanzadas en las subredes, debe habilitar ambas opciones de DNS. Para obtener más información, consulte Atributos DNS para la VPC.

- Habilitar nombres de host DNS: las instancias de EC2 que se lanzan en la VPC reciben nombres de host DNS públicos que corresponden a sus direcciones IPv4 públicas.
- Habilitar resolución de DNS: el servidor de DNS de Amazon, llamado Route 53 Resolver, proporciona la resolución de DNS para los nombres de host DNS privados de la VPC.

Puerta de enlace de Internet

Conecta la VPC a Internet. Las instancias de una subred pública pueden acceder a Internet porque la tabla de enrutamiento de la subred contiene una ruta que envía el tráfico vinculado a Internet a la puerta de enlace de Internet. No es necesaria su implementación en una subred pública si no se necesita acceder al servidor directamente desde Internet. Para obtener más información, consulte Puertas de enlace de Internet.

Nombre

Los nombres que especifica para la VPC y los demás recursos de la VPC se utilizan para crear etiquetas de nombre. Si utiliza la característica de generación automática de etiquetas de nombre de la consola, los valores de las etiquetas tienen el formato *name*-*resource*.

Puertas de enlace NAT

Permite que las instancias de una subred privada envíen tráfico saliente a Internet, pero evita que los recursos de Internet se conecten a las instancias. En producción, se recomienda implementar una puerta de enlace de NAT en cada zona de disponibilidad (AZ) activa. Para obtener más información, consulte Puerta de enlace NAT.

Tablas de enrutamiento

Contienen un conjunto de reglas, denominado rutas, que determinan hacia dónde se dirige el tráfico de red de la subred o la puerta de enlace. Para obtener más información, consulte Tablas de enrutamiento.

Subredes

Un intervalo de direcciones IP en la VPC. Puede lanzar recursos de AWS, como instancias de EC2, en las subredes. Cada subred reside exclusivamente en una zona de disponibilidad. Si lanza instancias en al menos dos zonas de disponibilidad, puede proteger las aplicaciones de los errores que se produzcan en una sola zona.

Una subred pública tiene una ruta directa a una puerta de enlace de Internet. Los recursos de una subred pública pueden acceder a la Internet pública. Una subred privada no tiene una ruta directa a una puerta de enlace de Internet. Los recursos de una subred privada necesitan otro componente, como un dispositivo NAT, para acceder a la Internet pública.

Para obtener más información, consulte Subredes.

Propiedad

Esta opción define si las instancias de EC2 que lance en la VPC se ejecutarán en hardware compartido con otras Cuentas de AWS o en hardware dedicado para su uso exclusivo. Si elige que la tenencia de la VPC sea `Default`, las instancias de EC2 lanzadas en esta VPC utilizarán el atributo de tenencia especificado al lanzar la instancia. Para más información, consulte Lanzar una instancia utilizando parámetros definidos en la Guía del usuario de Amazon EC2. Si elige que la tenencia de la VPC sea `Dedicated`, las instancias siempre se ejecutarán como Instancias dedicadas en hardware dedicado para su uso. Si está utilizando AWS Outposts, su Outpost requiere conectividad privada; debe utilizar la tenencia `Default`.

VPC predeterminadas

Cuando comienza a utilizar Amazon VPC, 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 es adecuada para comenzar a trabajar 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.

Puede agregar subredes a la VPC predeterminada. Para obtener más información, consulte the section called “Crear una subred”.

Contenido

- Componentes de VPC predeterminados
- Subredes predeterminadas
- Utilización de su VPC y subredes predetermiandas

Componentes de VPC predeterminados

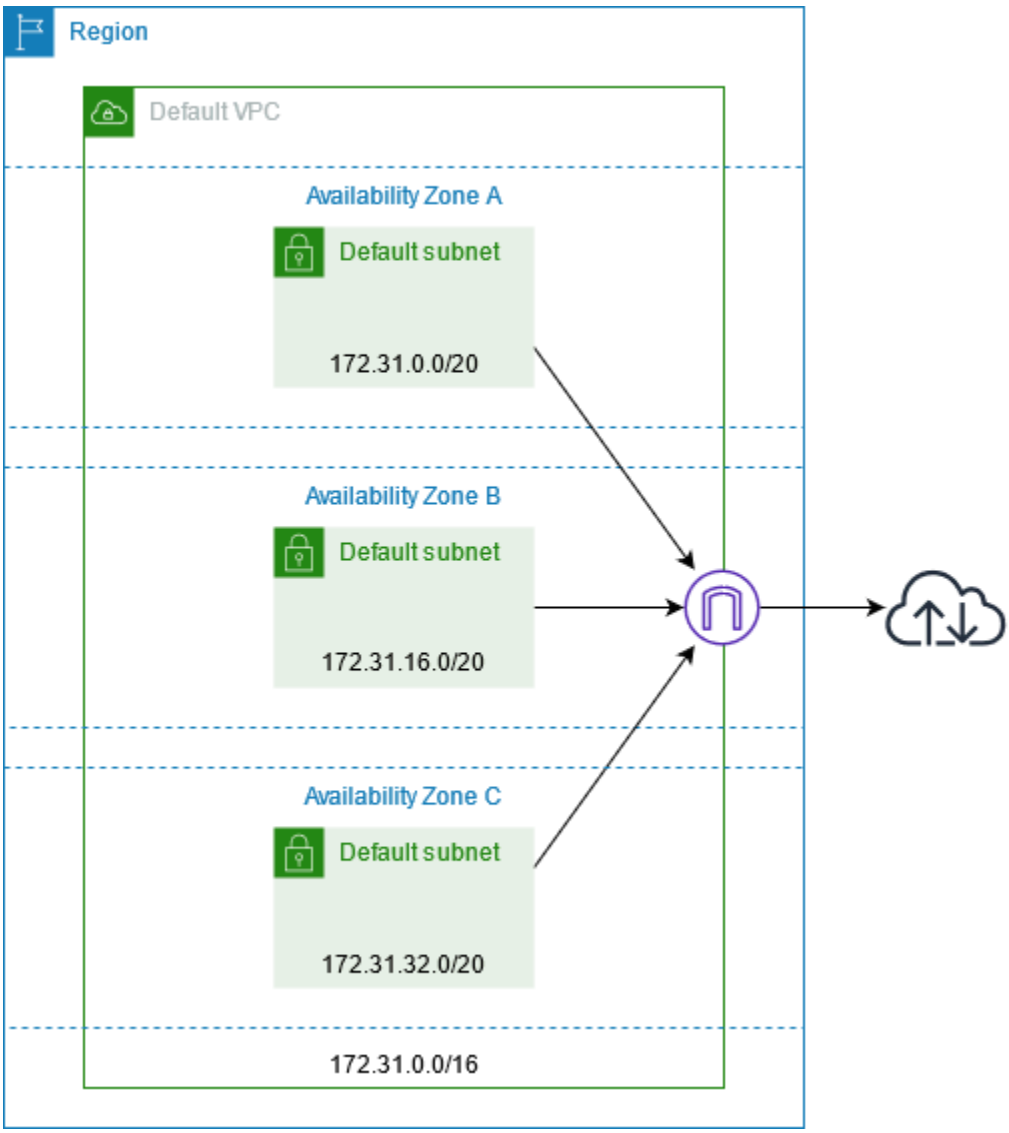
Al crear una VPC predeterminada, hacemos lo siguiente para configurarla para usted:

- 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 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. Para evitar que Amazon cree una puerta de enlace de Internet, debe denegar CreateDefaultVpc and CreateInternetGateway.
> - Para bloquear todo el tráfico que fluye a través de las puertas de enlace de Internet, consulte Bloqueo de acceso público de las VPC y subredes.

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	*internet_gateway_id*

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.

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 Modificación de los atributos de las direcciones IP de sus subredes.

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.

Utilización de su VPC y subredes predetermiandas

En esta sección, se describe cómo trabajar con su VPC y subredes predeterminadas.

Contenido

- Consultar la VPC y las subredes predeterminadas
- Crear una VPC predeterminada
- Crear una subred predeterminada
- Eliminar las subredes predeterminadas y la VPC predeterminada

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.

Al crear una VPC predeterminada, se crea con los componentes 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

> **Note**
>
> No es posible crear una subred predeterminada con la Consola de administración de AWS.

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.

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 Adición o eliminación de un bloque de CIDR de IPv6 en su subred.

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. Sin embargo, si elimina las subredes predeterminadas o la VPC predeterminada, deberá especificar de manera explícita una subred en una de las VPC

cuando lance instancias. Si no tiene otra VPC, deberá crear una VPC con una subred en al menos una zona de disponibilidad. Para obtener más información, consulte Creación de una VPC.

Si elimina la VPC predeterminada, puede crear otra. Para obtener más información, consulte Crear una VPC predeterminada.

Si elimina una subred predeterminada, puede crear otra. Para obtener más información, consulte Crear una subred predeterminada. 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 Modificación de los atributos de las direcciones IP de sus subredes. Solo puede tener una subred predeterminada por zona de disponibilidad. No es posible crear una subred predeterminada en una VPC que no sea predeterminada.

Creación de una VPC

Utilice los siguientes procedimientos para crear una nube privada virtual (VPC). Una VPC debe tener recursos adicionales, como subredes, tablas de enrutamiento y puertas de enlace, para poder crear recursos de AWS en ella.

Contenido

- Creación de una VPC y otros recursos de la VPC
- Crear una sola VPC
- Creación de una VPC mediante la AWS CLI

Para obtener información sobre cómo modificar una VPC, consulte the section called “Adición o eliminación de un bloque de CIDR”.

Creación de una VPC y otros recursos de la VPC

Utilice el siguiente procedimiento para crear una VPC y los recursos adicionales de la VPC que necesita para ejecutar la aplicación, como subredes, tablas de enrutamiento, puertas de enlace de Internet y puertas de enlace de NAT. Para ver configuraciones de ejemplo de VPC, consulte Ejemplos.

Para crear una VPC, subredes y otros recursos 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 VPC, elija Create VPC (Crear VPC).
3. En Resources to create (Recursos para crear), elija VPC and more (VPC y más).
4. Mantenga seleccionada la opción Generación automática de etiquetas de nombre para crear etiquetas de nombre para los recursos de la VPC o desactívela para proporcionar sus propias etiquetas de nombre para los recursos de la VPC.
5. En Bloque CIDR de IPv4, ingrese un rango de direcciones IPv4 para la VPC. Una VPC debe tener un rango de direcciones IPv4.
6. (Opcional) Para admitir tráfico IPv6, elija Bloque CIDR de IPv6 y Bloque CIDR de IPv6 proporcionado por Amazon.
7. Elija una opción de tenencia. Esta opción define si las instancias de EC2 que lance en la VPC se ejecutarán en hardware compartido con otras Cuentas de AWS o en hardware dedicado para su uso exclusivo. Si elige que la tenencia de la VPC sea `Default`, las instancias de EC2 lanzadas en esta VPC utilizarán el atributo de tenencia especificado al lanzar la instancia. Para obtener más información, consulte Lanzar una instancia mediante parámetros definidos en la Guía del usuario de Linux de Amazon EC2. Si elige que la tenencia de la VPC sea `Dedicated`, las instancias siempre se ejecutarán como Instancias dedicadas en hardware dedicado para su uso. Si está utilizando AWS Outposts, su Outpost requiere conectividad privada; debe utilizar la tenencia `Default`.
8. En Cantidad de zonas de disponibilidad (AZ), se recomienda aprovisionar subredes en al menos dos zonas de disponibilidad para un entorno de producción. Para elegir las AZ para las subredes, expanda Personalizar AZ. De lo contrario, deje que AWS las elija por usted.
9. Para configurar las subredes, elija valores para Cantidad de subredes públicas y Cantidad de subredes privadas. Para elegir los rangos de direcciones IP para las subredes, expanda Personalizar bloques CIDR de subredes. De lo contrario, deje que AWS las elija por usted.
10. (Opcional) Si los recursos de una subred privada necesitan acceso a la Internet pública a través de IPv4, en Puertas de enlace NAT, elija la cantidad de AZ en las que se crearán puertas de enlace NAT. En producción, se recomienda implementar una puerta de enlace de NAT en cada AZ con recursos que necesiten acceso a la Internet pública. Tenga en cuenta que existe un costo asociado a las puertas de enlace NAT. Para obtener más información, consulte Precios de las puertas de enlace NAT.
11. (Opcional) Si los recursos de una subred privada necesitan acceso a la Internet pública a través de IPv6, en la opción Puerta de enlace de Internet solo de salida, elija Sí.
12. (Opcional) Si necesita acceder a Amazon S3 directamente desde su VPC, elija Puntos de conexión de VPC, Puerta de enlace de S3. Se crea un punto de conexión de VPC de puerta

de enlace para Amazon S3. Para obtener más información, consulte Puntos de conexión de la puerta de enlace en la Guía de AWS PrivateLink.

13. (Opcional) En Opciones de DNS, ambas opciones de resolución de nombres de dominio están activadas de forma predeterminada. Si el valor predeterminado no satisface sus necesidades, puede deshabilitar estas opciones.
14. (Opcional) Para agregar una etiqueta a su VPC, expanda Etiquetas adicionales, elija Agregar etiqueta nueva e ingrese una clave y un valor de etiqueta.
15. En el panel Vista previa, puede visualizar las relaciones entre los recursos de la VPC que configuró. Las líneas continuas representan las relaciones entre los recursos. Las líneas punteadas representan el tráfico de red a las puertas de enlace de NAT, las puertas de enlace de Internet y los puntos de conexión de las puertas de enlace. Una vez que creó la VPC, puede visualizar los recursos de la VPC en este formato en cualquier momento en la pestaña Mapa de recursos. Para obtener más información, consulte Visualización de los recursos de su VPC.
16. Cuando termine de configurar la VPC, elija Crear VPC.

Crear una sola VPC

Utilice el siguiente procedimiento para crear una VPC sin recursos adicionales mediante la consola de Amazon VPC.

Para crear una VPC sin recursos adicionales de VPC mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de VPC, elija Create VPC (Crear VPC).
3. En Recursos para crear, elija Solo VPC.
4. (Opcional) En Etiqueta de nombre, ingrese un nombre para su VPC. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
5. Para IPv4 CIDR block (Bloque de CIDR de IPv4), realice una de las siguientes operaciones:
   - Elija Entrada manual de CIDR de IPv4 e ingrese un rango de direcciones IPv4 para su VPC.
   - Elija el bloque de CIDR IPv4 asignado por IPAM, seleccione su grupo de direcciones IPv4 del Administrador de direcciones IP (IPAM) de Amazon VPC y una máscara de red. El tamaño del bloque CIDR está limitado por las reglas de asignación del grupo de IPAM. IPAM es una función de VPC que le facilita la planificación, el seguimiento y la supervisión de las direcciones IP para sus cargas de trabajo de AWS. Para obtener más información, consulte la Guía del usuario de Amazon VPC IPAM.

Si utiliza IPAM para administrar las direcciones IP, le recomendamos que elija esta opción. De lo contrario, el bloque CIDR que especifique para la VPC podría superponerse con una asignación de CIDR de IPAM.

6. (Opcional) Para crear una VPC de doble pila, especifique un rango de direcciones IPv6 para la VPC. Para IPv6 CIDR block (Bloque de CIDR de IPv6), realice una de las siguientes operaciones:

   - Elija Bloque de CIDR de IPv6 asignado por el IPAM si utiliza el Administrador de direcciones IP de Amazon VPC y desea aprovisionar un CIDR de IPv6 desde un grupo de IPAM. Si utiliza el bloque CIDR IPv6 asignado por IPAM para aprovisionar CIDR IPv6 a las VPC, obtiene el beneficio de tener CIDR IPv6 contiguos para la creación de la VPC. Los CIDR asignados de forma contigua son CIDR asignados secuencialmente. Permiten simplificar las reglas de seguridad y redes; los CIDR IPv6 pueden agruparse en una sola entrada en estructuras de red y seguridad, como listas de control de acceso, tablas de enrutamiento, grupos de seguridad y firewalls.

     Tiene dos opciones para aprovisionar un rango de direcciones IP a la VPC en el Bloque de CIDR:

     - Longitud de la máscara de red: elija esta opción a fin de seleccionar una longitud de máscara de red para el CIDR. Realice una de las siguientes acciones:
       - Si se ha seleccionado una longitud de máscara de red predeterminada para el grupo de IPAM, puede elegir Longitud de máscara de red predeterminada del IPAM a fin de utilizar la longitud de máscara de red predeterminada establecida para el grupo de IPAM por el administrador de IPAM. Para obtener más información sobre la regla opcional de asignación de longitud de máscara de red predeterminada, consulte Crear un grupo IPv6 regional en la Guía del usuario de IPAM de Amazon VPC.
       - Si no se ha seleccionado una longitud de máscara de red predeterminada para el grupo de IPAM, elija una longitud de máscara de red que sea más específica que la longitud de máscara de red del CIDR del grupo de IPAM. Por ejemplo, si el CIDR del grupo de IPAM es /50, puede elegir una longitud de máscara de red entre /52 y /60 para la VPC. Las longitudes posibles de la máscara de red oscilan entre /44 y /60 en incrementos de /4.
     - Seleccionar un CIDR: elija esta opción para ingresar de forma manual una dirección IPv6. Solo puede elegir una longitud de máscara de red que sea más específica que la longitud de la máscara de red del grupo de IPAM. Por ejemplo, si el CIDR del grupo de IPAM es /50,

puede elegir una longitud de máscara de red entre /52 y /60 para la VPC. Las longitudes posibles de las máscaras de red IPv6 oscilan entre /44 y /60 en incrementos de /4.

- Elija Bloque CIDR de IPv6 proporcionado por Amazon para solicitar un bloque CIDR de 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.
- Elija CIDR de IPv6 de mi propiedad para aprovisionar un CIDR de IPv6 que ya haya traído a AWS. Para obterner más información sobre cómo traer sus propios rangos de direcciones IP a AWS, consulte Traiga sus propias direcciones IP (BYOIP) en la Guía del usuario de Amazon EC2. Puede aprovisionar un rango de direcciones IP para la VPC mediante las siguientes opciones para el bloque CIDR:
  - Sin preferencia: elija esta opción para utilizar una longitud de máscara de red de /56.
  - Seleccionar un CIDR: elija esta opción para ingresar de forma manual una dirección IPv6 y elegir una longitud de máscara de red que sea más específica que el tamaño del CIDR de BYOIP. Por ejemplo, si el CIDR del grupo de BYOIP es /50, puede elegir una longitud de máscara de red entre /52 y /60 para la VPC. Las longitudes posibles de las máscaras de red IPv6 oscilan entre /44 y /60 en incrementos de /4.

7. (Opcional) Elija una opción de tenencia. Esta opción define si las instancias de EC2 que lance en la VPC se ejecutarán en hardware compartido con otras Cuentas de AWS o en hardware dedicado para su uso exclusivo. Si elige que la tenencia de la VPC sea `Default`, las instancias de EC2 lanzadas en esta VPC utilizarán el atributo de tenencia especificado al lanzar la instancia. Para más información, consulte Lanzar una instancia utilizando parámetros definidos en la Guía del usuario de Amazon EC2. Si elige que la tenencia de la VPC sea `Dedicated`, las instancias siempre se ejecutarán como Instancias dedicadas en hardware dedicado para su uso. Si está utilizando AWS Outposts, su Outpost requiere conectividad privada; debe utilizar la tenencia `Default`.
8. (Opcional) Para agregar una etiqueta a su VPC, elija Agregar etiqueta nueva e ingrese una clave y un valor de etiqueta.
9. Seleccione Creación de VPC.
10. Una vez creada una VPC, podrá agregar las subredes. Para obtener más información, consulte Crear una subred.

Creación de una VPC mediante la AWS CLI

El siguiente procedimiento contiene comandos de la AWS CLI de ejemplo para crear una VPC, además de los recursos de VPC adicionales necesarios para ejecutar una aplicación. Si ejecuta todos los comandos en este procedimiento, creará una VPC, una subred pública, una subred privada, una tabla de enrutamiento para cada subred, una puerta de enlace de Internet, una puerta de enlace de Internet de solo salida y una puerta de enlace de NAT pública. Si no necesita todos estos recursos, puede utilizar solo los comandos de ejemplo que necesita.

Requisitos previos

Antes de comenzar, instale y configure la AWS CLI. Cuando configure la AWS CLI, se le solicitarán credenciales de AWS. En los ejemplos de este procedimiento se asume que configuró una región predeterminada. De lo contrario, agregue la opción `--region` para cada comando. Para obtener más información, consulte Installing or updating the AWS CLI and Configuring the AWS CLI (Instalación o actualización de la CLI y Configuración de la CLI).

Etiquetado

Puede agregar etiquetas a un recurso después de crearlo mediante el comando create-tags. Como alternativa, puede agregar la opción `--tag-specification` al comando de creación del recurso de la siguiente manera.

```
--tag-specifications ResourceType=vpc,Tags=[{Key=Name,Value=my-project}]
```

Para crear una VPC y otros recursos de la VPC mediante la AWS CLI

1. Utilice el siguiente comando create-vpc para crear una VPC con el bloque CIDR de IPv4 especificado.

   ```
   aws ec2 create-vpc --cidr-block 10.0.0.0/24 --query Vpc.VpcId --output text
   ```

   Como alternativa, para crear una VPC de doble pila, agregue la opción `--amazon-provided-ipv6-cidr-block` para agregar un bloque CIDR de IPv6 proporcionado por Amazon, como se muestra en el siguiente ejemplo.

   ```
   aws ec2 create-vpc --cidr-block 10.0.0.0/24 --amazon-provided-ipv6-cidr-block --
   query Vpc.VpcId --output text
   ```

Estos comandos devuelven el ID de la VPC nueva. A continuación, se muestra un ejemplo.

```
vpc-1a2b3c4d5e6f1a2b3
```

2. [VPC de doble pila] Obtenga el bloque de CIDR IPv6 asociado a su VPC mediante el siguiente comando describe-vpcs.

```
aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 Vpcs[].Ipv6CidrBlockAssociationSet[].Ipv6CidrBlock --output text
```

A continuación, se muestra un ejemplo del resultado.

```
2600:1f13:cfe:3600::/56
```

3. Cree una o más subredes, en función del caso de uso. En producción, le recomendamos que lance recursos en al menos dos zonas de disponibilidad. Utilice uno de los siguientes comandos para crear cada subred.

   - Subred de solo IPv4: para crear una subred con un bloque CIDR de IPv4 específico, utilice el siguiente comando create-subnet.

```
aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --cidr-block 10.0.1.0/20
 --availability-zone us-east-2a --query Subnet.SubnetId --output text
```

   - Subred de doble pila: si creó una VPC de doble pila, puede utilizar la opción `--ipv6-cidr-block` para crear una subred de doble pila, como se muestra en el siguiente comando.

```
aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --cidr-block 10.0.1.0/20
 --ipv6-cidr-block 2600:1f13:cfe:3600::/64 --availability-zone us-east-2a --
query Subnet.SubnetId --output text
```

   - Subred de solo IPv6: si creó una VPC de doble pila, puede utilizar la opción `--ipv6-native` para crear una subred de solo IPv6, como se muestra en el siguiente comando.

```
aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --ipv6-native --ipv6-
cidr-block 2600:1f13:cfe:3600::/64 --availability-zone us-east-2a --query
 Subnet.SubnetId --output text
```

Estos comandos devuelven el ID de la subred nueva. A continuación se muestra un ejemplo.

```
subnet-1a2b3c4d5e6f1a2b3
```

4. Si necesita una subred pública para los servidores web o para una puerta de enlace de NAT, haga lo siguiente:

   a. Cree una puerta de enlace de Internet mediante el siguiente comando create-internet-puerta de enlace. El comando devuelve el ID de la nueva puerta de enlace de Internet.

   ```
   aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --
   output text
   ```

   b. Adjunte la puerta de enlace de Internet a su VPC mediante el siguiente comando attach-internet-gateway. Utilice el ID de la puerta de enlace de Internet que obtuvo en el paso anterior.

   ```
   aws ec2 attach-internet-gateway --vpc-id vpc-1a2b3c4d5e6f1a2b3 --internet-
   gateway-id igw-id
   ```

   c. Cree una tabla de enrutamiento personalizada para la subred pública mediante el siguiente comando create-route-table. El comando devuelve el ID de la nueva tabla de enrutamiento.

   ```
   aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
    RouteTable.RouteTableId --output text
   ```

   d. Cree una ruta en la tabla de enrutamiento que envíe todo el tráfico IPv4 a la puerta de enlace de Internet mediante el siguiente comando create-route. Utilice el ID de la tabla de enrutamiento para la subred pública.

   ```
   aws ec2 create-route --route-table-id rtb-id-public --destination-cidr-block
    0.0.0.0/0 --gateway-id igw-id
   ```

   e. Asocie la tabla de enrutamiento a la subred pública mediante el siguiente comando associate-route-table. Utilice el ID de la tabla de enrutamiento para la subred pública y el ID de la subred pública.

   ```
   aws ec2 associate-route-table --route-table-id rtb-id-public --subnet-
   id subnet-id-public-subnet
   ```

5. [IPv6] Puede agregar una puerta de enlace de Internet de solo salida para que las instancias de una subred privada puedan acceder a Internet a través de IPv6 (por ejemplo, para obtener actualizaciones de software), pero los hosts de Internet no puedan acceder a las instancias.

   a. Cree una puerta de enlace de Internet de solo salida mediante el siguiente comando create-egress-only-internet-gateway. El comando devuelve el ID de la nueva puerta de enlace de Internet.

   ```
   aws ec2 create-egress-only-internet-gateway --vpc-id vpc-1a2b3c4d5e6f1a2b3 --
   query EgressOnlyInternetGateway.EgressOnlyInternetGatewayId --output text
   ```

   b. Cree una tabla de enrutamiento personalizada para la subred privada mediante el siguiente comando create-route-table. El comando devuelve el ID de la nueva tabla de enrutamiento.

   ```
   aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
    RouteTable.RouteTableId --output text
   ```

   c. Cree una ruta en la tabla de enrutamiento para que la subred privada envíe todo el tráfico IPv6 a la puerta de enlace de Internet de solo salida mediante el siguiente comando create-route. Utilice el ID de la tabla de enrutamiento que obtuvo en el paso anterior.

   ```
   aws ec2 create-route --route-table-id rtb-id-private --destination-cidr-
   block ::/0 --egress-only-internet-gateway eigw-id
   ```

   d. Asocie la tabla de enrutamiento a la subred privada mediante el siguiente comando associate-route-table.

   ```
   aws ec2 associate-route-table --route-table-id rtb-id-private --subnet-
   id subnet-id-private-subnet
   ```

6. Si necesita una puerta de enlace de NAT para los recursos de una subred privada, haga lo siguiente:

   a. Cree una dirección IP elástica para la puerta de enlace de NAT mediante el siguiente comando allocate-address.

   ```
   aws ec2 allocate-address --domain vpc --query AllocationId --output text
   ```

   b. Cree una puerta de enlace de NAT en la subred pública mediante el siguiente comando create-nat-gateway. Utilice el ID de asignación que obtuvo en el paso anterior.

```
aws ec2 create-nat-gateway --subnet-id subnet-id-public-subnet --allocation-
id eipalloc-id
```

c. (Opcional) Si ya creó una tabla de enrutamiento para la subred privada en el paso 5, omita este paso. De lo contrario, utilice el comando create-route-table para crear una tabla de enrutamiento para la subred privada. El comando devuelve el ID de la nueva tabla de enrutamiento.

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

d. Cree una ruta en la tabla de enrutamiento para que la subred privada envíe todo el tráfico IPv4 a la puerta de enlace de NAT mediante el siguiente comando create-route. Utilice el ID de la tabla de enrutamiento para la subred privada, que creó en este paso o en el paso 5.

```
aws ec2 create-route --route-table-id rtb-id-private --destination-cidr-
block 0.0.0.0/0 --gateway-id nat-id
```

e. (Opcional) Si ya asoció una tabla de enrutamiento a la subred privada en el paso 5, omita este paso. De lo contrario, utilice el comando associate-route-table para asociar la tabla de enrutamiento a la subred privada. Utilice el ID de la tabla de enrutamiento para la subred privada, que creó en este paso o en el paso 5.

```
aws ec2 associate-route-table --route-table-id rtb-id-private --subnet-
id subnet-id-private-subnet
```

Visualización de los recursos de su VPC

En esta sección, se describe cómo ver una presentación visual de los recursos en su VPC con la pestaña Mapa de recursos. Los siguientes recursos están visibles en el mapa de recursos:

- VPC
- Subredes
  - La zona de disponibilidad se representa con una letra.
  - Las subredes públicas están en verde.
  - Las subredes privadas están en azul.

- Tablas de enrutamiento
- Gateways de Internet
- Puerta de enlace de Internet de solo salida
- Puerta de enlace de NAT
- Puntos de conexión de puertas de enlace (Amazon S3 y Amazon DynamoDB)

El mapa de recursos muestra las relaciones entre los recursos de una VPC y cómo fluye el tráfico desde las subredes hasta las puertas de enlace de NAT, la puerta de enlace de Internet y los puntos de conexión de las puertas de enlace.

Puede utilizar el mapa de recursos para entender la arquitectura de una VPC, ver cuántas subredes contiene, qué subredes están asociadas a qué tablas de enrutamiento y qué tablas de enrutamiento tienen rutas a las puertas de enlace de NAT, las puertas de enlace de Internet y los puntos de conexión de las puertas de enlace.

También puede utilizar el mapa de recursos para detectar configuraciones incorrectas o no deseadas, como subredes privadas desconectadas de las puertas de enlace de NAT o subredes privadas con una ruta directa a la puerta de enlace de Internet. Puede elegir recursos dentro del mapa de recursos, como tablas de enrutamiento, y editar las configuraciones de estos.

Visualización de los recursos de su VPC

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.
4. Haga clic en la pestaña Mapa de recursos para mostrar una visualización de los recursos.
5. Elija Mostrar detalles para ver los detalles además de los ID de los recursos y las zonas que se muestran de forma predeterminada.

    - VPC: los rangos de CIDR de IPv4 e IPv6 asignados a la VPC.
    - Subredes: los rangos de CIDR de IPv4 e IPv6 asignados a cada subred.
    - Tablas de enrutamiento: las asociaciones de subredes y la cantidad de rutas en la tabla de enrutamiento.
    - Conexiones de red: la información relacionada con cada tipo de conexión:

- Si existen subredes públicas en la VPC, existe un recurso de puerta de enlace de Internet con la cantidad de rutas y las subredes de origen y destino para el tráfico que utiliza la puerta de enlace de Internet.
- Si hay una puerta de enlace de Internet de solo salida, hay un recurso de puerta de enlace de Internet de solo salida con la cantidad de rutas y las subredes de origen y destino para el tráfico que utiliza la puerta de enlace de Internet de solo salida.
- Si hay una puerta de enlace NAT, hay un recurso de puerta de enlace NAT con la cantidad de interfaces de red y direcciones IP elásticas de la puerta de enlace NAT.
- Si hay un punto de conexión de puerta de enlace, hay un recurso de punto de conexión de puerta de enlace con el nombre del servicio de AWS (Amazon S3 o Amazon DynamoDB) al que puede conectarse mediante el punto de conexión.

6. Coloque el ratón sobre un recurso para ver la relación entre los recursos. Las líneas continuas representan las relaciones entre los recursos. Las líneas punteadas representan el tráfico de red a las conexiones de red.

Adición o eliminación de un bloque de CIDR de su VPC

En esta sección, se describe cómo agregar o eliminar bloques de CIDR de IPv4 e IPv6 de una VPC.

⚠ Important

- Su VPC puede tener hasta cinco bloques CIDR de IPv4 y cinco de IPv6 de forma predeterminada, pero el límite se puede ajustar. Para obtener más información, consulte Cuotas de Amazon VPC. Para acceder a información sobre las restricciones de los bloques CIDR de una VPC, consulte Bloques de CIDR de VPC.
- Si la VPC tiene más de un bloque CIDR de IPv4 asociado a ella, se puede eliminar un bloque CIDR de IPv4 de la VPC. No se puede eliminar el bloque CIDR de IPv4 principal. Se debe eliminar un bloque CIDR completo, es decir, no se puede eliminar un subconjunto de un bloque CIDR o un rango fusionado de bloques CIDR. Primero debe eliminar todas las subredes del bloque de CIDR.
- Si ya no desea que la VPC admita IPv6, pero desea seguir utilizando la VPC para crear y comunicarse con recursos IPv4, puede eliminar el bloque CIDR de IPv6.
- Para eliminar un bloque CIDR de IPv6, primero debe anular la asignación de las direcciones IPv6 asignadas a las instancias de su subred.

- La eliminación de un bloque CIDR de IPv6 no elimina de manera automática las reglas del grupo de seguridad, las reglas de ACL de red ni las rutas de las tablas de enrutamiento que se hayan configurado para las redes IPv6. Por lo tanto, deberá modificar o eliminar manualmente dichas reglas o rutas.

Pasos para agregar o 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 (Sus VPC).
3. Seleccione la VPC y elija Actions (Acciones), Edit CIDRs (Editar CIDR).
4. Para eliminar una CIDR, seleccione la opción Eliminar junto a la CIDR.
5. Para agregar una CIDR, seleccione la opción Agregar nuevo CIDR de IPv4 o Agregar nuevo CIDR de IPv6.
6. Para agregar una CIDR en Bloque de CIDR de IPv4, haga uno de los siguientes pasos:
   - Elija IPv4 CIDR manual input (Entrada manual de IPv4 CIDR) e introduzca un bloque de CIDR IPv4.
   - Elija IPAM-allocated IPv4 CIDR (CIDR IPv4 asignado por IPAM) y seleccione un CIDR de un grupo de IPAM IPv4.
   - Seleccione Save.
7. Para agregar una CIDR en Bloque de CIDR de IPv6, haga lo siguiente:

   - Elija Bloque de CIDR de IPv6 asignado por el IPAM si utiliza el Administrador de direcciones IP de Amazon VPC y desea aprovisionar un CIDR de IPv6 desde un grupo de IPAM. Tiene dos opciones para aprovisionar un rango de direcciones IP a la VPC en el Bloque de CIDR:
     - Longitud de la máscara de red: elija esta opción a fin de seleccionar una longitud de máscara de red para el CIDR. Realice una de las siguientes acciones:
       - Si se ha seleccionado una longitud de máscara de red predeterminada para el grupo de IPAM, puede elegir Longitud de máscara de red predeterminada del IPAM a fin de utilizar la longitud de máscara de red predeterminada establecida para el grupo de IPAM por el administrador de IPAM. Para obtener más información sobre la regla opcional de asignación de longitud de máscara de red predeterminada, consulte Crear un grupo IPv6 regional en la Guía del usuario de IPAM de Amazon VPC.
       - Si no se ha seleccionado una longitud de máscara de red predeterminada para el grupo de IPAM, elija una longitud de máscara de red que sea más específica que la longitud

de máscara de red del CIDR del grupo de IPAM. Por ejemplo, si el CIDR del grupo de IPAM es /50, puede elegir una longitud de máscara de red entre /52 y /60 para la VPC. Las longitudes posibles de la máscara de red oscilan entre /44 y /60 en incrementos de /4.

- Seleccionar un CIDR: elija esta opción para ingresar de forma manual una dirección IPv6. Solo puede elegir una longitud de máscara de red que sea más específica que la longitud de la máscara de red del grupo de IPAM. Por ejemplo, si el CIDR del grupo de IPAM es /50, puede elegir una longitud de máscara de red entre /52 y /60 para la VPC. Las longitudes posibles de las máscaras de red IPv6 oscilan entre /44 y /60 en incrementos de /4.

- Elija Bloque CIDR de IPv6 proporcionado por Amazon para solicitar un bloque CIDR de 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.
- Elija CIDR de IPv6 de mi propiedad para aprovisionar un CIDR de IPv6 que ya haya traído a AWS. Para obtener más información, consulte Traer sus propias direcciones IP (BYOIP) a Amazon EC2 en la Guía del usuario de Amazon EC2. Tiene dos opciones para aprovisionar un rango de direcciones IP a la VPC en el Bloque de CIDR:
  - Sin preferencia: elija esta opción para utilizar una longitud de máscara de red de /56.
  - Seleccionar un CIDR: elija esta opción para ingresar de forma manual una dirección IPv6 y elegir una longitud de máscara de red que sea más específica que el tamaño del CIDR de BYOIP. Por ejemplo, si el CIDR del grupo de BYOIP es /50, puede elegir una longitud de máscara de red entre /52 y /60 para la VPC. Las longitudes posibles de las máscaras de red IPv6 oscilan entre /44 y /60 en incrementos de /4.
  - Seleccione Seleccionar CIDR cuando haya terminado.

8. Seleccione Cerrar.
9. Si ya agregó un bloque de CIDR en su VPC, puede crear subredes que utilicen el nuevo bloque de CIDR. Para obtener más información, consulte Crear una subred.

Asociación y desvinculación de un bloque de CIDR de una VPC con la AWS CLI

Utilice los comandos associate-vpc-cidr-block y disassociate-vpc-cidr-block.

Conjuntos de opciones de DHCP en Amazon VPC

Los dispositivos de red de la VPC utilizan el protocolo de configuración dinámica de host (DHCP). Puede utilizar conjuntos de opciones de DHCP para controlar los siguientes aspectos de la configuración de red de su red virtual:

- Los servidores DNS, los nombres de dominio o los servidores de protocolo de tiempo de red (NTP) utilizados por los dispositivos de la VPC.
- Si la resolución de DNS está habilitada en la VPC.

Contenido

- ¿Qué es DHCP?
- Conceptos de conjuntos de opciones de DHCP
- Trabajar con los conjuntos de opciones de DHCP

¿Qué es DHCP?

Todos los dispositivos de una red TCP/IP requieren una dirección IP para comunicarse a través de la red. En el pasado, las direcciones IP tenían que asignarse manualmente a cada dispositivo de la red. En la actualidad, los servidores DHCP utilizan el protocolo de configuración dinámica de host (DHCP) para asignar las direcciones IP de forma dinámica.

Las aplicaciones que se ejecutan en instancias de EC2 pueden comunicarse con los servidores DHCP de Amazon según sea necesario para recuperar la concesión de la dirección IP u otra información de configuración de red (como la dirección IP de un servidor DNS de Amazon o la dirección IP del enrutador de la VPC).

Puede especificar las configuraciones de red proporcionadas por los servidores DHCP de Amazon mediante el uso de conjuntos de opciones de DHCP.

Si tiene una configuración de VPC que requiere que las aplicaciones realicen solicitudes directas al servidor DHCP IPv6 de Amazon, tenga en cuenta lo siguiente:

- 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 y puede recuperar información adicional de configuración de red, tal como nombres de servidor DNS y nombres de dominio.
- Para una instancia EC2 en una subred únicamente IPv6, el servidor DHCP IPv4 devolverá 169.254.169.253 como el nombre del servidor si se menciona explícitamente «AmazonProvidedDNS» en el conjunto de opciones de DHCP. Si falta «AmazonProvidedDNS» en el conjunto de opciones, el servidor DHCP IPv4 no devolverá una dirección independientemente de si se mencionan otros nombres de servidores IPv4 en el conjunto de opciones o no.

Los servidores DHCP de Amazon también pueden proporcionar un prefijo IPv4 o IPv6 completo a una interfaz de red de la VPC mediante la delegación de prefijos (consulte Asignación de prefijos a las interfaces de red de Amazon EC2 en la Guía del usuario de Amazon EC2). La delegación de prefijos IPv4 no se proporciona en las respuestas DHCP. Los prefijos IPv4 asignados a la interfaz pueden recuperarse mediante IMDS (consulte Categorías de metadatos de instancia en la Guía del usuario de Amazon EC2).

Conceptos de conjuntos de opciones de DHCP

Un conjunto de opciones de DHCP es un grupo de configuraciones de red que los recursos de la VPC, como las instancias de EC2, utilizan para comunicarse a través de la red virtual.

Cada región tiene un conjunto de opciones de DHCP predeterminado. Cada VPC utiliza el conjunto de opciones de DHCP predeterminado para su región, a menos que usted cree y asocie un conjunto de opciones de DHCP personalizado a la VPC o configure la VPC sin un conjunto de opciones de DHCP.

Si su VPC no tiene ningún conjunto de opciones de DHCP configurado:

- En el caso de las instancias de EC2 basadas en el sistema Nitro, AWS establece `169.254.169.253` como el nombre del servidor de dominio predeterminado.
- En el caso de las instancias EC2 basadas en Xen, no se establece ningún nombre para los servidores de dominio y, dado que las instancias de la VPC no tienen acceso a un servidor DNS, no pueden acceder a Internet.

Un conjunto de opciones de DHCP puede asociarse a varias VPC, pero cada VPC puede asociarse solo a un conjunto de opciones de DHCP.

Si elimina una VPC, se desasocia el conjunto de opciones de DHCP que está asociado a la VPC.

Contenido

- Conjunto de opciones de DHCP predeterminado
- Conjunto de opciones de DHCP personalizado

Conjunto de opciones de DHCP predeterminado

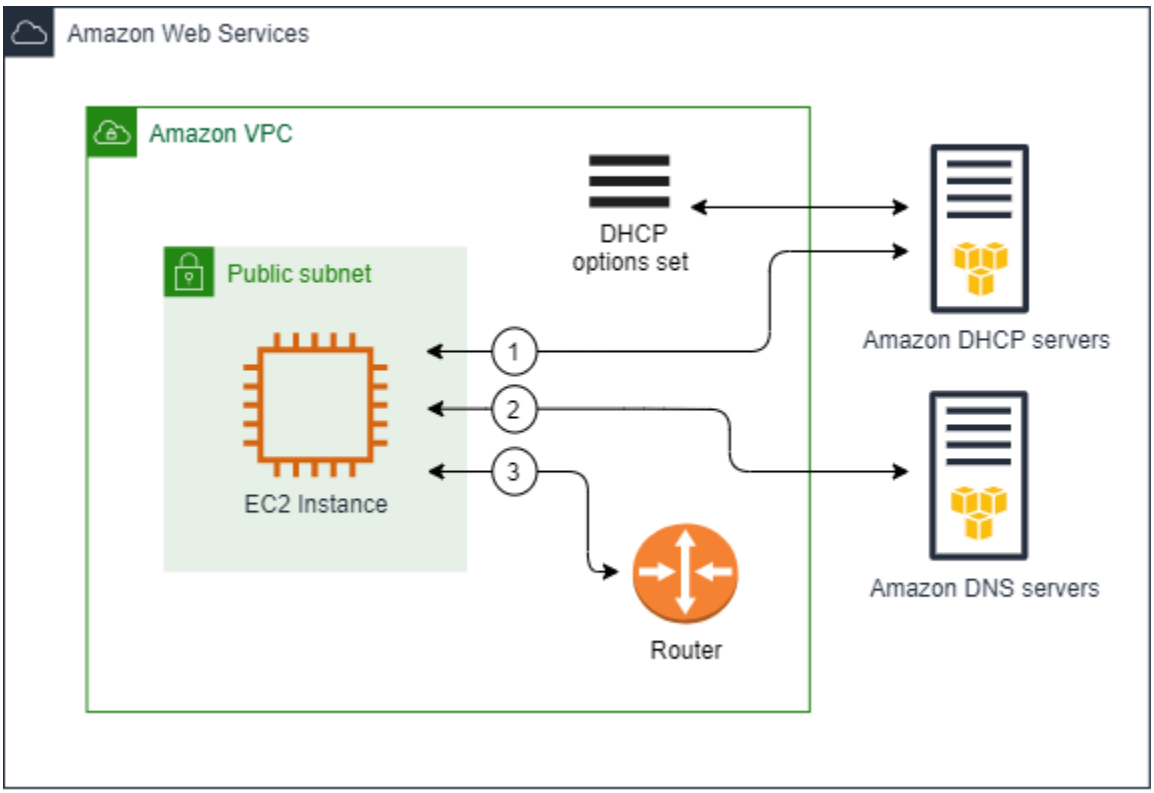
El conjunto de opciones de DHCP predeterminado tiene las siguientes configuraciones:

- Servidores de nombres de dominio: se trata de los servidores DNS que las interfaces de red utilizan para la resolución de nombres de dominio. En el caso de un conjunto de opciones de DHCP predeterminado, este es siempre `AmazonProvidedDNS`. Para obtener más información, consulte Servidor DNS de Amazon.
- Nombre de dominio: se trata del nombre de dominio que debe utilizar un cliente cuando resuelve nombres de host mediante el sistema de nombres de dominio (DNS). Para obtener más información acerca de los nombres de dominio que se utilizan para instancias de EC2, consulte Nombres de host de instancias de Amazon EC2.
- Tiempo de arrendamiento preferido para IPv6: frecuencia con la que se renueva la concesión de DHCPv6 a una instancia en ejecución con un IPv6 asignado. El tiempo de arrendamiento predeterminado es de 140 segundos. La renovación del arrendamiento suele producirse cuando ha transcurrido la mitad del tiempo de arrendamiento.

Cuando utiliza un conjunto de opciones de DHCP predeterminado, no se utilizan las siguientes configuraciones, pero hay opciones predeterminadas para las instancias de EC2:

- Servidores NTP: las instancias de EC2 utilizan de forma predeterminada el servicio de sincronización temporal de Amazon para obtener la hora.
- Servidores de nombres NetBIOS: en el caso de las instancias de EC2 que ejecutan Windows, 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.
- Tipo de nodo NetBIOS: en el caso de las instancias de EC2 que ejecutan Windows, este es el método que utilizan para resolver nombres NetBIOS en direcciones IP.

Cuando utiliza el conjunto de opciones predeterminado, el servidor DHCP de Amazon emplea la configuración de red en el conjunto de opciones predeterminado. Cuando se lanzan instancias en la VPC, sucede lo siguiente, como se muestra en el diagrama: las instancias (1) interactúan con el servidor DHCP, (2) interactúan con el servidor DNS de Amazon y (3) se conectan a otros dispositivos de la red a través del enrutador de la VPC. Las instancias pueden interactuar con el servidor DHCP de Amazon en cualquier momento para obtener la concesión de la dirección IP y las configuraciones de red adicionales.



Conjunto de opciones de DHCP personalizado

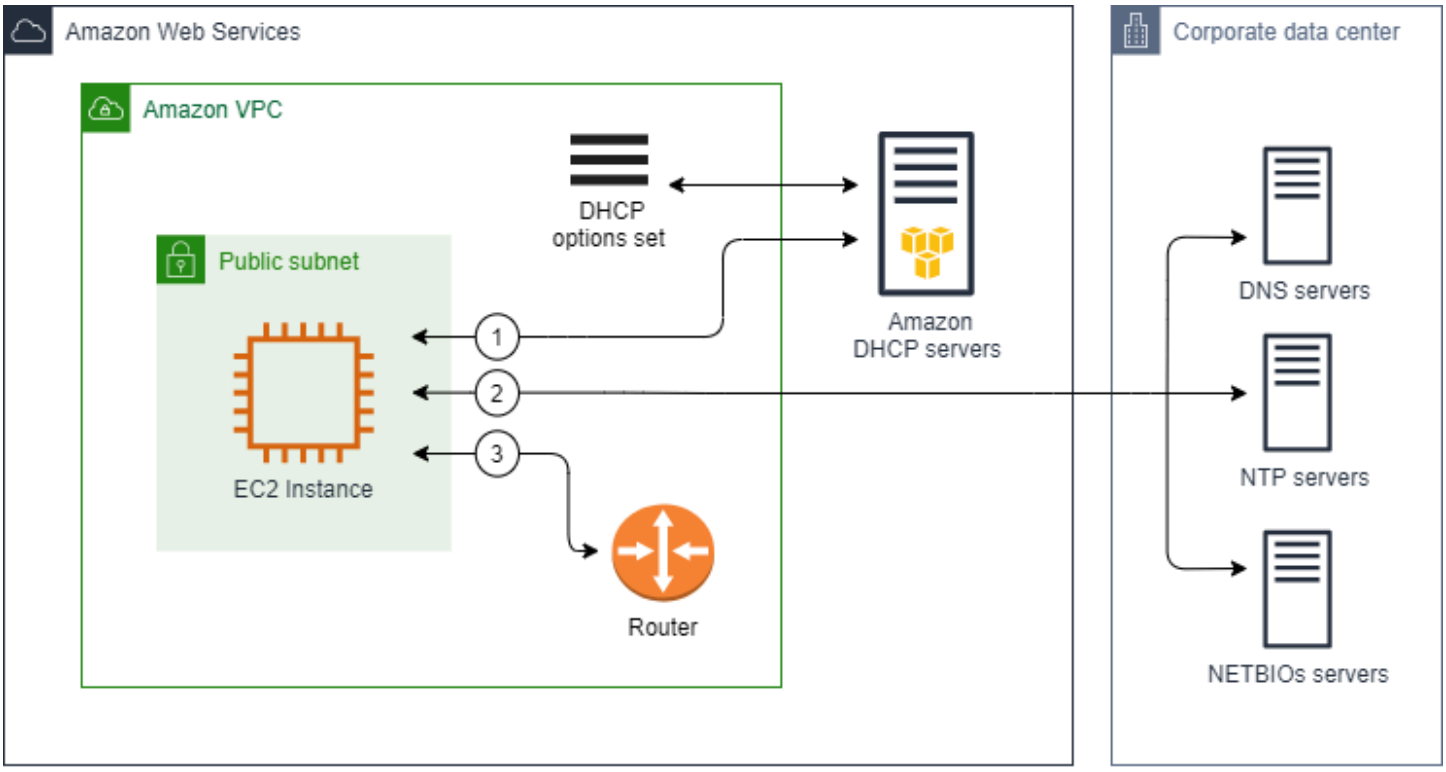
Puede crear un conjunto de opciones de DHCP personalizado con la siguiente configuración y luego, asociarlo a una VPC:

- Servidores de nombres de dominio: se trata de los servidores DNS que las interfaces de red utilizan para la resolución de nombres de dominio.
- Nombre de dominio: se trata del nombre de dominio que utiliza un cliente cuando resuelve nombres de host mediante el sistema de nombres de dominio (DNS).
- Servidores NTP: los servidores NTP que proporcionan la hora a las instancias.
- Servidores de nombres NetBIOS: en el caso de las instancias de EC2 que ejecutan Windows, 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.

- Tipo de nodo NetBIOS: en el caso de las instancias de EC2 que ejecutan Windows, este es el método que utilizan para resolver nombres NetBIOS en direcciones IP.
- Tiempo de arrendamiento preferido para IPv6 (opcional): un valor (en segundos, minutos, horas o años) que indica la frecuencia con la que se renueva la concesión de DHCPv6 a una instancia en ejecución con un IPv6 asignado. Los valores aceptables oscilan entre 140 y 4294967295 segundos (aproximadamente 138 años). Si no se especifica ningún valor, el tiempo de arrendamiento predeterminado es de 140 segundos. Si utiliza el direccionamiento a largo plazo para las instancias EC2, puede aumentar el tiempo de arrendamiento y evitar las solicitudes frecuentes de renovación del arrendamiento. La renovación del arrendamiento suele producirse cuando ha transcurrido la mitad del tiempo de arrendamiento.

Cuando se utiliza un conjunto de opciones personalizado, las instancias lanzadas en la VPC hacen lo siguiente, como se muestra en el diagrama: (1) utilizan las configuraciones de red en el conjunto de opciones de DHCP personalizado; (2) interactúan con los servidores DNS, NTP y NetBIOS especificados en el conjunto de opciones de DHCP personalizado; y (3) se conectan a otros dispositivos de la red a través del enrutador de la VPC.



Tareas relacionadas

- Crear un conjunto de opciones de DHCP
- Modificar el conjunto de opciones asociado a una VPC

Trabajar con los conjuntos de opciones de DHCP

Utilice los siguientes procedimientos para ver los conjuntos de opciones de DHCP y trabajar con ellos. Para obtener más información acerca de los conjuntos de opciones de DHCP, consulte the section called “Conceptos de conjuntos de opciones de DHCP”.

Tareas

- Crear un conjunto de opciones de DHCP
- Modificar el conjunto de opciones asociado a una VPC
- Eliminar un conjunto de opciones de DHCP

Crear un conjunto de opciones de DHCP

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

> **Note**
>
> Una vez que crea el conjunto de opciones de DHCP, no puede modificarlo. Para actualizar las opciones de DHCP para su VPC, debe crear un conjunto de opciones de DHCP nuevo y luego, asociarlo a la VPC.

Para crear un conjunto de opciones de DHCP mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija DHCP option sets (Conjuntos de opciones de DHCP).
3. Luego, Create DHCP options set (Crear conjunto de opciones de DHCP).

4. En el caso de Tag settings (Configuración de etiquetas), puede ingresar un nombre para el conjunto de opciones de DHCP. Si ingresa un valor, este crea automáticamente una etiqueta de nombre para el conjunto de opciones de DHCP.
5. En Opciones de DHCP, proporcione los ajustes de configuración que necesita.

   - Nombre de dominio (opcional): ingrese el nombre de dominio que deben utilizar los clientes al resolver nombres de host a través del DNS. 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.

     > **Note**
     >
     > Solo utilice nombres de dominio que pueda controlar completamente.

     Algunos sistemas operativos Linux aceptan el uso de varios nombres de dominio separados por espacios. Sin embargo, Windows y otros sistemas operativos de Linux 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 tiene instancias en las que se ejecutan los sistemas operativos que tratan el valor como un dominio único, especifique solo un nombre de dominio.

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

     Puede ingresar **`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 de AmazonProvidedDNS y el servidor DNS de Amazon, consulte Servidor DNS de Amazon.

     > **Important**
     >
     > Si la VPC tiene una puerta de enlace de Internet, asegúrese de especificar su propio servidor DNS o el servidor DNS de Amazon (AmazonProvidedDNS) en el valor

Servidores de nombres de dominio. De lo contrario, las instancias de la VPC no tendrán acceso a DNS, lo que inhabilita el acceso a Internet.

- NTP servers (Servidores NTP) (opcional): ingrese las direcciones IP de hasta ocho servidores de protocolo de tiempo de red (NTP) (cuatro direcciones IPv4 y cuatro direcciones IPv6).

  Los servidores NTP proporcionan el tiempo a la red. Puede especificar Amazon Time Sync Service en la dirección IPv4 `169.254.169.123` o la dirección IPv6 `fd00:ec2::123`. Las instancias se comunican con Amazon Time Sync Service de forma predeterminada. Tenga en cuenta que solo se puede acceder a la dirección IPv6 en instancias de EC2 creadas en el sistema Nitro.

  Para obtener más información acerca de la opción de servidores NTP, consulte RFC 2132. Para obtener más información acerca del Servicio de sincronización temporal de Amazon, consulte Configurar la hora para una instancia en la Guía del usuario 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 de EC2 que ejecutan un sistema operativo Windows, 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) (opcional): ingrese **1**, **2**, **4** o **8**. Le recomendamos que especifique **2** (punto a punto o nodo-P). Actualmente no se admiten la difusión ni la multidifusión. Par obtener más información sobre estos tipos de nodos, consulte la sección 8.7 de RFC 2132 y la sección 10 de RFC1001.

  Para las instancias de EC2 que ejecuten un sistema operativo Windows, este es el método que utilizan para resolver nombres NetBIOS en direcciones IP. En el conjunto de opciones predeterminadas, no existe ningún valor para el tipo de nodo NetBIOS.

- Tiempo de arrendamiento preferido para IPv6 (opcional): un valor (en segundos, minutos, horas o años) que indica la frecuencia con la que se renueva la concesión de DHCPv6 a una instancia en ejecución con un IPv6 asignado. Los valores aceptables oscilan entre 140 y 2147483647 segundos (aproximadamente 68 años). Si no se especifica ningún valor, el tiempo de arrendamiento predeterminado es de 140 segundos. Si utiliza el direccionamiento a largo plazo para las instancias EC2, puede aumentar el tiempo de arrendamiento y evitar

las solicitudes frecuentes de renovación del arrendamiento. La renovación del arrendamiento suele producirse cuando ha transcurrido la mitad del tiempo de arrendamiento.

6. Agregar Tags (Etiquetas).
7. Luego, Create DHCP options set (Crear conjunto de opciones de DHCP). Anote el nombre o el ID del conjunto de opciones de DHCP nuevo.
8. Para configurar una VPC para utilizar el conjunto de opciones nuevo, consulte Modificar el conjunto de opciones asociado a una VPC.

Para crear un conjunto de opciones de DHCP para la VPC mediante la línea de comandos

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

Modificar el conjunto de opciones asociado a una VPC

Una vez que crea un conjunto de opciones de DHCP, puede asociarlo a una o varias VPC. Solo podrá asociar una VPC a un conjunto de opciones de DHCP a la vez. Si no asocia un conjunto de opciones de DHCP a una VPC, se deshabilita la resolución de nombres de dominio en la VPC.

Cuando asocia un conjunto de opciones de DHCP nuevo a una VPC, las instancias existentes y todas las instancias nuevas que lanza en esa VPC utilizan las opciones nuevas. 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.

Para cambiar el conjunto de opciones de DHCP asociado a 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 la casilla de verificación de la VPC y, a continuación, elija Actions (Acciones) y Edit VPC settings (Editar la configuración de VPC).
4. Para DHCP options set (Conjunto de opciones de DHCP), elija un conjunto de opciones de DHCP nuevo. Como alternativa, elija Sin conjunto de opciones de DHCP para deshabilitar la resolución de nombres de dominio para la VPC.
5. Seleccione Save.

Para cambiar el conjunto de opciones de DHCP asociado a una VPC mediante la línea de comandos

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

Eliminar un conjunto de opciones de DHCP

Cuando ya no necesite un conjunto de opciones de DHCP, utilice el siguiente procedimiento para eliminarlo. No se puede eliminar un conjunto de opciones de DHCP si está en uso. Para cada VPC asociada al conjunto de opciones de DHCP que desea eliminar, debe asociar un conjunto de opciones de DHCP diferente a la VPC o configurar la VPC para que no utilice un conjunto de opciones de DHCP. Para obtener más información, consulte the section called “Modificar el conjunto de opciones asociado a una VPC”.

Para eliminar un conjunto de opciones de DHCP mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija DHCP option sets (Conjuntos de opciones de DHCP).
3. Seleccione el botón de opción del conjunto de opciones de DHCP y luego, elija Acciones y Eliminar conjunto de opciones de DHCP.
4. Cuando se le solicite confirmación, ingrese **`delete`** y luego, elija Eliminar conjunto de opciones de DHCP.

Para eliminar un conjunto de opciones de DHCP mediante la línea de comandos

- 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 para VPC y subredes.

Amazon proporciona un servidor DNS (the Amazon Route 53 Resolver) para 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.

Contenido

- Descripción de Amazon DNS
- Consultar los nombres de host DNS de su instancia EC2
- Ver y actualizar los atributos de DNS de su VPC

Descripción de Amazon DNS

Uno de los componentes básicos de la red con el que se encuentran los arquitectos o los administradores de AWS es el servidor de Amazon DNS, también conocido como Route 53 Resolver. Este servicio de resolución de DNS está integrado de forma nativa en cada zona de disponibilidad de su región de AWS, lo que brinda una solución fiable y escalable para la resolución de nombres de dominio dentro de su nube privada virtual (VPC). En esta sección, obtendrá información sobre las direcciones IP del servidor DNS de Amazon, los nombres de host DNS privados que puede resolver y las reglas que rigen su uso.

Contenido

- Servidor DNS de Amazon
- Reglas y consideraciones
- Nombres de host de DNS de instancias de EC2
- Atributos DNS para la VPC
- Cuotas de DNS
- Zonas alojadas privadas

Servidor DNS de Amazon

Route 53 Resolver (también llamado “servidor DNS de Amazon” o “AmazonProvidedDNS”) es un servicio de resolución de DNS integrado en cada zona de disponibilidad de una región de AWS.

Route 53 Resolver se encuentra en `169.254.169.253` (IPv4), `fd00:ec2::253` (IPv6) y en el rango de CIDR de IPV4 privado principal aprovisionado en su VPC más dos. Por ejemplo, si tiene una VPC con un CIDR de IPv4 de `10.0.0.0/16` y un CIDR de IPv6 de `2001:db8::/32`, puede comunicarse con Route 53 Resolver en `169.254.169.253` (IPv4), `fd00:ec2::253` (IPv6) o `10.0.0.2` (IPv4). Los recursos de una VPC utilizan una dirección de enlace local para las consultas de DNS. Estas consultas se transportan al Route 53 Resolver de forma privada y no están visibles en la red. En una subred exclusiva para IPv6, se puede seguir accediendo a la dirección de enlace local IPv4 (169.254.169.253) siempre que «AmazonProvidedDNS» sea el nombre del servidor en el conjunto de opciones de DHCP.

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 Tipos de nombres de host de instancias de Amazon EC2 en la Guía del usuario de Amazon 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.

- Amazon Route 53 Resolver sólo admite consultas DNS recursivas.

Nombres de host de DNS de instancias de EC2

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 DNS para la VPC.

Con el servidor DNS proporcionado por Amazon activado, los nombres de host de DNS se resuelven de la siguiente manera.

Nombre de DNS de IPv4 privado

El nombre de host de DNS de IPv4 privado de una instancia determina su dirección IPv4 privada. Puede utilizar el nombre de host de DNS de IPv4 privado para la comunicación entre instancias de la misma VPC o en VPC conectadas. Para obtener más información, consulte Direcciones IPv4 privadas en la Guía del usuario de Amazon EC2.

Nombre de DNS de IPv4 público

Un nombre de host de DNS de IPv4 público de una instancia resuelve la dirección IPv4 pública de la instancia (fuera de la red de la instancia), y la dirección IPv4 privada de la instancia (desde la red de la instancia). Para obtener más información, consulte Direcciones IPv4 públicas en la Guía del usuario de Amazon EC2.

Para convertir los nombres de DNS de IPv4 públicos en direcciones IPv4 privadas a través de una conexión de emparejamiento de VPC, debe activar la resolución de DNS para la conexión de emparejamiento. Para obtener más información, consulte Habilitación de la resolución de DNS para la conexión de emparejamiento de VPC.

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. Si desea obtener más información sobre RBN, consulte Tipos de nombres de host de instancias de EC2 en la Guía del usuario de Amazon EC2.

Atributos DNS para la 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.

Atributo	Descripción
`enableDnsHostnames`	Determina si la VPC admite la asignación de nombres de anfitrión de DNS público a las instancias con direcciones IP públicas. El valor predeterminado de este atributo es `false` a menos que la VPC sea una VPC predeterminada. Tenga en cuenta las reglas y las consideraciones para este atributo a continuación.
`enableDnsSupport`	Determina si la VPC admite la resolución de DNS a través del servidor DNS proporcionado por Amazon. Si este atributo es `true`, las consultas al servidor DNS proporcionado por Amazon se realizan de manera exitosa. Para obtener más información, consulte Servidor DNS de Amazon. El valor predeterminado de este atributo es `true`. Tenga en cuenta las reglas y las consideraciones para este atributo a continuación.

Reglas y consideraciones

- 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 de Route 53 Resolver puede resolver los nombres de host 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.
  - Route 53 Resolver no puede resolver los nombres de host 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. Si no utiliza el servidor de Route 53 Resolver, los servidores de nombres de dominio personalizados deben 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`.
- Route 53 Resolver puede resolver nombres de host DNS privados en direcciones IPv4 privadas para todos los espacios de direcciones, incluidos aquellos en los que el intervalo de direcciones IPv4 de la VPC queda fuera de los intervalos de direcciones IPv4 privadas especificados por RFC 1918. Sin embargo, si creó la VPC antes de octubre de 2016, 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 Soporte.

Cuotas de DNS

Hay un límite de 1024 paquetes por segundo (PPS) para los servicios que utilizan direcciones locales de enlace. Este límite incluye la suma de las consultas de DNS de Route 53 Resolver, las solicitudes del servicio de metadatos de instancias (IMDS), las solicitudes del protocolo de tiempo de red (NTP) del servicio temporal de Amazon y las solicitudes del Servicio de licencias de Windows (para instancias basadas en Microsoft Windows). 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.

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).

Las zonas alojadas privadas no admitirán las relaciones transitivas fuera de la VPC; por ejemplo, no es posible obtener acceso a sus recursos utilizando sus nombres DNS privados personalizados desde el otro lado de una conexión VPN.

> **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` en `true`.

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. Conocer estos nombres de host es importante para conectarse a sus recursos.

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 DNS para la VPC”.

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, elija 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

- 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

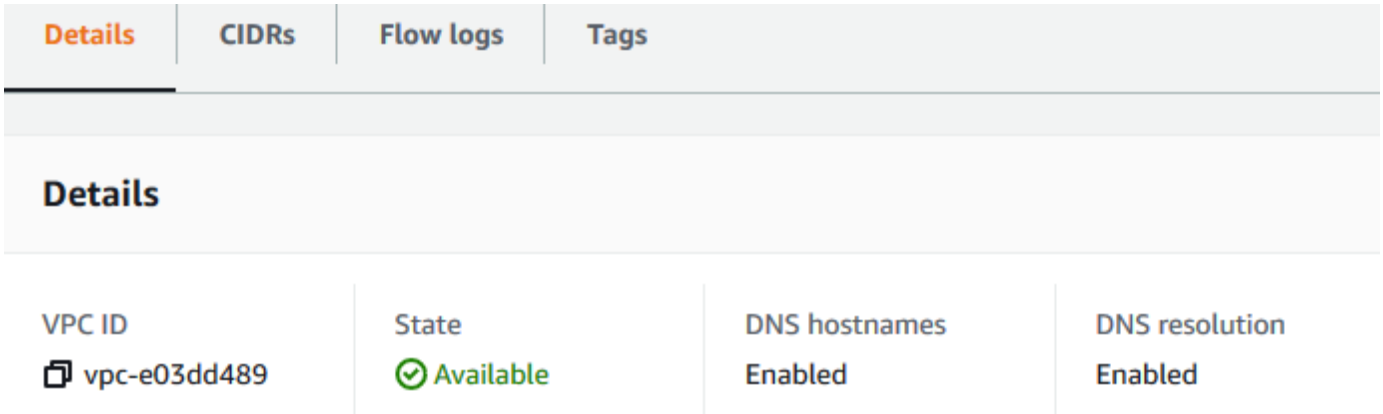
- describe-network-interfaces (AWS CLI)
- Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

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. Esta configuración controla si sus instancias obtienen nombres de host DNS públicos y si el servidor DNS de Amazon puede resolver sus nombres DNS privados. La correcta configuración de estos atributos es fundamental para garantizar una comunicación fluida dentro de su 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).



5. Para actualizar esta configuración, elija Actions (Acciones) y, a continuación, elija Edit VPC settings (Editar la configuración de VPC). Seleccione o borre Enable (Habilitar) en el atributo DNS correspondiente y elija Save changes (Guardar cambios).

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

- 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

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

Uso de direcciones de red para su VPC

El uso de direcciones de red (NAU) es una métrica que se aplica a los recursos de su red virtual para ayudarlo a planificar y supervisar el tamaño de su VPC. Cada unidad de NAU contribuye a un total que representa el tamaño de la VPC.

Es importante conocer el número total de unidades que componen el NAU de la VPC, ya que las siguientes cuotas de VPC limitan el tamaño de una VPC:

- Uso de direcciones de red: el número máximo de unidades de NAU que puede tener una sola VPC. Cada VPC puede tener hasta 64 000 unidades de NAU de forma predeterminada. Puede solicitar un aumento de cuota de hasta 256 000.
- Uso de direcciones de red interconectadas: el número máximo de unidades de NAU para una VPC y todas sus VPC interconectadas. Si una VPC está emparejada con otras VPC de la misma región, las VPC combinadas pueden tener hasta 128 000 unidades de NAU de forma predeterminada. Puede solicitar un aumento de cuota de hasta 512 000. Esta cuota se aplica a las interconexiones entre VPC de la misma región, incluidas las interconexiones entre VPC de cuentas de AWS diferentes. Las VPC interconectadas en diferentes regiones no contribuyen a esta cuota.

Puede usar el NAU de las siguientes formas:

- Antes de crear su red virtual, calcule las unidades de NAU para ayudarlo a decidir si debe distribuir las cargas de trabajo entre varias VPC.
- Una vez creada la VPC, utilice Amazon CloudWatch para supervisar el uso de NAU de la VPC a fin de que no supere las cuotas de NAU. Se recomienda crear alarmas de Amazon CloudWatch para supervisar las cuotas de NAU. Para obtener más información, consulte the section called “Métricas de CloudWatch”.

Superar las cuotas de NAU

Si supera las cuotas de NAU de la VPC, las siguientes llamadas a la API fallan con una excepción del lado del cliente:

- `RunInstances`
- `AttachNetworkInterface`
- `AssignPrivateIpAddresses`
- `AssignIpv6Addresses`
- `AcceptVpcPeeringConnection`

La excepción específica depende de qué cuota supere:

- `NetworkAddressUsageLimitExceeded`— La VPC supera su cuota de NAU.
- `NetworkAddressUsagePeeredLimitExceeded`— La VPC supera su cuota de NAU de VPC interconectadas.

Estos errores afectan a la capacidad de iniciar instancias, asociar interfaces de red, asignar nuevas direcciones, aceptar conexiones de interconexión de VPC y escalar o administrar las cargas de trabajo en las VPC afectadas. Para evitar interrupciones, supervise el uso de NAU con Amazon CloudWatch y solicite un aumento antes de que se alcance la cuota.

Cómo se calcula el NAU

Entender cómo se calcula el NAU puede ayudarlo a planificar el escalado de sus VPC.

La siguiente tabla explica qué recursos componen el recuento de NAU en una VPC y cuántas unidades de NAU usa cada recurso. Algunos recursos de AWS se representan como unidades de

NAU individuales y algunos recursos se representan como múltiples unidades de NAU. Puede usar la tabla para saber cómo se calcula el NAU.

Recurso	Unidades de NAU
Cada dirección IPv4 pública o privada y cada dirección IPv6 asignada a una interfaz de red para una instancia de EC2 en la VPC	1
Interfaces de red adicionales conectadas a una instancia de EC2	1
Prefijos asignados a una interfaz de red	1
Equilibrador de carga de red por AZ	6
Equilibrador de carga de puerta de enlace por AZ	6
Punto de conexión de VPC por AZ	6
Conexión de puerta de enlace de tránsito	6
Función de Lambda	6
Puerta de enlace de NAT	6
Objetivo de montaje EFS	6
Interfaz de EFA (EFA con un dispositivo ENA) o una interfaz solo de EFA	1
Pod de Amazon EKS	1

Ejemplos de NAU

En los siguientes ejemplos se muestra cómo calcular el NAU.

Ejemplo 1: dos VPC conectadas mediante emparejamiento de VPC.

Las VPC interconectadas en la misma región contribuyen a una cuota combinada de NAU.

- VPC 1
  - 50 equilibradores de carga de red en 2 subredes en diferentes zonas de disponibilidad: 600 unidades de NAU

  - 5000 instancias (cada una con una dirección IPv4 y una dirección IPv6) en una subred y 5000 instancias (cada una con una dirección IPv4 y una dirección IPv6) en otra subred: 20 000 unidades
  - 100 funciones Lambda: 600 unidades de NAU
- VPC 2
  - 50 equilibradores de carga de red en 2 subredes en diferentes zonas de disponibilidad: 600 unidades de NAU
  - 5000 instancias (cada una con una dirección IPv4 y una dirección IPv6) en una subred y 5000 instancias (cada una con una dirección IPv4 y una dirección IPv6) en otra subred: 20 000 unidades
  - 100 funciones Lambda: 600 unidades de NAU
- Recuento total de NAU de emparejamiento: 42 400 unidades
- Cuota de NAU de emparejamiento predeterminada: 128 000 unidades

Ejemplo 2: Dos VPC conectadas mediante una puerta de enlace de tránsito

Las VPC que se conectan mediante una puerta de enlace de tránsito no contribuyen a una cuota combinada de NAU como lo hacen con las VPC interconectadas.

- VPC 1
  - 50 equilibradores de carga de red en 2 subredes en diferentes zonas de disponibilidad: 600 unidades de NAU
  - 5000 instancias (cada una con una dirección IPv4 y una dirección IPv6) en una subred y 5000 instancias (cada una con una dirección IPv4 y una dirección IPv6) en otra subred: 20 000 unidades
  - 100 funciones Lambda: 600 unidades de NAU
- VPC 2
  - 50 equilibradores de carga de red en 2 subredes en diferentes zonas de disponibilidad: 600 unidades de NAU
  - 5000 instancias (cada una con una dirección IPv4 y una dirección IPv6) en una subred y 5000 instancias (cada una con una dirección IPv4 y una dirección IPv6) en otra subred: 20 000 unidades
  - 100 funciones Lambda: 600 unidades de NAU
- Recuento total de NAU por VPC: 21 200 unidades

- Cuota de NAU predeterminada por VPC: 64 000 unidades

Ejemplo 3: dos VPC conectadas mediante una interconexión de VPC entre regiones

Las VPC interconectadas en diferentes regiones no contribuyen a una cuota de NAU combinada. AWSevalúa cada VPC en función de su propia cuota de NAU por VPC, y los recursos de la VPC interconectada de la otra región no se tienen en cuenta para la cuota de NAU de VPC interconectadas de ninguna de las VPC. En este ejemplo, se supone que la única interconexión de cada VPC es la interconexión entre regiones que se muestra (no hay VPC interconectadas adicionales dentro de la misma región).

- VPC 1 (región A)
  - 50 equilibradores de carga de red en 2 subredes en diferentes zonas de disponibilidad: 600 unidades de NAU
  - 5000 instancias (cada una con una dirección IPv4 y una dirección IPv6) en una subred y 5000 instancias (cada una con una dirección IPv4 y una dirección IPv6) en otra subred: 20 000 unidades
  - 100 funciones Lambda: 600 unidades de NAU
- VPC 2 (región B)
  - 50 equilibradores de carga de red en 2 subredes en diferentes zonas de disponibilidad: 600 unidades de NAU
  - 5000 instancias (cada una con una dirección IPv4 y una dirección IPv6) en una subred y 5000 instancias (cada una con una dirección IPv4 y una dirección IPv6) en otra subred: 20 000 unidades
  - 100 funciones Lambda: 600 unidades de NAU
- Recuento total de NAU por VPC: 21 200 unidades
- Cuota de NAU predeterminada por VPC: 64 000 unidades
- Recuento de NAU de VPC interconectadas por VPC: 21.200 unidades (solo cuentan los recursos propios de la VPC; la VPC interconectada de la otra región contribuye con 0)
- Cuota predeterminada de NAU de VPC interconectadas por VPC: 128.000 unidades (la VPC interconectada de la otra región no cuenta para esta cuota)

Intercambio de sus subredes de VPC con otras cuentas

El uso compartido de subredes 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 privadas virtuales (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 subredes de VPC para utilizar 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 subredes de Amazon VPC compartidas mediante las características de conectividad, como AWS PrivateLink, puertas de enlaces de tránsito y emparejamiento de VPC. Para obtener más información sobre las ventajas de compartir las subredes de VPC, consulte VPC sharing: A new approach to multiple accounts and VPC management.

Hay cuotas relacionadas con el uso compartido de subredes de VPC. Para obtener más información, consulte Uso compartido de subredes de VPC.

Contenido

- Requisitos previos para las subredes compartidas
- Utilización de las subredes compartidas
- Facturación y medición para el propietario y los participantes
- Responsabilidades y permisos para propietarios y participantes
- AWSRecursos de y subredes de VPC compartidas

Requisitos previos para las subredes compartidas

En esta sección, se presentan los requisitos previos para trabajar con las subredes compartidas:

- debe administrar las cuentas del propietario y del participante de la VPC AWS Organizations.

- En la consola de AWS RAM, debe habilitar el uso compartido de recursos desde la cuenta de administración para la organización. Para obtener más información, consulte Habilitar el uso compartido de recursos dentro de AWS Organizations en la Guía del usuario de AWS RAM.
- Debe crear un recurso compartido. Puede especificar las subredes que se compartirán al crear el recurso compartido o al agregar las subredes al recurso compartido más adelante con el procedimiento que se detalla en la sección siguiente. Para obtener más información, consulte Crear un recurso compartido en la Guía del usuario de AWS RAM.

Utilización de las subredes compartidas

En esta sección, se describe cómo trabajar con las subredes compartidas en la consola de AWS y la AWS CLI.

Contenido

- Compartir una subred
- Dejar de compartir una subred compartida
- Identificar al propietario de una subred compartida

Compartir una subred

Puede compartir subredes distintas a las predeterminadas con otras cuentas en la organización de la manera que se detalla a continuación. Además, puede compartir grupos de seguridad en AWS Organizations. Para obtener más información, consulte Compartir grupos de seguridad con AWS Organizations.

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

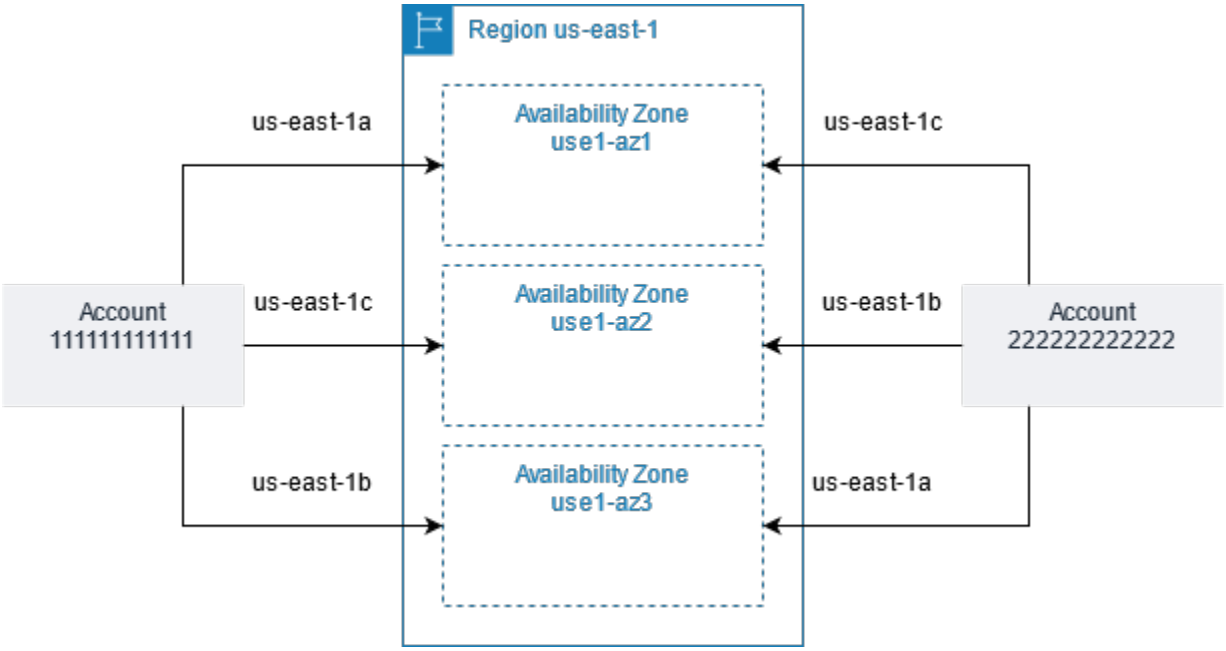
Utilice los comandos create-resource-share y associate-resource-share.

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 servicios administrados por AWS (por ejemplo, Elastic Load Balancing) que tienen

flujos de trabajo automatizados/administrados (como el escalado automático o la sustitución de nodos) pueden requerir acceso continuo a la subred compartida para algunos recursos.

- 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.

Facturación y medición para el propietario y los participantes

En esta sección, se incluyen los detalles de facturación y medición para los propietarios de la subred compartida y los que utilizan las subredes compartidas:

- 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, así como también la transferencia de datos a través de conecciones de emparejamiento de VPC, a través de puertas de enlace de Internet y a través de puertas de enlace 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 puerta de enlaces NAT, puerta de enlaces privadas virtuales, transit puerta de enlaces, puntos de enlace de la VPC y AWS PrivateLink. Además, las direcciones IPv4 públicas utilizadas en las VPC compartidas se facturan a los propietarios de las VPC. Para obtener más información sobre los precios de las direcciones IPv4 públicas, consulte la pestaña Dirección IPv4 pública en la página Precios de Amazon VPC.
- 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.

Responsabilidades y permisos para propietarios y participantes

En esta sección, se incluyen detalles sobre las responsabilidades y los permisos de los dueños de la subred compartida (el propietario) y de los que la utilizan (el participante).

Recursos del propietario

Los propietarios deben hacerse cargo de sus propios recursos de la VPC. Los propietarios de la VPC se encargan de crear, administrar y eliminar los recursos asociados a una VPC compartida. Esto incluye a las subredes, las tablas de enrutamiento, las ACL de red, las conexiones de emparejamiento, los puntos de conexión de la puerta de enlace, los puntos de conexión de la interfaz, los puntos de conexión de Route 53 Resolver, las puertas de enlace de Internet, las puertas de enlace NAT, las puertas de enlace privadas virtuales y las conexiones de puertas de enlace de tránsito.

Recursos del participante

Los participantes deben hacerse cargo de sus propios recursos de la VPC. Los participantes pueden crear un conjunto limitado de recursos de VPC en una VPC compartida. Pueden crear interfaces de red y grupos de seguridad, y habilitar los registros de flujo de VPC para las interfaces de red de las que son propietarios. Los recursos de VPC que crea un participante se calculan para las cuotas de VPC de la cuenta del participante, no para la cuenta del propietario. Para obtener más información, consulte Uso compartido de subredes de VPC.

Recursos de la VPC

Las siguientes responsabilidades y permisos se aplican a los recursos de VPC cuando se trabaja con subredes de VPC compartidas:

Logs de flujo

- Los participantes pueden crear, eliminar y describir registros de flujo para interfaces de red de su propiedad en una subred de VPC compartida.
- Los participantes no pueden crear, eliminar ni describir registros de flujo para interfaces de red que no son de su propiedad en una subred de VPC compartida.
- Los participantes no pueden crear, eliminar ni describir registros de flujo en una subred de VPC compartida.
- Los propietarios de VPC pueden crear, eliminar y describir registros de flujo para interfaces de red que no son de su propiedad en una subred de VPC compartida.
- Los propietarios de VPC pueden crear, eliminar y describir registros de flujo para una subred de VPC compartida.
- Los propietarios de VPC no pueden describir ni eliminar registros de flujo creados por un participante.

Puertas de enlace de Internet y puertas de enlace de Internet de solo salida

- Los participantes no pueden crear, adjuntar ni eliminar puertas de enlace de Internet ni puertas de enlace de Internet únicamente de salida en una subred de VPC compartida. Los participantes pueden describir las puertas de enlace de Internet en una subred de VPC compartida. Los participantes no pueden describir las puertas de enlace de Internet de solo salida en una subred de VPC compartida.

Puertas de enlace NAT

- Los participantes no pueden crear, eliminar ni describir puertas de enlace NAT en una subred de VPC compartida.

Listas de control de acceso a la red (NACL)

- Los participantes no pueden crear, eliminar ni reemplazar NACL en una subred de VPC compartida. Los participantes pueden describir las NACL creadas por propietarios de VPC en una subred de VPC compartida.

Interfaces de red

- Los participantes pueden crear interfaces de red en una subred de VPC compartida. Los participantes no pueden trabajar con interfaces de red creadas por propietarios de VPC en una subred de VPC compartida de ninguna otra manera, como adjuntar, desconectar o modificar las interfaces de red. Los participantes pueden modificar o eliminar las interfaces de red en una VPC compartida que crearon. Por ejemplo, los participantes pueden asociar o desasociar direcciones IP con las interfaces de red que crearon.
- Los propietarios de VPC pueden describir las interfaces de red que pertenecen a los participantes en una subred de VPC compartida. Los propietarios de VPC no pueden trabajar con las interfaces de red que pertenecen a los participantes como adjuntar, desconectar o modificar las interfaces de red que pertenecen a los participantes en una subred de VPC compartida.

Tablas de enrutamiento

- Los participantes no pueden trabajar con tabla de enrutamiento (por ejemplo, crear, eliminar o asociar tablas de rutas) en una subred de VPC compartida. Los participantes pueden describir tablas de rutas en una subred de VPC compartida.

Grupos de seguridad

- Los participantes pueden trabajar con (crear, eliminar, describir, modificar o crear reglas de entrada y salida para) grupos de seguridad que poseen en una subred de VPC compartida. Los participantes pueden trabajar con grupos de seguridad creados por los propietarios de la VPC si el propietario comparte el grupo de seguridad con el participante.

- Los participantes pueden crear reglas en los grupos de seguridad de los que son propietarios que hacen referencia a grupos de seguridad que pertenecen a otros participantes o al propietario de la VPC de la siguiente manera: número-cuenta/id-grupo-seguridad
- Los participantes no pueden lanzar instancias utilizando el grupo de seguridad predeterminado para la VPC porque pertenece al propietario.
- Los participantes no pueden lanzar instancias mediante grupos de seguridad no predeterminados que sean del propietario de la VPC o de otros participantes a menos que se les comparta el grupo de seguridad.
- Los propietarios de VPC pueden describir los grupos de seguridad creados por los participantes en una subred de VPC compartida. Los propietarios de VPC no pueden trabajar con grupos de seguridad creados por los participantes de ninguna otra forma. Por ejemplo, los propietarios de VPC no pueden lanzar instancias mediante grupos de seguridad creados por los participantes.

Subredes

- Los participantes no pueden modificar las subredes compartidas ni sus atributos relacionados. Solo el propietario de la VPC puede hacerlo. Los participantes pueden describir subredes en una subred VPC compartida.
- Los propietarios de VPC pueden compartir subredes solo con otras cuentas o unidades organizativas que estén en la misma organización desde Organizaciones de AWS. Los propietarios de VPC no pueden compartir subredes que estén en una VPC predeterminada.

Puertas de enlace de tránsito

- Solo el propietario de la VPC puede asociar una puerta de enlace de tránsito a una subred de VPC compartida. Los participantes no pueden hacerlo.

VPC

- Los participantes no pueden modificar las VPC ni sus atributos relacionados. Solo el propietario de la VPC puede hacerlo. Los participantes pueden describir las VPC, sus atributos y los conjuntos de opciones de DHCP.
- Las etiquetas de VPC y las etiquetas de los recursos de la VPC compartida no se comparten con los participantes.

- Los participantes pueden asociar sus propios grupos de seguridad a una VPC compartida. Esto permite que el participante use el grupo de seguridad con las interfaces de red Elastic de su propiedad en la VPC compartida.

AWSRecursos de y subredes de VPC compartidas

Los siguientes Servicios de AWS admiten recursos en subredes de VPC compartidas. Para obtener más información, siga los enlaces a la documentación del servicio correspondiente.

- Amazon Aurora
- AWS Database Migration Service
- Amazon EC2
- Amazon ECS
- Amazon ElastiCache (Redis OSS)
- Amazon EFS
- Amazon Elastic Kubernetes Service
- Elastic Load Balancing
  - Equilibradores de carga de aplicación
  - Equilibradores de carga de puerta de enlace
  - Equilibrador de carga de red
- Amazon EMR
- AWS Glue
- AWS Lambda
- Amazon MQ con Apache MQ (no Rabbit MQ)
- Amazon MSK
- AWS Network Manager
  - AWS WAN en la nube de
  - Analizador de acceso a la red
  - Analizador de accesibilidad
- Amazon OpenSearch Service
- AWS PrivateLink†
- Amazon Relational Database Service (RDS)

- Amazon Redshift
- Amazon Route 53
- Estudio unificado de Amazon SageMaker
- AWS Transit Gateway
- Acceso verificado de AWS
- Amazon VPC
  - Intercambio de tráfico
  - Creación de reflejo de tráfico
- Amazon VPC Lattice

† Puede conectarse a todos los servicios de AWS que admiten PrivateLink mediante un punto de conexión de VPC en una VPC compartida. Para ver una lista de los servicios compatibles con PrivateLink, consulte Servicios de AWS que se integran con AWS PrivateLink en la Guía de AWS PrivateLink.

Esta lista tiene por objeto incluir todos los servicios que admiten el lanzamiento de recursos en subredes de VPC compartidas. A pesar de nuestros mejores esfuerzos, es posible que haya otros servicios que admitan el lanzamiento de recursos en subredes de VPC compartidas, pero no estén listados aquí. Le animamos a enviar comentarios sobre la documentación si tiene alguna pregunta.

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 coubicación 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.

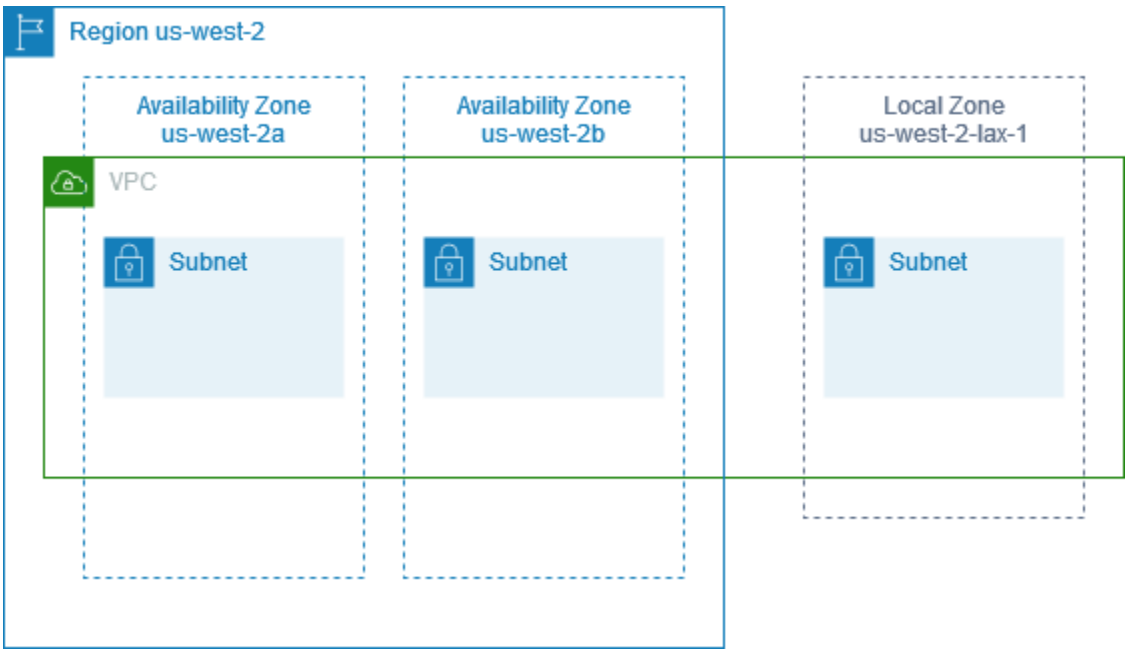
Subredes en AWS Local Zones

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. Cuando crea una subred en una Local Zone, extiende la VPC a esta Local Zone.

Para utilizar una Local Zone, debe seguir el siguiente proceso:

- Acceda a la Local Zone.
- Cree una subred en la zona local.
- Lance los recursos seleccionados en la subred de la Local Zone para que las aplicaciones estén más cerca de los usuarios.

El siguiente diagrama ilustra una VPC en la región Oeste de EE. UU. (Oregón) (`us-west-2`) que abarca zonas de disponibilidad y una Local Zone.



Al crear una VPC, puede optar por asignar un conjunto de direcciones IP públicas proporcionadas por Amazon a la VPC. También puede 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 tráfico de la red de la zona local irá directamente a Internet o a los puntos de presencia (PoP) sin atravesar la región principal de la zona local, lo que permite el acceso a la computación de baja latencia. Para obtener la lista completa de zonas locales y sus correspondientes regiones principales, consulte Zonas locales en la Guía del usuario de AWS Local Zones.

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.
- El tráfico de salida de Internet sale de una Local Zone de la Local Zone.
- 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`).
- Si la zona local admite IPv6, 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. Para ver la lista de

zonas locales que admiten IPv6, consulte Consideraciones en la Guía del usuario de AWS Local Zones

- No puede crear puntos de conexión de VPC en las subredes de la zona local.

Para obtener más información acerca del uso de Local Zones, consulte la Guía del usuario de AWS Local Zones.

Consideraciones para las puerta de enlaces 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”.

  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”.
- Puede utilizar puerta de enlaces 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 puerta de enlace de Internet”.

Acceder a Local Zones mediante una puerta de enlace 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 puerta de enlace privada virtual para la VPC asociada con la Local Zone para conectarse a una puerta de enlace de Direct Connect. La puerta de enlace de Direct Connect se conecta a una ubicación de Direct Connect de una región. El centro de datos en las instalaciones tiene una conexión de Direct Connect con la ubicación de Direct Connect.

> **Note**
>
> El tráfico destinado a una subred en una zona local mediante Direct Connect no viaja a través de la región principal de la zona local. En cambio, el tráfico toma la ruta más corta

hacia la zona local. Esto reduce la latencia y ayuda a que las aplicaciones tengan más capacidad de respuesta.

Se deben configurar los siguientes recursos para esta configuración:

- Una puerta de enlace 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 consola de Amazon VPC o utilizar el comando describe-subnets.

  Para obtener información acerca de cómo crear una puerta de enlace privada virtual, consulte Crear una puerta de enlace de destino en la Guía del usuario de AWS Site-to-Site VPN.
- Una conexión de Direct Connect. Para obtener el mejor rendimiento de latencia, AWS recomienda utilizar la ubicación de Direct Connect más cercana a la zona local en la que ampliará la subred.

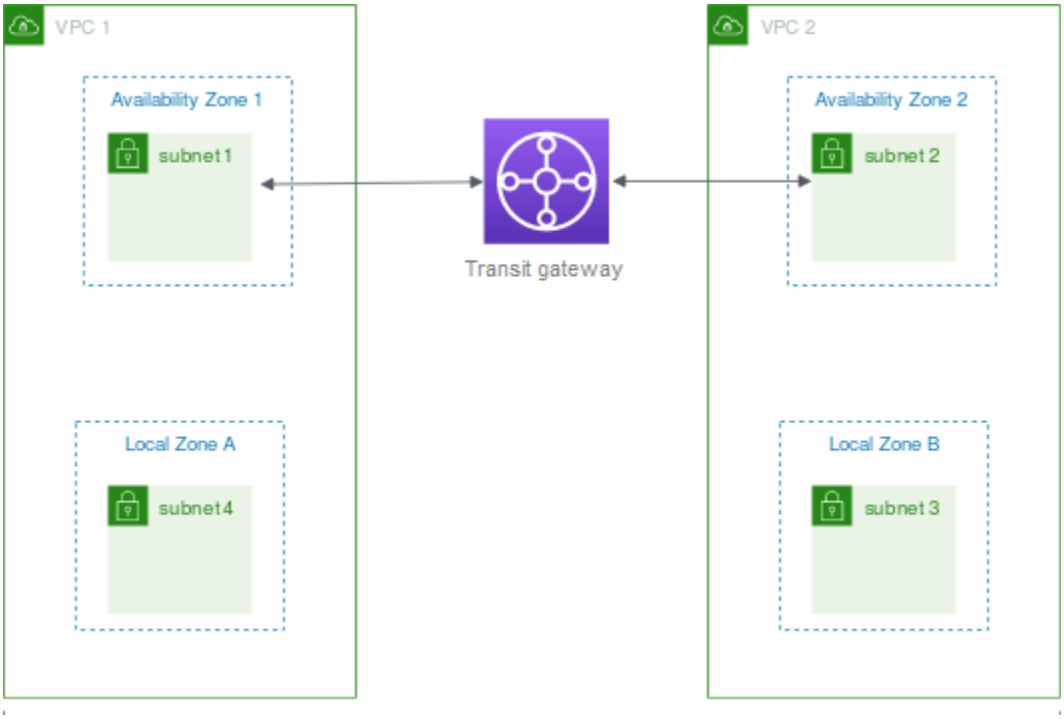
  Para obtener información acerca de cómo solicitar una conexión, consulte Conexiones cruzadas en la Guía del usuario de Direct Connect.
- Una puerta de enlace de Direct Connect. Para obtener información acerca de cómo crear una puerta de enlace de Direct Connect, consulte Crear una puerta de enlace de Direct Connect en la Guía del usuario de Direct Connect.
- Una asociación de puerta de enlace privada virtual para conectar la VPC a la puerta de enlace de Direct Connect. Para obtener información acerca de cómo crear una asociación de puerta de enlace privada virtual, consulte Asociación y desasociación de puerta de enlaces privadas virtuales en la Guía del usuario de Direct Connect.
- Una interfaz virtual privada en la conexión desde la ubicación de Direct Connect hasta el centro de datos en las instalaciones. Para obtener información acerca de cómo crear una puerta de enlace de Direct Connect, consulte Creación de una interfaz virtual privada para la puerta de enlace de Direct Connect en la Guía del usuario de Direct Connect.

Conectar las subredes de una zona local a una transit puerta de enlace

No se puede crear una conexión de puerta de enlace de tránsito 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 puerta de enlace de tránsito

> **Note**
>
> El tráfico destinado a una subred en una zona local que se origina en una puerta de enlace de tránsito atravesará primero la región principal.



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”.
- Una transit puerta de enlace. Para obtener más información, consulte Creación de Transit Gateway en Transit Gateways de Amazon VPC.
- Una conexión de puerta de enlace de tránsito para cada VPC mediante la zona de disponibilidad principal. Para obtener más información, consulte Creación de una conexión de puerta de enlace de tránsito a VPC en Transit Gateways de Amazon VPC.
- Una tabla de enrutamiento de la transit puerta de enlace asociada con la conexión de puerta de enlace de tránsito. Para obtener más información, consulte Tablas de enrutamiento de Transit Gateway en Transit Gateways de Amazon VPC.

- Para cada VPC, una entrada en la subred de la tabla de enrutamiento de las subredes de la zona local que tiene el otro CIDR de la VPC como destino, y el ID de la interfaz de red de la conexión de puerta de enlace de tránsito como destino. A fin de buscar la interfaz de red para la conexión de puerta de enlace de tránsito, busque en las descripciones de las interfaces de red el ID de la conexión de puerta de enlace de tránsito. Para obtener más información, consulte the section called “Enrutar para una transit puerta de enlace”.

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

Destino	Objetivo
CIDR de VPC 1	*local*
CIDR de VPC 2	*vpc1-attachment-network-interface-id*

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

Destino	Objetivo
CIDR de VPC 2	*local*
CIDR de VPC 1	*vpc2-attachment-network-interface-id*

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

CIDR	Conexión	Tipo de ruta
CIDR de VPC 1	*Conexión de la VPC 1*	propagada
		propagada

CIDR	Conexión	Tipo de ruta
CIDR de VPC 2	*Conexión de la VPC 2*	

Subredes en AWS 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 nube privada virtual (VPC) a una o varias zonas de Wavelength y, a continuación, utilizar recursos de AWS como instancias de Amazon EC2 para ejecutar aplicaciones que requieren una latencia extremadamente baja y conectarse a los servicios de 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 puerta de enlaces 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 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 puerta de enlace de operador utiliza la dirección para el tráfico desde la interfaz a Internet o dispositivos móviles. La puerta de enlace 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 puerta de enlace 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 puerta de enlace 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 puerta de enlace de tránsito 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 puerta de enlace. 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 puerta de enlace 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”. Utilice el comando describe-availability-zones para encontrar la zona principal.
- Una transit puerta de enlace. La transit puerta de enlace conecta las VPC. Para obtener información acerca de cómo crear una transit puerta de enlace, consulte Crear una transit puerta de enlace en la Guía de transit puerta de enlaces de Amazon VPC.
- Para cada VPC, hay una conexión de VPC a la transit puerta de enlace en la zona de disponibilidad principal de la zona de Wavelength. Para obtener más información, consulte

Creación de una conexión de puerta de enlace de tránsito a VPC en Guía de Transit Gateways de Amazon VPC.

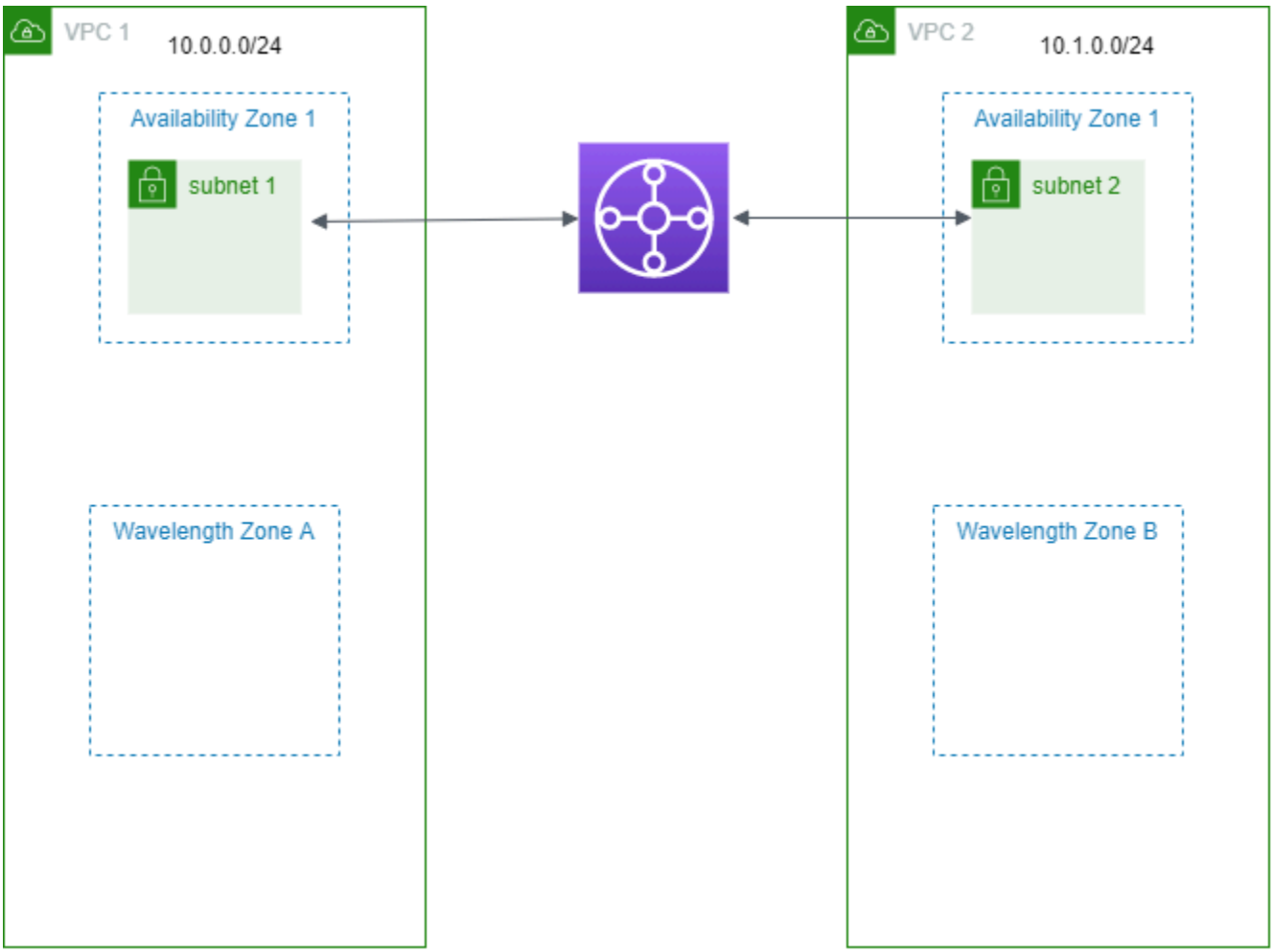
- Entradas para cada VPC en la tabla de enrutamiento de la transit puerta de enlace. Para obtener información acerca de cómo crear rutas de transit puerta de enlace, consulte Tablas de enrutamiento de la transit puerta de enlace en la Guía de transit puerta de enlace de Amazon VPC.
- Para cada VPC, una entrada en la tabla de enrutamiento de la VPC que tiene el otro CIDR de la VPC como destino y el ID de transit puerta de enlace como destino. Para obtener más información, consulte the section called “Enrutar para una transit puerta de enlace”.

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

Destino	Objetivo
10.1.0.0/24	tgw-22222222222222222

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

Destino	Objetivo
10.0.0.0/24	tgw-22222222222222222



Subredes en AWS Outposts

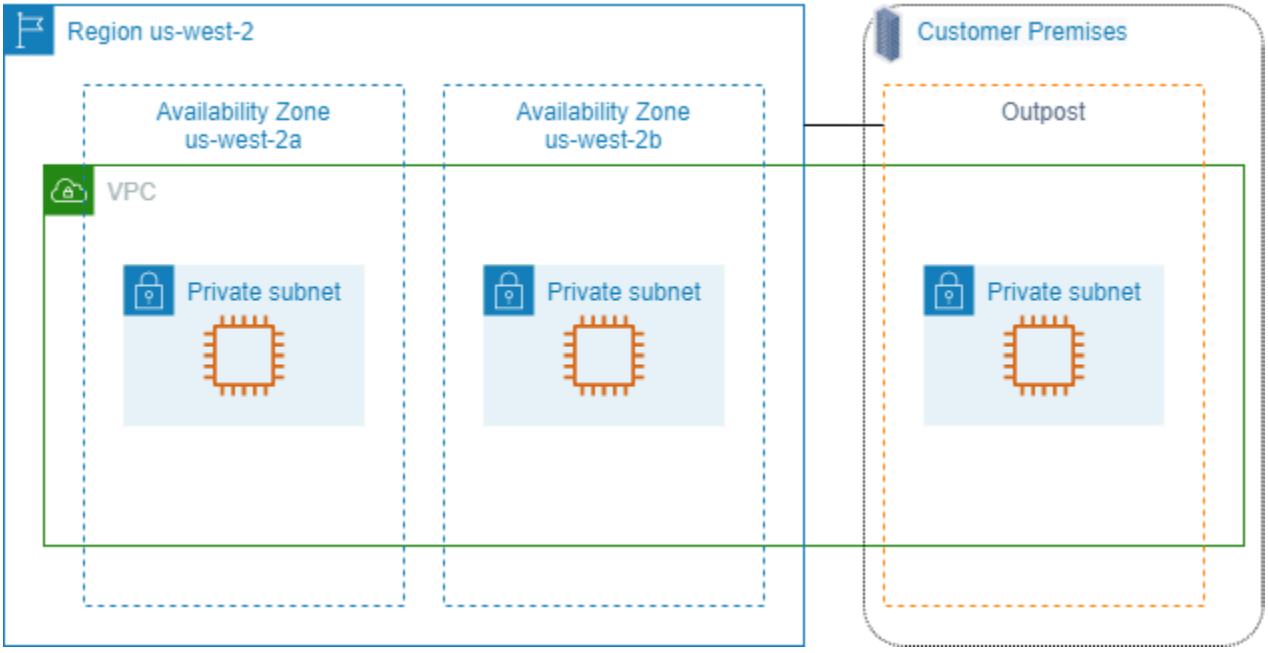
AWS Outposts le ofrece las mismas herramientas, API, servicios e infraestructura de hardware de AWS para crear y ejecutar sus aplicaciones en las instalaciones y en la nube. AWS Outposts es ideal para cargas de trabajo que necesitan acceso de baja latencia a los sistemas o las aplicaciones en las instalaciones, 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.

Una VPC abarca todas las zonas de disponibilidad de una región de AWS. Tras conectar el Outpost a su región principal, puede extender cualquier VPC de la región a su Outpost al crear una subred para el Outpost en esa VPC.

Las siguientes reglas se aplican a AWS Outposts:

- Las subredes deben residir en una ubicación de Outpost.

- Para agregar una subred para un Outpost, especifique el nombre de recurso de Amazon (ARN) del Outpost al crear la subred.
- Bastidor de Outposts: una puerta de enlace local gestiona la conectividad de red entre la VPC y las redes en las instalaciones. Para obtener más información, consulte Puertas de enlace locales en la Guía del usuario de AWS Outposts para bastidores de Outposts.
- Servidores de Outposts: una interfaz de red local gestiona la conectividad de red entre la VPC y las redes en las instalaciones. Para obtener más información, consulte Interfaces de red locales en la Guía del AWS Outposts usuario para servidores de Outposts.
- De forma predeterminada, cada subred que crea en una VPC, incluidas subredes para sus Outposts, se asocia implícitamente a la tabla de enrutamiento principal de la VPC principal. De manera alternativa, también puede asociar de manera explícita una tabla de enrutamiento personalizada a las subredes de la VPC y tener una puerta de enlace local como destino del siguiente salto para todo el tráfico destinado a su red en las instalaciones.



Eliminar su VPC

Cuando ya no necesite una VPC, puede eliminarla.

Requisito

Para poder eliminar una VPC, primero debe terminar o eliminar cualquier recurso que haya creado una interfaz de red administrada por el solicitante en la VPC. Por ejemplo, debe terminar las

instancias de EC2 y eliminar los equilibradores de carga, las puertas de enlace NAT, las conexiones de VPC de la puerta de enlace de tránsito y los puntos de conexión de VPC de la interfaz.

> **Note**
>
> Si ha creado un registro de flujo para la VPC que va a eliminar, tenga en cuenta que los registros de flujo de las VPC eliminadas finalmente se eliminan automáticamente.

Contenido

- Eliminación de una VPC mediante la consola
- Eliminación de una VPC mediante la línea de comandos

Eliminación de una VPC mediante la consola

Si elimina una VPC mediante la consola de Amazon VPC, también se eliminan los siguientes componentes de VPC en su nombre:

- Opciones de DHCP
- Puerta de enlace de Internet de solo salida
- Puntos de enlace de gateway
- Gateways de Internet
- ACL de red
- Tablas de enrutamiento
- Grupos de seguridad
- Subredes

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 una instancia en la Guía del usuario de Amazon EC2.
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 hay recursos que debe eliminar o terminar antes de que se elimine la VPC, se los mostraremos. Elimine o termine estos recursos e inténtelo de nuevo. De lo contrario, se mostrarán los recursos que se eliminarán junto con la VPC. Revise la lista y continúe con el siguiente paso.
7. (Opcional) Si tiene una conexión de Site-to-Site VPN, puede seleccionar la opción para eliminarla. 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.
8. Cuando le pidan confirmación, escriba **`delete`** y elija Eliminar.

Eliminación de una VPC mediante la línea de comandos

Antes de poder eliminar una VPC mediante la línea de comandos, debe finalizar o eliminar cualquier recurso que haya creado una interfaz de red administrada por el solicitante en la VPC. También debe eliminar o desvincular todos los recursos de la VPC que haya creado, como subredes, grupos de seguridad, ACL de red, tablas de enrutamiento, puertas de enlace de Internet y puertas de enlace de Internet de solo salida. No es necesario que elimine el grupo de seguridad, la tabla de enrutamiento ni la ACL de red predeterminados.

En el siguiente procedimiento se muestran los comandos usados para eliminar los recursos comunes de VPC y luego, eliminar la VPC. Debe utilizar estos comandos en este orden. Si creó recursos adicionales de VPC, también deberá utilizar el comando de eliminación correspondiente antes de eliminar la VPC.

Para eliminar una VPC mediante la AWS CLI

1. Elimine el grupo de seguridad mediante el comando delete-security-group.

```
aws ec2 delete-security-group --group-id sg-id
```

2. Elimine cada ACL de red mediante el comando delete-network-acl.

```
aws ec2 delete-network-acl --network-acl-id acl-id
```

3. Elimine cada subred mediante el comando delete-subnet.

```
aws ec2 delete-subnet --subnet-id subnet-id
```

4. Elimine cada tabla de enrutamiento personalizada mediante el comando delete-route-table.

```
aws ec2 delete-route-table --route-table-id rtb-id
```

5. Desconecte la puerta de enlace de Internet de la VPC mediante el comando detach-internet-gateway.

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-id --vpc-id vpc-id
```

6. Elimine la puerta de enlace de Internet mediante el comando delete-internet-gateway.

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-id
```

7. [VPC de doble pila] Elimine la puerta de enlace de Internet de solo salida mediante el comando delete-egress-only-internet-gateway.

```
aws ec2 delete-egress-only-internet-gateway --egress-only-internet-gateway-id eigw-id
```

8. Elimine la VPC mediante el comando delete-vpc.

```
aws ec2 delete-vpc --vpc-id vpc-id
```

Se puede generar infraestructura como código a partir de las acciones de su consola de VPC con Console-to-Code

La consola proporciona una ruta guiada para crear recursos y probar prototipos. Si desea crear los mismos recursos a escala, necesitará un código de automatización. Console-to-Code es una característica de Amazon Q Developer que puede ayudarlo a empezar a usar el código de automatización. Console-to-Code registra las acciones de la consola, incluidos los valores predeterminados y los parámetros compatibles. A continuación, utiliza la IA generativa para sugerir código en el formato de infraestructura como código (IaC) que prefiera para las acciones que desee. Como el flujo de trabajo de la consola garantiza que los valores de los parámetros que especifique sean válidos juntos, el código que genere mediante el uso de Console-to-Code tiene valores de parámetros compatibles. Puede usar el código como punto de partida y luego personalizarlo para que esté listo para producción en función de su caso de uso específico.

Por ejemplo, Console-to-Code, le permite grabarse con la consola de VPC para crear subredes, grupos de seguridad, NACL, una tabla de enrutamiento personalizada y una puerta de enlace de Internet, y generar código en formato CloudFormation JSON. Luego, puede copiar ese código y personalizarlo para usarlo en su plantilla CloudFormation.

Actualmente, Console-to-Code puede generar infraestructura como código (IaC) en los siguientes formatos e idiomas:

- Java de CDK
- Python de CDK
- TypeScript de CDK
- JSON de CloudFormation
- YAML de CloudFormation

Para obtener más información e instrucciones sobre cómo utilizar Console-to-Code, consulte Automatización de servicios AWS con Console-to-Code de Amazon Q Developer en la Guía del usuario de Amazon Q Developer.

Subredes para la VPC

Una subred es un rango de direcciones IP en su VPC. Puede crear recursos de AWS, como instancias de EC2, en subredes específicas.

Contenido

- Conceptos básicos sobre subredes
- Seguridad de la subred
- Crear una subred
- Adición o eliminación de un bloque de CIDR de IPv6 en su subred
- Modificación de los atributos de las direcciones IP de sus subredes
- Reservas de CIDR de subred
- Configurar tablas de enrutamiento
- Asistente de enrutamiento de Middlebox
- Eliminar una subred

Conceptos básicos sobre subredes

Cada subred debe residir enteramente en una zona de disponibilidad y no puede abarcar otras zonas. Si lanza recursos de AWS en diferentes zonas de disponibilidad, puede proteger sus aplicaciones de errores que se produzcan en una única zona de disponibilidad.

Contenido

- Rango de direcciones IP de una subred
- Tipos de subred
- Diagrama de la subred
- Enrutar la subred
- Configuración de subredes

Rango de direcciones IP de una subred

Al crear una subred, debe especificar sus direcciones IP, según la configuración de la VPC:

- Solo IPv4: la subred tiene un bloque de CIDR IPv4 pero no tiene un bloque de CIDR IPv6. Los recursos de una subred solo de IPv4 deben comunicarse a través de IPv4.
- Doble pila: la subred tiene un bloque de CIDR IPv4 y un bloque de CIDR IPv6. La VPC debe tener tanto un bloque de CIDR IPv4 como un bloque de CIDR IPv6. Los recursos de una subred de doble pila se pueden comunicar mediante IPv4 e IPv6.
- Solo IPv6: la subred tiene un bloque de CIDR IPv6 pero no tiene un bloque de CIDR IPv4. La VPC debe tener un bloque de CIDR IPv6. Los recursos de una subred solo de IPv6 deben comunicarse a través de IPv6.

> **Note**
>
> A los recursos de las subredes exclusivas de IPv6 se les asignan direcciones locales de enlace IPv4 desde el bloque de CIDR 169.254.0.0/16. Estas direcciones se utilizan para comunicarse con los servicios que solo están disponibles en la VPC. Para ver ejemplos, consulte las Direcciones de enlace local en la Guía del usuario de Amazon EC2.

Para obtener más información, consulte Direccionamiento IP para VPC y subredes.

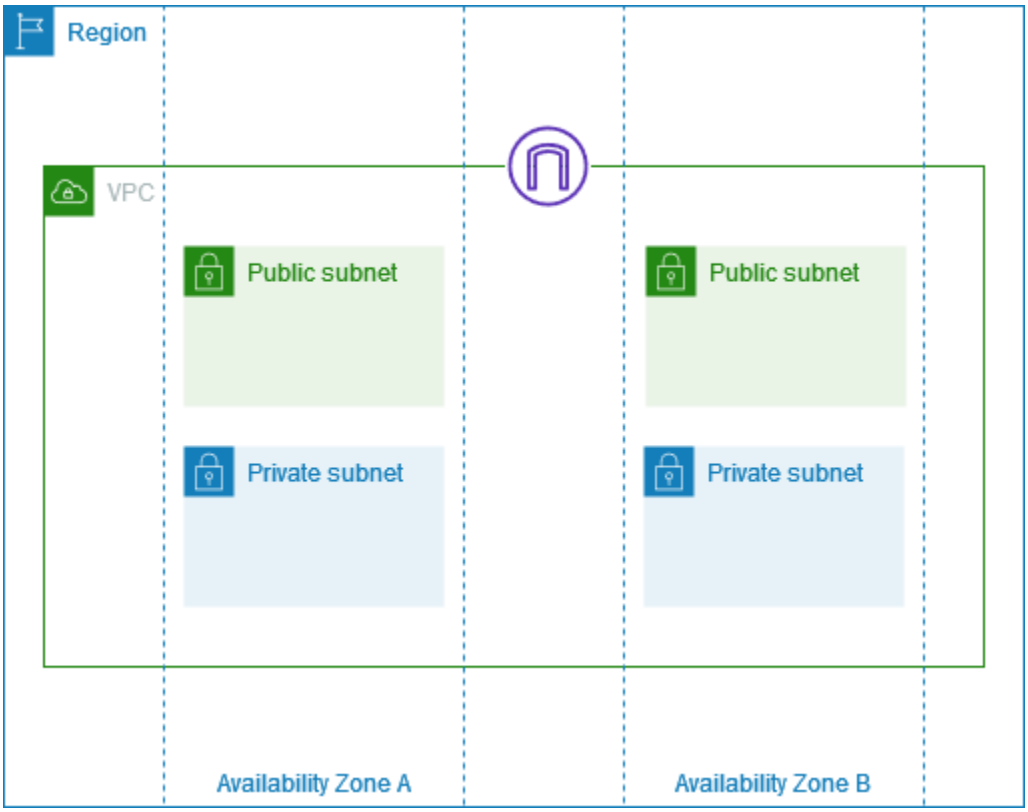
Tipos de subred

El tipo de subred viene determinado por cómo configure el enrutamiento para sus subredes. Por ejemplo:

- Subred pública: la subred tiene una ruta directa a una puerta de enlace de Internet. Los recursos de una subred pública pueden acceder a la Internet pública.
- Subred privada: la subred no tiene una ruta directa a una puerta de enlace de Internet. Los recursos de una subred privada requieren un dispositivo NAT para acceder a la Internet pública.
- Subred solo de VPN: la subred tiene una ruta a una conexión de Site-to-Site VPN mediante una puerta de enlace privada virtual. La subred no tiene una ruta a una puerta de enlace de Internet.
- Subred aislada: la subred no tiene rutas a destinos fuera de su VPC. Los recursos de una subred aislada solo pueden acceder o ser accesibles por otros recursos de la misma VPC.
- Subred de EVS: este tipo de subred se crea mediante Amazon EVS. Para obtener más información, consulte Subred de VLAN en la Guía del usuario de Amazon EVS.

Diagrama de la subred

En el siguiente diagrama se muestra una VPC con subredes en dos zonas de disponibilidad y una puerta de enlace de Internet. Cada zona de disponibilidad tiene una subred pública y una subred privada.



Para consultar diagramas que muestren subredes en zonas locales y zonas de Wavelength, consulte Cómo funcionan las zonas locales de AWS y Cómo funcionan las zonas de AWS Wavelength Wavelength.

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.

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 (por ejemplo, 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.

Después de crear una subred, puede modificar la siguiente configuración:

- 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, consulte Tipos de nombres de host de instancias de Amazon EC2 en la Guía del usuario de Amazon EC2.

Seguridad de la subred

Para proteger sus recursos de AWS, le recomendamos que utilice subredes privadas. Utilice un host bastión o dispositivo NAT para proporcionar acceso a Internet a los recursos, como instancias EC2, en una subred privada.

AWS proporciona funciones que se pueden utilizar para aumentar la seguridad de los recursos de la VPC. Los grupos de seguridad permiten tráfico entrante y saliente para recursos asociados, tales como instancias EC2. Las ACL de red permiten o deniegan el tráfico entrante y saliente en el nivel de subred. En la mayoría de los casos, los grupos de seguridad pueden satisfacer sus necesidades. No obstante, puede utilizar ACL de red si desea una capa de seguridad adicional. Para obtener más información, consulte the section called “Comparar grupos de seguridad y ACL de red”.

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. La ACL de red predeterminada permite el tráfico de entrada y de salida. Puede actualizar la ACL de red predeterminada, o bien crear ACL de red personalizadas y asociarlas a sus subredes. Para obtener más información, consulte Control del tráfico de la subred con listas de control de acceso a la red.

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.

Crear una subred

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

Consideraciones

- Debe especificar un bloque de CIDR IPv4 para la subred del rango de su VPC. También puede especificar un bloque de CIDR IPv6 para una subred si existe un bloque de CIDR IPv6 asociado a la VPC. Para obtener más información, consulte Direccionamiento IP para VPC y subredes.
- 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 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).
3. Elija Create subnet (Crear subred).
4. En ID de 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. En Bloque de CIDR de IPv4, seleccione Entrada manual a fin de ingresar un bloque de CIDR de IPv4 para su subred (por ejemplo, `10.0.1.0/24`) o seleccione Sin CIDR de IPv4. Si utiliza el Administrador de direcciones IP (IPAM) de Amazon VPC para planificar, rastrear y monitorear las direcciones IP de las cargas de trabajo de AWS, al crear una subred tiene la opción de asignar un bloque de CIDR desde el IPAM (asignado por el IPAM). A fin de obtener más información sobre la planificación del espacio de direcciones IP de la VPC para las asignaciones de IP de subred, consulte Tutorial: Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred en la Guía del usuario de IPAM de Amazon VPC.

8. En Bloque de CIDR de IPv6, seleccione Entrada manual para elegir el CIDR de IPv6 de la VPC en el que desea crear una subred. Esta opción solo está disponible si la VPC tiene un bloque de CIDR IPv6 asociado. Si utiliza el Administrador de direcciones IP (IPAM) de Amazon VPC para planificar, rastrear y monitorear las direcciones IP de las cargas de trabajo de AWS, al crear una subred tiene la opción de asignar un bloque de CIDR desde el IPAM (asignado por el IPAM). A fin de obtener más información sobre la planificación del espacio de direcciones IP de la VPC para las asignaciones de IP de subred, consulte Tutorial: Planificar el espacio de direcciones IP de la VPC para las asignaciones de IP de subred en la Guía del usuario de IPAM de Amazon VPC.
9. Elija un Bloque de CIDR de IPv6 de VPC.
10. En Bloque de CIDR de IPv6 de subred, elija un CIDR para la subred que sea igual o más específico que el CIDR de VPC. Por ejemplo, si el CIDR del grupo de VPC es /50, puede elegir una longitud de máscara de red entre /50 y /64 para la subred. Las longitudes posibles de las máscaras de red IPv6 oscilan entre /44 y /64 en incrementos de /4.
11. Elija Create subnet (Crear subred).

Para agregar una subred a su VPC mediante la AWS CLI

Utilice el comando create-subnet.

Pasos a seguir a continuación

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

- Configurar el enrutamiento. A continuación, puede crear una tabla de enrutamiento y una ruta personalizadas que envíen 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.
- 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 Modificación de los atributos de las direcciones IP de sus subredes.
- Modifique la configuración del nombre basado en recursos (RBN). Para obtener más información, consulte Tipos de nombres de host de instancias de Amazon EC2.
- Cree o modifique sus ACL de la red. Para obtener más información, consulte Control del tráfico de la subred con listas de control de acceso a la red.
- Compartir la subred con otras cuentas. Para obtener más información, consulte ???.

Adición o eliminación de un bloque de CIDR de IPv6 en su subred

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

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

Antes de eliminar un bloque CIDR de IPv6, primero debe anular la asignación de las direcciones IPv6 asignadas a las instancias de su subred.

Pasos para agregar o eliminar un bloque de CIDR de IPv6 en su subred

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Subnets (Subredes).
3. Seleccione su subred y elija Actions (Acciones), Edit IPv6 CIDRs (Editar CIDR IPv6).
4. Para agregar un CIDR, seleccione Agregar CIDR de IPv6, elija un bloque de CIDR de la VPC, ingrese un bloque de CIDR de subred y seleccione una longitud de la máscara de red que sea igual o más específica que la del CIDR de la VPC. Por ejemplo, si el CIDR del grupo de VPC es /50, puede elegir una longitud de máscara de red entre /50 y /64 para la subred. Las longitudes posibles de las máscaras de red IPv6 oscilan entre /44 y /64 en incrementos de /4.
5. Para eliminar un CIRD, busque el bloque de CIRD de IPv6 y seleccione Eliminar.
6. Seleccione Save.

Para asociar un bloque CIDR de IPv6 a una subred mediante la AWS CLI

Utilice el comando associate-subnet-cidr-block.

Para desasociar un bloque CIDR de IPv6 de una subred mediante la AWS CLI

Utilice el comando disassociate-subnet-cidr-block.

Modificación de los atributos de las direcciones IP de sus subredes

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.

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.

Pasos para modificar el comportamiento de las direcciones IP 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 (Subredes).
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.
5. 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.

Para modificar un atributo de subred mediante la AWS CLI

Utilice el comando modify-subnet-attribute.

Reservas de CIDR de subred

Una reserva de subred de CIDR es un rango de direcciones IPv4 o IPv6 que se deja de lado para que AWS no los asigne a interfaces de red. Esto permite reservar bloques de CIDR de IPv4 o IPv6 (también llamados “prefijos”) para utilizarlos con las interfaces de red.

Cuando crea la reserva CIDR de subred, debe especificar cómo va a utilizar las direcciones IP reservadas. Están disponibles las siguientes opciones:

- Prefijo: le permite asignar un prefijo a una única interfaz de red. 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.
- Explícito: le permite asignar manualmente una dirección IP individual a una única interfaz de red.

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

- Al crear una reserva CIDR de subred, el rango de dirección IP puede incluir direcciones que ya están en uso. La creación de una reserva de subred no anula la asignación de ninguna dirección IP que ya esté en uso.
- Puede reservar varios rangos de CIDR por subred. Cuando se reservan varios rangos de CIDR dentro de la misma VPC, los rangos de CIDR no pueden superponerse.
- 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.
- Al eliminar una reserva de subred, las direcciones IP no utilizadas están disponibles para que AWS las asigne a sus interfaces de red. La eliminación de una reserva de subred no anula la asignación de ninguna dirección IP que esté en uso.
- El tipo de reserva afecta el recuento de direcciones IP disponibles para la subred. Si crea una reserva de prefijos, el recuento disminuye inmediatamente. Si crea una reserva de prefijos explícita, el recuento disminuye cuando se asignan las direcciones IP.

Para obtener más información acerca de la notación de enrutamiento entre dominios sin clases (CIDR), consulte Direccionamiento IP.

Contenido

- Trabaje con reservas de CIDR de subred mediante la consola

- Trabajar con reservas de CIDR de subred mediante la AWS CLI

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 (Subredes).
3. Seleccione la subred.
4. Seleccione la pestaña Reservas de CIDR para obtener información sobre cualquier reserva de CIDR de subred existente.
5. Para añadir o eliminar reservas de CIDR de subred, seleccione Acciones, Editar reservas de CIDR y, a continuación, haga 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 del CIDR, seleccione Quitar en la reserva de CIDR de subred.

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
- Cómo visualizar las reservas de CIDR de subred
- Cómo eliminar una reserva de CIDR de subred

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
```

Configurar tablas de enrutamiento

Una tabla de enrutamiento funciona como el controlador de tráfico de su nube privada virtual (VPC). Cada tabla de enrutamiento contiene conjuntos de reglas, denominadas rutas, que determinan adónde se dirige el tráfico de red desde la subred o puerta de enlace. Cuando crea una VPC, también creamos la tabla de enrutamiento principal de la VPC. Puede crear tablas de enrutamiento adicionales para su VPC, de modo que tenga un control más detallado sobre las rutas de red de su VPC.

Puede usar tablas de enrutamiento para especificar con qué redes se puede comunicar su VPC, como otras VPC o redes en las instalaciones. Cada ruta especifica un destino (bloque CIDR o lista

de prefijos) y un destino (como una puerta de enlace de Internet, una puerta de enlace NAT, una conexión de emparejamiento de VPC o una conexión de VPN). El tráfico se enruta a los destinos en función de su dirección IP de destino. Las tablas de enrutamiento le permiten crear arquitecturas de red complejas que incluyen subredes públicas, subredes privadas, subredes exclusivas de VPN y subredes aisladas.

Contenido

- Conceptos de las tablas de enrutamiento
- Tablas de enrutamiento de subred
- Tablas de ruteo de puerta de enlace
- Cómo funciona la prioridad de enrutamiento
- Opciones de enrutamiento de ejemplo
- Creación de una tabla de enrutamiento personalizada para su VPC
- Administración de las tablas de enrutamiento de subred
- Sustituir la tabla de enrutamiento principal
- Control del tráfico que ingresa a la VPC mediante una tabla de enrutamiento de puerta de enlace
- Reemplazar o restaurar el destino de una ruta local
- Enrutamiento avanzado con la VPC
- Solución de problemas de accesibilidad en su VPC

Conceptos de las tablas de enrutamiento

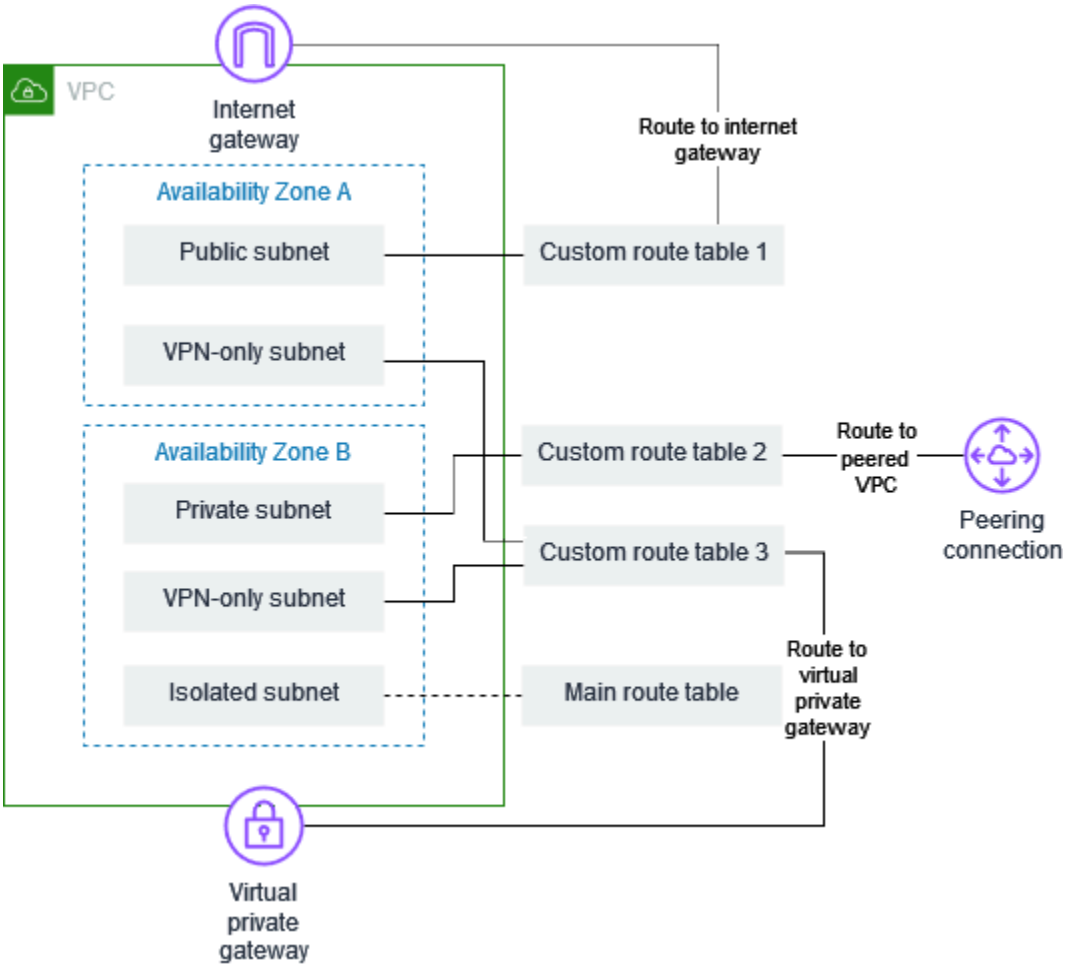
A continuación se enumeran los conceptos clave de las tablas de enrutamiento:

- 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 enrutamiento.
- 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 puerta de enlace, interfaz de red o conexión a través de la cual enviar el tráfico de destino, por ejemplo, una puerta de enlace de Internet.
- Ruta local: una ruta predeterminada para la comunicación dentro de la VPC. Si la VPC tiene direcciones IPv4 e IPv6, hay una ruta local para IPv4 y una ruta local para IPv6.

- Asociación de tabla de enrutamiento: la asociación entre una tabla de enrutamiento y una subred, puerta de enlace de Internet o puerta de enlace privada virtual.
- Tabla de enrutamiento de subred: una tabla de enrutamiento asociada con una subred.
- Propagación: si ha asociado una puerta de enlace privada virtual a la VPC y ha habilitado la propagación de rutas, agregamos automáticamente rutas para la conexión de su VPN a las tablas de enrutamiento de la subred. Esto significa que no es necesario agregar o eliminar rutas de VPN manualmente. Para obtener más información, consulte Opciones de enrutamiento de Site-to-Site VPN en la Guía del usuario de Site-to-Site VPN.
- Tabla de enrutamiento de puerta de enlace: una tabla de enrutamiento asociada con una puerta de enlace de Internet o puerta de enlace 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 enrutamiento a la puerta de enlace de Internet o a la puerta de enlace privada virtual y especifique la interfaz de red del dispositivo como objetivo para el tráfico de la VPC.
- Tabla de enrutamiento de la transit puerta de enlace: una tabla de enrutamiento asociada con una transit puerta de enlace. Para obtener más información, consulte Tablas de enrutamiento de Transit Gateway en Transit Gateways de Amazon VPC.
- Tabla de enrutamiento de puerta de enlace local: una tabla de enrutamiento asociada con una puerta de enlace local de Outposts. Para obtener más información, consulte Gateways locales en la Guía del usuario de AWS Outposts.

VPC de ejemplo con tablas de enrutamiento

En el siguiente diagrama se muestra una VPC con cinco subredes, una tabla de enrutamiento principal y tres tablas de enrutamiento personalizadas. Las cuatro tablas de enrutamiento tienen rutas locales. La tabla de enrutamiento personalizada 1 tiene un enrutamiento a una puerta de enlace de Internet y está asociada a la subred pública de la zona de disponibilidad A. La tabla de enrutamiento personalizada 2 tiene un enrutamiento a una VPC interconectada y está asociada a la subred privada de la zona de disponibilidad B. La tabla de enrutamiento personalizada 3 tiene un enrutamiento a una puerta de enlace privada virtual y está asociada a las subredes exclusivas de VPN en ambas zonas de disponibilidad.



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 enrutamiento que controla el direccionamiento de la subred (tabla de enrutamiento de la subred). Puede asociar de forma explícita una subred con una tabla de enrutamiento particular. De lo contrario, la subred se asocia de forma implícita con la tabla de enrutamiento principal. La subred solo puede asociarse a una tabla de enrutamiento a la vez. Sin embargo, puede asociar varias subredes a la misma tabla de enrutamiento de la subred.

Contenido

- Rutas
- Tabla de enrutamiento principal
- Tablas de enrutamiento personalizadas
- Asociar una subred a la tabla de enrutamiento

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 puerta de enlace de Internet, añada la siguiente ruta a su tabla de enrutamiento de la subred. El destino de la ruta es `0.0.0.0/0`, que representa todas las direcciones IPv4. El objetivo es la puerta de enlace de Internet que se conecta a su VPC.

Destino	Objetivo
0.0.0.0/0	*igw-id*

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 para agruparlos. A continuación, puede especificar la lista de prefijos como destino en la entrada de la tabla de enrutamiento.

Cada tabla de enrutamiento 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 CAD 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. Puede reemplazar o restaurar el destino de cada ruta local según sea necesario.

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 puerta de enlace NAT, una interfaz de red o un punto de enlace del equilibrador de carga de la puerta de enlace.
- 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: 169.254.168.0/22. Este rango se encuentra dentro del espacio de direcciones locales de enlace 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 instancias (IMDS)

y el servidor DNS de Amazon. Puede utilizar un bloque de CIDR que sea mayor que el rango 169.254.168.0/22, pero se solape con este. No obstante, los paquetes destinados a las direcciones de 169.254.168.0/22 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 instancias (IMDS) y el servidor DNS de Amazon. Puede utilizar un bloque de CIDR que sea mayor que el rango fd00:ec2::/32, pero se solape con este. No obstante, 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”.

Ejemplo

En el siguiente ejemplo, suponga que la VPC tiene tanto un bloque de CIDR IPv4 como un bloque de CIDR IPv6. El tráfico IPv4 e IPv6 se tratan por separado, como se muestra en la siguiente tabla de enrutamiento.

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-aabbccddee1122334

- El tráfico IPv4 que se enrutará dentro de la VPC (10.0.0.0/16) está cubierto por la ruta Local.
- El tráfico IPv6 que se enrutará dentro de la VPC (2001:db8:1234:1a00::/56) está cubierto por la ruta Local.
- La ruta para 172.31.0.0/16 envía tráfico a una conexión de emparejamiento.

- La ruta de todo el tráfico IPv4 (0.0.0.0/0) envía el tráfico a una puerta de enlace de Internet. Por lo tanto, todo el tráfico IPv4, excepto el tráfico dentro de la VPC y hacia la interconexión, se enruta a la puerta de enlace de Internet.
- La ruta para todo el tráfico IPv6 (::/0) envía tráfico a una puerta de enlace de Internet de solo salida. Por lo tanto, todo el tráfico IPv6, excepto el tráfico dentro de la VPC, se enruta a la puerta de enlace de Internet de solo salida.

Tabla de enrutamiento principal

Al crear una VPC, esta cuenta de manera automática con una tabla de enrutamiento 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 enrutamiento) de la consola de Amazon VPC, puede consultar la tabla de enrutamiento de una 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 enrutamiento principal contiene sólo una ruta local. Si Creación de una VPC y elija una puerta de enlace NAT, Amazon VPC añade automáticamente rutas a la tabla de enrutamiento principal de las puertas de enlace.

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

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

  Es posible que desee hacerlo si cambia qué tabla es la tabla de enrutamiento principal. Cuando modifica la tabla que se considerará como tabla de enrutamiento 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 enrutamiento. Para obtener más información, consulte Sustituir la tabla de enrutamiento principal.

Tablas de enrutamiento personalizadas

De forma predeterminada, una tabla de enrutamiento contiene una ruta local para la comunicación dentro de la VPC. Si Creación de una VPC y elija una subred pública, Amazon VPC crea una tabla de enrutamiento personalizada y agrega una ruta que apunta a la puerta de enlace de Internet. Una forma de proteger la VPC es dejar la tabla de enrutamiento 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 enrutamiento personalizada. Sólo puede eliminar una tabla de enrutamiento personalizada si no tiene asociaciones.

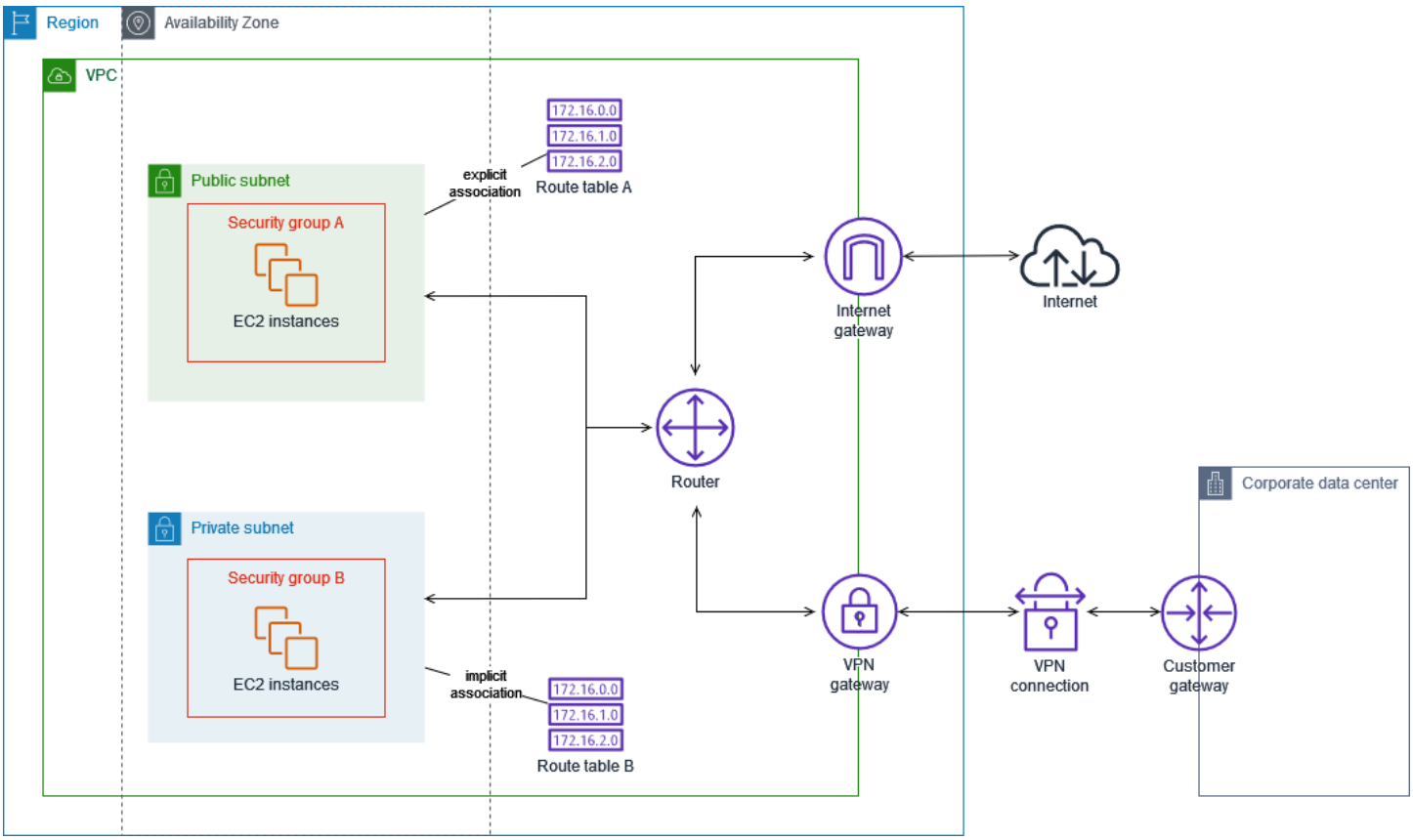
Asociar una subred a la tabla de enrutamiento

Cada subred de su VPC debe estar asociada a una tabla de enrutamiento. Una subred se puede asociar de forma explícita a la tabla de enrutamiento personalizada o de manera implícita o explícita a la tabla de enrutamiento principal. Para obtener más información sobre la visualización de las asociaciones de la subred y la tabla de enrutamiento, consulte Determinación de las asociaciones explícitas.

Las subredes que se encuentran en VPC asociadas a Outposts pueden tener un tipo de objetivo adicional de una puerta de enlace 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 puerta de enlace de Internet, una puerta de enlace privada virtual, una subred pública y una subred de solo VPN.



La tabla de enrutamiento A es una tabla de enrutamiento personalizada asociada de forma explícita a la subred pública. Tiene una ruta que envía todo el tráfico a la puerta de enlace de Internet, que es lo que convierte a la subred en una subred pública.

Destino	Objetivo
CIDR DE VPC	Local
0.0.0.0/0	*igw-id*

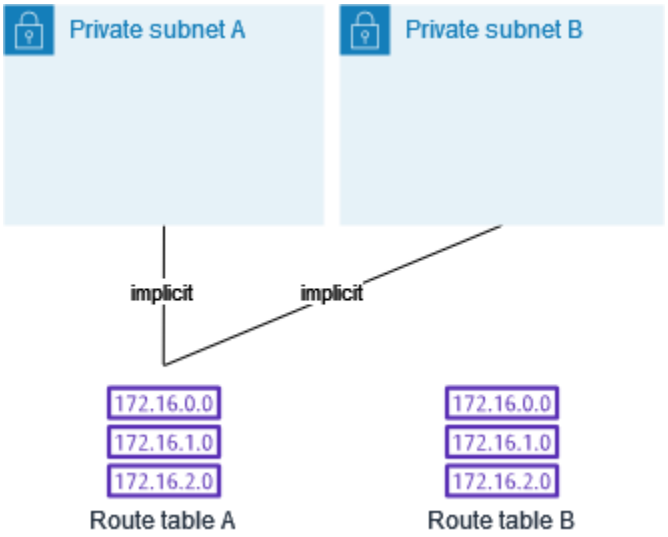
La tabla de enrutamiento B es la tabla de enrutamiento principal. Está asociado implícitamente a la subred privada. Tiene una ruta que envía todo el tráfico a la puerta de enlace privada virtual, pero ninguna ruta a la puerta de enlace de Internet, que es lo que hace que la subred sea una subred solo de VPN. Si crea otra subred en esta VPC y no asocia una tabla de enrutamiento personalizada, la subred también se asociará implícitamente con esta tabla de enrutamiento porque es la tabla de rutas principal.

Destino	Objetivo
CIDR DE VPC	Local
0.0.0.0/0	*vgw-id*

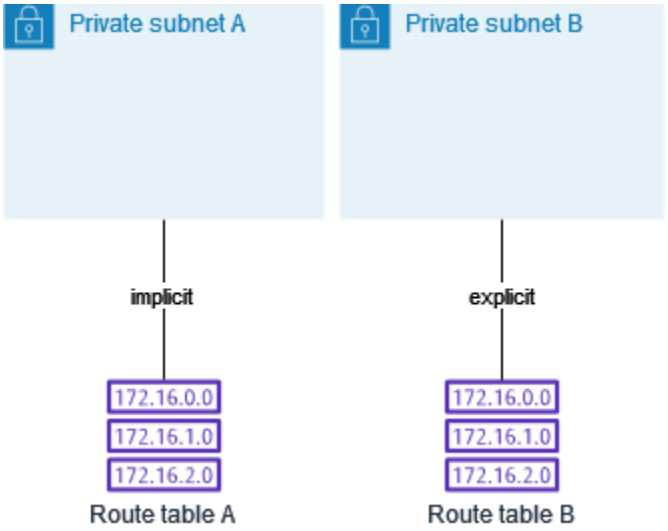
Ejemplo 2: sustitución de la tabla de enrutamiento principal

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

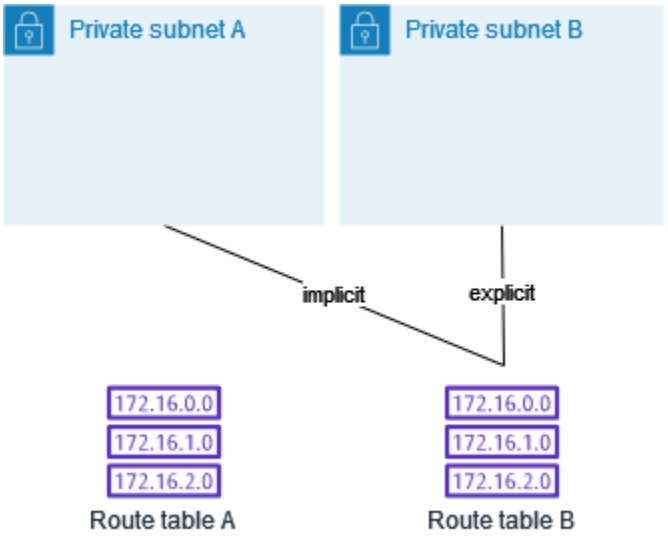
El siguiente diagrama muestra dos subredes y dos tablas de enrutamiento. La subred A está asociada implícitamente a la tabla de enrutamiento A, la tabla de enrutamiento principal. La subred B está implícitamente asociada con la tabla de enrutamiento a la tabla de enrutamiento B, una tabla de enrutamiento personalizada, no está asociada con ninguna de las subredes.



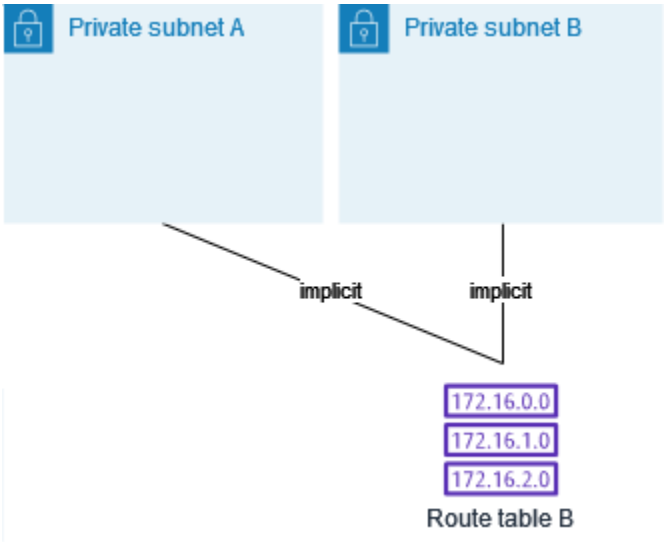
Para reemplazar la tabla de enrutamiento principal, comience por crear una asociación explícita entre la subred B y la tabla de rutas B. Pruebe la tabla de rutas B.



Una vez probada la tabla de enrutamiento B, podrá convertirla en tabla de enrutamiento principal. La subred B todavía tiene una asociación explícita con la tabla de enrutamiento B. Sin embargo, la subred A ahora tiene una asociación implícita con la tabla de enrutamiento B, porque la tabla de enrutamiento B es la nueva tabla de enrutamiento principal. La tabla de enrutamiento A ya no está asociada a ninguna de las subredes.



(Opcional) Si desasocia la subred B de la tabla de enrutamiento B, aún existe una asociación implícita entre la subred B y la tabla de enrutamiento B. Si ya no necesita la tabla de enrutamiento A, puede eliminarla.



Tablas de ruteo de puerta de enlace

Puede asociar una tabla de enrutamiento a una puerta de enlace de Internet o a una puerta de enlace privada virtual. Cuando una tabla de enrutamiento está asociada a una puerta de enlace, se denomina tabla de enrutamiento de puerta de enlace. Puede crear una tabla de enrutamiento de puerta de enlace 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 puerta de enlace 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 puerta de enlace
- Reglas y consideraciones

Rutas de la tabla de enrutamiento de puerta de enlace

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

- La ruta local predeterminada
- Un Punto de enlace del equilibrador de carga de puerta de enlace
- Una interfaz de red para un dispositivo middlebox

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

- La ruta local predeterminada
- Un Punto de enlace del equilibrador de carga de puerta de enlace
- Una interfaz de red para un dispositivo middlebox

Cuando el destino es punto de enlace del equilibrador de carga de puerta de enlace 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 enrutamiento de puerta de enlace 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.

Ejemplo

En la siguiente tabla de enrutamiento de puerta de enlace, 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	*eni-id*

Ejemplo

En la siguiente tabla de enrutamiento de puerta de enlace, 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	*eni-id*

Reglas y consideraciones

No se puede asociar una tabla de enrutamiento con una puerta de enlace 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 equilibrador de carga de puerta de enlace o la ruta local predeterminada.
- La tabla de enrutamiento 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 enrutamiento.

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 equilibrador de carga de puerta de enlace 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”.
- No se puede especificar una lista de prefijos como destino.
- No puede utilizar una tabla de enrutamiento de puerta de enlace para controlar o interceptar el tráfico fuera de la VPC, por ejemplo, el tráfico a través de una transit puerta de enlace 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 puerta de enlace 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.
- 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 puerta de enlace 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.
- No todas las zonas locales admiten la asociación de periferia con puertas de enlace privadas virtuales. Para obtener más información sobre las zonas disponibles, consulte Consideraciones en la Guía del usuario de Zonas locales de AWS.

Cómo funciona la prioridad de enrutamiento

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:

En la siguiente lista se muestra un resumen de prioridades de ruta con enlaces a las secciones siguientes con información más detallada y ejemplos:

1. El prefijo más largo (por ejemplo, 10.10.2.15/32 tiene prioridad sobre 10.10.2.0/24)
2. Rutas estáticas (como conexiones de emparejamiento de VPC y puertas de enlace de Internet)
3. Rutas de lista de prefijos
4. Rutas propagadas
   a. Rutas de BGP de Direct Connect (rutas dinámicas)
   b. Rutas estáticas de VPN
   c. Rutas de BGP de VPN (rutas dinámicas) (como puertas de enlace privadas virtuales)

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 puerta de enlace 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 puerta de enlace 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 puerta de enlace 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 para las rutas que se propagan de forma estática y dinámica

Si ha asociado una puerta de enlace 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 es idéntico al destino de una ruta estática, la ruta estática tiene prioridad. Los siguientes recursos utilizan rutas estáticas:

- puerta de enlace de Internet
- Puerta de enlace de NAT
- Interfaz de red
- ID de instancia
- punto de conexión de VPC de la puerta de enlace
- Transit puerta de enlace
- Interconexión de VPC
- Punto de enlace del equilibrador de carga de puerta de enlace

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 puerta de enlace de Internet y una ruta propagada hacia una puerta de enlace privada virtual. Ambas rutas tienen el

destino `172.31.0.0/24`. Dado que una ruta estática hacia una puerta de enlace de Internet tiene prioridad, todo el tráfico destinado a`172.31.0.0/24` se dirige a la puerta de enlace de Internet.

Destino	Objetivo	Propagado
10.0.0.0/16	local	No
172.31.0.0/24	vgw-11223344556677889	Sí
172.31.0.0/24	igw-12345678901234567	No

Prioridad de ruta para listas de prefijos

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 propagada que coincide con una ruta que hace referencia a una lista de prefijos, la ruta que hace referencia a la lista de prefijos tiene prioridad. Tenga en cuenta que para las rutas que se superponen, las rutas más específicas siempre tienen prioridad independientemente de si se trata de rutas propagadas, rutas estáticas o rutas que hacen referencia a listas de prefijos.
- Si la tabla de enrutamiento hace referencia a varias listas de prefijos que tienen bloques de CIDR superpuestos a diferentes destinos, elegimos aleatoriamente qué ruta tiene prioridad. A partir de entonces, la misma ruta siempre tiene prioridad.

Opciones de enrutamiento de ejemplo

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

Contenido

- Enrutar a una puerta de enlace de Internet
- Enrutar a un dispositivo NAT
- Enrutar a una puerta de enlace privada virtual
- Enrutamiento a una puerta de enlace local de AWS Outposts
- Enrutar a una interconexión de VPC

- Enrutar a un punto de conexión de VPC de la puerta de enlace
- Enrutar a la puerta de enlace de Internet de solo salida
- Enrutar para una transit puerta de enlace
- Enrutamiento para un dispositivo middlebox
- Enrutamiento mediante una lista de prefijos
- Enrutamiento a un punto de enlace del equilibrador de carga de puerta de enlace

Enrutar a una puerta de enlace de Internet

Puede convertir una subred en una subred pública añadiendo una ruta en su tabla de enrutamiento de la subred hacia una puerta de enlace de Internet. Para ello, cree y adjunte una puerta de enlace 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 puerta de enlace de Internet (`igw-xxxxxxxxxxxxxxxxx`).

Destino	Objetivo
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Para obtener más información, consulte Activación del acceso a Internet de una VPC con una puerta de enlace de Internet.

Enrutar a un dispositivo NAT

Para habilitar instancias en una subred privada para conectarse a Internet, puede crear una puerta de enlace NAT o lanzar una instancia NAT en una subred pública. A continuación, agregue una ruta para la tabla de enrutamiento 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	*nat-puerta de enlace-id*

También puede crear rutas más específicas a otros objetivos para evitar cargos innecesarios de procesamiento de datos innecesarios por utilizar la puerta de enlace NAT o para dirigir el tráfico de forma privada. En el siguiente ejemplo, el tráfico de Amazon S3 (pl-xxxxxxxx, una lista de prefijos que contiene los rangos de direcciones IP para Amazon S3 en una región específica) se enruta al punto de conexión de VPC de la puerta de enlace y el tráfico 10.25.0.0/16 se enruta a una conexión de emparejamiento de VPC. Estos rangos de direcciones IP 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 conexión de VPC de la puerta de enlace o a la interconexión de la VPC. El resto del tráfico se envía a la puerta de enlace NAT.

Destino	Objetivo
0.0.0.0/0	*nat-puerta de enlace-id*
pl-*xxxxxxxx*	*vpce-id*
10.25.0.0/16	*pcx-id*

Para obtener más información, consulte Dispositivos NAT.

Enrutar a una puerta de enlace 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 puerta de enlace privada virtual a su VPC. A continuación, agregue una ruta en la tabla de enrutamiento de subred con el destino de la red y un objetivo de la puerta de enlace privada virtual (`vgw-xxxxxxxxxxxxxxxxx`).

Destino	Objetivo
10.0.0.0/16	*vgw-id*

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 puerta de enlace privada virtual no admite tráfico IPv6. Sin embargo, sí que se admite el direccionamiento de tráfico IPv6 a través de puerta de enlaces

privadas virtuales a conexiones de Direct Connect. Para obtener más información, consulte la Guía del usuario de Direct Connect.

Enrutamiento a una puerta de enlace local de AWS Outposts

En esta sección se describen las configuraciones de la tabla de enrutamiento para el direccionamiento a una puerta de enlace local de AWS Outposts.

Contenido

- Habilite el tráfico entre las subredes de Outpost y la red en las instalaciones
- Habilite el tráfico entre subredes de la misma VPC en Outposts

Habilite el tráfico entre las subredes de Outpost y la red en las instalaciones

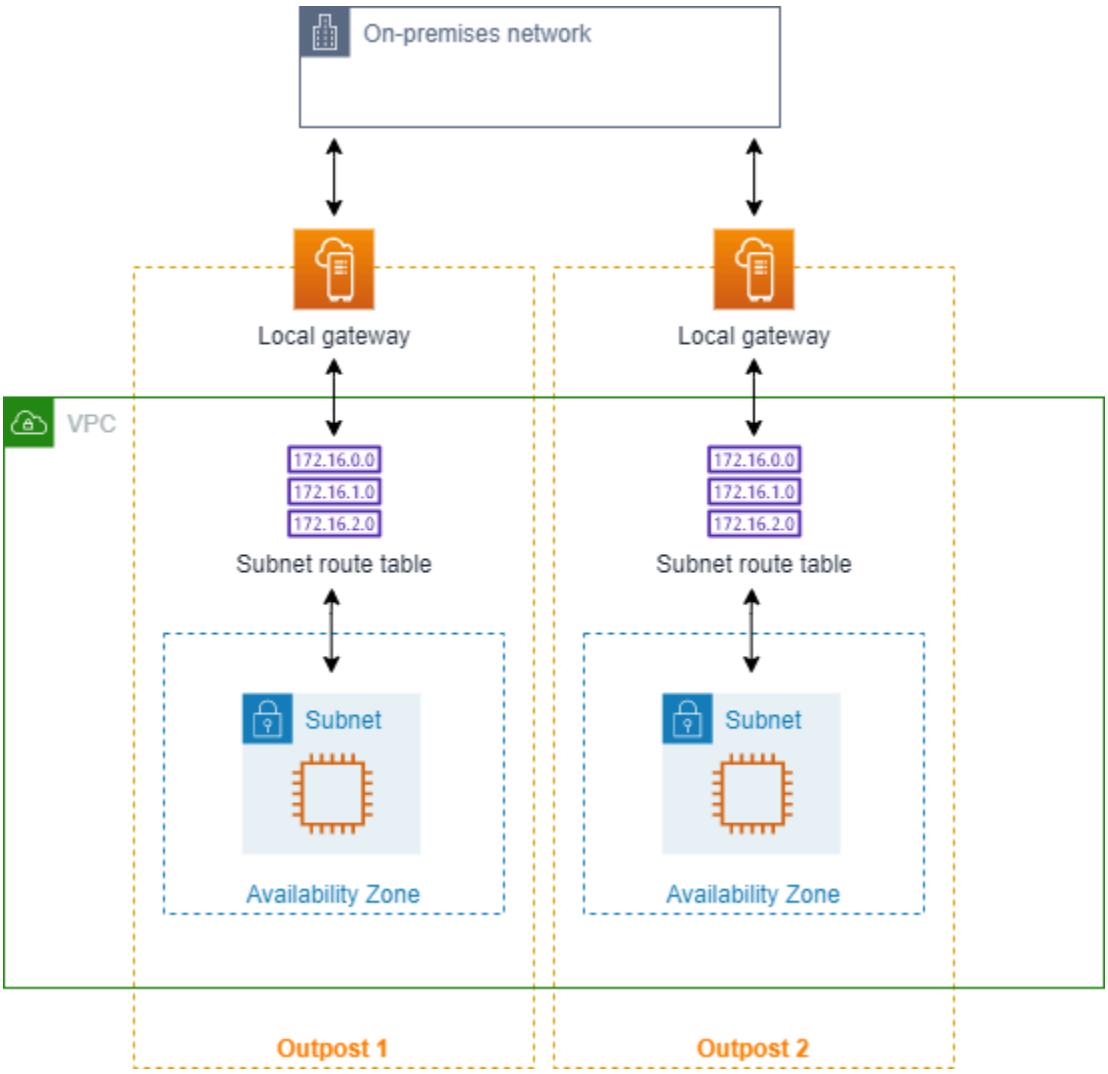
Las subredes que se encuentran en VPC asociadas a AWS Outposts pueden tener un tipo de objetivo adicional de una puerta de enlace local. Tenga en cuenta el caso en el que desea que la puerta de enlace local dirija el tráfico con una dirección de destino de 192.168.10.0/24 a la red del cliente. Para ello,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

Destino	Objetivo
192.168.10.0/24	*lgw-id*

Habilite el tráfico entre subredes de la misma VPC en Outposts

Para establecer la comunicación entre las subredes que se encuentran en la misma VPC en diferentes Outposts, utilice las puertas de enlace locales de Outpost y la red en las instalaciones.

Puede utilizar esta característica para crear arquitecturas similares a las arquitecturas de las zonas de disponibilidad (AZ) múltiple para las aplicaciones en las instalaciones que se ejecutan en los bastidores de Outposts mediante el establecimiento de conectividad entre bastidores de Outposts que están anclados a diferentes zonas de disponibilidad.



Para habilitar esta característica, agregue una ruta a la tabla de enrutamiento de la subred del bastidor de Outpost que sea más específica que la ruta local de esa tabla de enrutamiento y que tenga un tipo de destino de puerta de enlace local. El destino de la ruta debe coincidir con el bloque completo de IPv4 de una subred de su VPC que se encuentra en otro Outpost. Repita esta configuración en todas las subredes de Outpost que necesiten comunicarse.

Important

- Para usar esta característica, debe utilizar el enrutamiento directo de VPC. No puede usar direcciones IP propiedad de los clientes.
- La red en las instalaciones a la que están conectadas las puertas de enlace locales de Outposts debe tener el direccionamiento necesario para que se pueda acceder de una subred a otra.

- Si desea usar grupos de seguridad para los recursos de las subredes, debe utilizar reglas que incluyan rangos de direcciones IP como origen o destino en las subredes de Outpost. No puede usar los ID de los grupos de seguridad.
- Es posible que sea necesario actualizar los bastidores de Outposts existentes para permitir la comunicación dentro de la VPC entre varios Outposts. Si esta característica no funciona, póngase en contacto con el servicio de soporte de AWS.

Example Ejemplo

Para una VPC con un CIDR de 10.0.0.0/16, una subred de Outpost 1 con un CIDR de 10.0.1.0/24 y una subred de Outpost 2 con un CIDR de 10.0.2.0/24, la entrada para la tabla de enrutamiento de la subred de Outpost 1 sería la siguiente:

Destino	Objetivo
10.0.0.0/16	Local
10.0.2.0/24	*lgw-1-id*

La entrada para la tabla de enrutamiento de la subred de Outpost 2 sería la siguiente:

Destino	Objetivo
10.0.0.0/16	Local
10.0.1.0/24	*lgw-2-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 tabas 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 enrutamiento 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 enrutamiento 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 habilitar el enrutamiento del tráfico IPv6 entre las VPC, añada una ruta a la tabla de enrutamiento que apunte a la conexión de emparejamiento de VPC para acceder 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 enrutamiento 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 enrutamiento 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 conexión de VPC de la puerta de enlace

Un punto de conexión de VPC de la puerta de enlace permite crear una conexión privada entre la VPC y otros servicios de AWS. Cuando crea un punto de enlace de la puerta de enlace, especifica las tablas de ruteo de la subred en su VPC que utiliza el punto de enlace de la puerta de enlace. Se añadirá automáticamente una ruta a cada una de las tablas de ruteo con el ID de la lista de prefijos del servicio (`pl-`*`xxxxxxxx`*) como destino y el ID del punto de conexión (`vpce-`*`xxxxxxxxxxxxxxxxx`*) 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 puerta de enlace.

Enrutar a la puerta de enlace de Internet de solo salida

Puede crear puerta de enlaces 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 puerta de enlace de Internet de solo salida se utiliza únicamente para el tráfico IPv6. Para configurar el direccionamiento de la puerta de enlace de Internet de solo salida, añada una ruta a la tabla de enrutamiento de la subred privada que direccione el tráfico de Internet IPv6 (`::/0`) a la puerta de enlace de Internet de solo salida.

Destino	Objetivo
::/0	*eigw-id*

Para obtener más información, consulte Habilitar el tráfico IPv6 saliente mediante una puerta de enlace de Internet de solo salida.

Enrutar para una transit puerta de enlace

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

Considere el siguiente escenario, en el que tiene tres VPC asociadas a una transit puerta de enlace. En este escenario, todas las conexiones se asocian a la tabla de enrutamiento de la transit puerta de enlace y se propagan a la tabla de enrutamiento de la transit puerta de enlace. Por lo tanto, todas las conexiones pueden enrutar paquetes entre sí y la transit puerta de enlace 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-11111111111111111
- VPC B: 10.2.0.0/16, ID de vinculación tgw-attach-22222222222222222

Para permitir el tráfico entre las VPC y permitir el acceso a la transit puerta de enlace, 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	*tgw-id*

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

Destino	Objetivo
10.1.0.0/16	tgw-attach-11111111111111111
10.2.0.0/16	tgw-attach-22222222222222222

Para obtener más información acerca de las tablas de enrutamiento de la transit puerta de enlace, consulte Enrutamiento en Tansit puerta de enlaces 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 puerta de enlace de Internet o una puerta de enlace 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 puerta de enlace, el middlebox y la subred de destino. Para obtener más información, consulte the section called “Asistente de enrutamiento de Middlebox”.
- 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 equilibrador de carga de puerta de enlace, una puerta de enlace 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 equilibrador de carga de puerta de enlace, puerta de enlace 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 Direct Connect que admita tramas jumbo).

Para dirigir el tráfico de VPC entrante a un dispositivo, asocie una tabla de enrutamiento a la puerta de enlace de Internet o a la puerta de enlace 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 puerta de enlace. 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 Middlebox.

Contenido

- Consideraciones sobre el dispositivo
- Enrutamiento del tráfico entre una puerta de enlace y un dispositivo
- Enrutamiento del tráfico entre subredes a un dispositivo

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:

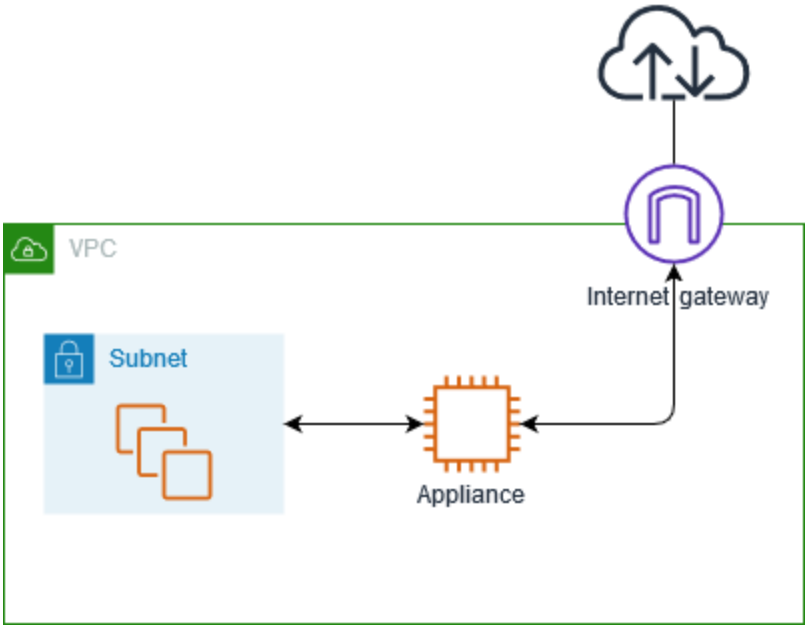
- El dispositivo debe configurarse en una subred independiente para el tráfico de origen o destino.
- Debe deshabilitar la comprobación de origen/destino en el dispositivo. Para obtener más información, consulte Cambio de la comprobación de origen o destino en la Guía del usuario de Amazon EC2.
- No 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 que la VPC, la subred y el dispositivo sean compatibles con IPv6.
- **Important**

  No dirija el tráfico de los servicios administrados de AWS (como una puerta de enlace de tránsito, una puerta de enlace NAT o un Equilibrador de carga de red) a través de un dispositivo middlebox de vuelta a la subred a la que está conectado ese servicio. Esta configuración provoca un comportamiento de enrutamiento impredecible y no es compatible.

Enrutamiento del tráfico entre una puerta de enlace y un dispositivo

Para dirigir el tráfico de VPC entrante a un dispositivo, asocie una tabla de enrutamiento a la puerta de enlace de Internet o a la puerta de enlace 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 puerta de enlace de Internet, un dispositivo y una subred con instancias. El tráfico de Internet se dirige a través de un dispositivo.



Asocie esta tabla de enrutamiento con su puerta de enlace de Internet o puerta de enlace 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
CIDR DE VPC	Local
CIDR de subred	*ID de interfaz de red del dispositivo*

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
CIDR de VPC	*ID de interfaz de red del dispositivo*

Para dirigir el tráfico de la subred a un dispositivo de otra subred, añada una ruta a la tabla de enrutamiento 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.

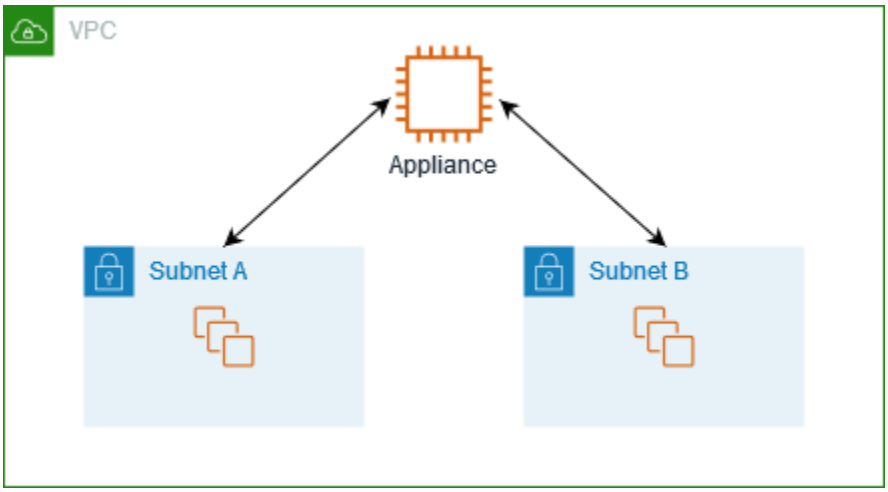
Destino	Objetivo
CIDR DE VPC	Local
0.0.0.0/0	*ID de interfaz de red del dispositivo*

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

Destino	Objetivo
CIDR DE VPC	Local
0.0.0.0/0	*igw-id*

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.

Enrutamiento

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
CIDR DE VPC	Local
CIDR de subred B	*ID de interfaz de red del dispositivo*

A continuación se muestra un ejemplo de tabla de enrutamiento 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
CIDR DE VPC	Local
CIDR de subred A	*ID de interfaz de red del dispositivo*

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
CIDR de VPC	*ID de interfaz de red del dispositivo*

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 para agruparlos. A continuación, puede especificar la lista de prefijos como destino en la entrada de la tabla de enrutamiento. Posteriormente, puede agregar o quitar entradas para la lista de prefijos sin necesidad de actualizar las tablas de ruteo.

Por ejemplo, tiene una transit puerta de enlace con varios archivos adjuntos de VPC. Las VPC deben poder comunicarse con dos adjuntos VPC específicos que tengan los siguientes bloques de 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 puerta de enlace como destino.

Destino	Objetivo
172.31.0.0/16	Local
pl-123abc123abc123ab	*tgw-id*

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

Enrutamiento a un punto de enlace del equilibrador de carga de puerta de enlace

Un equilibrador de carga de puerta de enlace le permite distribuir tráfico a una flota de dispositivos virtuales, como firewalls. Puede crear un equilibrador de carga de puerta de enlace, configurar un servicio de punto de conexión del equilibrador de carga de puerta de enlace, y luego crear un punto de conexión del equilibrador de carga de puerta de enlace en su VPC para conectarla al servicio.

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

Para obtener un ejemplo de dispositivos de seguridad detrás de un equilibrador de carga de puerta de enlace, consulte the section called “Inspeccionar el tráfico mediante dispositivos de seguridad”.

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

Destino	Objetivo
10.0.1.0/24	*vpc-endpoint-id*

Cuando se utiliza un punto de conexión del equilibrador de carga de la puerta de enlace como destino, no se puede especificar una lista de prefijos como destino. Si intenta crear o reemplazar una ruta de lista de prefijos dirigida a un punto de conexión de VPC, recibirá el error: “No se puede crear ni reemplazar una ruta de lista de prefijos dirigida a un punto de conexión de VPC”.

Para obtener más información, consulte Balanceadores de carga de puerta de enlace.

Creación de una tabla de enrutamiento personalizada para su VPC

Realice las siguientes tareas para crear y configurar una tabla de enrutamiento personalizada para su VPC. De forma predeterminada, una tabla de enrutamiento contiene una ruta local para la comunicación dentro de la VPC. Puede agregar rutas para dirigir el tráfico de red a destinos específicos en función del rango de direcciones IP de destino.

Para aplicar rutas de tablas de ruteo a una subred determinada, debe asociar la tabla de enrutamiento a la subred. Una tabla de enrutamiento se puede asociar con varias subredes. Sin embargo, una subred sólo puede asociarse a una tabla de enrutamiento a la vez. Las subredes que no estén asociadas de manera explícita a ninguna tabla se asociarán implícitamente a la tabla de enrutamiento principal de forma predeterminada.

Puede desvincular una subred de una tabla de enrutamiento. Hasta que asocie la subred a otra tabla de enrutamiento, esta quedará implícitamente asociada a la tabla de enrutamiento principal.

> **Note**
>
> 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 enrutamiento. Para obtener más información, consulte Cuotas de Amazon VPC.

Tareas

- Creación de la tabla de enrutamiento
- Adición de rutas a la tabla de enrutamiento

- Asociación de una subred con la tabla de enrutamiento

Creación de la tabla de enrutamiento

Para crear una tabla de ruteo de mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Tablas de enrutamiento.
3. Elija Create Route Table (Crear tabla de enrutamiento).
4. (Opcional) En Name (Etiqueta), escriba el nombre de la tabla de enrutamiento.
5. En VPC, elija su VPC.
6. (Opcional) Para agregar una etiqueta, elija Add new tag (Agregar etiqueta nueva) e ingrese la clave y el valor de la etiqueta.
7. Elija Create Route Table (Crear tabla de enrutamiento).

Creación de una tabla de enrutamiento mediante la AWS CLI

Utilice el comando create-route-table.

Adición de rutas a la tabla de enrutamiento

Cómo añadir rutas a una tabla de enrutamiento 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 enrutamiento) y, a continuación, seleccione la tabla de enrutamiento.
3. Elija Actions (Acciones), Edit routes (Editar rutas).
4. Seleccione Add route (Agregar ruta).
5. En Destino, ingrese uno de los siguientes:
   - Un rango de direcciones IP (por ejemplo, 192.168.0.0/16)
   - Una dirección IP única (por ejemplo, 192.168.10.1/32)
   - El ID de una lista de prefijos (por ejemplo, pl-0abcdef1234567890)
6. En Destino, seleccione un tipo de recurso (por ejemplo, una interfaz de red) y, a continuación, introduzca el ID del recurso (por ejemplo, eni-11223344556677889).

7. Seleccione Save changes (Guardar cambios).

Adición de rutas a una tabla de enrutamiento mediante la AWS CLI

Utilice el comando create-route.

Asociación de una subred con la tabla de enrutamiento

Para asociar una tabla de enrutamiento 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 enrutamiento.
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.
5. Seleccione Save associations (Guardar asociaciones).

Asociación o desasociación de una subred con una tabla de enrutamiento mediante la AWS CLI

- associate-route-table
- disassociate-route-table

Administración de las tablas de enrutamiento de subred

Use los siguientes procedimientos para administrar el enrutamiento de la VPC mediante tablas de enrutamiento.

Tareas

- Determinar la tabla de enrutamiento de una subred
- Determinación de las asociaciones explícitas
- Adición, modificación y eliminación de rutas
- Habilitar o deshabilitar la propagación de rutas
- Cambiar la tabla de enrutamiento de una subred

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.

Cómo determinar la tabla de enrutamiento 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 (Subredes).
3. Seleccione la subred.
4. Elija la pestaña Route table (Tabla de enrutamiento) para ver el ID de la tabla de enrutamiento y sus rutas. Para determinar la asociación con la tabla de enrutamiento principal, y si dicha asociación es explícita, consulte Determinación de las asociaciones explícitas.

Determinación de las asociaciones explícitas

Puede determinar el número y el tipo de subredes o puerta de enlaces explícitamente asociadas a la tabla de enrutamiento.

La tabla de enrutamiento 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 enrutamiento tienen una asociación implícita a la tabla de enrutamiento principal. Puede asociar de forma explícita una subred con la tabla de enrutamiento principal. Para obtener un ejemplo de las razones para hacer eso, consulte Sustituir la tabla de enrutamiento principal.

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 Tablas de enrutamiento.
3. Consulte la columna Explicit subnet association (Asociación de subredes explícita) para determinar las subredes asociadas de manera explícita y la columna Main (Principal) para determinar si esta es la tabla de enrutamiento principal.
4. Seleccione la tabla de enrutamiento y elija la pestaña Subnet associations (Asociaciones de subred).
5. Las subredes en Explicit subnet associations (Asociaciones de subred explícitas) están asociadas de manera explícita a la tabla de enrutamiento. Las subredes en Subnets without

explicit associations (Subredes sin asociaciones explícitas) pertenecen a la misma VPC que la tabla de enrutamiento, pero no están asociadas a ninguna tabla de enrutamiento, por lo que están asociadas de manera implícita a la tabla de enrutamiento principal de la VPC.

Para determinar las puerta de enlaces 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 Tablas de enrutamiento.
3. Seleccione la tabla de enrutamiento y elija la pestaña Edge associations (Asociaciones de periferia).

Descripción de una o varias tablas de enrutamiento y visualización de sus asociaciones mediante la AWS CLI

Utilice el comando describe-route-tables.

Adición, modificación y eliminación de rutas

Puede añadir, modificar y eliminar rutas en las tablas de enrutamiento.

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.

Consideraciones

- Solo podrá modificar rutas que haya añadido.
- Al modificar o eliminar una ruta, se ven afectadas las conexiones existentes que las utilizan. Las conexiones que utilizan las otras rutas no se ven afectadas.
- Existe una cuota en el número de rutas que puede añadir por cada tabla de enrutamiento. Para obtener más información, consulte Cuotas de Amazon VPC.

Para actualizar las rutas de una tabla de enrutamiento 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 enrutamiento) y, a continuación, seleccione la tabla de enrutamiento.

3. Elija Actions (Acciones), Edit routes (Editar rutas).
4. Para agregar una ruta, elija Add route (Añadir ruta). En Destino, introduzca un intervalo de direcciones IP, una única dirección IP o el ID de una lista de prefijos. En Objetivo, seleccione el tipo de recurso y, a continuación, introduzca el ID del recurso.
5. Para modificar una ruta, introduzca el nuevo bloque de CIDR de destino o el ID de la lista de prefijos y elija un objetivo.
6. Para eliminar una ruta, elija Remove (Eliminar).
7. Seleccione Save changes (Guardar cambios).

Actualización de las rutas de una tabla de enrutamiento mediante la AWS CLI

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`.

- create-route
- replace-route
- delete-route

Habilitar o deshabilitar la propagación de rutas

La propagación de rutas permite que una puerta de enlace privada virtual propague automáticamente rutas a las tablas de enrutamiento. Esto significa que no es necesario agregar o eliminar rutas de VPN manualmente.

Para completar este proceso, debe tener una puerta de enlace privada virtual.

Para obtener más información, consulte Opciones de enrutamiento de Site-to-Site VPN en la Guía del usuario de Site-to-Site VPN.

Habilitación o deshabilitación de la propagación de rutas 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 enrutamiento.
3. Elija Actions (Acciones), Edit route propagation (Editar propagación de rutas).

4. Seleccione o deseleccione la casilla de verificación Enable (Habilitar) situada junto a la puerta de enlace privada virtual.
5. Seleccione Save.

Habilitación o deshabilitación de la propagación de rutas mediante la AWS CLI

- enable-vgw-route-propagation
- disable-vgw-route-propagation

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 enrutamiento 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 enrutamiento) elija Edit route table association (Editar asociación de la tabla de enrutamiento).
4. Para Route Table ID (Id. de tabla de enrutamiento), seleccione la nueva tabla de enrutamiento.
5. Seleccione Save.

Cambio de la tabla de enrutamiento asociada a una subred mediante la AWS CLI

Utilice el comando replace-route-table-association.

Sustituir la tabla de enrutamiento principal

En esta sección, se describe cómo establecer qué tabla de enrutamiento es la principal de su VPC.

Para sustituir la tabla de enrutamiento 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 y, a continuación, seleccione la tabla de enrutamiento.

3. Elija Actions (Acciones), Set main route table (Definir la tabla de enrutamiento principal).
4. Cuando se le solicite confirmación, ingrese **`set`** y luego, elija OK (Aceptar).

Sustitución de la tabla de enrutamiento principal mediante la AWS CLI

- Utilice el comando replace-route-table-association.

El procedimiento siguiente describe cómo quitar una asociación explícita entre una subred y la tabla de enrutamiento principal. El resultado es una asociación implícita entre la subred y la tabla de enrutamiento 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 enrutamiento 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 enrutamiento.
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.
5. Seleccione Save associations (Guardar asociaciones).

Control del tráfico que ingresa a la VPC mediante una tabla de enrutamiento de puerta de enlace

Para controlar el tráfico que ingresa a su VPC con una tabla de enrutamiento de puerta de enlace, puede asociar o desvincular una puerta de enlace de Internet o una puerta de enlace virtual privada y una tabla de enrutamiento. Para obtener más información, consulte Tablas de ruteo de puerta de enlace.

Pasos para asociar o desvincular una puerta de enlace y una tabla de enrutamiento 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 Route tables y, a continuación, seleccione la tabla de enrutamiento.

3. En la pestaña Edge associations (Asociaciones de periferia, elija Edit edge associations (Editar asociaciones de periferia).
4. Marque o desmarque la casilla de verificación de la puerta de enlace.
5. Seleccione Save changes (Guardar cambios).

Para asociar una puerta de enlace a la tabla de enrutamiento mediante la AWS CLI

Utilice el comando associate-route-table. En el siguiente ejemplo se asocia la tabla de enrutamiento especificada con la puerta de enlace de Internet especificada.

```
aws ec2 associate-route-table
    --route-table-id rtb-01234567890123456 \
    --gateway-id igw-11aa22bb33cc44dd1
```

Cómo desasociar una puerta de enlace de una tabla de enrutamiento mediante la AWS CLI

Utilice el comando disassociate-route-table. Especifique el ID de la asociación entre la tabla de enrutamiento y la puerta de enlace.

```
aws ec2 disassociate-route-table \
    --association-id rtbassoc-0abcdef1234567890
```

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, 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.

Cómo reemplazar la 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 enrutamiento.
3. En la pestaña Routes (Rutas), elija Edit routes (Editar rutas).
4. Para la ruta local, desactive Target (Objetivo) y, a continuación, elija un nuevo objetivo.
5. Seleccione Save changes (Guardar cambios).

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 enrutamiento.
3. Elija Actions (Acciones), Edit routes (Editar rutas).
4. Para la ruta local, desactive Target (Objetivo) y, a continuación, elija local (local).
5. Seleccione Save changes (Guardar cambios).

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 con la interfaz de red especificada.

```
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 para la tabla de enrutamiento especificada.

```
aws ec2 replace-route \
    --route-table-id rtb-01234567890123456 \
    --destination-cidr-block 10.0.0.0/16 \
    --local-target
```

Enrutamiento avanzado con la VPC

Configure escenarios de enrutamiento avanzados para la VPC. Esta sección abarca los enfoques de enrutamiento estático y dinámico para administrar el flujo de tráfico:

- Enrutamiento de entrada estático: configure los enrutamientos estáticos para dirigir el tráfico de Internet entrante destinado a los grupos de direcciones BYOIP (traiga su propia IP) para las interfaces de red específicas dentro de la VPC.
- Enrutamiento dinámico con servidor de rutas de VPC: con el enrutamiento dinámico basado en BGP, actualice automáticamente las tablas de enrutamiento de VPC y puertas de enlace de

Internet. Esto genera tolerancia a errores y conmutación por error automática para las cargas de trabajo.

Contenido

- Enrutar el tráfico de Internet a una sola interfaz de red
- Enrutamiento dinámico en su VPC con VPC Route Server

Enrutar el tráfico de Internet a una sola interfaz de red

Enrute el tráfico de Internet entrante dirigido a grandes grupos de direcciones IP públicas hacia una sola interfaz de red elástica (ENI) en la VPC.

Las puertas de enlace de Internet previamente aceptaban solo el tráfico dirigido a direcciones IP públicas que estaban directamente relacionadas con las interfaces de red en la VPC. Los límites de las direcciones IP en la cantidad de tipos de instancias se pueden relacionar con las interfaces de red, lo cual genera un desafío para los sectores de telecomunicaciones e Internet de las cosas (IoT) que deben gestionar el tráfico de grupos de IP que superan dichos límites.

Este enrutamiento permite eliminar la compleja traducción de direcciones en las conexiones de Internet entrantes. Es posible crear sus propios grupos de IP públicos (BYOIP) y configurar la puerta de enlace de Internet de VPC para aceptar el tráfico de todo el grupo, así como enrutarlo a una única interfaz de red. Esta característica es muy útil para lo siguiente:

- Telecomunicaciones: administración de grandes grupos de IP de suscriptores sin la sobrecarga de la traducción de direcciones
- Aplicaciones de IoT: consolidación del tráfico proveniente de numerosas direcciones IP de dispositivos
- Cualquier escenario: que requiera el enrutamiento de tráfico que exceda los límites de asociación de la ENI

Este enrutamiento se puede integrar con el servidor de rutas de VPC para obtener actualizaciones de las rutas dinámicas en los escenarios de conmutación por error.

Ventajas principales

Los siguientes son beneficios de este enfoque de enrutamiento:

- Sin necesidad de la traducción de direcciones: el enrutamiento directo elimina la complejidad de la NAT
- Omisión de los límites de la ENI: gestione grupos de IP que excedan los límites de asociación de instancias
- Optimización para la industria: diseñado específicamente para los requisitos de telecomunicaciones e IoT
- Conmutación por error dinámica: integra con Route Server para realizar actualizaciones automáticas

Disponibilidad

Esta característica se puede utilizar en todas las regiones comerciales de AWS, regiones de AWS China y regiones de AWS GovCloud.

Contenido

- Antes de empezar
- Cómo funciona esta característica
- Paso 1: Crear una VPC
- Paso 2: crear y adjuntar una puerta de enlace de Internet
- Paso 3: crear una subred para la instancia de destino
- Paso 4: crear una tabla de enrutamiento para la subred
- Paso 5: crear un grupo de seguridad para la instancia de destino
- Paso 6: lanzar una instancia EC2 de destino
- Paso 7: crear tabla de enrutamiento para la puerta de enlace de Internet
- Paso 8: asociar la tabla de enrutamiento con la puerta de enlace de Internet
- Paso 9: asociar el grupo BYOIP a la puerta de enlace de Internet
- Paso 10: agregar una ruta estática para dirigir la instancia
- Paso 11: configurar la instancia de destino
- Paso 12: configurar la instancia para la administración del tráfico
- Paso 13: probar la conectividad
- Solución de problemas
- Opción avanzada: integración del servidor de rutas para el enrutamiento dinámico

- Limpieza

Antes de empezar

Antes de empezar este tutorial, asegúrese de que cuenta con lo siguiente:

1. Un grupo BYOIP: ya debe haber incorporado su propio rango de direcciones IP a AWS. Complete los pasos en Traiga sus propias direcciones IP (BYOIP) en Amazon EC2.
2. Verificación del grupo BYOIP: confirme que su grupo esté listo al ejecutar:

   ```
   aws ec2 describe-public-ipv4-pools --region us-east-1
   ```

   Busque su grupo en el resultado y asegúrese de que `PoolAddressRanges` muestre las direcciones `Available`.
3. Permisos adecuados: asegúrese de que su cuenta de AWS posee permisos para crear recursos de VPC e instancias de EC2, además de administrar grupos de BYOIP.

Cómo funciona esta característica

Esta sección explica los conceptos técnicos en que se basa el enrutamiento de entrada a la puerta de enlace de Internet y el flujo del tráfico de Internet a la instancia de destino.

Por qué usar el enrutamiento de entrada de una puerta de enlace de Internet

Debido los límites de asociación de la ENI, antes había que realizar la traducción de direcciones para consolidar el tráfico de una gran cantidad de direcciones IP. Con esta mejora se puede eliminar esa complejidad, ya que permite que los grupos BYOIP se enruten directamente a las instancias de destino.

Cómo funciona el enrutamiento

Esta característica solo funciona con los CIDR de IP públicos que se entregan a AWS al seguir el proceso BYOIP. El proceso BYOIP asegura que su cuenta sea propietaria del CIDR de IP público. En cuanto tenga el CIDR público de BYOIP:

1. Debe asociar este conjunto de direcciones IP públicas a una tabla de enrutamiento de una puerta de enlace de Internet. La puerta de enlace de Internet ya debe estar asociada a una VPC. Esta asociación permite que la VPC acepte el tráfico dirigido al CIDR de IP. Asegúrese de que la puerta de enlace de Internet posea una tabla de enrutamiento que no se comparta con ninguna subred.

2. Tras haber asociado el grupo BYOIP a la tabla de enrutamiento de la puerta de enlace de Internet, deberá ingresar una ruta con un destino igual al CIDR de IP o un subconjunto del mismo en la tabla de enrutamiento de la puerta de enlace de Internet. El objetivo de esta ruta es la ENI al que desea enrutar el tráfico.
3. Cuando el tráfico dirigido a CIDR BYOIP ingresa a AWS, AWS consulta la tabla de enrutamiento de la puerta de enlace de Internet y, por consiguiente, enruta el tráfico a la VPC correspondiente.
4. Dentro de la VPC, la puerta de enlace de Internet enruta el tráfico a la ENI de destino.
5. El destino (una interfaz de red elástica asociada a la carga de trabajo) procesa el tráfico.

Prácticas recomendadas

- Mantener las tablas de enrutamiento separadas: la tabla de enrutamiento de la puerta de enlace de Internet debe estar dedicada exclusivamente a la puerta de enlace de Internet. No asocie esta tabla de enrutamiento con las subredes de VPC. Pero sí puede utilizar tablas de enrutamiento serparadas para el enrutamiento de subredes.
- No asignar las IP de BYOIP directamente: no asocie direcciones IP públicas del grupo BYOIP directamente a instancias de EC2 o interfaces de red. La característica del enrutamiento de entrada de la puerta de enlace de Internet enruta el tráfico a las instancias sin la necesidad de una asociación IP directa.

> **Important**
>
> Cuando esté habilitado el BPA, el Bloqueo de acceso público de las VPC (BPA) bloqueará el tráfico a las subredes con el enrutamiento de entrada, incluso si se ha establecido una exclusión de BPA a nivel de subred. Sin embargo, las exclusiones a nivel de subred no funcionan para el enrutamiento de entrada. Si desea permitir el tráfico de enrutamiento de entrada con el BPA activado debe realizar lo siguiente:
>
> - Desactivar el BPA por completo o
> - Utilizar una exclusión a nivel de VPC

Paso 1: Crear una VPC

Complete este paso para crear una VPC que aloje la instancia de destino y la puerta de enlace de Internet.

> **Note**
>
> Asegúrese de no haber alcanzado el límite de cuota de VPC. Para obtener más información, consulte Cuotas de Amazon VPC.

AWS Consola de

1. Abra la Consola de Amazon VPC.
2. En el panel de VPC, elija Create VPC (Crear VPC).
3. En Recursos para crear, elija Solo VPC.
4. En Etiqueta de nombre, ingrese un nombre para la VPC (por ejemplo, **`IGW-Ingress-VPC`**).
5. En Bloque CIDR de IPv4, ingrese un bloque de CIDR (por ejemplo, **`10.0.0.0/16`**).
6. Seleccione Creación de VPC.

AWS CLI

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications
 'ResourceType=vpc,Tags=[{Key=Name,Value=IGW-Ingress-VPC}]' --region us-east-1
```

Paso 2: crear y adjuntar una puerta de enlace de Internet

Complete este paso para crear una puerta de enlace de Internet y adjuntarla a la VPC con el fin de habilitar la conectividad de Internet.

AWS Consola de

1. Abra la Consola de Amazon VPC.
2. En la consola de VPC, seleccione Puertas de enlace de Internet.
3. Elija Crear puerta de enlace de Internet.
4. En Etiqueta de nombre, ingrese un nombre para la puerta de enlace de Internet (por ejemplo, **`IGW-Ingress-Gateway`**).
5. Elija Crear puerta de enlace de Internet.
6. Seleccione la puerta de enlace de Internet y elija Acciones, Asociar a VPC.
7. Seleccione la VPC y elija Adjuntar puerta de enlace de Internet.

AWS CLI

```
aws ec2 create-internet-gateway --tag-specifications 'ResourceType=internet-
gateway,Tags=[{Key=Name,Value=IGW-Ingress-Gateway}]' --region us-east-1

aws ec2 attach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0 --region us-east-1
```

Nota: Sustituya los ID de recursos por los del paso anterior.

Paso 3: crear una subred para la instancia de destino

Complete este paso para crear una subred en la que se implementará la instancia de destino.

AWS Consola de

1. En el panel de navegación de la consola de la VPC, elija Subnets (Subredes).
2. Elija Create subnet (Crear subred).
3. En ID de la VPC, elija la VPC.
4. En Nombre de subred, ingrese un nombre (por ejemplo, **`Target-Subnet`**).
5. 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.
6. En Bloque CIDR de IPv4, seleccione Entrada manual e ingrese un bloque de CIDR (por ejemplo, **`10.0.1.0/24`**).
7. Elija Create subnet (Crear subred).

AWS CLI

```
aws ec2 create-subnet \
    --vpc-id vpc-0123456789abcdef0 \
    --cidr-block 10.0.1.0/24 \
    --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Target-Subnet}]' \
    --region us-east-1
```

Paso 4: crear una tabla de enrutamiento para la subred

Complete este paso para crear una tabla de enrutamiento para la subred y asociarla a ella.

AWS Consola de

1. En el panel de navegación de la consola de VPC, elija Tablas de enrutamiento.
2. Elija Create Route Table (Crear tabla de enrutamiento).
3. En Nombre, escriba un nombre para la tabla de enrutamiento (por ejemplo, **`Target-Subnet-Route-Table`**).
4. En VPC, elija su VPC.
5. Elija Create Route Table (Crear tabla de enrutamiento).
6. Seleccione la tabla de enrutamiento y elija Acciones, Editar asociaciones de subred.
7. Seleccione la subred y elija Guardar asociaciones.

AWS CLI

```
aws ec2 create-route-table \
    --vpc-id vpc-0123456789abcdef0 \
    --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Target-Subnet-
Route-Table}]' \
    --region us-east-1

aws ec2 associate-route-table \
    --route-table-id rtb-0987654321fedcba0 \
    --subnet-id subnet-0123456789abcdef0 \
    --region us-east-1
```

Paso 5: crear un grupo de seguridad para la instancia de destino

Complete este paso para crear un grupo de seguridad que controlará el acceso de red a la instancia de destino.

AWS Consola de

1. En el panel de navegación de la consola de la VPC, elija Grupos de seguridad.
2. Elija Creación de grupo de seguridad.
3. En Nombre del grupo de seguridad, escriba un nombre (por ejemplo, **`IGW-Target-SG`**).
4. En Descripción, escriba **`Security group for IGW ingress routing target instance`**.
5. En VPC, seleccione la VPC.

6. Para agregar reglas de entrada, elija Reglas de entrada. Para cada regla, elija Agregar regla y especifique lo siguiente:

   - Tipo: todo ICMP - IPv4, origen: 0.0.0.0/0 (para pruebas de ping).
   - Tipo: SSH, puerto: 22, origen: 0.0.0.0/0 (para EC2 Instance Connect).

> **Note**
>
> Este grupo de seguridad abre los puertos SSH a todo el tráfico de Internet para este tutorial. Dicho tutorial tiene fines educativos y no debe configurarse para entornos de producción. En caso de producción, restrinja el acceso SSH a rangos de IP específicos.

- Elija Creación de grupo de seguridad.

AWS CLI

```
aws ec2 create-security-group \
    --group-name IGW-Target-SG \
    --description "Security group for IGW ingress routing target instance" \
    --vpc-id vpc-0123456789abcdef0 \
    --region us-east-1

aws ec2 authorize-security-group-ingress \
    --group-id sg-0123456789abcdef0 \
    --protocol icmp \
    --port -1 \
    --cidr 0.0.0.0/0 \
    --region us-east-1

aws ec2 authorize-security-group-ingress \
    --group-id sg-0123456789abcdef0 \
    --protocol tcp \
    --port 22 \
    --cidr 0.0.0.0/0 \
    --region us-east-1
```

Paso 6: lanzar una instancia EC2 de destino

Complete este paso para lanzar la instancia EC2 que recibirá el tráfico del grupo BYOIP.

AWS Consola de

1. Abra la consola de Amazon EC2.
2. Seleccione Iniciar instancia.
3. En Nombre, escriba un nombre para la instancia (por ejemplo, **`IGW-Target-Instance`**).
4. En Imágenes de aplicaciones y sistema operativo (Imagen de máquina de Amazon), elija AMI de Amazon Linux 2023.
5. En Tipo de instancia, elija t2.micro (compatible con el nivel gratuito).
6. En Par de claves (inicio de sesión), seleccione un par de claves existente o cree uno nuevo.
7. En Configuración de red, elija Editar y configure:
   - VPC: seleccione la VPC
   - Subred: seleccione la subred
   - Asignar automáticamente IP pública: habilítelo
   - Firewall (grupos de seguridad): seleccione un grupo de seguridad
8. Seleccione Iniciar instancia.
9. Importante: Tras el lanzamiento, diríjase a los detalles de la instancia y tenga en cuenta el ID de la interfaz de red (empieza con “eni-”). Lo necesitará para el paso 10.

AWS CLI

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 1 \
    --instance-type t2.micro \
    --key-name your-key-pair \
    --security-group-ids sg-0123456789abcdef0 \
    --subnet-id subnet-0123456789abcdef0 \
    --associate-public-ip-address \
    --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=IGW-Target-
Instance}]' \
    --region us-east-1
```

Para buscar el ID de ENI en la consolsa deberá:

1. Seleccionar la instancia en la consola de EC2.
2. Diríjase a la pestaña Redes.

3. Tener en cuenta el ID de la interfaz de red (por ejemplo, `eni-0abcdef1234567890`).

Para encontrar el ID de ENI con AWS CLI:

```
aws ec2 describe-instances --instance-ids i-0123456789abcdef0 --query
 'Reservations[0].Instances[0].NetworkInterfaces[0].NetworkInterfaceId' --output text
 --region us-east-1
```

Paso 7: crear tabla de enrutamiento para la puerta de enlace de Internet

Complete este paso para crear una tabla de enrutamiento para la puerta de enlace de Internet que gestionará el enrutamiento de entrada.

AWS Consola de

1. En la consola de VPC, elija Tablas de enrutamiento.
2. Elija Create Route Table (Crear tabla de enrutamiento).
3. En Nombre, escriba un nombre para la tabla de enrutamiento (por ejemplo, **`IGW-Ingress-Route-Table`**).
4. En VPC, elija su VPC.
5. Elija Create Route Table (Crear tabla de enrutamiento).
6. Seleccione la tabla de enrutamiento y elija la pestaña Asociaciones de periferia.
7. Seleccione Editar asociaciones de periferia.
8. Seleccione la puerta de enlace de Internet y elija Guardar cambios.

AWS CLI

```
aws ec2 create-route-table \
    --vpc-id vpc-0123456789abcdef0 \
    --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=IGW-Ingress-
Route-Table}]' \
    --region us-east-1
```

Paso 8: asociar la tabla de enrutamiento con la puerta de enlace de Internet

Complete este paso para asociar la tabla de enrutamiento con la puerta de enlace de Internet con el fin de habilitar la funcionalidad de enrutamiento de entrada.

AWS Consola de

1. En el panel de navegación de la consola de VPC, seleccione Tablas de enrutamiento y elija la tabla de enrutamiento que ha creado.
2. En la pestaña Edge associations (Asociaciones de periferia, elija Edit edge associations (Editar asociaciones de periferia).
3. Seleccione la casilla para la puerta de enlace de Internet.
4. Seleccione Save changes (Guardar cambios).

AWS CLI

```
aws ec2 associate-route-table \
    --route-table-id rtb-0123456789abcdef0 \
    --gateway-id igw-0123456789abcdef0 \
    --region us-east-1
```

Paso 9: asociar el grupo BYOIP a la puerta de enlace de Internet

Complete este paso para asociar el grupo BYOIP a la tabla de enrutamiento de la puerta de enlace de Internet, lo que permitirá que la VPC acepte el tráfico del rango de IP.

AWS Consola de

1. En el panel de navegación de la consola de VPC, seleccione Tablas de enrutamiento y elija la tabla de enrutamiento de la puerta de enlace de Internet que ha creado.
2. Elija la pestaña Asociaciones de grupos IPv4.
3. Elija el botón Editar asociaciones.
4. Seleccione el grupo BYOIP (por ejemplo, `pool-12345678901234567`).
5. Elija el botón Guardar asociaciones.

AWS CLI

```
aws ec2 associate-route-table \
    --route-table-id rtb-0123456789abcdef0 \
    --public-ipv4-pool pool-12345678901234567 \
    --region us-east-1
```

Nota: Reemplace `rtb-0123456789abcdef0` con el ID de la tabla de enrutamiento de la puerta de enlace de Internet y `pool-12345678901234567` con el ID del grupo BYOIP.

Paso 10: agregar una ruta estática para dirigir la instancia

Complete este paso para agregar una ruta que dirija el tráfico desde el rango de BYOIP a la interfaz de red de la instancia de destino.

AWS Consola de

1. En el panel de navegación de la consola de VPC, seleccione Tablas de enrutamiento y elija la tabla de enrutamiento de la puerta de enlace de Internet que ha creado.
2. Elija Actions (Acciones), Edit routes (Editar rutas).
3. Seleccione Add route (Agregar ruta).
4. En Destino, ingrese BYOIP CIDR o un subconjunto (por ejemplo, **`203.0.113.0/24`**). Este prefijo debe estar entre /23 y /28.
5. En Destino, seleccione Interfaz de red e ingrese el ID de ENI de la instancia (por ejemplo, `eni-0abcdef1234567890`).
6. Seleccione Save changes (Guardar cambios).

AWS CLI

```
aws ec2 create-route \
    --route-table-id rtb-0123456789abcdef0 \
    --destination-cidr-block 203.0.113.0/24 \
    --network-interface-id eni-0abcdef1234567890 \
    --region us-east-1
```

Paso 11: configurar la instancia de destino

Complete este paso para configurar la instancia de destino para que gestione correctamente el tráfico dirigido a las direcciones BYOIP.

Importante: Complete este paso de configuración de instancia antes de probar la conectividad (paso 12). Para que el enrutamiento de entrada funcione correctamente, la instancia debe configurarse para responder a las direcciones BYOIP.

AWS Consola de

1. Conéctese a la instancia de destino con EC2 Instance Connect:
   - Seleccione la instancia en la consola de EC2.
   - Seleccione Acciones > Conectar.
   - Seleccione la pestaña EC2 Instance Connect.
   - Elija Conectar.
2. Agregue una dirección IP de BYOIP específica a la interfaz de la instancia:

   En primer lugar, busque el nombre de la interfaz de red:

   ```
   ip link show
   ```

   Luego, agregue la dirección IP (sustituya `203.0.113.10` por una IP del rango BYOIP):

   ```
   sudo ip addr add 203.0.113.10/32 dev eth0
   ```

   Nota: Sustituya `203.0.113.10` por cualquier dirección IP del rango BYOIP que desee probar. El nombre de la interfaz puede ser `eth0`, `ens5`, o similar, según el tipo de instancia.
3. En la consola de EC2, deshabilite la comprobación de origen y destino:
   - Seleccione la instancia.
   - Vaya a la pestaña Redes y elija la interfaz de red.
   - Elija Acciones, Cambiar comprobación de origen y destino, Deshabilitar.

AWS CLI

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-0abcdef1234567890 \
    --no-source-dest-check \
    --region us-east-1
```

Paso 12: configurar la instancia para la administración del tráfico

Complete este paso para agregar direcciones BYOIP a la instancia y deshabilite la comprobación de origen y destino para administrar el tráfico de forma adecuada.

AWS Consola de

1. Conéctese a la instancia de destino con EC2 Instance Connect:
   - Seleccione la instancia en la consola de EC2.
   - Seleccione Acciones > Conectar.
   - Seleccione la pestaña EC2 Instance Connect.
   - Elija Conectar.
2. Agregue una dirección IP de BYOIP específica a la interfaz de la instancia:

   En primer lugar, busque el nombre de la interfaz de red:

   ```
   ip link show
   ```

   Luego, agregue la dirección IP (sustituya `ens5` por el nombre de la interfaz):

   ```
   sudo ip addr add 203.0.113.10/32 dev ens5
   ```

   Nota: Sustituya `203.0.113.10` por cualquier dirección IP del rango BYOIP que desee probar. El nombre de la interfaz puede ser `eth0`, `ens5`, o similar, según el tipo de instancia.
3. En la consola de EC2, deshabilite la comprobación de origen y destino:
   - Seleccione la instancia.
   - Vaya a la pestaña Redes y elija la interfaz de red.
   - Elija Acciones, Cambiar comprobación de origen y destino, Deshabilitar.

AWS CLI

```
aws ec2 modify-network-interface-attribute \
    --network-interface-id eni-0abcdef1234567890 \
    --no-source-dest-check \
    --region us-east-1
```

Paso 13: probar la conectividad

Complete este paso para verificar que el tráfico de Internet se enruta correctamente a la instancia de destino a través de las direcciones BYOIP.

1. En la instancia de destino, monitoree el tráfico entrante con tcpdump:

```
sudo tcpdump -i any icmp
```

2. Pruebe la conectividad con la dirección IP de BYOIP desde otro terminal u otra computadora:

```
ping 203.0.113.10
```

3. Resultados esperados:

   - El ping debe funcionar correctamente y mostrar las respuestas de la dirección IP de BYOIP.
   - tcpdump debe mostrar los paquetes entrantes de la dirección BYOIP, de forma similar a:

     ```
     12:34:56.789012 IP 203.0.113.100 > 203.0.113.10: ICMP echo request, id 1234, seq
      1, length 64
     12:34:56.789123 IP 203.0.113.10 > 203.0.113.100: ICMP echo reply, id 1234, seq 1,
      length 64
     ```

   - El tráfico debe provenir de direcciones IP externas, lo que demuestra que el enrutamiento de entrada de la puerta de enlace de Internet está enviando el tráfico de Internet a la instancia.

Solución de problemas

Con esta sección, podrá resolver los problemas más comunes que pueden surgir al configurar el enrutamiento de entrada de la puerta de enlace de Internet.

El tráfico no llega a la instancia

- Revise que la tabla de enrutamiento contenga el ID de ENI correcto como destino.
- Confirme que el grupo BYOIP esté asociado a la tabla de enrutamiento de la puerta de enlace de Internet.
- Verifique que la comprobación de origen y destino esté deshabilitada en la instancia.
- Asegúrese de que los grupos de seguridad permitan el tipo de tráfico que está probando.

Error de creación de rutas

- Verifique que el grupo BYOIP esté asociado correctamente a la tabla de enrutamiento.
- Confirme que el CIDR de destino esté dentro del rango de BYOIP.
- Compruebe que el ENI de destino existe y que esté conectado a una instancia en ejecución.
- Asegúrese de que el prefijo BYOIP esté entre /23 y /28 (no se admiten prefijos que estén fuera de este rango).

Error en el ping o la conectividad

- Verifique que las direcciones IP se agreguen a la interfaz de la instancia.
- Compruebe que los grupos de seguridad admitan el ICMP (para ping) o los puertos relevantes.
- Confirme que la instancia se esté ejecutando.
- Realice pruebas desde varias ubicaciones externas.

Opción avanzada: integración del servidor de rutas para el enrutamiento dinámico

Para los entornos que necesitan de una conmutación por error automática, esta característica se integra con el servidor de rutas de VPC para realizar lo siguiente:

- Actualice las rutas de forma dinámica durante los errores de las instancias.
- Elimine la intervención manual para la administración de rutas.
- Brinde una disponibilidad de nivel empresarial para las cargas de trabajo claves.

Esto es sumamente importante para los casos de uso de telecomunicaciones e IoT donde la alta disponibilidad es esencial.

> **Note**
>
> Al utilizar Route Server con varios pares de BGP, tenga presente que, con el servidor de rutas, un máximo de 32 pares de BGP pueden anunciar el mismo prefijo en la misma tabla de enrutamiento.

Considere la posibilidad de integrar entornos con Route Server de AWS para los que necesitan un enrutamiento dinámico, una conmutación por error automática y una distribución de la carga entre numerosas instancias. Route Server permite el enrutamiento dinámico basado en BGP en lugar de rutas estáticas, lo que ofrece:

- Anuncio de rutas dinámicas desde instancias a través de BGP.
- Conmutación por error automática entre numerosas instancias de destino.
- Distribución de cargas en numerosos puntos de conexión.
- Administración centralizada de rutas a través de protocolos BGP.

Este es un caso de uso importante para las implementaciones empresariales en donde las capacidades de enrutamiento dinámico y de alta disponibilidad son obligatorias. Consulte la documentación de Route Server de AWS para obtener instrucciones detalladas de configuración de Route Server.

Limpieza

Elimine los recursos que haya creado en este tutorial para evitar cargos recurrentes:

Paso 1: finalizar la instancia de EC2

Complete este paso para finalizar la instancia de EC2 y evitar cargos adicionales por los recursos de cómputo.

AWS Consola de

1. Abra la consola de Amazon EC2.
2. En el panel de navegación de la consola EC2, elija Instancias.
3. Seleccione la instancia y elija Estado de la instancia, Finalizar instancia.
4. Seleccione Finalizar para confirmar.

AWS CLI

```
aws ec2 terminate-instances --instance-ids i-0123456789abcdef0 --region us-east-1
```

Paso 2: separar un puerta de enlace de Internet de una VPC

Complete este paso para separar y eliminar la puerta de enlace de Internet de la VPC.

AWS Consola de

1. Abra la Consola de Amazon VPC.
2. En el panel de navegación de la consola de VPC, elija Puertas de enlace de Internet.
3. Seleccione el puerta de enlace de Internet y elija Acciones, Separar de la VPC.
4. Elija Separar la puerta de enlace de Internet.
5. Elija Acciones, Eliminar puerta de enlace de Internet tras haber realizado la separación.
6. Elija Eliminar puerta de enlace de Internet.

AWS CLI

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0 --region us-east-1

aws ec2 delete-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --region
 us-east-1
```

Paso 3: eliminar la VPC

Complete este paso para eliminar la VPC y todos los recursos asociados para completar el proceso de limpieza.

AWS Consola de

1. En la consola de VPC, seleccione Sus VPC.
2. Seleccione la VPC y elija Acciones, Eliminar VPC.
3. Escriba **`delete`** para confirmar y seleccione Eliminar.

AWS CLI

```
aws ec2 delete-vpc --vpc-id vpc-0123456789abcdef0 --region us-east-1
```

> **Note**
>
> Cuando elimine la VPC, también se eliminarán las subredes asociadas, las tablas de enrutamiento y los grupos de seguridad.

> **Note**
>
> El grupo BYOIP permanecerá disponible para su uso futuro y no se elimina como parte de este proceso de limpieza.

Enrutamiento dinámico en su VPC con VPC Route Server

VPC Route Server de Amazon simplifica el enrutamiento del tráfico entre las cargas de trabajo que se implementan dentro de una VPC y sus puertas de enlace de Internet. Con esta característica,

VPC Route Server actualiza dinámicamente las tablas de enrutamiento de la VPC y las puertas de enlace de Internet con sus rutas IPv4 o IPv6 preferidas para lograr la tolerancia a errores de enrutamiento para esas cargas de trabajo. Esto permite redirigir automáticamente el tráfico dentro de una VPC, lo que aumenta la capacidad de administración del enrutamiento de la VPC y la interoperabilidad con cargas de trabajo de terceros.

El servidor de enrutamiento admite los siguientes tipos de tabla de enrutamiento:

- Tablas de enrutamiento de VPC no asociadas a subredes
- Tablas de enrutamiento de subred
- Tabla de enrutamiento de puerta de enlace de Internet

El servidor de rutas no admite tablas de enrutamiento asociadas a las puertas de enlace privadas virtuales. Para propagar rutas en una tabla de enrutamiento de puerta de enlace, utilice Transit Gateway Connect.

Cuotas

Para ver las cuotas asociadas a VPC Route Server de Amazon, consulte Cuotas de servidores de rutas.

Precios de

Para obtener información sobre los costos asociados a VPC Route Server de Amazon, consulte la pestaña VPC Route Server en la página de precios de VPC de Amazon.

Contenido

- Terminología
- Cómo funciona VPC Route Server de Amazon
- Registro de pares del servidor de enrutamiento
- Tutorial de introducción

Terminología

Los siguientes términos se utilizan en esta guía:

- FIB: La Base de información de reenvío (FIB, Forwarding Information Base) sirve como tabla de reenvío para indicar las rutas que el servidor de enrutamiento determinó que son las mejores rutas

de la RIB tras evaluar toda la información y las políticas de enrutamiento disponibles. Las rutas FIB que están instaladas en las tablas de enrutamiento. La FIB se vuelve a calcular cada vez que se producen cambios en la RIB.

- RIB: La base de información de enrutamiento (RIB, Routing Information Base) sirve como una base de datos que almacena toda la información de enrutamiento y los datos de topología de red recopilados por un enrutador o sistema de enrutamiento, como las rutas aprendidas de los pares de BGP. La RIB se actualiza constantemente a medida que se recibe nueva información de enrutamiento o cambian las rutas existentes. Esto garantiza que el servidor de enrutamiento siempre tenga la vista más actualizada de la topología de la red y pueda tomar decisiones de enrutamiento óptimas.
- Servidor de enrutamiento: el componente del servidor de enrutamiento actualiza las tablas de enrutamiento de la VPC y la puerta de enlace de Internet con las rutas IPv4 o IPv6 de su Base de información de reenvío (FIB). El servidor de enrutamiento representa una FIB y una Base de información de enrutamiento (RIB) únicas.
- Asociación de servidores de enrutamiento: una asociación de servidores de enrutamiento es la conexión que se establece entre un servidor de enrutamiento y una VPC.
- Punto de conexión del servidor de enrutamiento: un punto de conexión del servidor de enrutamiento es un componente administrado por AWS dentro de una subred que facilita las conexiones BGP (Border Gateway Protocol) entre su servidor de enrutamiento y sus pares de BGP.
- Servidor de enrutamiento homólogo: un servidor de enrutamiento homólogo es una sesión entre un punto de conexión del servidor de enrutamiento y el dispositivo instalado en AWS (por ejemplo, un dispositivo de firewall u otra función de seguridad de red que se ejecute en una instancia EC2). El dispositivo debe cumplir los requisitos siguientes:
  - Disponer de una interface de red elástica en la VPC
  - Support BGP (Border Gateway Protocol)
  - Poder iniciar sesiones de BGP
- Propagación del servidor de enrutamiento: cuando está habilitada, la propagación del servidor de enrutamiento instala las rutas de la FIB en la tabla de enrutamiento que haya especificado. El servidor de enrutamiento admite la propagación de rutas IPv4 e IPv6.

Cómo funciona VPC Route Server de Amazon

Esta sección explica cómo funciona VPC Route Server de Amazon y le ayuda a entender cómo logra la tolerancia a errores de enrutamiento para las cargas de trabajo que se ejecutan en subredes.

Contenido

- Descripción general
- Diagramas

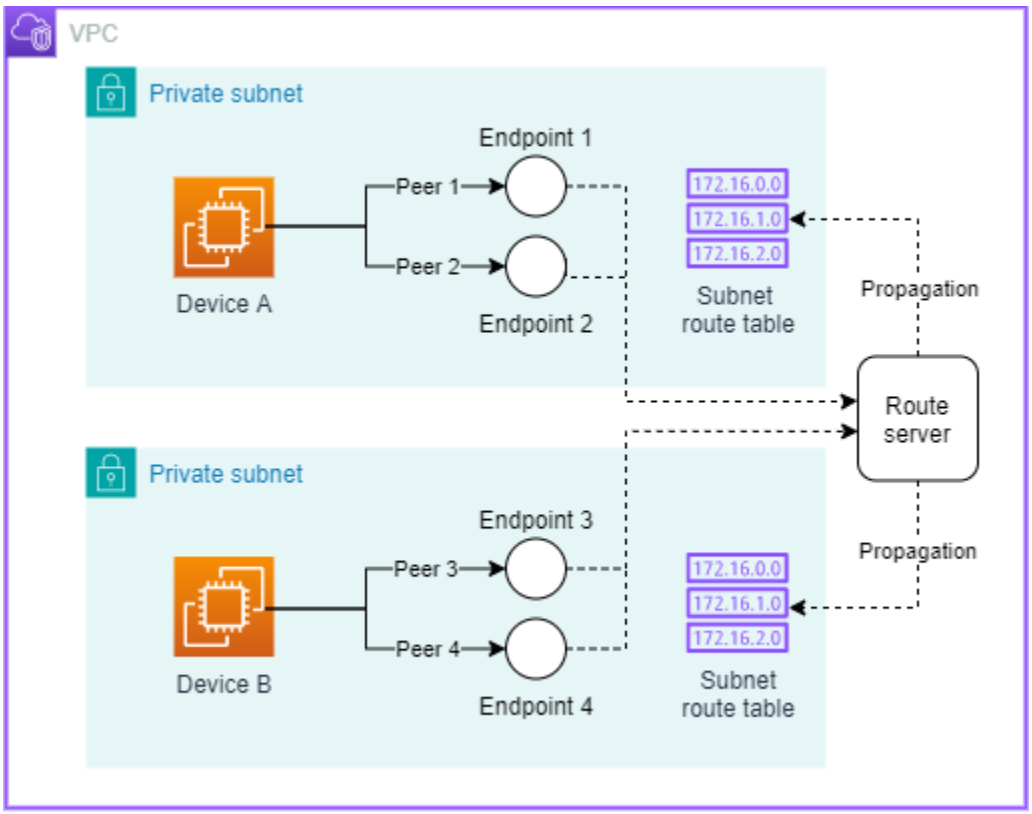
Descripción general

Cómo funciona VPC Route Server de Amazon:

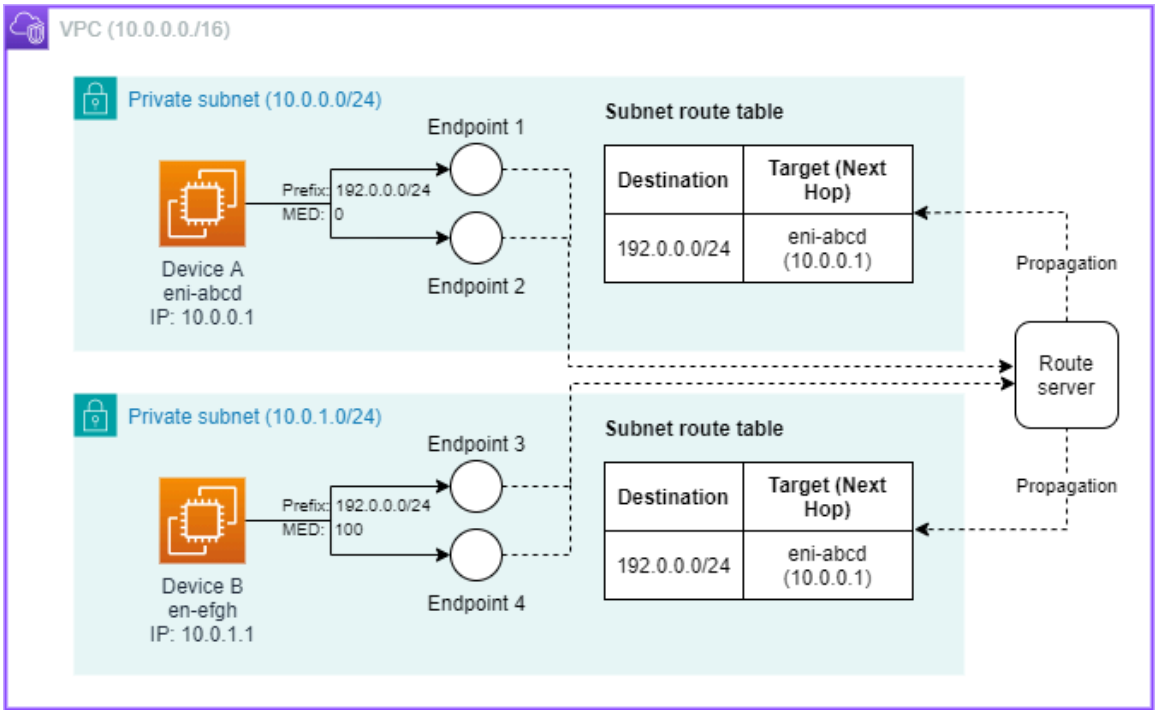
1. Debe configurar un dispositivo de red (como un firewall que se ejecuta en una instancia EC2 de la VPC) para usar VPC Route Server de Amazon.
2. Se produce un error en el dispositivo de red.
3. Los puntos de conexión del servidor de rutas detectan la falla mediante la BFD (detección de reenvío bidireccional) configurada en el servidor de rutas par.
4. Los puntos de conexión del servidor de rutas actualizan el servidor de rutas para retirar las rutas de una Base de información de enrutamiento (RIB), donde el dispositivo que falla es el siguiente salto.
5. El servidor de rutas calcula una Base de información de reenvío (FIB) desde la RIB y selecciona las mejores rutas disponibles.
6. El servidor de rutas actualiza las tablas de enrutamiento configuradas con las rutas de la FIB.
7. Todo el tráfico nuevo se reenvía al dispositivo en espera.

Diagramas

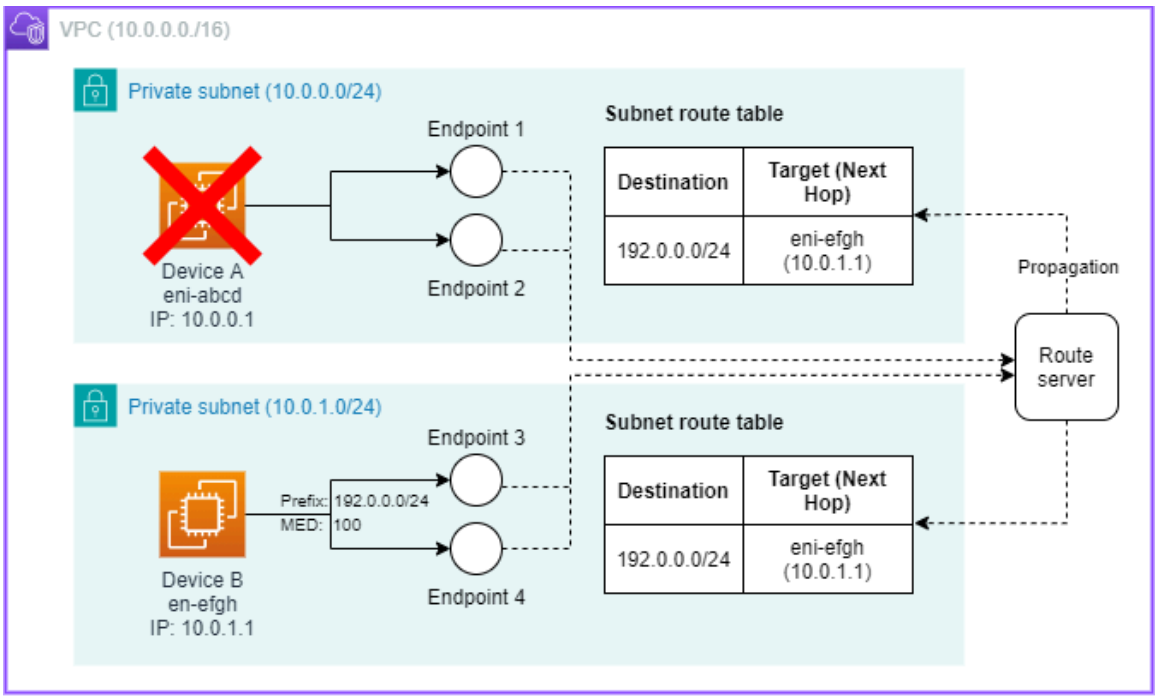
El siguiente es un diagrama de ejemplo de un servidor de rutas de VPC con puntos de conexión de servidor de rutas configurados para dispositivos en dos subredes.



Si se toma el ejemplo anterior como referencia, el ejemplo siguiente muestra un diseño más detallado, en el que tanto el dispositivo A como el dispositivo B anuncian a través de BGP que pueden aceptar cualquier tráfico con una IP de destino en el rango de 192.0.0.0/24 (de 192.0.0.0 a 192.0.0.255). El atributo MED (discriminador de salidas múltiples) de 0 indica al servidor de rutas que se debe preferir al dispositivo A sobre el dispositivo B. El servidor de rutas recibe la ruta y el atributo MED del dispositivo A e instala esa ruta en las tablas de rutas de subred con la interfaz de red del dispositivo A como “siguiente salto”. Como resultado, cualquier tráfico dentro de la subred con una IP de destino en el rango 192.0.0.0/24 se envía al dispositivo A. Luego, el dispositivo A procesa el tráfico y lo envía al siguiente paso. El tráfico dentro de cualquiera de las subredes (10.0.0.0/24 o 10.0.1.0/24) que se dirija a 192.0.0.0/24 se enrutará al dispositivo A eni-abcd (10.0.0.1) en el siguiente salto.



El último ejemplo que aparece a continuación muestra cómo el servidor de rutas administra la conmutación por error. Si bien el atributo MED más alto indica al servidor de rutas que el dispositivo B es menos preferido que el dispositivo A, si el dispositivo A eni-abcd (10.0.0.1) deja de funcionar, el servidor de rutas actualiza las tablas de rutas de la subred y el tráfico a 192.0.0.0/24 se enruta al dispositivo B eni-efgh (10.0.1.1) en el siguiente salto.



Registro de pares del servidor de enrutamiento

Utilice el registro de pares del servidor de enrutamiento de VPC cuando necesite realizar lo siguiente:

- Supervisar el estado de las sesiones de BGP y BFD
- Solucionar problemas de conexión
- Revisar los cambios históricos de las sesiones
- Realizar un seguimiento del estado de la red

Precios

- CloudWatch: se aplican costos por archivo e ingesta de datos para los registros a la venta cuando se publican registros de pares de servidor de enrutamiento en registros de CloudWatch.
- S3: se aplican costos por archivo e ingesta de datos para los registros a la venta cuando se publican registros pares de servidor de enrutamiento en registros en Amazon S3.
- Data Firehose: se aplican los cargos estándar de ingesta y entrega.

Los registros a la venta son registros de servicios específicos de AWS que están disponibles con precios escalonados según el volumen y se entregan a registros de CloudWatch, Amazon S3 o Amazon Data Firehose. Para obtener más información, abra Precios de Amazon CloudWatch seleccione Logs (Registros) y consulte Vended Logs (Registros distribuidos).

Ejemplo de formato de registro

```
{
    "resource_arn": "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0",
    "event_timestamp": 1746643505367,
    "type": "RouteStatus",
    "status": "ADVERTISED",
    "message": {
        "prefix": "10.24.34.0/32",
        "asPath": "65000",
        "med": 100,
        "nextHopIp": "10.24.34.1"
    }
}

{
```

```
    "resource_arn": "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0",
    "event_timestamp": 1746643490000,
    "type": "BGPStatus",
    "status": "UP",
    "message": null
}
```

Donde:

- El `resource_arn` es el ARN del par del servidor de enrutamiento.
- La `event_timestamp` es la marca de tiempo del evento.
- El `type` de eventos de registro que producimos (`RouteStatus`, `BGPStatus`, `BFDStatus`).
- El campo `status` es la actualización de estado.
  - Para mensajes de tipo `RouteStatus`
    - `ADVERTISED` (el enrutamiento fue anunciado por el par)
    - `UPDATED` (el par actualizó el enrutamiento existente)
    - `WITHDRAWN` (el par retiró el enrutamiento)
  - Para actualizaciones de `BFDStatus` y `BGPStatus`
    - `UP`, `DOWN`.
- Actualmente, el campo `message` solo se usa para los atributos de enrutamiento del tipo de mensaje RouteStatus, pero puede rellenarse con información relevante para cualquier tipo.

AWS Management Console

Cómo crear registros de par de servidor de enrutamiento:

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en Nube privada de virtualización, seleccione Servidores de ruta.
3. En la página Servidores de rutas, elija Pares servidor de enrutamiento.
4. Elija la pestaña Entrega de registros.
5. Elija Añadir entrega de registros.
6. Elija un destino y configure los ajustes:
   - Registros de Amazon CloudWatch

- Tipo de registro: los tipos de registros que se van a entregar. El único tipo de registro compatible es EVENT_LOGS.
- Grupo de registros de destino: el grupo de registros de CloudWatch al que se enviarán los registros. Puede elegir un grupo de registros existente o crear uno nuevo (por ejemplo: /aws/vpc/route-server-peers).
- Selección de campos: los campos de datos que incluirá en sus registros.
- Formato de salida: cómo se formatean los registros:
  - JSON: formato estructurado para procesamiento por computadora
  - Texto: formato de texto sin formato
- Delimitador de campo: cuando se utiliza el formato de texto, es el carácter que separa los campos (por ejemplo: coma, tabulación, espacio).

- Amazon S3
  - Cuenta cruzada: envío de registros a diferentes cuentas de AWS
    - Tipo de registro: los tipos de registros que se van a entregar. El único tipo de registro compatible es EVENT_LOGS.
    - ARN de destino de entrega: el nombre del recurso de Amazon del bucket de S3 en otra cuenta de AWS a la que se enviarán los registros.
    - Selección de campos: los campos de datos que incluirá en sus registros.
    - Sufijo: la extensión que se añade a los nombres de los archivos de registro (por ejemplo: .log, .txt).
    - Compatible con Hive: cuando está activado, organiza los registros en una estructura de carpetas que funciona con las herramientas basadas en Hive para facilitar la búsqueda con servicios como Amazon Athena.
    - Delimitador de campos: cuando se utiliza el formato de texto, es el carácter que separa los campos.
  - En la cuenta actual
    - Tipo de registro: los tipos de registros que se van a entregar. El único tipo de registro compatible es EVENT_LOGS.
    - Bucket de S3 de destino: el bucket de S3 de su cuenta al que se enviarán los registros. Puede especificar la ruta de una subcarpeta.
    - Selección de campos: los campos de datos que incluirá en sus registros.

- Sufijo: la extensión que se añade a los nombres de los archivos de registro (por ejemplo: .log, .txt).
- Compatible con Hive: cuando está activado, organiza los registros en una estructura de carpetas que funciona con las herramientas basadas en Hive para facilitar la búsqueda.
- Delimitador de campos: cuando se utiliza el formato de texto, es el carácter que separa los campos.

- Amazon Data Firehose
  - Entre cuentas
    - Tipo de registro: los tipos de registros que se van a entregar. El único tipo de registro compatible es EVENT_LOGS.
    - ARN de destino de entrega: el nombre de recurso de Amazon del flujo de entrega de Firehose en otra cuenta de AWS.
    - Selección de campos: los campos de datos que incluirá en sus registros.
    - Delimitador de campos: cuando se utiliza el formato de texto, es el carácter que separa los campos.
  - En la cuenta actual
    - Tipo de registro: los tipos de registros que se van a entregar. El único tipo de registro compatible es EVENT_LOGS.
    - Flujo de destino de la entrega: el flujo de entrega de Firehose de su cuenta a la que se enviarán los registros. El flujo debe usar el tipo de origen "Direct Put".
    - Selección de campos: los campos de datos que incluirá en sus registros.
    - Formato de salida: cómo se formatean los registros:
      - JSON: formato estructurado para procesamiento por computadora
      - Texto: formato de texto sin formato
    - Delimitador de campos: cuando se utiliza el formato de texto, es el carácter que separa los campos.

Command line

Los comandos de esta sección contienen enlaces a la Referencia de comandos de la AWS CLI. La documentación proporciona descripciones detalladas de las opciones que puede utilizar al ejecutar los comandos.

Cómo crear registros de par de servidor de enrutamiento:

1. Utilice el comando put-delivery-source.

   - Ejemplo de solicitud

```
aws logs put-delivery-source --name "source-rsp-1234567890abcdef0" --
resource-arn "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0" --log-type "EVENT_LOGS"
```

   - Respuesta de ejemplo

```
{
     "deliverySource": {
        "name": "source-rsp-1234567890abcdef0",
        "arn": "arn:aws:logs:us-east-1:111122223333:delivery-source:source-
rsp-1234567890abcdef0",
        "resourceArns": [
            "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0"
        ],
        "service": "ec2",
        "logType": "EVENT_LOGS"
    }
}
```

2. Utilice el comando put-delivery-destination.

   - El siguiente ejemplo de la CLI de AWS crea un registro del servidor de enrutamiento. Los registros se entregan al grupo de registros especificado.
   - Ejemplo de solicitud

```
aws logs put-delivery-destination --name "destination-rsp-abcdef01234567890"
 --destination-resource-arn "arn:aws:logs:us-east-1:111122223333:log-group:/
aws/vendedlogs/ec2/route-server-peer/EVENT_LOGS/rsp-abcdef01234567890"
```

   - Respuesta de ejemplo

```
{
     "deliveryDestination": {
        "name": "destination-rsp-abcdef01234567890",
```

```
        "arn": "arn:aws:logs:us-east-1:111122223333:delivery-
destination:destination-rsp-abcdef01234567890",
        "deliveryDestinationType": "CWL",
        "deliveryDestinationConfiguration": {
            "destinationResourceArn": "arn:aws:logs:us-
east-1:111122223333:log-group:/aws/vendedlogs/ec2/route-server-peer/
EVENT_LOGS/rsp-abcdef01234567890"
        }
    }
}
```

3. Utilice el comando create-delivery.

   - Ejemplo de solicitud

```
aws logs create-delivery --delivery-source-name "source-rsp-1234567890abcdef0"
 --delivery-destination-arn "arn:aws:logs:us-east-1:111122223333:delivery-
destination:destination-rsp-abcdef01234567890"
```

   - Respuesta de ejemplo

```
{
     "delivery": {
        "id": "1234567890abcdef0",
        "arn": "arn:aws:logs:us-
east-1:111122223333:delivery:1234567890abcdef0",
        "deliverySourceName": "source-rsp-1234567890abcdef0",
        "deliveryDestinationArn": "arn:aws:logs:us-
east-1:111122223333:delivery-destination:destination-rsp-abcdef01234567890",
        "deliveryDestinationType": "CWL",
        "recordFields": [
            "resource_arn",
            "event_timestamp",
            "type",
            "status",
            "message"
        ]
    }
}
```

Tutorial de introducción

En este tutorial, se muestra el proceso de configuración y configuración de VPC Route Server de Amazon para habilitar el enrutamiento dinámico en la VPC. Aprenderá a crear y configurar todos los componentes necesarios, a establecer el emparejamiento de BGP y a verificar su correcto funcionamiento. El tutorial abarca todo, desde la configuración inicial de IAM hasta las pruebas y la limpieza.

Antes de iniciar este tutorial, asegúrese de que cuenta con:

- Acceso administrativo a una cuenta AWS
- Una VPC con al menos dos subredes en las que desee habilitar el enrutamiento dinámico
- Dispositivos de red (como firewalls que se ejecutan en instancias EC2) que admiten BGP y pueden servir como dispositivos homólogos del servidor de rutas
- Familiaridad básica con los conceptos de BGP y las redes AWS

Los pasos se pueden completar mediante la consola de administración AWS o AWS CLI. Se proporcionan ambos métodos para cada paso.

Tiempo estimado para completar la operación: 15-30 minutos

Steps

- Paso 1: Configurar los permisos del rol de IAM requeridos
- Paso 2: Creación de un servidor de ruta
- Paso 3: asociar el servidor de enrutamiento a una VPC
- Paso 4: Crear puntos de conexión del servidor de enrutamiento
- Paso 5: habilitar la propagación del servidor de enrutamiento
- Paso 6: Crear el par de servidor de enrutamiento
- Paso 7: Iniciar sesiones de BGP desde los dispositivos
- Paso 8: Eliminar

Paso 1: Configurar los permisos del rol de IAM requeridos

Para utilizar VPC Route Server, asegúrese de que el usuario o rol de IAM que utiliza tiene los permisos de IAM necesarios. A continuación, encontrará una guía sobre los permisos necesarios para cada API:

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateRouteServer",
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteRouteServer",
            "Effect": "Allow",
            "Action": [
                "sns:DeleteTopic"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateRouteServerEndpoint",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateTags",
                "ec2:DeleteTags"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteRouteServerEndpoint",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateTags",
```

```
                "ec2:DeleteTags"
            ],
            "Resource": "*"
        },
        {
            "Sid": "CreateRouteServerPeer",
            "Effect": "Allow",
            "Action": [
                "ec2:AuthorizeSecurityGroupIngress"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DeleteRouteServerPeer",
            "Effect": "Allow",
            "Action": [
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Resource": "*"
        }
    ]
}
```

Paso 2: Creación de un servidor de ruta

Complete los pasos de esta sección para crear un servidor de ruta.

El componente del servidor de rutas actualiza las tablas de enrutamiento de la VPC y la puerta de enlace de Internet con las rutas IPv4 o IPv6 de la Base de información de reenvío (FIB). El servidor de enrutamiento representa una FIB y una Base de información de enrutamiento (RIB) únicas.

AWS Management Console

Para crear un servidor de ruta

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en Nube privada de virtualización, seleccione Servidores de ruta.
3. En la página Servidores de rutas, elija Crear servidor de rutas.
4. En la página Crear servidor de rutas, configure los siguientes ajustes:

- En Nombre, introduzca un nombre para su servidor de rutas (por ejemplo, “my-route-server-01”). El nombre debe tener menos de 255 caracteres de longitud.
- Para Amazon Side ASN, introduzca un valor de ASN BGP. El valor debe estar en el rango de 1 a 4294967295. Recomendamos utilizar un ASN privado en el rango de 64512 a 65534 (ASN de 16 bits) o en el rango de 4200000000 a 4294967294 (ASN de 32 bits).
- Para las rutas persistentes seleccione Activar o Desactivar. Esta opción determina si las rutas deben mantenerse una vez finalizadas todas las sesiones de BGP:
  - Si está habilitada: las rutas se conservarán en la base de datos de enrutamiento del servidor de rutas incluso si finalizan todas las sesiones de BGP
  - Si está deshabilitada: las rutas se eliminarán de la base de datos de enrutamiento cuando finalicen todas las sesiones de BGP
- Si activó las rutas persistentes, para Duración de la persistencia, introduzca un valor entre 1 y 5 minutos. Esta duración especifica cuánto tiempo esperará el servidor de rutas después de restablecer el BGP para dejar de persistir las rutas. Por ejemplo, si lo configura en 1 minuto, el dispositivo dispondrá de 1 minuto después de restablecer el BGP para volver a aprender y anunciar sus rutas antes de que el servidor de rutas reanude su funcionamiento normal. Si bien 1 minuto suele ser suficiente, puede configurar hasta 5 minutos si su red BGP necesita más tiempo para restablecer y volver a aprender por completo todas las rutas.
- (Opcional) Para activar las notificaciones de SNS para los cambios de estado de BGP, active la opción Activar notificaciones de SNS. Al activar las notificaciones de SNS, se mantienen los cambios de estado de las sesiones de BGP o BFD en los servidores de rutas homólogos y las notificaciones de mantenimiento en los puntos de conexión del servidor de rutas se mantienen en un tema de SNS proporcionado por AWS. Para obtener más información sobre estas notificaciones, consulte la tabla de detalles de las notificaciones de SNS. que aparece a continuación.

5. (Opcional) Para añadir etiquetas a su servidor de rutas, desplácese hacia abajo hasta la sección Etiquetas (opcional) y seleccione Añadir nueva etiqueta. Introduzca una clave y un valor opcional para cada etiqueta. Puede añadir hasta 50 etiquetas.
6. Revise la configuración y seleccione Crear servidor de enrutamiento.
7. Espere a que se cree el servidor de enrutamiento. Una vez completado, se le redirigirá a la página de servidores de enrutamiento, donde podrá ver su nuevo servidor de enrutamiento en la lista con el estado Disponible.

Command line

Utilice el siguiente procedimiento para crear un nuevo servidor de enrutamiento para administrar el enrutamiento dinámico en una VPC.

Para `--amazon-side-asn`, introduzca un valor ASN de BGP. El valor debe estar en el rango de 1 a 4294967295. Recomendamos utilizar un ASN privado en el rango de 64512 a 65534 (ASN de 16 bits) o en el rango de 4200000000 a 4294967294 (ASN de 32 bits).

1. Comando:

```
aws ec2 create-route-server --amazon-side-asn 65000
```

   Respuesta:

```
{
    "RouteServer": {
        "RouteServerId": "rs-1",
        "AmazonSideAsn": 65000,
        "State": "pending"
    }
}
```

2. Espere a que el servidor de enrutamiento esté disponible.

   Comando:

```
aws ec2 describe-route-servers
```

   Respuesta:

```
{
    "RouteServer": {
        "RouteServerId": "rs-1",
        "AmazonSideAsn": 65000,
        "State": "available"
    }
}
```

Detalles de notificaciones SNS

En la siguiente tabla se muestran detalles sobre los mensajes que Amazon VPC Route Server enviará mediante Amazon SNS:

Campos estándar		Atributos del mensaje (metadatos)			
Mensaje	Cuándo se envía	timestamp	eventCode	routeServerEndpointId	affectedRouteServerPeerIds
El Punto de conexión de Route Server [ENDPOINT ID] se encuentra ahora en fase de mantenimiento. Es posible que las sesiones de BFD y BGP se vean afectadas.	Mantenimiento de puntos de conexión de Route Server	Formato: 2025-02-17T15:55:00 Z	ROUTE_SERVER_ENDPOINT_MAINTENANCE	ID de punto de conexión afectado	Lista de identificadores de pares afectados
Mensaje	Cuándo se envía	timestamp	eventCode	routeServerPeerId	newBgpStatus
El BGP para Route Server Peer [PEER ID] ahora está [ACTIVO/DESACTIVADO].	Cambio de estado de BGP del mismo servidor de enrutamiento	Formato: 2025-02-17T15:55:00 Z	ROUTE_SERVER_PEER_BGP_STATUS_CHANGE	ID de par afectado	ACTIVO o DESACTIVADO

Campos estándar		Atributos del mensaje (metadatos)			
Mensaje	Cuándo se envía	timestamp	eventCode	routeServerPeerId	newBfdStatus
El BFD de Route Server Peer [PEER ID] ahora está [ACTIVO/DESACTIVADO].	Cambio de estado del BFD del mismo servidor de enrutamiento	Formato: 2025-02-17T15:55:00 Z	ROUTE_SERVER_PEER_BFD_STATUS_CHANGE	ID de par afectado	ACTIVO o DESACTIVADO

Paso 3: asociar el servidor de enrutamiento a una VPC

Complete los pasos de esta sección para asociar el servidor de enrutamiento a una VPC.

Una asociación de servidores de enrutamiento es la conexión que se establece entre un servidor de rutas y una VPC. Este es un paso de configuración fundamental que permite que el servidor de enrutamiento funcione con los dispositivos de su VPC.

Al crear una asociación de servidores de enrutamiento:

- Vincula el servidor de enrutamiento a una VPC específica.
- Permite que el servidor de enrutamiento interactúe con las tablas de enrutamiento de las subredes de la VPC.
- Permite al servidor de enrutamiento recibir y propagar rutas dentro de la VPC asociada.
- Establece el ámbito en el que puede operar el servidor de enrutamiento.

Aspectos clave de una asociación de servidores de enrutamiento:

- Cada servidor de enrutamiento se puede asociar a una VPC. Cada VPC puede tener hasta 5 asociaciones de servidores de enrutamiento independientes de forma predeterminada. Para obtener más información sobre cuotas, consulte cuotas del servidor de enrutamiento.

- Debe crearse la asociación para que el servidor de enrutamiento pueda administrar rutas.
- La asociación se puede monitorear para rastrear su estado (por ejemplo, asociar y asociar).
- La asociación se puede eliminar (disociar) si ya no desea que el servidor de enrutamiento funcione en esa VPC.

AWS Management Console

Asociar una VPC a una tabla de enrutamiento

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en Nube privada de virtualización, seleccione Servidores de ruta.
3. Seleccione el servidor de enrutamiento que desea asociar a una VPC.
4. En la pestaña Asociación, elija Asociar servidor de enrutamiento.
5. En el cuadro de diálogo Asociar servidor de enrutamiento:
   - El campo ID del servidor de enrutamiento se rellena automáticamente con el servidor de enrutamiento seleccionado
   - Para el ID de VPC, elija la VPC que desea asociar en la lista desplegable.
6. Elija Asociar servidor de enrutamiento.
7. Espere a que se complete la asociación del ASN. Una vez finalizado, el Estado aparecerá como Asociado en la pestaña Asociación.

Command line

Utilice el siguiente procedimiento para asociar una VPC a un servidor de enrutamiento.

1. Comando:

```
aws ec2 associate-route-server --route-server-id rs-1 --vpc-id vpc-1
```

Respuesta:

```
{
    "RouteServerAssociation": {
        "RouteServerId": "rs-1",
        "VpcId": "vpc-1",
        "State": "associating"
```

```
    }
}
```

2. Espere a que se complete la asociación del ASN.

   Comando:

   ```
   aws ec2 get-route-server-associations --route-server-id rs-1
   ```

   Respuesta:

   ```
   {
       "RouteServerAssociation": {
           "RouteServerId": "rs-1",
           "VpcId": "vpc-1",
           "State": "associated"
       }
   }
   ```

Paso 4: Crear puntos de conexión del servidor de enrutamiento

Complete los pasos de esta sección para crear puntos de conexión del servidor de enrutamiento. Cree dos puntos de conexión por subred para garantizar la redundancia.

Un punto de conexión del servidor de enrutamiento es un componente AWS administrado dentro de una subred que ayuda las conexiones BGP (Border Gateway Protocol) entre su servidor de enrutamiento y sus pares de BGP.

Los puntos de conexión del servidor de enrutamiento son los “puntos de contacto” en los que los dispositivos de red establecen sesiones de BGP con el servidor de enrutamiento. Son los componentes que realmente administran las conexiones BGP, mientras que el propio servidor de enrutamiento administra las decisiones de enrutamiento y la propagación de las rutas.

> **Note**
>
> Los puntos de conexión del servidor de enrutamiento pagan 0,75 USD por hora.

AWS Management Console

Para crear puntos de conexión del servidor de enrutamiento

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, en Nube privada de virtualización, seleccione Servidores de ruta.
3. Seleccione el servidor de enrutamiento para el que desea crear puntos de conexión.
4. En el panel inferior, elija la pestaña Puntos de conexión del servidor de enrutamiento.
5. Seleccione Crear punto de conexión del servidor de enrutamiento.
6. En la página Crear punto de conexión del servidor de enrutamiento, configure los siguientes ajustes:
   - En Name (Nombre), ingrese un nombre descriptivo para el punto de conexión.
   - Para el servidor de enrutamiento, confirme que se seleccionó el servidor de enrutamiento correcto.
   - En Subredes, seleccione la subred en la cual desea crear el punto de conexión.
7. (Opcional) Para añadir etiquetas al punto de conexión del servidor de enrutamiento, desplácese hacia abajo hasta la sección Etiquetas: opcional y seleccione Añadir nueva etiqueta. Introduzca una clave y un valor opcional para cada etiqueta.
8. Revise la configuración y seleccione Crear punto de conexión para el servidor de enrutamiento.
9. Espere a que se cree el punto de conexión. Una vez finalizado, verá un mensaje indicándole que la operación se realizó correctamente.
10. Repita los pasos 5 a 9 para crear un segundo punto de conexión en la misma subred, con un nombre diferente.
11. Repita los pasos 5 a 10 para cada subred en la que necesite punto de conexión del servidor de enrutamiento.
12. Tras crear los punto de conexión, vuelva a la pestaña punto de conexión del servidor de enrutamiento correspondiente a su servidor de enrutamiento.
13. Compruebe que aparecen dos punto de conexión en la lista para cada subred.
14. Compruebe que el estado de cada punto de conexión esté disponible.

Command line

Utilice el siguiente procedimiento para crear un punto de conexión para el servidor de enrutamiento.

1. Comando:

```
aws ec2 create-route-server-endpoint --route-server-id rs-1 --subnet-id subnet-1
```

Respuesta:

```
{
    "RouteServerEndpoint": {
        "RouteServerId": "rs-1",
        "RouteServerEndpointId": "rse-1",
        "VpcId": "vpc-1",
        "SubnetId": "subnet-1",
        "State": "pending"
    }
}
```

2. Puede que tenga que esperar unos minutos para que los puntos de conexión estén completamente disponibles después de crearlos.

Comando:

```
aws ec2 describe-route-server-endpoints
```

Respuesta:

```
{
    "RouteServerEndpoint": {
        "RouteServerId": "rs-1",
        "RouteServerEndpointId": "rse-1",
        "VpcId": "vpc-1",
        "SubnetId": "subnet-1",
        "EniId": "eni-123",
        "EniAddress": "10.1.2.3",
        "State": "available"
    }
}
```

Repita los pasos para crear un segundo punto de conexión en la misma subred con un nombre diferente y cree un punto de conexión para cada subred en la que necesite punto de conexión del servidor de enrutamiento.

Paso 5: habilitar la propagación del servidor de enrutamiento

Complete este paso para habilitar la propagación del servidor de enrutamiento.

Cuando está habilitada, la propagación del servidor de enrutamiento instala las rutas de la FIB en la tabla de enrutamiento que haya especificado. El servidor de enrutamiento admite la propagación de rutas IPv4 e IPv6.

La propagación del servidor de enrutamiento es el mecanismo que automatiza las actualizaciones de las tablas de enrutamiento: en lugar de actualizar manualmente las tablas de rutas, el servidor de enrutamiento propaga automáticamente las rutas apropiadas a las tablas de enrutamiento configuradas con las rutas de la FIB.

Aspectos clave de la propagación del servidor de enrutamiento:

- Configuración
  - Vincula un servidor de rutas a tablas de enrutamiento específicas
  - Determina qué tablas de enrutamiento recibirán actualizaciones de rutas dinámicas
  - Se puede habilitar o deshabilitar por tabla de enrutamiento
- Funcionalidad
  - Actualiza automáticamente las tablas de enrutamiento con las rutas aprendidas de los pares de BGP
  - Propaga las mejores rutas disponibles en función de los atributos de BGP
  - Mantiene la coherencia de las rutas en las tablas de enrutamiento especificadas
  - Actualiza las rutas de forma dinámica cuando cambian las condiciones de la red
- Estados
  - Se puede activar (las rutas se propagan)
  - Se puede desactivar (las rutas no se propagan)

AWS Management Console

Para habilitar la propagación del servidor de enrutamiento

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Seleccione el servidor de enrutamiento para el que desea habilitar la propagación.
3. Seleccione la pestaña Propagaciones en el panel de detalles del servidor de enrutamiento.
4. Elija Enable propagation (Activar propagación).
5. En el cuadro de diálogo Activar la propagación:
   - El ID del servidor de enrutamiento se rellenará automáticamente.
   - En Tabla de enrutamiento, seleccione la tabla de enrutamiento de destino en el menú desplegable para las rutas recién propagadas.
6. Seleccione Activar la propagación para confirmar.
7. Espere a que el estado de propagación cambie a Disponible en la lista de propagaciones.
8. Compruebe que la tabla de enrutamiento seleccionada aparezca en la lista de propagaciones con el estado Disponible.

Command line

Utilice el siguiente procedimiento para habilitar la propagación del servidor de enrutamiento.

1. Comando:

```
aws ec2 enable-route-server-propagation --route-table-id rtb-1 --route-server-id
 rs-1
```

Respuesta:

```
{
    "RouteServerRoutePropagation": {
        "RouteServerId": "rs-1",
        "RouteTableId": "rtb-1",
        "State": "pending"
    }
}
```

2. Espere a que el estado de la propagación cambie a disponible.

Comando:

```
aws ec2 get-route-server-propagations --route-server-id rs-1
```

Respuesta:

```
{
    "RouteServerRoutePropagation": {
        "RouteServerId": "rs-1",
        "RouteTableId": "rtb-1",
        "State": "available"
    }
}
```

Paso 6: Crear el par de servidor de enrutamiento

Un servidor de enrutamiento homólogo es una sesión entre un punto de conexión del servidor de enrutamiento y el dispositivo instalado en AWS (como un dispositivo de firewall u otra función de seguridad de red que se ejecute en una instancia EC2). El dispositivo debe cumplir los requisitos siguientes:

- Disponer de una interface de red elástica en la VPC
- Support BGP (Border Gateway Protocol)
- Poder iniciar sesiones de BGP

> **Note**
>
> Se recomienda crear un servidor de enrutamiento equivalente por punto de conexión del servidor de enrutamiento para garantizar la redundancia.

AWS Management Console

Para crear un servidor de enrutamiento par

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

2. En la ruta de navegación, elija VPC > Parejas de servidor de enrutamiento > Crear par de servidor de enrutamiento.
3. En Detalles, configure lo siguiente:
   - Nombre: escriba un nombre para su par de servidor de enrutamiento (hasta 255 caracteres). Ejemplo: my-route-server-peer-01
   - ID de punto final del servidor de rutas: elija un punto de conexión del servidor de enrutamiento en el menú desplegable. Si lo desea, elija Crear un punto de conexión del servidor de enrutamiento para crear uno nuevo.
   - Dirección de par: escriba la dirección IPv4 del par. Debe ser una dirección IP válida. Se debe poder acceder a la dirección del mismo nivel desde el punto de conexión del servidor de enrutamiento.
   - ASN del par: introduzca el ASN (número de sistema autónomo) para el par BGP. El valor debe estar en el rango de 1 a 4294967295. El ASN normalmente debe utilizar rangos privados (64512-65534 para 16 bits o 4200000000-4294967294 para 32 bits)
   - Detección de vitalidad por pares:
     - BGP keepalive (predeterminado): mecanismo estándar de mantenimiento de BGP
     - BFD: detección de reenvío bidireccional para una conmutación por error más rápida
   - (Opcional) En Etiquetas, seleccione Añadir nueva etiqueta para añadir etiquetas de pares clave-valor. Las etiquetas ayudan a identificar y realizar un seguimiento de los recursos de AWS.
4. Revise la configuración y elija Crear servidor de enrutamiento de par.

Command line

Utilice el siguiente procedimiento para crear un servidor de enrutamiento de par.

1. Comando:

```
aws ec2 create-route-server-peer --route-server-endpoint-id rse-1 --peer-address
 10.0.2.3 --bgp-options PeerAsn=65001,PeerLivenessDetection=bfd
```

   Respuesta:

   En la respuesta, los valores de estado pueden ser `pending|available|deleting|deleted`.

```
{
    "RouteServerPeer": {
        "RouteServerPeerId": "rsp-1",
        "RouteServerId": "rs-1",
        "VpcId": "vpc-1",
        "SubnetId": "subnet-1",
        "State": "pending",
        "EndpointEniId": "eni-2,
        "EndpointEniAddress": "10.0.2.4",
        "PeerEniId": "eni-1",
        "PeerAddress": "10.0.2.3",
        "BgpOptions": {
            "PeerAsn": 65001,
   "PeerLivenessDetection": "bfd"
        },
        "BgpStatus": {
            "Status": "Up"
        }
    }
}
```

2. Espere a que el estado de la propagación cambie a disponible.

   Comando:

   ```
   aws ec2 describe-route-server-peers
   ```

   Respuesta:

   ```
   {
       "RouteServerPeer": {
           "RouteServerPeerId": "rsp-1",
           "RouteServerId": "rs-1",
           "VpcId": "vpc-1",
           "SubnetId": "subnet-1",
           "State": "available",
           "EndpointEniId": "eni-2,
           "EndpointEniAddress": "10.0.2.4",
           "PeerEniId": "eni-1",
           "PeerAddress": "10.0.2.3",
           "BgpOptions": {
               "PeerAsn": 65001,
   ```

```
   "PeerLivenessDetection": "bfd"
        },
        "BgpStatus": {
            "Status": "down"
        }
    }
}
```

Paso 7: Iniciar sesiones de BGP desde los dispositivos

Cuando el estado del servidor de rutas homólogo esté disponible, configure su carga de trabajo para iniciar la sesión de BGP con el punto de conexión del servidor de enrutamiento.

En esta guía, no hablaremos de iniciar una sesión de BGP desde los dispositivos de las subredes. El punto de conexión del servidor de enrutamiento no inicia la sesión de BGP.

Para comprobar que la característica del servidor de rutas de VPC funciona, compruebe que la tabla de enrutamiento contiene las mejores rutas propagadas por el servidor de enrutamiento.

Paso 8: Eliminar

Se completó la parte de creación del tutorial. Complete los pasos de esta sección para quitar los componentes del servidor de enrutamiento de VPC que creó.

7.1: Retirar la publicidad de BGP en los dispositivos

Retirar la publicidad de BGP en los dispositivos de sus subredes está fuera del alcance de esta guía. Consulte a su proveedor externo para obtener las configuraciones de BGP según sea necesario.

7.2: Deshabilite la propagación del servidor de enrutamiento

Utilice el siguiente procedimiento para deshabilitar la propagación del servidor de enrutamiento.

AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Seleccione el servidor de enrutamiento para el que desea deshabilitar la propagación.
3. Elija Acciones > Modificar servidor de enrutamiento.
4. Seleccione la pestaña Propagaciones en el panel de detalles del servidor de enrutamiento.

5. Elija la propagación que desee deshabilitar y, a continuación, elija Desactivar la propagación.
6. En el cuadro de diálogo, elija Desactivar la propagación del servidor de enrutamiento.

Command line

1. Desactivar la propagación:

```
aws ec2 disable-route-server-route-propagation --route-table-id rtb-1 --route-
server-id rs-1
```

2. Confirme que se eliminó la propagación:

```
aws ec2 get-route-server-route-propagations --route-server-id rs-1 [--route-
table-id rtb-1]
```

7.3: Eliminar pares del servidor de enrutamiento

Utilice el siguiente procedimiento para eliminar pares de servidor de enrutamiento.

AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En la ruta de navegación, elija Servidores de enrutamiento > Servidores de enrutamiento homólogos.
3. Seleccione un servidor de enrutamiento homólogo.
4. Elija Acciones > Eliminar servidor de enrutamiento homólogo.

Command line

1. Eliminar pares:

```
aws ec2 delete-route-server-peer --route-server-peer-id rsp-1
```

2. Confirme la eliminación:

```
aws ec2 describe-route-server-peers [--route-server-peer-ids rsp-1] [--filters
 Key=RouteServerId|RouteServerEndpointId|VpcId]
```

7.4: Eliminar los punto de conexión del servidor de enrutamiento

Utilice el siguiente procedimiento para eliminar puntos de conexión del servidor de enrutamiento.

AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Seleccione el servidor de enrutamiento para el que desea eliminar puntos de conexión.
3. Elija los punto de conexión del servidor de enrutamiento.
4. Seleccione el punto de conexión y elija Acciones, Eliminar punto de conexión de acceso verificado.
5. Ingrese en Delete (Suprimir) y haga clic en Delete (Suprimir).

Command line

1. Describa punto de conexión:

```
aws ec2 describe-route-server-endpoints
```

2. Elimine los punto de conexión del servidor de enrutamiento:

```
aws ec2 delete-route-server-endpoint --route-server-endpoint-id rse-1
```

3. Confirme que se eliminaron los puntos de conexión:

```
aws ec2 describe-route-server-endpoints [--route-server-endpoint-ids rsp-1] [--
filters Key=RouteServerId|VpcId|SubnetId]
```

7.5: Desasociar el servidor de rutas de la VPC

Utilice el siguiente procedimiento para desasociar el servidor de enrutamiento de la VPC.

AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Seleccione el servidor de enrutamiento para el que desea desasociarse.

3. Elija Asociar.
4. Elija Desasociar el servidor de rutas.
5. Confirme los cambios que se van a realizar y elija Desasociar el servidor de enrutamiento.

Command line

1. Desasocie el servidor de enrutamiento de la VPC:

```
aws ec2 disassociate-route-server --route-server-id rs-1 --vpc-id vpc-1
```

2. Confirme la disociación:

```
aws ec2 get-route-server-associations --route-server-id rs-1
```

7.6 Eliminar el servidor de enrutamiento

Siga este procedimiento para eliminar los servidores de enrutamiento.

AWS Management Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Seleccione el servidor de enrutamiento que desea eliminar.
3. Elija Actions (Acciones), Delete route table (Eliminar servidor de enrutamiento).
4. Escriba Delete (Suprimir) y haga clic en Delete (Suprimir).

Command line

1. Elimine el servidor de enrutamiento.

```
aws ec2 delete-route-server --route-server-id rs-1
```

2. Confirme la eliminación:

```
aws ec2 describe-route-servers [--route-server-ids rs-1] [--filters Key=VpcId]
```

Se completó el tutorial de VPC Route Server de Amazon.

Solución de problemas de accesibilidad en su VPC

Reachability Analyzer es una herramienta de análisis de configuración estática. Utilice Reachability Analyzer para analizar y depurar la accesibilidad de la red entre dos recursos en la VPC. Reachability Analyzer produce detalles salto a salto de la ruta virtual entre estos recursos cuando son accesibles y, en caso contrario, identifica el componente de bloqueo. Por ejemplo, puede identificar las rutas de la tabla de enrutamiento que faltan o están mal configuradas.

Para obtener más información, consulte la Guía del Analizador de accesibilidad.

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 equilibrador de carga de puerta de enlace. 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 Middlebox”.

Contenido

- Requisitos previos del asistente de enrutamiento de Middlebox
- Redirección del tráfico de VPC a un dispositivo de seguridad
- Consideraciones del asistente de enrutamiento de Middlebox
- Escenarios de Middlebox

Requisitos previos del asistente de enrutamiento de Middlebox

Consulte the section called “Consideraciones del asistente de enrutamiento de Middlebox”. A continuación, asegúrese de que dispone de la siguiente información antes de utilizar el asistente de enrutamiento de cuadro intermedio.

- La VPC.
- El recurso en el que el tráfico se origina o entra en la VPC, por ejemplo, una puerta de enlace de Internet, una puerta de enlace 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.

Redirección del tráfico de VPC a un dispositivo de seguridad

El asistente de enrutamiento de middlebox está disponible en la consola de Amazon VPC.

Contenido

- 1. Cree rutas mediante el asistente de enrutamiento de middlebox
- 2. Modificar rutas de Middlebox
- 3. Elimine la configuración del asistente de enrutamiento de middlebox

1. 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).

2. 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 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).

3. 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.

   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.

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.
- 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 enrutamiento”.
- 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 destino 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.

- Si utiliza el enrutamiento de middlebox para enrutar a través de un dispositivo de seguridad, no se admite la referencia a grupos de seguridad entre el origen y el destino final después de la inspección.

Escenarios de Middlebox

Amazon Virtual Private Cloud (VPC) ofrece una gran variedad de capacidades de red con las cuales puede personalizar y controlar el enrutamiento del tráfico dentro de su red virtual. Una de estas

características es el asistente de enrutamiento de middlebox, el cual ofrece un control preciso sobre la ruta de enrutamiento del tráfico que entra o sale de la VPC.

Si necesita redirigir el tráfico a un dispositivo de seguridad, equilibrador de carga u otro dispositivo de red para realizar inspecciones, supervisiones u optimizaciones, el asistente de enrutamiento de middlebox puede simplificar el proceso. Este asistente crea, de manera automática, las tablas de enrutamiento necesarias y las rutas (saltos) para redirigir el tráfico especificado según sea necesario, lo cual elimina el esfuerzo manual que requieren las configuraciones de enrutamiento complejas.

El asistente de enrutamiento de middlebox puede utilizarse en una gran variedad de situaciones. Por ejemplo, puede utilizarlo para inspeccionar el tráfico destinado a una subred en particular, configurar el enrutamiento y la inspección del tráfico de middlebox en toda su VPC o inspeccionar de manera selectiva el tráfico entre subredes específicas. Este control granular sobre el enrutamiento del tráfico permite implementar políticas de seguridad avanzadas, habilitar la supervisión centralizada de la red u optimizar el rendimiento de sus aplicaciones basadas en la nube.

Los siguientes ejemplos describen escenarios para el asistente de enrutamiento de Middlebox.

Contenido

- Inspeccione el tráfico destinado a una subred
- Configuración del enrutamiento y la inspección del tráfico de middlebox en una VPC
- Inspeccione el tráfico entre subredes

Inspeccione 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 EC2 en una subred independiente de la subred B de su VPC, por ejemplo, la subred C. A continuación, podrá utilizar el asistente de enrutamiento de middlebox para configurar rutas para el tráfico entre la subred B y la puerta de enlace de Internet.

El asistente de enrutamiento Middlebox realiza automáticamente las operaciones siguientes:

- Crea las siguientes tablas de enrutamiento:
  - Tabla de enrutamiento para la puerta de enlace de Internet
  - Tabla de enrutamiento para la subred de destino

  - Tabla de enrutamiento para la subred de middlebox
- 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 puerta de enlace de Internet (el origen 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.

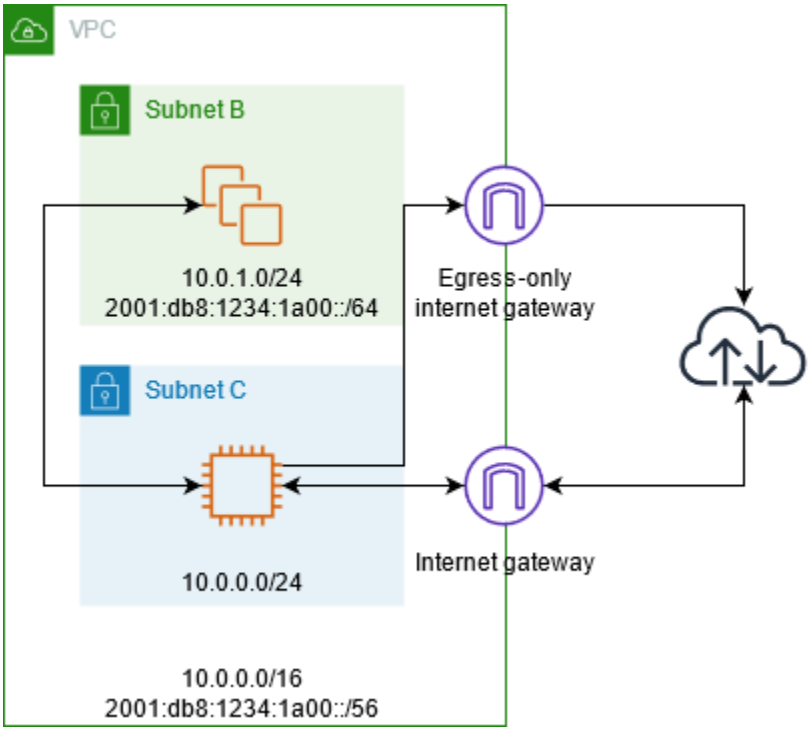


Tabla de enrutamiento de la gateway de Internet

Agregue las siguientes rutas a la tabla de enrutamiento para la puerta de enlace de Internet.

Destino	Objetivo	Finalidad
10.0.0.0/16	Local	Ruta local para IPv4
10.0.1.0/24	*appliance-eni*	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	*appliance-eni*	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, asocia las siguientes etiquetas a la tabla de enrutamiento:

- La clave es “Origin” (Origen) y el valor es “Middlebox wizard” (Asistente de Middlebox)
- La clave es “date_created” (fecha de creación) y el valor es el tiempo de creación (por ejemplo, “2021-02-18T22:25:49.137Z”)

Tabla de enrutamiento de subred de destino

Agregue las siguientes rutas a la tabla de enrutamiento de la subred de destino (subred B del diagrama de ejemplo).

Destino	Objetivo	Finalidad
10.0.0.0/16	Local	Ruta local para IPv4
0.0.0.0/0	*appliance-eni*	Dirija el tráfico IPv4 destinado a Internet al middlebox

Destino	Objetivo	Finalidad
2001:db8:1234:1a00::/56	Local	Enrutamiento local de IPv6
::/0	*appliance-eni*	Dirija el tráfico IPv6 que tenga como destino Internet al middlebox

Existe una asociación de subred con la subred de middlebox.

Cuando utiliza el asistente de enrutamiento de Middlebox, asocia las siguientes etiquetas a la tabla de enrutamiento:

- La clave es “Origin” (Origen) y el valor es “Middlebox wizard” (Asistente de Middlebox)
- La clave es “date_created” (fecha de creación) y el valor es el tiempo de creación (por ejemplo, “2021-02-18T22:25:49.137Z”)

Tabla de enrutamiento de la subred Middlebox

Agregue las siguientes rutas a la tabla de enrutamiento para la subred de middlebox (subred C del diagrama de ejemplo).

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 el tráfico de IPv6 a la puerta de enlace de Internet de solo salida

Existe una asociación de subred con la subred de destino.

Cuando utiliza el asistente de enrutamiento de Middlebox, asocia las siguientes etiquetas a la tabla de enrutamiento:

- La clave es “Origin” (Origen) y el valor es “Middlebox wizard” (Asistente de Middlebox)
- La clave es “date_created” (fecha de creación) y el valor es el tiempo de creación (por ejemplo, “2021-02-18T22:25:49.137Z”)

Configuración del enrutamiento y la inspección del tráfico de middlebox en una VPC

Considere el escenario en el que necesita inspeccionar el tráfico que entra a una VPC desde la puerta de enlace de Internet y destinado a una subred mediante una flota de dispositivos de seguridad configurados detrás de un equilibrador de carga de puerta de enlace. El propietario de la VPC del consumidor de servicios crea un punto de conexión del equilibrador de carga de puerta de enlace en una subred en su VPC (representada por una interfaz de red de punto de conexión). Todo el tráfico que entra en la VPC a través de la puerta de enlace de Internet se dirige primero al punto de conexión del equilibrador de carga de puerta de enlace para su inspección en la VPC de seguridad antes de que se enrute a la subred de la aplicación. Del mismo modo, todo el tráfico que sale de la subred de la aplicación se dirige primero al punto de conexión del equilibrador de carga de puerta de enlace para su inspección en la VPC de seguridad antes de que se enrute a Internet.

El asistente de enrutamiento Middlebox realiza automáticamente las siguientes operaciones:

- 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.

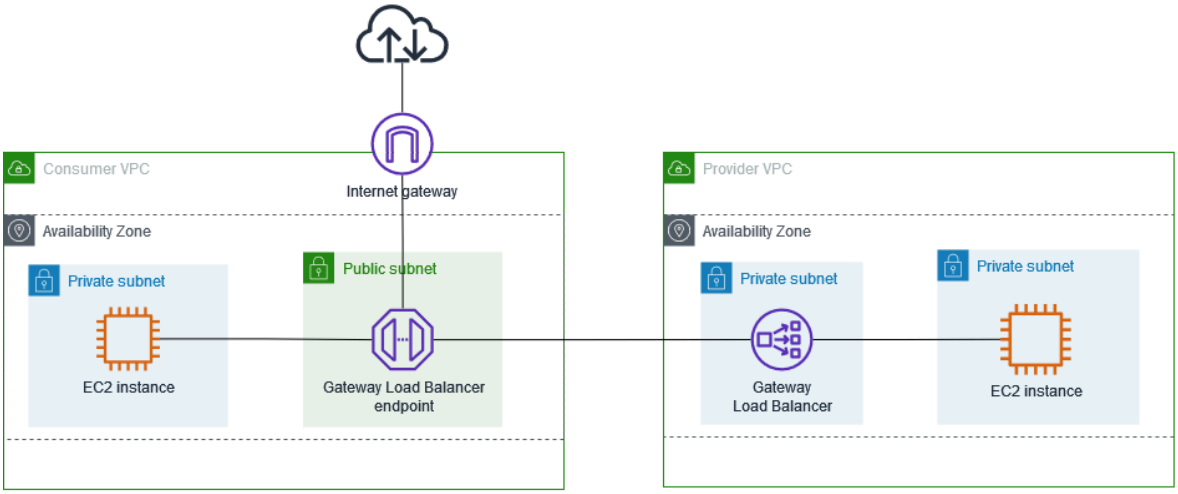


Tabla de enrutamiento de la gateway de Internet

La tabla de enrutamiento de la puerta de enlace de internet tiene las rutas que se indican a continuación.

Destino	Objetivo	Finalidad
CIDR de la VPC del consumidor	Local	Ruta local
CIDR de la subred de la aplicación	*endpoint-id*	Enruta el tráfico destinado a la subred de la aplicación al punto de conexión del equilibrador de carga de puerta de enlace

Existe una asociación de borde con la gateway.

Cuando utiliza el asistente de enrutamiento de Middlebox, asocia las siguientes etiquetas a la tabla de enrutamiento:

- La clave es “Origin” (Origen) y el valor es “Middlebox wizard” (Asistente de Middlebox)
- La clave es “date_created” (fecha de creación) y el valor es el tiempo de creación (por ejemplo, “2021-02-18T22:25:49.137Z”)

Tabla de enrutamiento de la subred de la aplicación

La tabla de enrutamiento de la subred de la aplicación tiene las rutas que se indican a continuación.

Destino	Objetivo	Finalidad
CIDR de la VPC del consumidor	Local	Ruta local
0.0.0.0/0	*endpoint-id*	Enrute el tráfico de los servidores de aplicaciones al punto de conexión del equilibrador de carga de puerta de enlace de Internet antes de que se enrute a Internet

Cuando utiliza el asistente de enrutamiento de Middlebox, asocia las siguientes etiquetas a la tabla de enrutamiento:

- La clave es “Origin” (Origen) y el valor es “Middlebox wizard” (Asistente de Middlebox)
- La clave es “date_created” (fecha de creación) y el valor es el tiempo de creación (por ejemplo, “2021-02-18T22:25:49.137Z”)

Tabla de enrutamiento de la subred del proveedor

La tabla de enrutamiento de la subred del proveedor tiene las rutas que se indican a continuación.

Destino	Objetivo	Finalidad
CIDR de la VPC del proveedor	Local	Ruta local. Garantiza que el tráfico originado en Internet se enrute a los servidores de aplicaciones
0.0.0.0/0	*igw-id*	Dirige todo el tráfico a la gateway de Internet

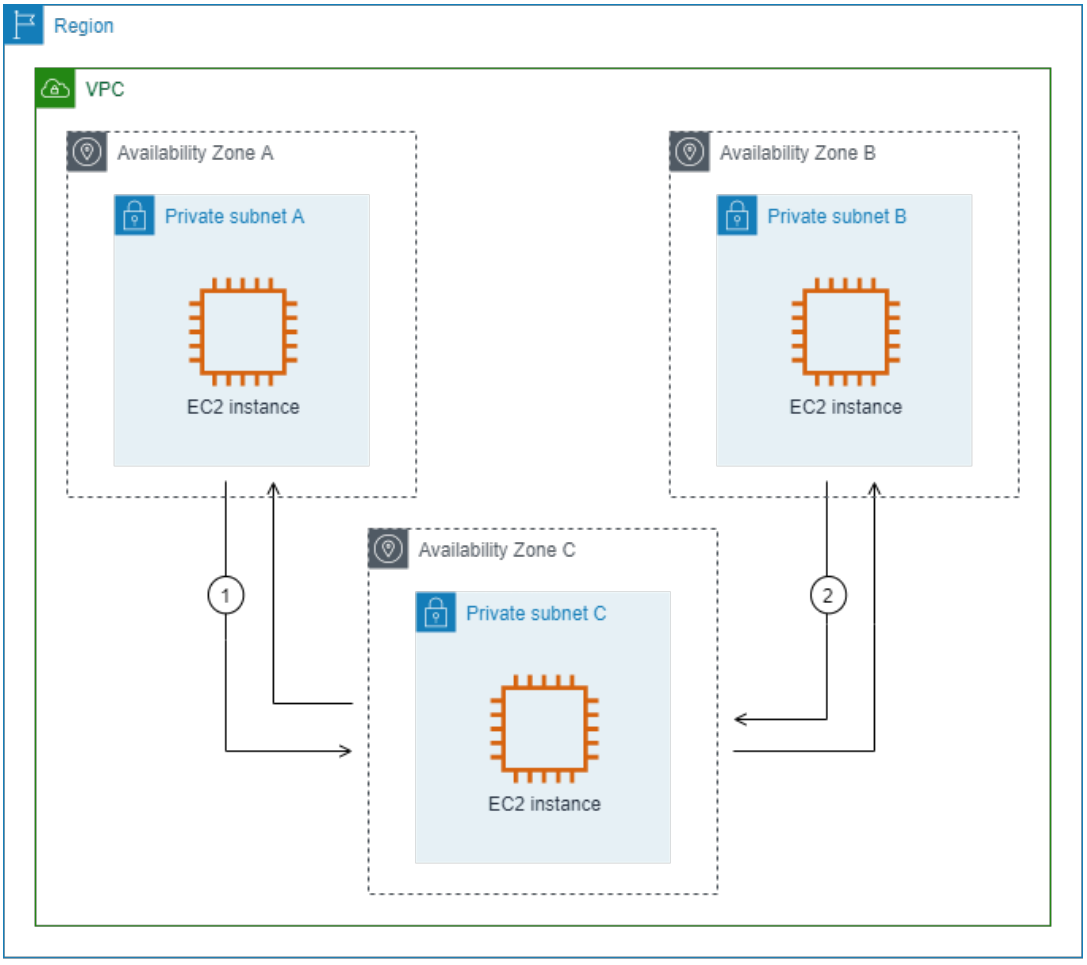
Cuando utiliza el asistente de enrutamiento de Middlebox, asocia las siguientes etiquetas a la tabla de enrutamiento:

- La clave es “Origin” (Origen) y el valor es “Middlebox wizard” (Asistente de Middlebox)
- La clave es “date_created” (fecha de creación) y el valor es 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 dichas subredes mediante un dispositivo de firewall. Configure e instale el dispositivo de firewall en una instancia de EC2 en una subred separada de la VPC.

El siguiente diagrama muestra un dispositivo de firewall instalado en una instancia de EC2 de la subred C. El dispositivo inspecciona todo el tráfico que pasa de la subred A a la subred B (consulte 1) y de la subred B a la subred A (consulte 2).



Utilice la tabla de enrutamiento principal para la VPC y la subred de middlebox. Cada una de las subredes A y B tiene una tabla de enrutamiento 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 enrutamiento personalizada para la subred A

La tabla de enrutamiento de la subred A tienen las rutas que se indican a continuación.

Destino	Objetivo	Finalidad
CIDR DE VPC	Local	Ruta local
CIDR de subred B	*appliance-eni*	Enrutar el tráfico destinado a la subred B a la caja intermedia

Cuando utiliza el asistente de enrutamiento de Middlebox, asocia las siguientes etiquetas a la tabla de enrutamiento:

- La clave es “Origin” (Origen) y el valor es “Middlebox wizard” (Asistente de Middlebox)
- La clave es “date_created” (fecha de creación) y el valor es el tiempo de creación (por ejemplo, “2021-02-18T22:25:49.137Z”)

Tabla de enrutamiento personalizada para la subred B

La tabla de enrutamiento de la subred B tiene las rutas que se indican a continuación.

Destino	Objetivo	Finalidad
CIDR DE VPC	Local	Ruta local
CIDR de subred A	*appliance-eni*	Enrute el tráfico destinado a la subred A a la middlebox

Cuando utiliza el asistente de enrutamiento de Middlebox, asocia las siguientes etiquetas a la tabla de enrutamiento:

- La clave es “Origin” (Origen) y el valor es “Middlebox wizard” (Asistente de Middlebox)
- La clave es “date_created” (fecha de creación) y el valor es el tiempo de creación (por ejemplo, “2021-02-18T22:25:49.137Z”)

Tabla de enrutamiento principal

La subred C usa la tabla de enrutamiento principal. La tabla de enrutamiento principal tiene la siguiente ruta.

Destino	Objetivo	Finalidad
CIDR DE VPC	Local	Ruta local

Cuando utiliza el asistente de enrutamiento de Middlebox, asocia las siguientes etiquetas a la tabla de enrutamiento:

- La clave es “Origin” (Origen) y el valor es “Middlebox wizard” (Asistente de Middlebox)
- La clave es “date_created” (fecha de creación) y el valor es el tiempo de creación (por ejemplo, “2021-02-18T22:25:49.137Z”)

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.

Al eliminar una subred, el bloque de CIDR asociado a esa subred se devuelve al conjunto de direcciones IP disponibles de la VPC. Esto significa que las direcciones IP dentro del rango de CIDR de la subred se pueden reasignar a otras subredes o recursos dentro de la misma VPC.

Es importante tener en cuenta que, cuando se elimina una subred, los recursos dentro de ella no se eliminan automáticamente. Primero, debe terminar todas las instancias de EC2 y eliminar todas las interfaces de red y cualquier otro recurso asociado a la subred para poder continuar con su eliminación.

Para eliminar una subred mediante la consola

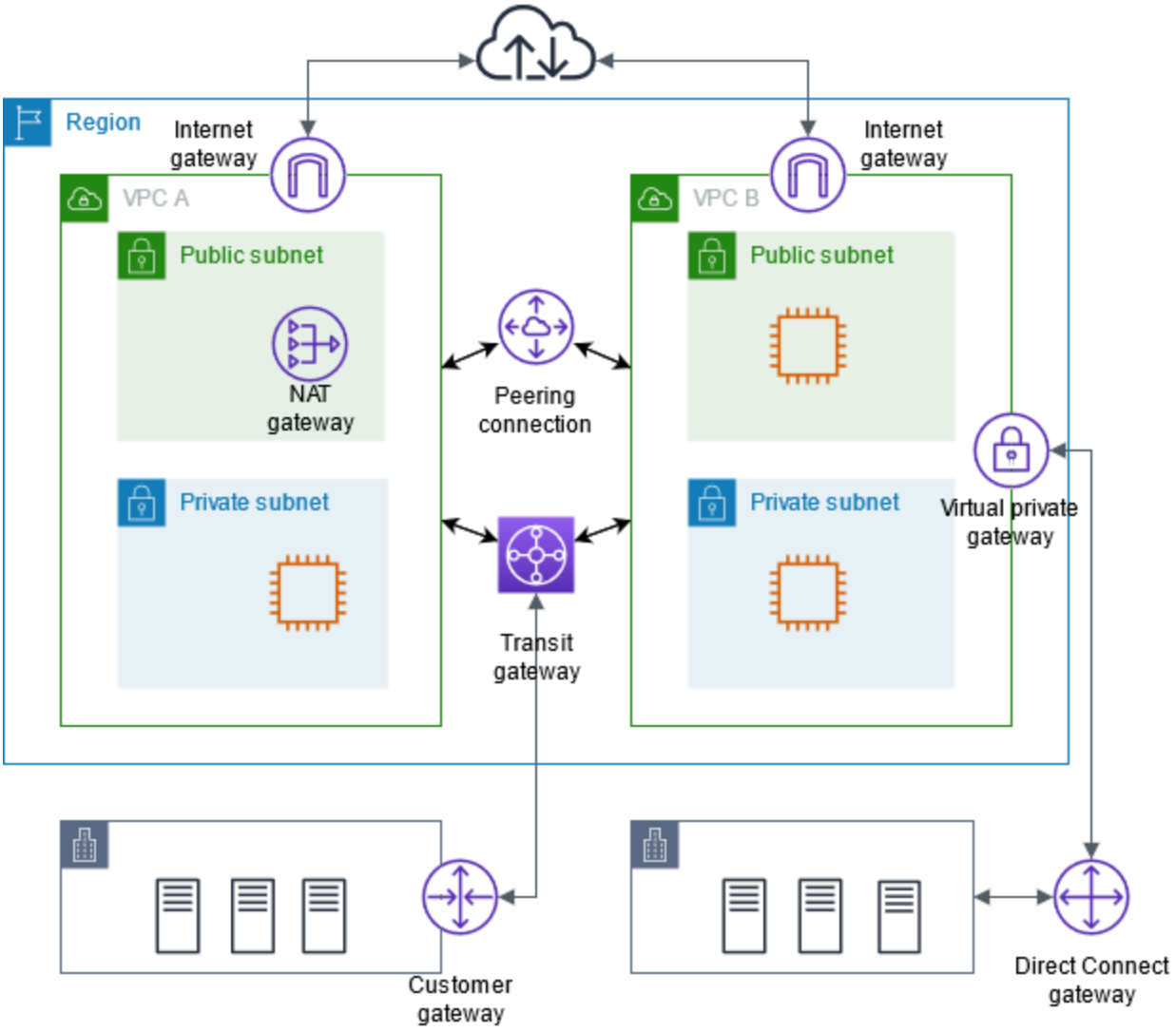
1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Termine todas las instancias de la subred. Para obtener más información, consulte Terminar una instancia en la Guía del usuario de Amazon EC2.
3. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
4. En el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

Para eliminar una subred mediante la AWS CLI

Utilice el comando delete-subnet.

Conectar la VPC a otras redes

Puede conectar la nube privada virtual (VPC) a otras redes, como otras VPC, Internet o la red en las instalaciones.



Puede conectar la nube privada virtual (VPC) a otras redes, como otras VPC, Internet o la red en las instalaciones.

En el siguiente diagrama, se muestran algunas de estas opciones de conectividad. La VPC A está conectada a Internet a través de la puerta de enlace de Internet, mientras que la instancia de EC2 de la subred privada puede conectarse a Internet con la puerta de enlace NAT en la subred pública. La VPC B también está conectada a Internet, pero a través de una puerta de enlace de Internet directa, lo que permite que la instancia de EC2 de la subred pública acceda a Internet.

Además, 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 vinculación de VPN al centro de datos y la VPC B tiene una conexión Direct Connect al mismo centro de datos. Gracias a esta interconectividad las organizaciones integran sus recursos en la nube con la infraestructura en las instalaciones, lo que crea un entorno de nube híbrida.

La conexión de las VPC con otras redes es un aspecto importante para la creación de una infraestructura en la nube dentro de AWS. Las organizaciones obtienen flexibilidad y control sobre sus configuraciones de red, lo que les permite diseñar arquitecturas de VPC que se alineen a sus necesidades empresariales y de seguridad. Estas opciones de conectividad facilitan el flujo de datos eficiente entre varios componentes de un entorno de IT distribuido, tanto dentro de la nube como en las instalaciones.

AWS ofrece una variedad de herramientas y características para habilitar estas conexiones en la VPC, incluidas las puertas de enlace de Internet, las puertas de enlace NAT, el emparejamiento de VPC, las puertas de enlace de tránsito y Direct Connect. Gracias a estas capacidades, las organizaciones pueden crear entornos de nube seguros e integrados que se incorporen a la perfección con su infraestructura de TI existente.

Puede conectar la nube virtual privada (VPC) a otras redes. Por ejemplo, otras VPC, Internet o la red en las instalaciones.

Para obtener más información, consulte Amazon Virtual Private Cloud Connectivity Options (Opciones de conectividad de Amazon Virtual Private Cloud).

Contenido

- Activación del acceso a Internet de una VPC con una puerta de enlace de Internet
- Habilitar el tráfico IPv6 saliente mediante una puerta de enlace de Internet de solo salida
- Conexión a Internet u otras redes mediante dispositivos NAT
- Asociar direcciones IP elásticas con recursos en la VPC
- Conectar la VPC a otras VPC y redes utilizando una puerta de enlace de tránsito
- Conectar la VPC a redes remotas mediante AWS Virtual Private Network
- Conecte las VPC utilizando el emparejamiento de VPC

Activación del acceso a Internet de una VPC con una puerta de enlace de Internet

Una puerta de enlace 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. Admite el tráfico IPv4 e IPv6. No genera riesgos de disponibilidad ni restricciones del ancho de banda del tráfico de red.

Una puerta de enlace de Internet permite que los recursos en las subredes públicas (como las instancias de EC2) 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.

Una puerta de enlace de Internet proporciona un destino en las tablas de enrutamiento de VPC para el tráfico enrutable a Internet. Para las comunicaciones mediante IPv4, la puerta de enlace de Internet también realiza la traducción de direcciones de red (NAT). Para obtener más información, consulte Direcciones IP y NAT.

Precios

Las puertas de enlace de Internet son gratuitas, pero se aplican cargos por la transferencia de datos para las instancias EC2 que utilizan puertas de enlace de Internet. Para obtener más información, consulte Precios de Amazon EC2 bajo demanda.

Contenido

- Conceptos básicos de la puerta de enlace de Internet
- Adición de acceso a Internet en una subred
- Eliminar un puerta de enlace de Internet

Conceptos básicos de la puerta de enlace de Internet

Para utilizar una puerta de enlace de Internet, debe adjuntarla a una VPC y configurar el enrutamiento.

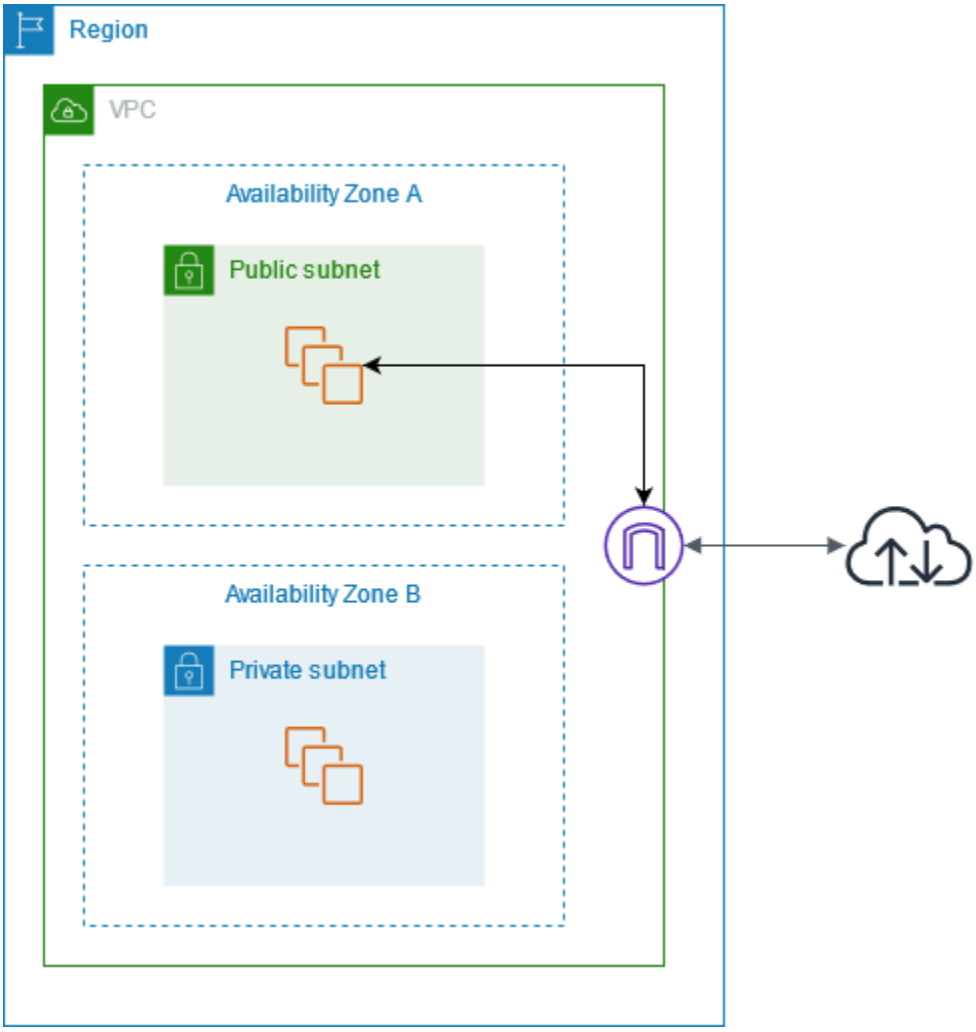
Configuración de enrutamiento

Si la subred está asociada a una tabla de enrutamiento que tiene una ruta a una puerta de enlace de Internet, esta se denomina subred pública. Si una subred está asociada a una tabla de enrutamiento que no tiene ninguna ruta a una puerta de enlace de Internet, se denomina subred privada.

En la tabla de enrutamiento de la subred pública, puede especificar la ruta de la puerta de enlace 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.

Diagrama de la puerta de enlace de Internet

En el siguiente diagrama, la subred en la zona de disponibilidad A es una subred pública porque su tabla de enrutamiento tiene una ruta que envía todo el tráfico IPv4 destinado 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, incluso si cuentan con direcciones IP públicas, debido a que no existe una ruta a la puerta de enlace de Internet.



Direcciones IP y NAT

Para permitir la comunicación a través de Internet para IPv4, su instancia debe tener una dirección IPv4 pública. Puede definir su VPC para que asigne automáticamente direcciones IPv4 públicas a las instancias, o puede asignar direcciones IP elásticas a las instancias. Su instancia solo tendrá en cuenta el espacio de dirección IP (interno) privado definido en la VPC y la subred. El puerta de enlace 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.

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	No
Tabla de ruteo con ruta al puerta de enlace de Internet para el tráfico IPv4 (0.0.0.0/0)	Sí	No
Tabla de ruteo con ruta al puerta de enlace de Internet para el tráfico IPv6 (::/0)	No	No
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)

Adición de acceso a Internet en una subred

A continuación, se describe cómo admitir el acceso a Internet desde una subred en una VPC no predeterminada mediante una puerta de enlace de Internet. Debe crear la puerta de enlace de Internet, adjuntarla a la VPC y configurar el enrutamiento de la subred.

Después de configurar el acceso a Internet para la subred, debe asegurarse de que los recursos de la subred puedan acceder a Internet. Por ejemplo, las instancias de EC2 deben tener una dirección IPv4 o IPv6 pública y los grupos de seguridad de las instancias deben permitir el tráfico específico hacia y desde Internet.

De manera alternativa, para proporcionar acceso a Internet a sus instancias sin asignarles direcciones IP públicas puede utilizar un dispositivo NAT en su lugar. Para obtener más información, consulte Dispositivos NAT.

Para eliminar el acceso a Internet, puede desconectar la puerta de enlace de Internet de la VPC y, a continuación, eliminarla. Para obtener más información, consulte the section called “Eliminar un puerta de enlace de Internet”.

Tareas

- Paso 1: cree un puerta de enlace de Internet
- Paso 2: adjunte la puerta de enlace de Internet a la VPC
- Paso 3: agregue una ruta a la tabla de enrutamiento de la subred

Paso 1: cree un puerta de enlace de Internet

Utilice el siguiente procedimiento para crear una puerta de enlace de Internet.

Creación de una puerta de enlace de Internet mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Internet Gateways (Puertas de enlace de Internet).
3. Elija Crear puerta de enlace de Internet.
4. (Opcional) Ingrese un nombre para la puerta de enlace de Internet.
5. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
6. Elija Crear puerta de enlace de Internet.
7. (Opcional) Para adjuntar la puerta de enlace de Internet a una VPC ahora, elija Adjuntar a una VPC en el banner de la parte superior de la pantalla, seleccione una VPC disponible y, a continuación, elija Adjuntar una puerta de enlace de Internet. De lo contrario, puede adjuntar la puerta de enlace de Internet a una VPC en otro momento.

Creación de una puerta de enlace de Internet mediante la línea de comandos

- create-internet-puerta de enlace (AWS CLI)
- New-EC2InternetGateway (AWS Tools for Windows PowerShell)

Paso 2: adjunte la puerta de enlace de Internet a la VPC

Para utilizar una puerta de enlace de Internet, debe adjuntarla a una VPC.

Asociación de un puerta de enlace de Internet a 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 Internet Gateways (Puertas de enlace de Internet).
3. Seleccione la casilla para la puerta de enlace de Internet.
4. Para adjuntarla, seleccione Acciones seguido de Adjuntar a la PVC, elija una VPC disponible y luego seleccione Adjuntar una puerta de enlace de Internet.
5. Para separarla, seleccione Acciones seguido de Desconectar de la VPC y luego seleccione Desconectar puerta de enlace de Internet. Cuando se le solicite confirmación, elija Desasociar puerta de enlace de Internet.

Asociación de una puerta de enlace de Internet a una VPC mediante la línea de comandos

- attach-internet-puerta de enlace (AWS CLI)
- Add-EC2InternetGateway (AWS Tools for Windows PowerShell)

Paso 3: agregue una ruta a la tabla de enrutamiento de la subred

La tabla de enrutamiento para la subred debe tener una ruta que envíe tráfico de Internet a la instancia NAT.

Configurar la tabla de enrutamiento de la 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 Tablas de enrutamiento.
3. Seleccione la tabla de enrutamiento de la subred. De forma predeterminada, una subred utiliza la tabla de enrutamiento principal de la VPC. Como alternativa, puede crear una tabla de enrutamiento y, a continuación, asociar la subred a la nueva tabla de enrutamiento.
4. En la pestaña Rutas, elija Editar rutas y luego elija Agregar ruta.
5. Ingrese 0.0.0.0/0 como Destino y seleccione la puerta de enlace de Internet para Objetivo.
6. Seleccione Save changes (Guardar cambios).

Configurar la tabla de enrutamiento de la subred mediante la línea de comandos

- create-route (AWS CLI)
- New-EC2Route (AWS Tools for Windows PowerShell)

Eliminar un puerta de enlace de Internet

Si ya no necesita que una VPC tenga acceso a Internet, puede desasociar la puerta de enlace de Internet de la VPC y, a continuación, eliminarla. Tenga en cuenta que no podrá eliminar el puerta de enlace de Internet si sigue adjunto a la VPC. Tenga en cuenta que no es posible separar el puerta de enlace de Internet si la VPC tiene recursos con las direcciones IP públicas o las direcciones IP elásticas.

Desasociación de una puerta de enlace de Internet de 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 Internet Gateways (Puertas de enlace de Internet).
3. Seleccione la casilla para la puerta de enlace de Internet.
4. Para adjuntarla, seleccione Acciones seguido de Adjuntar a la PVC, elija una VPC disponible y luego seleccione Adjuntar una puerta de enlace de Internet.
5. Para separarla, seleccione Acciones seguido de Desconectar de la VPC y luego seleccione Desconectar puerta de enlace de Internet. Cuando se le solicite confirmación, elija Desasociar puerta de enlace de Internet.

Descripción de sus puertas de enlace de Internet, incluidos los elementos asociados, mediante la línea de comandos

- describe-internet-puerta de enlaces (AWS CLI)
- Get-EC2InternetGateway (AWS Tools for Windows PowerShell)

Desasociación de una puerta de enlace de Internet de una VPC mediante la línea de comandos

- detach-internet-puerta de enlace (AWS CLI)
- Dismount-EC2InternetGateway (AWS Tools for Windows PowerShell)

Eliminación de una puerta de enlace de Internet mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Internet Gateways (Puertas de enlace de Internet).
3. Seleccione la casilla para la puerta de enlace de Internet.
4. Elija Acciones, Eliminar puerta de enlace de Internet.
5. Cuando se le solicite confirmación, ingrese **`delete`** y elija Eliminar puerta de enlace de Internet.

Eliminación de una puerta de enlace de Internet mediante la línea de comandos

- delete-internet-puerta de enlace (AWS CLI)
- Remove-EC2InternetGateway (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.

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.

Precios

Las puertas de enlace de Internet de solo salida son gratuitas, pero se aplican cargos por la transferencia de datos para las instancias EC2 que utilizan puertas de enlace de Internet. Para obtener más información, consulte Precios de Amazon EC2 bajo demanda.

Contenido

- Conceptos básicos de las gateways de Internet de solo salida
- Adición de acceso a Internet de solo salida en una subred

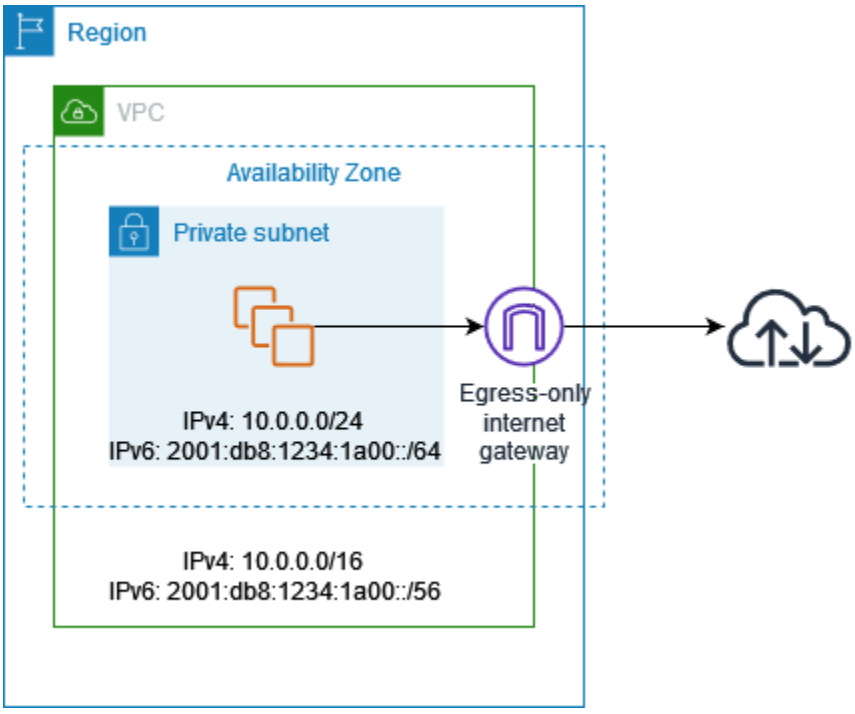
Conceptos básicos de las gateways de Internet de solo salida

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.

No se puede asociar un grupo de seguridad a una puerta de enlace de Internet solo de salida para controlar el tráfico que puede llegar o salir de la puerta de enlace de Internet solo de salida. 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	*eigw-id*

Adición de acceso a Internet de solo salida en una subred

Las tareas que se detallan a continuación describen cómo crear una puerta de enlace de Internet de solo salida (saliente) en su subred privada y cómo configurar el enrutamiento de la subred.

Tareas

- 1. Creación de una gateway de internet de solo salida
- 2. Creación de una tabla de ruteo personalizada
- 3. Eliminación de una gateway de internet de solo salida
- Descripción general de la línea de comandos

1. 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 nueva etiqueta y haga lo siguiente:

   - En Clave, escriba el nombre de la clave.

- En Valor, escriba el valor de la clave.

[Eliminar una etiqueta] Elija Eliminar a la derecha de la clave y del 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).

2. 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, pude 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.

3. 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.

Descripción general de la línea de comandos

Puede utilizar la línea de comandos para realizar las tareas descritas en esta página.

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)

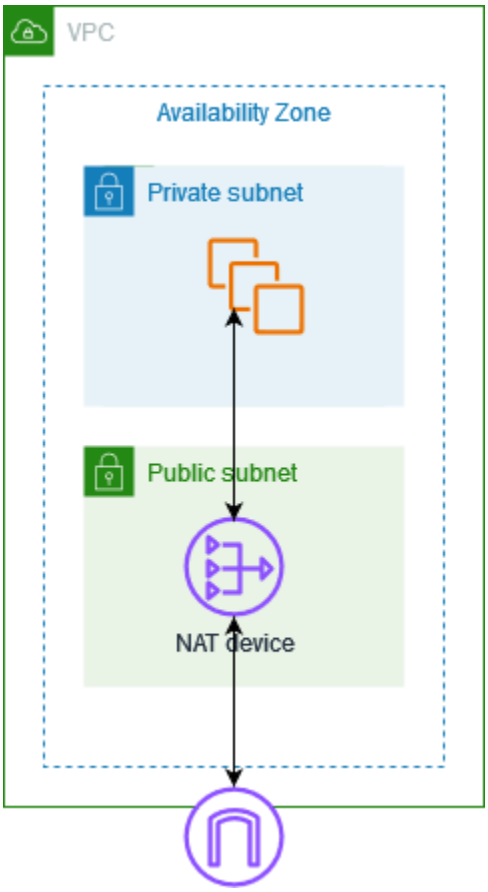
Eliminación de una gateway de internet de solo salida

- 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.

Por ejemplo, el siguiente diagrama muestra un dispositivo NAT en una subred pública que permite que las instancias de EC2 en una subred privada se conecten a Internet a través de una puerta de enlace de Internet. 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.



Important

- 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).

- 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 puertas de enlace NAT, ya que proporcionan mayor disponibilidad y ancho de banda y requieren menos esfuerzo de administración por su parte.

Contenido

- Gateways NAT
- Instancias de NAT
- Comparar las puertas de enlace NAT con las instancias NAT

Gateways NAT

Una gateway NAT es un servicio de traducción de direcciones de red (NAT). Puede utilizar una puerta de enlace 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 puerta de enlace NAT pública, pero no pueden recibir conexiones entrantes no solicitadas de Internet. Crea una puerta de enlace de NAT pública en una subred pública y debe asociar una dirección IP elástica a la puerta de enlace 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 puerta de enlace NAT privada, pero las instancias no pueden recibir conexiones entrantes no solicitadas de las otras VPC ni de la red en las instalaciones. 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 puerta de enlace de 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 puerta de enlace NAT se utiliza para el tráfico IPv4 e IPv6 (con DNS64 y NAT64). Otra opción para iniciar comunicaciones de solo salida a Internet mediante IPv6, utilizar una puerta de enlace de Internet de solo salida.

Tanto las puertas de enlace NAT privadas como las públicas asignan la dirección IPv4 privada de origen de las instancias a la dirección IPv4 privada de la puerta de enlace NAT. En el caso de una puerta de enlace NAT pública, la puerta de enlace de Internet entonces asigna la dirección IPv4 privada de la puerta de enlace NAT pública a la dirección IP elástica asociada a la puerta de enlace NAT.

Cuando envía tráfico de respuesta a las instancias, ya sea una puerta de enlace NAT pública o privada, la puerta de enlace NAT traduce la dirección a la dirección IP de origen.

Consideraciones

- Las conexiones siempre se deben iniciar desde la VPC que contiene la puerta de enlace de NAT.
- Puede utilizar una puerta de enlace NAT pública o privada para enrutar el tráfico a puertas de enlace de tránsito y puertas de enlace privadas virtuales.
- Si utiliza una puerta de enlace NAT privada para conectarse a una puerta de enlace de tránsito o a una puerta de enlace privada virtual, el tráfico hacia el destino procederá de la dirección IP privada de la puerta de enlace NAT privada.
- Si utiliza una puerta de enlace NAT pública para conectarse a una puerta de enlace de tránsito o a una puerta de enlace privada virtual, el tráfico hacia el destino procederá de la dirección IP privada de la puerta de enlace NAT pública. La puerta de enlace de NAT pública solo usa su dirección IP elástica como dirección IP de origen cuando se utiliza junto con una puerta de enlace de Internet en la misma VPC.

Contenido

- Conceptos básicos de la gateway NAT
- Trabajar con gateways NAT
- Puertas de enlace NAT regionales para la expansión automática en varias zonas de disponibilidad
- Casos de uso de puerta de enlace NAT
- DNS64 y NAT64
- Inspección del tráfico proveniente de las puertas de enlace NAT
- Monitorear las puertas de enlace NAT mediante Amazon CloudWatch
- Solucionar problemas de las gateways NAT

- Precios de las puertas de enlace NAT

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 Puertas de enlace.

Si tiene recursos en varias zonas de disponibilidad que comparten una puerta de enlace NAT y la zona de disponibilidad de la puerta de enlace NAT no funciona, los recursos de las demás zonas de disponibilidad perderán el acceso a Internet. Para mejorar la resiliencia, puede crear una puerta de enlace NAT en cada zona de disponibilidad y configurar el direccionamiento para asegurarse de que los recursos utilicen la puerta de enlace NAT en 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 puertas de enlace NAT admiten 5 Gbps de ancho de banda y se amplían automáticamente hasta 100 Gbps. Si necesita más ancho de banda, puede dividir los recursos en varias subredes y crear una gateway NAT en cada subred.
- Una puerta de enlace NAT puede procesar un millón de paquetes por segundo y escalar automáticamente hasta 10 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.
- Cada dirección IPv4 puede admitir hasta 55 000 conexiones simultáneas a cada destino único. Un destino único se identifica mediante una combinación única de dirección IP de destino, puerto de destino y protocolo (TCP/UDP/ICMP). Puede aumentar este límite si asocia hasta ocho direcciones IPv4 a sus puertas de enlace NAT (una dirección IPv4 principal y siete direcciones IPv4 secundarias). De forma predeterminada, está limitado a asociar 2 direcciones IP elásticas a su puerta de enlace de NAT pública. Puede aumentar este límite si solicita un ajuste de cuota. Para obtener más información, consulte Direcciones IP elásticas.

- Cuando crea una puerta de enlace de NAT, puede seleccionar la dirección IPv4 privada principal que desea asignar a la puerta de enlace NAT. De lo contrario, seleccionaremos una en su nombre a partir del rango de direcciones IPv4 de la subred. No es posible cambiar ni eliminar la dirección IPv4 privada principal. Puede agregar direcciones IPv4 privadas secundarias según sea necesario.
- No puede asociar un grupo de seguridad a una puerta de enlace NAT. Puede asociar grupos de seguridad a las instancias para controlar su tráfico entrante y saliente.
- Se crea una interfaz de red administrada por el solicitante para la puerta de enlace de NAT. Puede ver esta interfaz de red mediante la consola de Amazon EC2. Busque el ID de la puerta de enlace de NAT en la descripción. Puede agregar etiquetas a la interfaz de red, pero no puede modificar otras propiedades de esta interfaz de red.
- 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 ACL de red.
- No se puede dirigir el tráfico a una puerta de enlace NAT mediante una conexión de emparejamiento de VPC. Sin embargo, el tráfico desde una puerta de enlace de NAT a través de la interconexión de VPC hacia destinos en VPC interconectadas admite el comportamiento “Devolución al remitente”: el tráfico de retorno se dirige automáticamente a la puerta de enlace de NAT de origen, incluso si no hay rutas de retorno configuradas en la VPC de destino. Este comportamiento es exclusivo de las puertas de enlace NAT y no se aplica a las instancias de EC2 estándar. Para evitar esto, use las NACL para bloquear el tráfico de retorno.

  No admitido:

  ```
  Client # Peering # NAT # Internet
  ```

  Compatible:

  ```
  Client # NAT # Peering # Destination
  ```
- No se puede dirigir el tráfico a una puerta de enlace NAT desde Site-to-Site VPN ni Direct Connect mediante una puerta de enlace privada virtual. Puede dirigir el tráfico a una puerta de enlace NAT desde Site-to-Site VPN o Direct Connect si utiliza una puerta de enlace de tránsito en lugar de una puerta de enlace privada virtual.
- Las puertas de enlace NAT admiten tráfico con una unidad de transmisión (MTU) máxima de 8500, pero es importante tener en cuenta lo siguiente:

- La unidad de transmisión máxima (MTU) de una conexión de red es el tamaño, en bytes, del mayor paquete permitido que se puede transferir a través de la conexión. Cuanto mayor sea la MTU de una conexión, mayor cantidad de datos se podrán transferir en un solo paquete.
- Los paquetes con un tamaño superior a 8500 bytes que llegan a la puerta de enlace de NAT se descartan (o se fragmentan, si corresponde).
- Para evitar la posible pérdida de paquetes al comunicarse con los recursos a través de Internet mediante una puerta de enlace NAT pública, la configuración de MTU de las instancias EC2 no debe superar los 1500 bytes. Para obtener más información sobre cómo comprobar y configurar la MTU en una instancia, consulte MTU de red para la instancia de EC2 en la Guía del usuario de Amazon EC2.
- Las puertas de enlace NAT admiten Path MTU Discovery (PMTUD) mediante paquetes ICMPv4 FRAG_NEEDED y paquetes ICMPv6 Packet Too Big (PTB).
- Las puertas de enlace NAT aplican el bloqueo de tamaño máximo del segmento (MSS) a todos los paquetes. Para obtener más información, consulte RFC879.

Trabajar con gateways NAT

Puede utilizar la consola de Amazon VPC para crear y administrar sus gateways NAT.

Tareas

- Controlar el uso de gateways NAT
- Creación de una gateway NAT
- Edición de asociaciones de direcciones IP secundarias
- Etiquetar una gateway NAT
- Eliminación de una gateway NAT
- Descripción general de la línea de comandos

Controlar el uso de gateways NAT

De forma predeterminada, los usuarios de no tienen permiso para trabajar con gateways NAT. Puede crear un rol de IAM con una política asociada que conceda permisos a los usuarios para crear, describir y eliminar puertas de enlace NAT. Para obtener más información, consulte Identity and Access Management para Amazon VPC.

Creación de una gateway NAT

Utilice el siguiente procedimiento para crear una puerta de enlace NAT.

Cuotas relacionadas

- No podrá crear una puerta de enlace de NAT pública si ha agotado la cantidad de direcciones IP elásticas asignadas a la cuenta. Para obtener más información, consulte Direcciones IP elásticas.
- Puede asignar hasta ocho direcciones IPv4 privadas a la puerta de enlace de NAT privada. Este límite no se puede ajustar.
- De forma predeterminada, está limitado a asociar 2 direcciones IP elásticas a su puerta de enlace de NAT pública. Puede aumentar este límite si solicita un ajuste de cuota. Para obtener más información, consulte Direcciones IP elásticas.

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 Puertas de enlace de NAT.
3. Elija Crear una puerta de enlace de NAT.
4. (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.
5. Seleccione la subred en la que crear la gateway NAT.
6. En Tipo de conectividad, seleccione Pública para crear una puerta de enlace de NAT pública o Privada para crear una puerta de enlace de NAT privada. Para obtener más información acerca de la diferencia entre una puerta de enlace de NAT pública y privada, consulte Gateways NAT.
7. Si eligió Public (Pública), haga lo que se indica a continuación. Si no eligió esta opción, diríjase al paso 8:

    1. Elija un ID de asignación de IP elástica para asignar una dirección IP elástica a la puerta de enlace de NAT, o elija Asignar IP elástica para asignar una automáticamente a la puerta de enlace NAT pública. De forma predeterminada, está limitado a asociar 2 direcciones IP elásticas a su puerta de enlace de NAT pública. Puede aumentar este límite si solicita un ajuste de cuota. Para obtener más información, consulte Direcciones IP elásticas.

> **Important**
>
> Cuando asigne una dirección IP elástica a una puerta de enlace de NAT pública, el grupo de borde de red de la IP elástica debe coincidir con el grupo de borde de red de la zona de disponibilidad (AZ) en la que va a crear la puerta de enlace NAT pública. Si no coinciden, la puerta de enlace NAT no se podrá iniciar. Para ver el grupo de bordes de red de la zona de disponibilidad de la subred, consulte los detalles de la subred. Del mismo modo, puede ver el grupo de bordes de red de una EIP si consulta los detalles de la dirección de la EIP. Para obtener más información, consulte 1. Asignar una dirección IP elástica.

2. (Opcional) Elija Configuración adicional y, en Dirección IP privada: opcional, ingrese una dirección IPv4 privada para la puerta de enlace de NAT. Si no ingresa ninguna dirección, AWS asignará automáticamente una dirección IPv4 privada a su puerta de enlace de NAT de forma aleatoria desde la subred en la que se encuentra la puerta de enlace de NAT.
3. Vaya al paso 11.

8. Si eligió Privada, diríjase a Configuración adicional, luego a Método de asignación de direcciones IPv4 privadas y elija una de las siguientes opciones:

   - Asignación automática: AWS elige la dirección IPv4 privada principal para la puerta de enlace de NAT. En Cantidad de direcciones IPv4 privadas asignadas de manera automática, puede especificar la cantidad de direcciones IPv4 privadas secundarias para la puerta de enlace de NAT. AWS elige estas direcciones IP de forma aleatoria de la subred para la puerta de enlace de NAT.
   - Personalizada: en Dirección IPv4 privada principal, elija la dirección IPv4 privada principal para la puerta de enlace de NAT. En Direcciones IPv4 privadas secundarias, puede especificar hasta 7 direcciones IPv4 privadas secundarias para la puerta de enlace de NAT.

9. Si ha elegido Personalizado en el paso 8, omita este paso. Si ha elegido Asignación automática, en Número de direcciones IP privadas asignadas automáticamente, elija la cantidad de direcciones IPv4 secundarias que desea que AWS asigne a esta puerta de enlace de NAT privada. Puede elegir hasta 7 direcciones IPv4.

> **Note**
>
> Las direcciones IPv4 secundarias son opcionales y deben asignarse cuando las cargas de trabajo que utilizan una puerta de enlace NAT superen las 55 000 conexiones

simultáneas a un único destino (la misma IP de destino, puerto de destino y protocolo). Las direcciones IPv4 secundarias aumentan la cantidad de puertos disponibles y, por lo tanto, aumentan el límite de conexiones simultáneas que las cargas de trabajo pueden establecer mediante una puerta de enlace NAT.

10. Si ha elegido Asignación automática en el paso 9, omita este paso. Si ha elegido Personalizado, proceda de la siguiente manera:
    1. En Dirección IPv4 privada principal, ingrese la dirección IPv4 privada.
    2. En Dirección IPv4 privada secundaria, ingrese hasta 7 direcciones IPv4 privadas secundarias.
11. (Opcional) Para agregar una etiqueta a la puerta de enlace NAT, elija Add new tag (Agregar etiqueta nueva) e ingrese la clave y el valor de la etiqueta. Puede añadir hasta 50 etiquetas.
12. Elija Crear una puerta de enlace de NAT.
13. 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. Asegúrese de actualizar las tablas de enrutamiento según sea necesario. Para ver ejemplos, consulte the section called “Casos de uso”.

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.

Edición de asociaciones de direcciones IP secundarias

Cada dirección IPv4 puede admitir hasta 55 000 conexiones simultáneas a cada destino único. Un destino único se identifica mediante una combinación única de dirección IP de destino, puerto de destino y protocolo (TCP/UDP/ICMP). Puede aumentar este límite si asocia hasta ocho direcciones IPv4 a sus puertas de enlace NAT (una dirección IPv4 principal y siete direcciones IPv4 secundarias). De forma predeterminada, está limitado a asociar 2 direcciones IP elásticas a su puerta de enlace de NAT pública. Puede aumentar este límite si solicita un ajuste de cuota. Para obtener más información, consulte Direcciones IP elásticas.

Puede utilizar las métricas de la puerta de enlace de NAT de CloudWatch ErrorPortAllocation y PacketsDropCount para determinar si su puerta de enlace de NAT genera errores de asignación de puertos o descarta paquetes. Para resolver este problema, agregue direcciones IPv4 secundarias a su puerta de enlace de NAT.

Consideraciones

- Puede agregar direcciones IPv4 privadas secundarias al crear una puerta de enlace de NAT privada o después de crear la puerta de enlace de NAT mediante el procedimiento de esta sección. Solo puede agregar direcciones IP elásticas a las puertas de enlace de NAT públicas después de crear la puerta de enlace de NAT, mediante el procedimiento descrito en esta sección.
- Su puerta de enlace de NAT puede tener hasta 8 direcciones IPv4 asociadas (1 dirección IPv4 principal y 7 direcciones IPv4 secundarias). Puede asignar hasta ocho direcciones IPv4 privadas a la puerta de enlace de NAT privada. De forma predeterminada, está limitado a asociar 2 direcciones IP elásticas a su puerta de enlace de NAT pública. Puede aumentar este límite si solicita un ajuste de cuota. Para obtener más información, consulte Direcciones IP elásticas.

Edición de asociaciones de direcciones IPv4 secundarias

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puertas de enlace de NAT.
3. Seleccione la puerta de enlace de NAT cuyas asociaciones de direcciones IPv4 secundarias desee editar.
4. Elija Acciones y, a continuación, elija Editar asociaciones de direcciones IP secundarias.
5. Si está editando las asociaciones de direcciones IPv4 secundarias de una puerta de enlace de NAT privada, en Acción, elija Asignar nuevas direcciones IPv4 o Anular asignación de direcciones IPv4 existentes. Si está editando las asociaciones de direcciones IPv4 secundarias de una puerta de enlace de NAT pública, en Acción, elija Asociar nuevas direcciones IPv4 o Desasociar direcciones IPv4 existentes.
6. Realice una de las siguientes acciones:

   - Si ha elegido asignar o asociar direcciones IPv4 nuevas, haga lo siguiente:

     1. Este paso es necesario. Debe seleccionar una dirección IPv4 privada. Elija el Método de asignación de direcciones IPv4 privadas:

        - Asignación automática: AWS elige automáticamente una dirección IPv4 privada principal y usted elige si desea que AWS asigne hasta 7 direcciones IPv4 privadas secundarias para asignarlas a la puerta de enlace de NAT. AWS las elige y las asigna automáticamente de forma aleatoria desde la subred en la que se encuentra la puerta de enlace de NAT.

- Personalizado: elija la dirección IPv4 privada principal y hasta 7 direcciones IPv4 privadas secundarias para asignarlas a la puerta de enlace de NAT.

2. En ID de asignación de IP elástica, elija una dirección IP elástica para agregar con una dirección IPv4 secundaria. Este paso es necesario. Debe seleccionar una dirección IP elástica junto con una dirección IPv4 privada. Si eligió Personalizado como método de asignación de dirección IP privada, también debe ingresar una dirección IPv4 privada para cada dirección IP elástica que agregue.

> **Important**
>
> Al asignar una EIP secundaria a una puerta de enlace NAT pública, el grupo de bordes de red de la EIP debe coincidir con el grupo de bordes de red de la zona de disponibilidad (AZ) en la que se encuentra la puerta de enlace NAT pública. Si no coinciden, no se podrá asignar la EIP. Para ver el grupo de bordes de red de la zona de disponibilidad de la subred, consulte los detalles de la subred. Del mismo modo, puede ver el grupo de bordes de red de una EIP si consulta los detalles de la dirección de la EIP. Para obtener más información, consulte 1. Asignar una dirección IP elástica.

Su puerta de enlace de NAT puede tener hasta 8 direcciones IP asociadas. Si se trata de una puerta de enlace de NAT pública, existe un límite de cuota predeterminado para las direcciones IP elásticas por región. Para obtener más información, consulte Direcciones IP elásticas.

- Si ha elegido desasociar o anular la asignación de nuevas direcciones IPv4, realice lo siguiente:

  1. En Dirección IP secundaria existente para anular asignación, seleccione las direcciones IP secundarias que desee anular.
  2. (opcional) En Duración del drenaje de conexiones, ingrese el tiempo máximo de espera (en segundos) antes de forzar la liberación de las direcciones IP si las conexiones siguen en curso. Si no ingresa un valor, el valor predeterminado es de 350 segundos.

7. Seleccione Save changes (Guardar cambios).

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.

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.

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. 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.

Para etiquetar una puerta de enlace de NAT

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puertas de enlace de NAT.
3. Seleccione la puerta de enlace de NAT que desee etiquetar y elija Acciones. A continuación, elija Administrar etiquetas.
4. Elija Agregar nueva etiqueta y defina una Clave y un Valor para la etiqueta. Puede añadir hasta 50 etiquetas.
5. Seleccione Save.

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 eliminar 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 Puertas de enlace de NAT.

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 5. Liberar una dirección IP elástica.

Descripción general de la línea de comandos

Puede utilizar la línea de comandos para realizar las tareas descritas en esta página.

Asignación de una dirección IPv4 privada a una puerta de enlace de NAT privada

- assign-private-nat-gateway-address (AWS CLI)
- Register-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)

Asociación de direcciones IP elásticas y direcciones IPv4 privadas a una puerta de enlace de NAT pública

- associate-nat-gateway-address (AWS CLI)
- Register-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)

Creación de una gateway NAT

- create-nat-gateway (AWS CLI)
- New-EC2NatGateway (AWS Tools for Windows PowerShell)

Eliminación de una gateway NAT

- delete-nat-gateway (AWS CLI)
- Remove-EC2NatGateway (AWS Tools for Windows PowerShell)

Descripción de una gateway NAT

- describe-nat-gateways (AWS CLI)
- Get-EC2NatGateway (AWS Tools for Windows PowerShell)

Desasociación de direcciones IP elásticas secundarias de una puerta de enlace de NAT pública

- disassociate-nat-gateway-address (AWS CLI)
- Unregister-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)

Etiquetar una gateway NAT

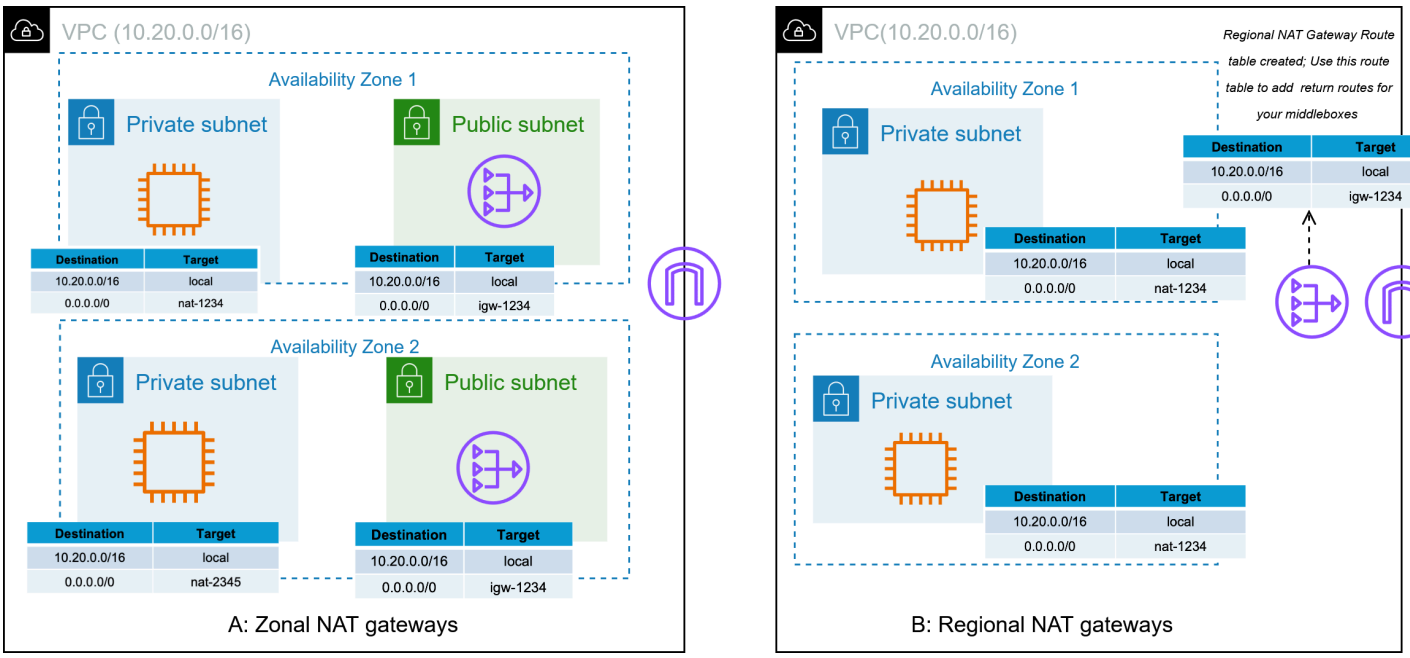
- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Anulación de asignación de direcciones IPv4 secundarias de una puerta de enlace de NAT privada

- unassign-private-nat-gateway-address (AWS CLI)
- Unregister-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)

Puertas de enlace NAT regionales para la expansión automática en varias zonas de disponibilidad

Utilice puertas de enlace NAT regionales cuando desee simplificar la arquitectura de red, mejorar la postura de seguridad y configurar la alta disponibilidad de forma predeterminada. Una puerta de enlace NAT regional se expande automáticamente entre las zonas de disponibilidad en función de la presencia de las cargas de trabajo. A diferencia de las puertas de enlace NAT estándar (denominadas puertas de enlace NAT zonales), que funcionan en una sola zona de disponibilidad, las puertas de enlace NAT regionales siguen a las cargas de trabajo para ofrecer una alta disponibilidad de forma automática.



El diagrama A de la izquierda representa la configuración actual con una puerta de enlace NAT zonal. Primero se crean puertas de enlace NAT zonales por zona de disponibilidad y se alojan en subredes públicas. A continuación, se configuran rutas independientes por zona de disponibilidad desde las subredes privadas hacia la puerta de enlace NAT de esa zona de disponibilidad. Este paso se repite cada vez que las cargas de trabajo se expanden a una nueva zona de disponibilidad para ofrecer alta disponibilidad. Además, se deben agregar rutas hacia la puerta de enlace de Internet en la tabla de enrutamiento de la subred de la puerta de enlace NAT para cada zona de disponibilidad.

Por otro lado, con una puerta de enlace NAT regional, no es necesario crear una subred pública para alojarla. Tampoco hay que crear ni eliminar puertas de enlace NAT ni editar las tablas de enrutamiento cada vez que las cargas de trabajo se expanden a nuevas zonas de disponibilidad. En su lugar, basta con crear una puerta de enlace NAT en modo regional, seleccionar la VPC, y esta se expande y se contrae automáticamente en todas las zonas de disponibilidad en función de la presencia de las cargas de trabajo, con el fin de ofrecer alta disponibilidad. Como se muestra en el diagrama B, puede enrutar el tráfico desde los recursos en una subred privada a través de todas las zonas de disponibilidad hacia este único ID de puerta de enlace NAT regional, o bien utilizar la misma tabla de enrutamiento en las subredes de la zona de disponibilidad para realizar la traducción de direcciones de red. Una vez que crea su puerta de enlace NAT regional, AWS crea automáticamente para esta una tabla de enrutamiento, que incluye una ruta preconfigurada hacia la puerta de enlace de Internet. Puede utilizar esta tabla de enrutamiento para agregar rutas de retorno hacia los dispositivos intermedios.

Ventajas

Las puertas de enlace NAT regionales ofrecen las siguientes ventajas:

- Configuración simplificada: utilice un único ID de NAT en todas las zonas de disponibilidad que tengan interfaces de red, de modo que pueda usar la misma entrada de ruta para subredes en distintas zonas de disponibilidad.
- Seguridad mejorada: no se requieren subredes públicas. Una puerta de enlace NAT regional es un recurso independiente con su propia tabla de enrutamiento, y no se necesita una subred pública en la VPC para alojarla, lo que reduce las probabilidades de configurar incorrectamente recursos privados en subredes con conectividad pública.
- Alta disponibilidad automática: se expande y se contrae automáticamente según la presencia de las cargas de trabajo para mantener la afinidad zonal, lo que garantiza una alta disponibilidad de forma predeterminada.
- Límites superiores de puertos y direcciones IP: las puertas de enlace NAT regionales admiten hasta 32 direcciones IP por zona de disponibilidad (en comparación con 8 en las puertas de enlace NAT zonales). Cada dirección IP aumenta en 55 000 el límite de conexiones simultáneas hacia un destino popular (identificado por una combinación única de dirección IP de destino, puerto de destino y protocolo).

Cuándo usar puertas de enlace NAT regionales

Las puertas de enlace NAT regionales son convenientes para todos los casos de uso, excepto aquellos que requieren conectividad privada. Las puertas de enlace NAT regionales no ofrecen conectividad privada y se recomienda usar puertas de enlace NAT en modo de disponibilidad zonal para los casos de uso de NAT privados.

Cómo funcionan las puertas de enlace NAT regionales

Cuando lanza recursos en una nueva zona de disponibilidad, la puerta de enlace NAT regional detecta la presencia de una interfaz de red (ENI) en esa zona de disponibilidad y se expande automáticamente hacia esa zona. De forma similar, la puerta de enlace NAT se contrae en la zona de disponibilidad que no tiene cargas de trabajo activas.

La expansión de la puerta de enlace NAT regional hacia una nueva zona de disponibilidad puede tardar hasta 60 minutos desde que se crea una instancia de recurso en esta. Hasta que se completa esta expansión, la puerta de enlace NAT regional procesa el tráfico pertinente de este recurso, entre todas las zonas, en una de las zonas de disponibilidad existentes.

Las puertas de enlace NAT regionales admiten dos modos:

- Modo automático: en este modo, AWS administra automáticamente las direcciones IP y la expansión de zonas de disponibilidad (recomendado). Si desea utilizar sus propias direcciones IP en este modo y usa Amazon VPC IPAM, consulte Definición de la estrategia de asignación de IPv4 pública con las políticas de IPAM en la Guía del usuario de Amazon VPC IPAM.
- Modo manual: en este modo, se administran las direcciones IP y se controla la traducción de direcciones de red para cada zona de disponibilidad de forma manual. En el modo manual, el usuario es responsable de expandir y contraer la puerta de enlace NAT entre las zonas de disponibilidad.

> **Important**
>
> Las puertas de enlace NAT regionales admiten AWS Transit Gateway como ruta válida en la tabla de enrutamiento de la puerta de enlace NAT regional. Las puertas de enlace NAT regionales no admiten NAT privada. Si necesita una NAT privada, utilice puertas de enlace NAT zonales en su lugar. Las puertas de enlace NAT regionales no se admiten en zonas de disponibilidad restringida.

Precios

Para obtener información sobre los precios, consulte Precios de Amazon VPC.

Creación de una puerta de enlace NAT regional

Uso de la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Puertas de enlace de NAT.
3. Elija Crear una puerta de enlace de NAT.
4. En Modo de disponibilidad, seleccione Regional. No necesita especificar ninguna subred cuando selecciona la disponibilidad regional
5. Elija una VPC.
6. Complete la configuración restante y seleccione Crear puerta de enlace NAT.

Uso de la CLI de AWS

Creación de una puerta de enlace NAT regional

```
aws ec2 create-nat-gateway --vpc-id vpc-12345678 --availability-mode regional
```

Ver detalles de la puerta de enlace NAT

```
aws ec2 describe-nat-gateways --nat-gateway-ids nat-12345678
```

Agregar direcciones IP (modo manual)

```
aws ec2 associate-nat-gateway-address --nat-gateway-id nat-12345678 --availability-zone
 us-east-1b --allocation-ids eipalloc-12345678
```

Eliminar direcciones IP

```
aws ec2 disassociate-nat-gateway-address --nat-gateway-id nat-12345678 --association-
ids eipassoc-12345678
```

Eliminar una puerta de enlace NAT regional

```
aws ec2 delete-nat-gateway --nat-gateway-id nat-12345678
```

Conversión de puertas de enlace NAT zonales a regionales

> **Important**
>
> Esto restablecerá las conexiones existentes. Se recomienda completar estos pasos durante el periodo de mantenimiento.

Puede convertir puertas de enlace NAT zonales existentes en una puerta de enlace NAT regional mediante uno de los dos enfoques siguientes:

Si está de acuerdo con usar puertas de enlace NAT regionales con nuevas direcciones IP:

1. Crear una nueva puerta de enlace NAT regional
2. Actualizar las tablas de enrutamiento para que apunten a la puerta de enlace NAT regional
3. Eliminar las puertas de enlace NAT zonales antiguas

Con este enfoque, se utilizan nuevas direcciones IP y se restablecen las conexiones existentes cuando se actualizan las rutas.

Si desea reutilizar direcciones IP existentes con puertas de enlace NAT regionales:

1. Eliminar las puertas de enlace NAT zonales existentes para liberar sus direcciones IP
2. Crear una puerta de enlace NAT regional con las direcciones IP liberadas
3. Actualizar las tablas de enrutamiento para que apunten a la puerta de enlace NAT regional

Con este enfoque se conservan las direcciones IP, pero se requiere un periodo de mantenimiento, ya que el tráfico se interrumpe durante la transición.

Casos de uso de puerta de enlace NAT

Los siguientes son ejemplos de casos de uso de gateways NAT públicas y privadas.

Escenarios

- Acceso a Internet desde una subred privada
- Acceso a la red mediante las direcciones IP permitidas
- Habilitar la comunicación entre redes superpuestas

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

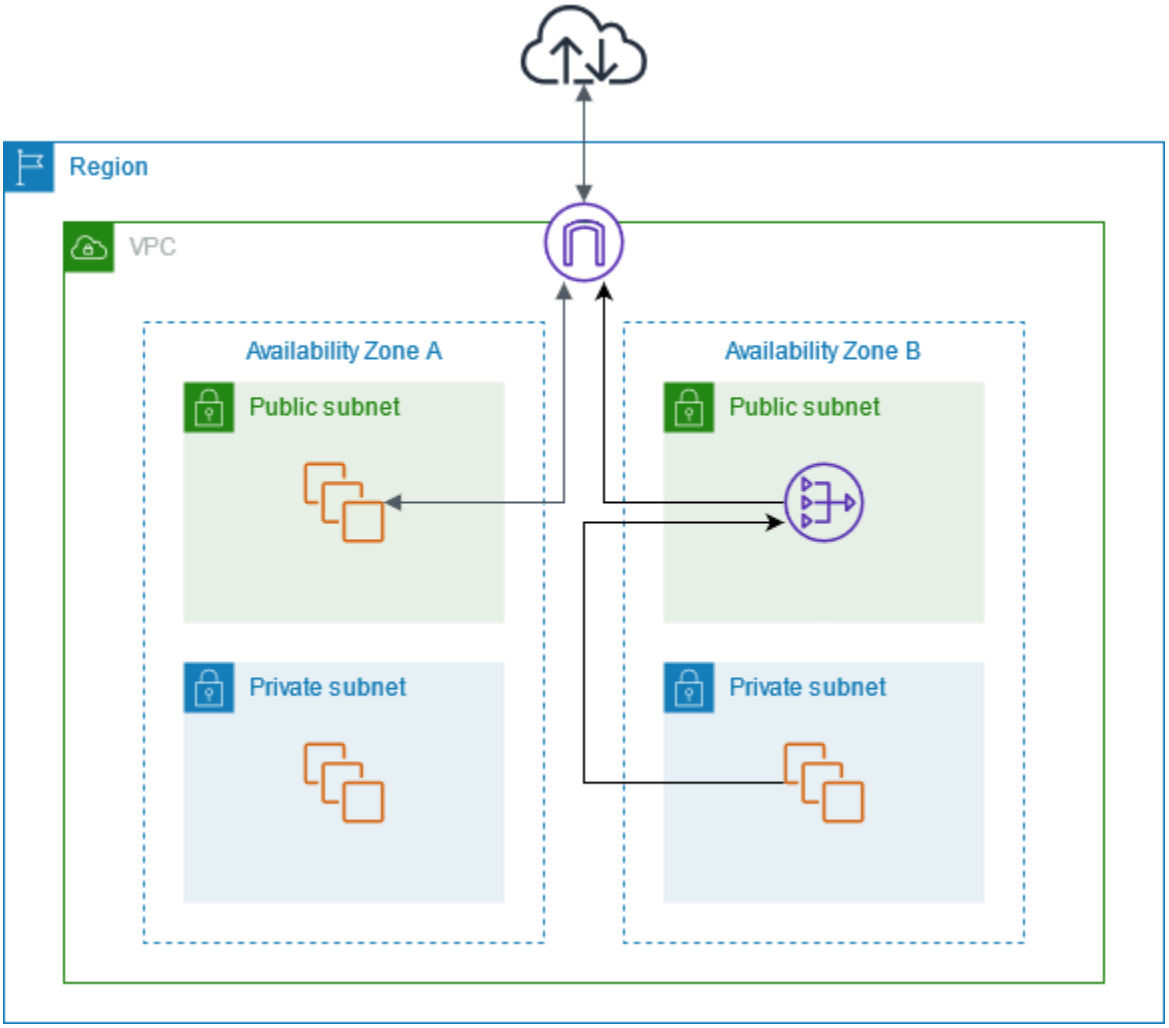
- Descripción general
- Enrutamiento
- Prueba de la gateway NAT pública

Descripción 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.

Tanto las puertas de enlace NAT privadas como las públicas asignan la dirección IPv4 privada de origen de las instancias a la dirección IPv4 privada de la puerta de enlace NAT privada, pero en el caso de una puerta de enlace NAT pública, la puerta de enlace de Internet asigna la dirección IPv4 privada de la puerta de enlace NAT pública a la dirección IP elástica asociada a la puerta de enlace NAT. Cuando envía tráfico de respuesta a las instancias, ya sea una puerta de enlace NAT pública o privada, la puerta de enlace NAT traduce la dirección a la dirección IP de origen.



Tenga en cuenta que, si las instancias de la subred privada de la zona de disponibilidad A también necesitan acceder a Internet, puede crear una ruta desde esta subred hasta la puerta de enlace NAT en la zona de disponibilidad B. También, puede mejorar la resiliencia al crear una puerta de enlace

NAT en cada zona de disponibilidad que contenga recursos que requieren acceso a Internet. Para ver un diagrama de ejemplo, consulte the section called “Servidores privados”.

Enrutamiento

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
CIDR DE VPC	local
0.0.0.0/0	*internet-puerta de enlace -id*

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
CIDR DE VPC	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
CIDR DE VPC	local
0.0.0.0/0	*internet-puerta de enlace -id*

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
CIDR DE VPC	local
0.0.0.0/0	*nat-gateway-id*

Para obtener más información, consulte the section called “Administración de las tablas de enrutamiento de subred”.

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.

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 puerta de enlace de NAT.

Si estas pruebas no son satisfactorias, consulte Solucionar problemas de las gateways NAT.

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 host 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 intervalo de direcciones IP de su red local y el tráfico SSH saliente al intervalo de direcciones IP de su subred privada. También se puede utilizar `0.0.0.0/0` para el tráfico SSH entrante y 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 o Para configurar el reenvío de agentes SSH para Windows.
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.

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

Puede usar el cliente OpenSSH disponible en Windows o instalar el cliente SSH que prefiera (por ejemplo, PuTTY).

OpenSSH

Instale OpenSSH para Windows como se describe en este artículo: Introducción a OpenSSH para Windows. A continuación, agregue su clave al agente de autenticación. Para obtener más información, consulte Autenticación basada en claves en OpenSSH 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.
3. Inicie Pageant, abra el menú contextual para el icono de Pageant de la barra de tareas (puede estar oculto) y elija Agregar clave. 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 más información, consulte Conectarse a su instancia Linux mediante PuTTY. 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.

3. (Opcional) Si ya no necesita las instancias, termínelas. Para obtener más información, consulte Terminar una instancia en la Guía del usuario de Amazon EC2.

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.

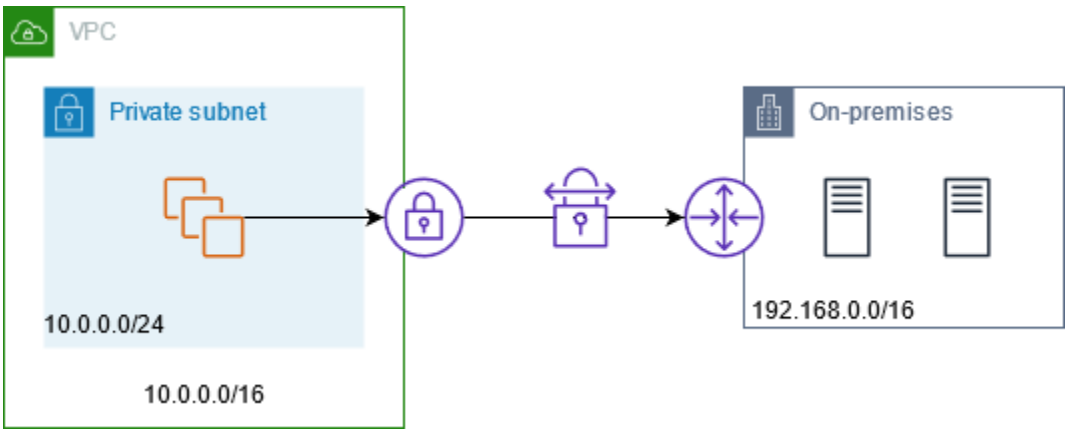
En lugar de asignar a cada instancia una dirección IP independiente del rango de la lista de permitidas, puede dirigir el tráfico desde la subred a través de una puerta de enlace NAT privada con una dirección IP del rango de la lista de permitidas.

Contenido

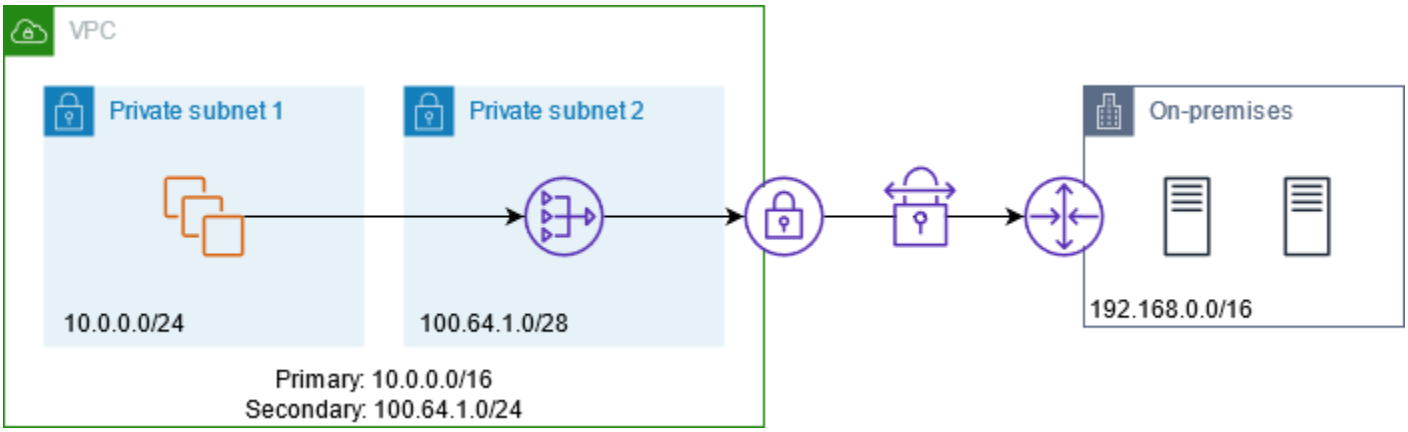
- Descripción general
- Recursos
- Enrutamiento

Descripción general

En el siguiente diagrama se muestra cómo las instancias pueden acceder a los recursos en las instalaciones mediante Site-to-Site 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.

Enrutamiento

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.

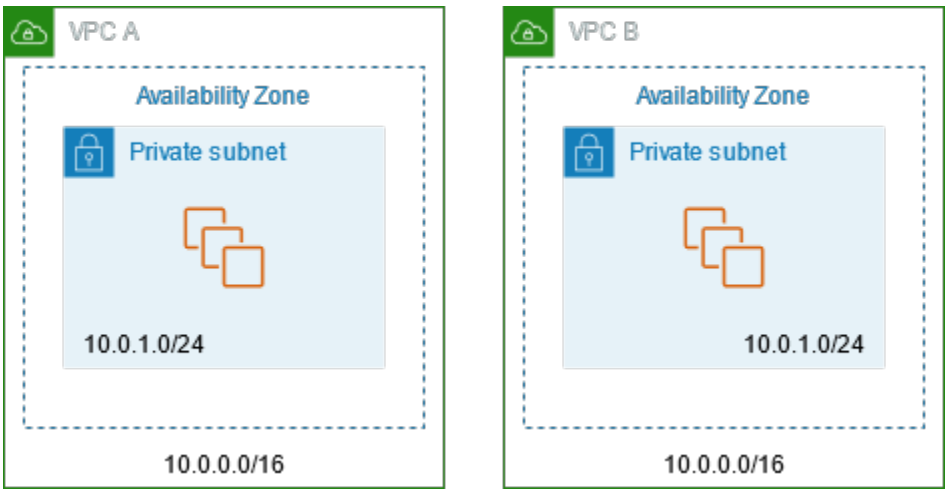
Destino	Objetivo
10.0.0.0/16	local
100.64.1.0/24	local
192.168.0.0/16	*nat-gateway-id*

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
10.0.0.0/16	local
100.64.1.0/24	local
192.168.0.0/16	*vgw-id*

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

- Descripción general
- Recursos
- Enrutamiento

Descripción general

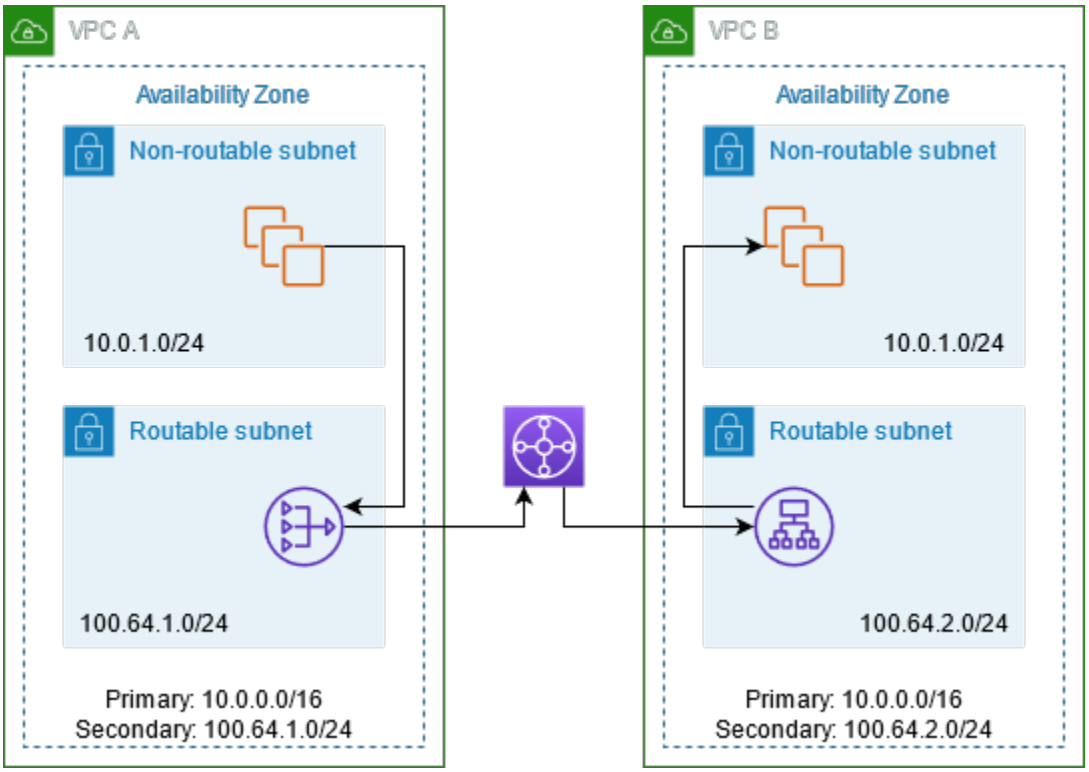
El siguiente diagrama muestra los componentes clave de la configuración de este escenario. En primer lugar, su equipo de administración de IP determina qué rangos de direcciones pueden superponerse (rangos de direcciones no enrutables) y cuáles no (rangos de direcciones enrutables). El equipo de administración 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 Equilibrador de carga de aplicación. El Equilibrador de carga de aplicación obtiene las direcciones IP de sus subredes.

El tráfico de una instancia de la subred no enrutable de la VPC A destinado a las instancias de la subred no enrutable de la VPC B se envía a través de la puerta de enlace NAT privada. A continuación, se enruta a la puerta de enlace de tránsito.

La puerta de enlace de tránsito envía el tráfico al equilibrador de carga de aplicación, que dirige el tráfico a una de las instancias de destino de la subred no enrutable de la VPC B. Este tráfico de

puerta de enlace de tráfico al equilibrador de carga de aplicación 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 Equilibrador de carga de aplicación 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.

Enrutamiento

La siguiente es la tabla de enrutamiento de la subred no enrutable de la VPC A.

Destino	Objetivo
10.0.0.0/16	local
100.64.1.0/24	local
100.64.2.0/24	*nat-gateway-id*

La siguiente es la tabla de enrutamiento de la subred enrutable de la VPC A.

Destino	Objetivo
10.0.0.0/16	local
100.64.1.0/24	local
100.64.2.0/24	*transit-gateway-id*

La siguiente es la tabla de enrutamiento de la subred no enrutable de la VPC B.

Destino	Objetivo
10.0.0.0/16	local
100.64.2.0/24	local

La siguiente es la tabla de enrutamiento de la subred enrutable de la VPC B.

Destino	Objetivo
10.0.0.0/16	local
100.64.2.0/24	local
100.64.1.0/24	*transit-gateway-id*

A continuación, se muestra la tabla de enrutamiento de la puerta de enlace de tránsito.

CIDR	Conexión	Tipo de ruta
100.64.1.0/24	*Vinculación de la VPC A*	Estático
100.64.2.0/24	*Vinculación de la VPC B*	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?
- ¿Qué es NAT64?
- Configuración de DNS64 y NAT64

¿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 puerta de enlace 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. La subred en la que se encuentra la puerta de enlace NAT no necesita ser una subred de doble pila para que NAT64 funcione.

Después de habilitar DNS64, si el servicio solo de IPv6 envía paquetes de red a la dirección IPv6 sintetizada a través de la puerta de enlace 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 que se haya establecido una conexión, la puerta de enlace NAT acepta los paquetes IPv4 de respuesta de los hosts externos.
- Los paquetes IPv4 de respuesta están destinados a la puerta de enlace 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 puerta de enlace NAT permite que las cargas de trabajo solo de IPv6 de una subred se comuniquen con los servicios solo de IPv4 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
- Habilitar la comunicación con los servicios solo de IPv4 en su entorno en las instalaciones

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 puerta de enlace NAT debe tener una ruta `0.0.0.0/0` con dirección a la puerta de enlace 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 conexión de salida de Route 53 Resolver, debe habilitar DNS64 en la subred que contiene sus cargas de trabajo solo de IPv6. También debe enrutar los datos destinados a su red en las instalaciones a través de una puerta de enlace 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.

Inspección del tráfico proveniente de las puertas de enlace NAT

Puede asociar un proxy de Network Firewall a la puerta de enlace NAT para inspeccionar y filtrar el tráfico que pasa por la puerta de enlace NAT. Este control de seguridad permite evitar filtraciones de datos fuera del perímetro de confianza y bloquea cualquier respuesta entrante no deseada.

Funcionamiento

Al crear un proxy de Network Firewall, es obligatorio seleccionar una puerta de enlace NAT existente con la que asociar el proxy. Una vez creado, el proxy:

- El proxy incluye un nombre de dominio completo y es necesario configurar las aplicaciones para que envíen las solicitudes HTTP y HTTPS CONNECT al proxy. El proxy filtra primero el nombre de dominio de la solicitud CONNECT en función de las reglas definidas por el cliente. Si las reglas lo permiten, el proxy realiza a continuación una consulta de DNS para obtener la dirección IP del dominio. A continuación, establece una conexión TCP con el destino final. En función de si el descifrado de TLS está habilitado, el proxy filtra a continuación la conexión TLS según la dirección IP y los atributos del encabezado, y solo establece una conexión TLS con el destino si la dirección IP y los atributos del encabezado (incluida la acción del encabezado y la ruta de la URL) están permitidos por las políticas.
- El dispositivo inspecciona y filtra el tráfico.
- El tráfico permitido continúa hacia el destino, ya sea en Internet, en un entorno en las instalaciones o en otra VPC.

Asociación de dispositivos

Los dispositivos se asocian a las puertas de enlace NAT a través de AWS Network Firewall. Para conocer los pasos necesarios para crear y asociar dispositivos, consulte la Guía para desarrolladores del proxy de Network Firewall.

Visualización de dispositivos asociados

Para ver los dispositivos asociados a la puerta de enlace NAT, utilice el comando describe-nat-gateways:

```
aws ec2 describe-nat-gateways --nat-gateway-ids nat-1234567890abcdef0
```

La respuesta incluye un campo `AttachedAppliances` que muestra lo siguiente:

- Type: el tipo de dispositivo (por ejemplo, `network-firewall-proxy`)
- ApplianceArn: el ARN del dispositivo asociado
- AttachmentState: estado de asociación actual (`attached`, `detaching`, `detached`, `attach_failed` y `detach_failed`)
- ModificationState: estado de modificación actual (`modifying`, `completed` y `failed`)
- VpcEndpointId: el ID de punto de conexión de VPC que se utiliza para enrutar el tráfico desde las VPC de aplicaciones hacia el proxy para su inspección y filtrado
- FailureCode: el código de error en caso de que la operación de asociación o modificación del dispositivo haya fallado

- FailureMessage: un mensaje descriptivo que explica el error en caso de que la operación de asociación o modificación del dispositivo haya fallado

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. Estas métricas brindan información sobre el estado y el rendimiento de su puerta de enlace NAT, lo que da lugar a una supervisión de cerca de sus operaciones y una rápida solución de problemas.

Las métricas de la puerta de enlace de NAT que recopila CloudWatch incluye puntos de datos como los bytes procesados, la cantidad de paquetes, la cantidad de conexiones y las tasas de errores. Con esto, puede comprender el tráfico que fluye por la puerta de enlace de NAT e identificar cualquier anormalidad o cuello de botella. CloudWatch envía estos datos métricos en intervalos de un minuto, lo que brinda un vista granular y actualizada del comportamiento de su puerta de enlace de NAT.

Además, CloudWatch retiene los datos métricos de esta puerta de enlace de NAT por un período prolongado de 15 meses, lo que permite analizar las tendencias y los patrones a lo largo del tiempo. Estos datos históricos se pueden utilizar para planificar la capacidad, optimizar el rendimiento y comprender la evolución a largo plazo del uso de su puerta de enlace de NAT.

Para utilizar estas potentes capacidades de supervisión, puede crear paneles y alarmas personalizados de CloudWatch adaptados a sus necesidades específicas. Por ejemplo, puede configurar alertas que notifiquen cada vez que la transferencia de datos salientes de su puerta de enlace de NAT supere un determinado umbral, lo que permitirá el abordaje proactivo de las posibles limitaciones del ancho de banda.

Para obtener más información sobre precios, consulte Precios de Amazon CloudWatch.

Contenido

- Métricas y dimensiones de gateway NAT
- Consultar las métricas de CloudWatch para las gateways NAT
- Crear alarmas de CloudWatch para monitorear una gateway NAT

Métricas y dimensiones de gateway NAT

Las siguientes métricas están disponibles para las gateways de NAT. La columna de descripción incluye una descripción de cada métrica, así como las unidades y las estadísticas.

Métrica	Descripción
`ActiveConnectionCount`	Número total de conexiones TCP simultáneas activas a través de la gateway NAT. Si el valor es cero, indica que no hay conexione s activas a través de la gateway NAT. Unidades: recuento Estadísticas: la estadística más útil es `Max`.
`BytesInFromDestination`	Número de bytes recibidos por la gateway NAT desde el destino. Si el valor de `BytesOutToSource` es menor que el valor de `BytesInFromDestina tion` , puede que se estén perdiendo datos durante el procesamiento de la gateway NAT o que la gateway NAT esté bloqueando el tráfico. Unidades: bytes Estadísticas: la estadística más útil es `Sum`.
`BytesInFromSource`	Número de bytes recibidos por la gateway NAT desde los clientes de la VPC. Si el valor de `BytesOutToDestination` es menor que el valor de `BytesInFromSource` , puede que se estén perdiendo datos durante el procesamiento de la gateway NAT. Unidades: bytes

Métrica	Descripción
	Estadísticas: la estadística más útil es Sum.
BytesOutToDestination	Número de bytes enviados a través de la gateway NAT al destino. 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 BytesOutToDestination es menor que el valor de BytesInFromSource, puede que se estén perdiendo datos durante el procesamiento de la gateway NAT. Unidades: bytes Estadísticas: la estadística más útil es Sum.
BytesOutToSource	Número de bytes enviados a través de la gateway NAT a los clientes de la VPC. 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 BytesOutToSource es menor que el valor de BytesInFromDestination, puede que se estén perdiendo datos durante el procesamiento de la gateway NAT o que la gateway NAT esté bloqueando el tráfico. Unidades: bytes Estadísticas: la estadística más útil es Sum.

Métrica	Descripción
ConnectionAttemptCount	Número de intentos de conexión realizados a través de la gateway NAT. Esto incluye solo el SYN inicial. En algunos casos, ConnectionAttemptCount puede ser inferior a ConnectionEstablishedCount debido a la retransmisión del SYN. Si el valor de ConnectionEstablishedCount es menor que el valor de ConnectionAttemptCount, esto indica que los clientes que se encuentran detrás de la gateway NAT han intentado establecer nuevas conexiones, pero que no han obtenido respuesta. Unidad: recuento Estadísticas: la estadística más útil es Sum.
ConnectionEstablishedCount	Número de conexiones establecidas a través de la gateway NAT. Esto incluye SYN y retransmisiones de SYN. Si el valor de ConnectionEstablishedCount es menor que el valor de ConnectionAttemptCount, esto indica que los clientes que se encuentran detrás de la gateway NAT han intentado establecer nuevas conexiones, pero que no han obtenido respuesta. Unidad: recuento Estadísticas: la estadística más útil es Sum.

Métrica	Descripción
`ErrorPortAllocation`	Número de veces que la gateway NAT no pudo asignar un puerto de origen. Un valor mayor que cero indica que hay demasiadas conexiones simultáneas abiertas a través de la gateway NAT. Unidades: recuento Estadísticas: la estadística más útil es `Sum`.
`IdleTimeoutCount`	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. Un valor mayor que cero indica que hay conexiones han entrado en el estado de inactividad. Si el valor de `IdleTimeoutCount` aumenta, podría indicar que los clientes que se encuentran detrás de la gateway NAT están reutilizando conexiones obsoletas. Unidad: recuento Estadísticas: la estadística más útil es `Sum`.

Métrica	Descripción
`PacketsDropCount`	Número de paquetes que la gateway NAT ha perdido. Para calcular el número de paquetes descartados como porcentaje del tráfico total de paquetes, utilice esta fórmula: `PacketsDropCount/(PacketsInFromSource+PacketsInFromDestination)*100`. Si este valor supera el 0,01 % del tráfico total en la puerta de enlace NAT, es posible que se produzca un problema con el servicio Amazon VPC. Utilice el AWS panel de estado del servicio para identificar cualquier problema con el servicio que pueda estar provocando que las puertas de enlace NAT descarten paquetes. Unidades: recuento Estadísticas: la estadística más útil es `Sum`.
`PacketsInFromDestination`	Número de paquetes recibidos por la gateway NAT desde el destino. 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. Unidad: recuento Estadísticas: la estadística más útil es `Sum`.

Métrica	Descripción
PacketsInFromSource	Número de paquetes recibidos por la gateway NAT desde los clientes de la VPC. Si el valor de PacketsOutToDestination es menor que el valor de PacketsInFromSource, puede que se estén perdiendo datos durante el procesamiento de la gateway NAT. Unidad: recuento Estadísticas: la estadística más útil es Sum.
PacketsOutToDestination	Número de paquetes enviados a través de la gateway NAT al destino. 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 PacketsOutToDestination es menor que el valor de PacketsInFromSource, puede que se estén perdiendo datos durante el procesamiento de la gateway NAT. Unidad: recuento Estadísticas: la estadística más útil es Sum.

Métrica	Descripción
PacketsOutToSource	Número de paquetes enviados a través de la gateway NAT a los clientes de la VPC. 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. Unidad: recuento Estadísticas: la estadística más útil es Sum.
PeakBytesPerSecond	Esta métrica indica el promedio más alto de bytes por segundo de 10 segundos en un minuto determinado. Unidades: recuento Estadísticas: la estadística más útil es Maximum.
PeakPacketsPerSecond	Esta métrica calcula la velocidad promedio de paquetes (paquetes procesados por segundo) cada 10 segundos durante 60 segundos y, a continuación, muestra la velocidad máxima de las seis velocidades (la velocidad promedio de paquetes más alta). Unidades: recuento Estadísticas: la estadística más útil es Maximum.

Para filtrar los datos de las métricas, use las siguientes dimensiones.

Dimensión	Descripción
`NatGatewayId`	Filtra los datos de las métricas en función del ID de gateway NAT. Las puertas de enlace NAT zonales solo utilizan esta dimensión. Las puertas de enlace NAT regionales utilizan esta dimensión junto con `AvailabilityZone` .
`AvailabilityZone`	Filtra los datos de métricas por zona de disponibilidad. Las puertas de enlace NAT regionales utilizan esta dimensión junto con `NatGatewayId` . Las puertas de enlace NAT zonales no utilizan esta dimensión.

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 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 Período, seleccione 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 períodos 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 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 Período, elija 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
- Cuota de gateways NAT
- Cuota de direcciones IP elásticas

- La zona de disponibilidad no es compatible
- La gateway NAT ya no está visible
- La gateway NAT no responde a un comando ping
- Las instancias no pueden obtener acceso a Internet
- Error de la conexión TCP a un destino
- La salida del comando traceroute no muestra la dirección IP privada de la gateway NAT
- La conexión a Internet se pierde después de 350 segundos
- La conexión IPsec no se puede establecer
- No se pueden iniciar más conexiones

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 asignada desde el rango de la subred.	Vaya a la página Subnets (Subredes) de la consola de Amazon VPC para comprobar cuántas direcciones IP hay disponibles en 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-xxxxxxxx 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 Adición de acceso a Internet en una subred.
Elastic IP address eipalloc-xxxxxxxx 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

Error mostrado	Causa	Solución
		más información, consulte Introducción a las direcciones IP elásticas.

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.

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 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.

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 de Amazon VPC, vaya a la página Puertas de enlace 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.
- Asegúrese de haber configurado las tablas de ruteo correctamente:
  - La gateway NAT debe estar en una subred pública con una tabla de ruteo que direccione 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 direccione 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.
- 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 puertas de enlace NAT con las instancias NAT.
- 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 puerta de enlace NAT, pero no puede 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. Si sus instancias de la subred privada crean un gran número de conexiones, puede que alcance este límite.

Solución

Realice una 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` en CloudWatch para monitorear los aumentos de las conexiones inactivas. Cierre las conexiones inactivas para liberar capacidad.
- Cree una puerta de enlace NAT con varias direcciones IP o agregue direcciones IP secundarias a una puerta de enlace NAT existente. Cada dirección IPv4 nueva puede admitir hasta 55 000 conexiones simultáneas. Para obtener más información, consulte Creación de una gateway NAT o Edición de asociaciones de direcciones IP secundarias.

Precios de las puertas de enlace NAT

Cuando aprovisione una puerta de enlace 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 puerta de enlace NAT. También puede crear una puerta de enlace NAT en cada zona de disponibilidad con 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.

Instancias de NAT

Una instancia NAT proporciona traducción de direcciones de red (NAT). Puede usar una instancia NAT para permitir que los recursos de una subred privada se comuniquen con destinos fuera de la nube privada virtual (VPC), como Internet o una red en las instalaciones. Los recursos de la subred privada pueden iniciar el tráfico IPv4 saliente a Internet, pero no pueden recibir el tráfico entrante iniciado en Internet.

> **Important**
>
> NAT AMI se basa en la última versión de Amazon Linux AMI, 2018.03, cuya compatibilidad estándar llegó a su fin el 31 de diciembre de 2020 y su mantenimiento llegó a su fin el 31 de diciembre de 2023. Para obtener más información, consulte la siguiente entrada del blog: Amazon Linux AMI end of life.
> Si utiliza una AMI NAT existente, AWS recomienda que migre a una puerta de enlace NAT. Las puertas de enlace NAT ofrecen una mejor disponibilidad, un mayor ancho de banda y que requieren menos esfuerzo administrativo. Para obtener más información, consulte Comparar las puertas de enlace NAT con las instancias NAT.
> Si las instancias NAT coinciden mejor con su caso práctico que las puertas de enlace NAT, puede crear su propia AMI NAT de una versión actual de Amazon Linux como se describe en the section called “3. Creación de una AMI de NAT”.

Contenido

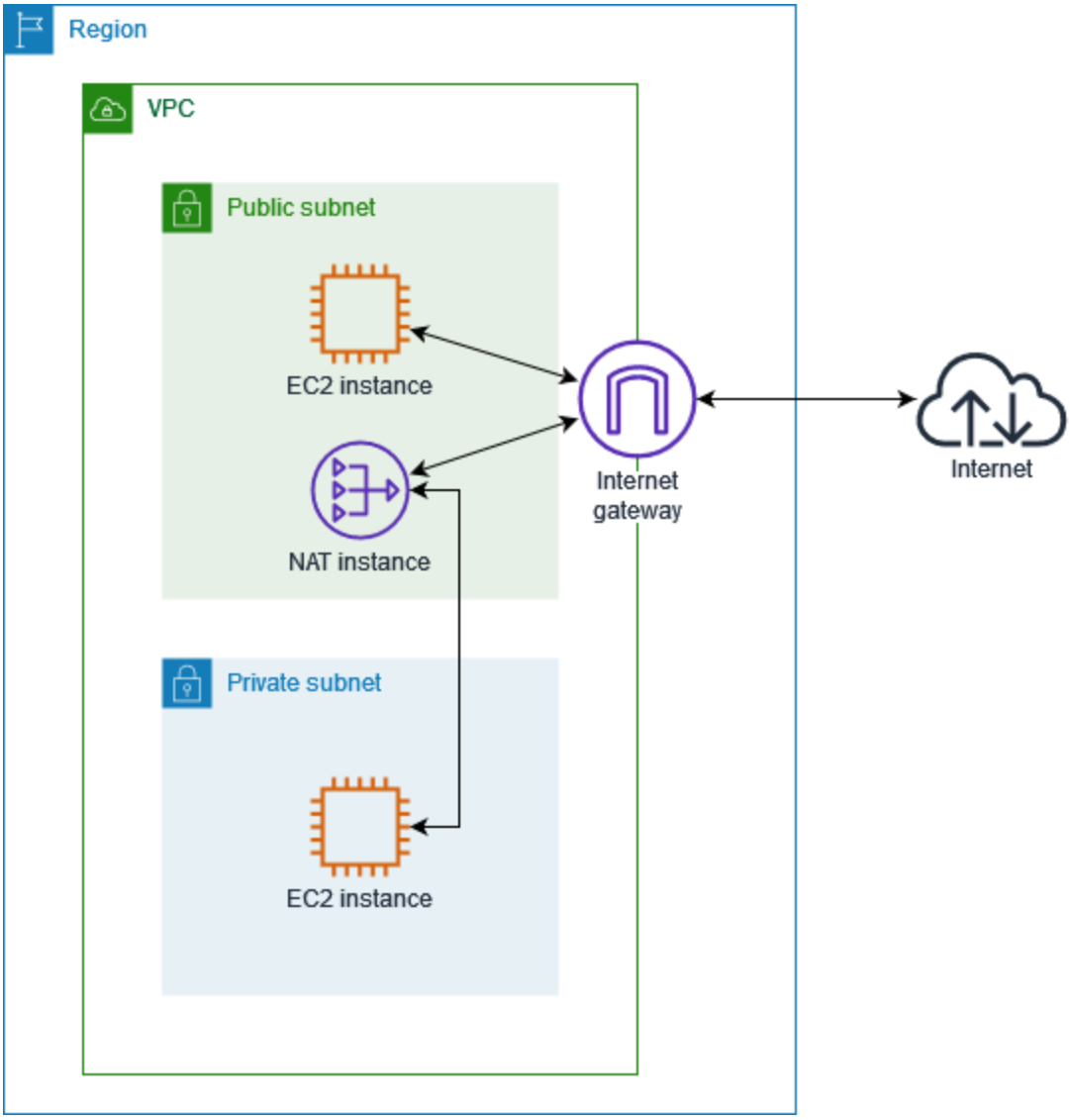
- Conceptos básicos de las instancias NAT
- Habilitación de recursos privados para la comunicación fuera de la VPC

Conceptos básicos de las instancias NAT

El siguiente gráfico muestra los conceptos básicos de las instancias NAT. La tabla de enrutamiento asociada con la subred privada envía tráfico de Internet desde las instancias de la subred privada a la instancia NAT en la subred pública. La instancia NAT luego envía el tráfico a la puerta de enlace de Internet. El tráfico se atribuye a la dirección IP pública 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.

La instancia NAT debe tener acceso a Internet, por lo que debe estar en una subred pública (una subred que tiene una tabla de enrutamiento con una ruta a la puerta de enlace de Internet) y debe tener una dirección IP pública o una dirección IP elástica.



Comience a utilizar las instancias NAT, cree una AMI de NAT, cree un grupo de seguridad para la instancia NAT y lance la instancia de NAT en su VPC.

Su cuota de instancias NAT depende de la cuota de instancias para la región. Para obtener más información, consulte Service Quotas de Amazon EC2 en Referencia general de AWS.

Habilitación de recursos privados para la comunicación fuera de la VPC

En esta sección, se describe cómo crear instancias de NAT y trabajar con ellas para que los recursos de una subred privada puedan comunicarse fuera de la nube virtual privada.

Tareas

- 1. Crear una VPC para la instancia NAT
- 2. Crear un grupo de seguridad para instancias NAT
- 3. Creación de una AMI de NAT
- 4. Lanzamiento de una instancia NAT
- 5. Deshabilitar las comprobaciones de origen/destino
- 6. Actualización de la tabla de enrutamiento
- 7. Pruebe su instancia NAT

1. Crear una VPC para la instancia NAT

Utilice el siguiente procedimiento para crear una VPC con una subred pública y una subred privada.

Para crear la VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Seleccione Creación de VPC.
3. En Resources to create (Recursos para crear), elija VPC and more (VPC y más).
4. En Generación automática de etiquetas de nombre, ingrese un nombre para la VPC.
5. Para configurar las subredes, haga lo siguiente:
    a. En Number of Availability Zones (Número de zonas de disponibilidad), elija 1 o 2, según sus necesidades.
    b. En Number of public subnets (Número de subredes públicas), asegúrese de tener una subred pública por zona de disponibilidad.
    c. En Number of private subnets (Número de subredes privadas), asegúrese de tener una subred privada por zona de disponibilidad.
6. Seleccione Create VPC (Crear VPC).

2. Crear un grupo de seguridad para instancias NAT

Cree un grupo de seguridad con las reglas que se describen en la tabla siguiente. Estas reglas permiten que su instancia NAT reciba tráfico vinculado a Internet de instancias en la subred privada, así como también 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 de entrada recomendadas.

Origen	Protocolo	Rango de puerto	Comentarios
CIDR de subred privada	TCP	80	Permite el tráfico HTTP entrante de servidores en la subred privada.
CIDR de subred privada	TCP	443	Permite el tráfico HTTPS entrante de servidores en la subred privada.
Rango de direcciones IP públicas de su red	TCP	22	Permite el acceso SSH entrante a la instancia NAT desde su red (a través de la puerta de enlace de Internet).

A continuación, se muestran las reglas de salida recomendadas.

Destino	Protocolo	Rango de puerto	Comentarios
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

Para crear el grupo de seguridad

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Grupos de seguridad.
3. Elija Create Security Group (Creación de grupo de seguridad).
4. Ingrese un nombre y una descripción para el grupo de seguridad.
5. Para VPC, seleccione el ID de la VPC para su instancia NAT.
6. Agregue reglas para el tráfico entrante en Reglas entrantes de la siguiente manera:
    a. Seleccione Agregar regla. Elija HTTP para Tipo e ingrese el rango de direcciones IP de su subred privada para Fuente.
    b. Seleccione Agregar regla. Elija HTTPS para Tipo e ingrese el rango de direcciones IP de su subred privada para Fuente.
    c. Seleccione Agregar regla. Elija SSH para Tipo e ingrese el rango de direcciones IP de su red para Origen.
7. Agregue reglas para el tráfico saliente en Reglas salientes de la siguiente manera:
    a. Seleccione Agregar regla. Elija HTTP como Tipo e introduzca 0.0.0.0/0 como Destino.
    b. Seleccione Agregar regla. Elija HTTPS como Tipo e introduzca 0.0.0.0/0 como Destino.
8. Elija Create Security Group (Crear grupo de seguridad).

Para obtener más información, consulte Grupos de seguridad.

3. Creación de una AMI de NAT

Una AMI de NAT está configurada para ejecutar NAT en una instancia de EC2. Debe crear una AMI de NAT y, a continuación, lanzar la instancia NAT con su AMI de NAT.

Si piensa utilizar un sistema operativo que no sea Amazon Linux para su AMI de NAT, consulte la documentación de este sistema operativo para obtener información sobre cómo configurar la NAT. Asegúrese de guardar esta configuración para que se mantenga incluso después de reiniciar la instancia.

Para crear una AMI de NAT para Amazon Linux

1. Lance una instancia EC2 que ejecute AL2023 o Amazon Linux 2. Asegúrese de especificar el grupo de seguridad que creó para la instancia de NAT.

2. Conéctese a la instancia y ejecute los comandos siguientes en la instancia para habilitar iptables.

```
sudo yum install iptables-services -y
sudo systemctl enable iptables
sudo systemctl start iptables
```

3. Haga lo siguiente en la instancia para habilitar el reenvío de IP de forma que persista después del reinicio:

   a. Mediante un editor de texto, como nano o vim, cree el siguiente archivo de configuración: `/etc/sysctl.d/custom-ip-forwarding.conf`.

   b. Agregue la siguiente línea al archivo de configuración.

```
net.ipv4.ip_forward=1
```

   c. Guarde el archivo de configuración y salga del editor de texto.

   d. Ejecute el siguiente comando para aplicar el archivo de configuración.

```
sudo sysctl -p /etc/sysctl.d/custom-ip-forwarding.conf
```

4. Ejecute el siguiente comando en la instancia y anote el nombre de la interfaz de red principal. Necesitará esta información para el siguiente paso.

```
netstat -i
```

   En el ejemplo de salida a continuación, `docker0` es una interfaz de red creada por Docker, `eth0` es la interfaz de red principal y `lo` es la interfaz de bucle invertido.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
docker0   1500        0      0      0 0             0      0      0      0 BMU
eth0      9001  7276052      0      0 0       5364991      0      0      0 BMRU
lo       65536   538857      0      0 0        538857      0      0      0 LRU
```

   En el ejemplo de salida a continuación, la interfaz de red principal es `enX0`.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enX0      9001     1076      0      0 0          1247      0      0      0 BMRU
lo       65536       24      0      0 0            24      0      0      0 LRU
```

En el ejemplo de salida a continuación, la interfaz de red principal es `ens5`.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens5      9001    14036      0      0 0          2116      0      0      0 BMRU
lo       65536       12      0      0 0            12      0      0      0 LRU
```

5. Ejecute los comandos siguientes en la instancia para configurar NAT. Si la interfaz de red principal no es `eth0`, reemplace *`eth0`* por la interfaz de red principal que anotó en el paso anterior.

```
sudo /sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo /sbin/iptables -F FORWARD
sudo service iptables save
```

6. Cree una AMI de NAT desde la instancia EC2. Para obtener más información, consulte Crear una AMI de Linux desde una instancia en la Guía del usuario de Amazon EC2.

4. Lanzamiento de una instancia NAT

Utilice el siguiente procedimiento para lanzar una instancia NAT mediante la VPC, el grupo de seguridad y la AMI de NAT que ha creado.

Para lanzar una instancia NAT

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel, elija Iniciar instancia.
3. En Nombre, ingrese un nombre para la instancia NAT.
4. Para las imágenes de aplicaciones y sistemas operativos, seleccione su AMI de NAT (elija Buscar más AMI, Mis AMI).
5. En Tipo de instancia, elija un tipo de instancia que proporcione los recursos de computación, memoria y almacenamiento que necesita su instancia NAT.
6. (Opcional) En Par de claves, seleccione un par de claves existente o elija Crear nuevo par de claves.
7. En Network settings (Configuración de red), haga lo siguiente:
   a. Elija Edit (Edición de).
   b. En VPC, elija la VPC que ha creado.

c. En Subred, elija la subred pública que creó para la VPC.

d. En Auto-assign public IP (Autoasignar IP pública), elija Enable (Habilitar). Como alternativa, después de lanzar la instancia NAT, asigne una dirección IP elástica y asígnela a la instancia NAT.

e. En Firewall, elija Seleccionar un grupo de seguridad existente y, a continuación, elija el grupo de seguridad que creó.

8. Seleccione Iniciar instancia. Elija el ID de la instancia para abrir la página de detalles de la instancia. Espere a que el estado de la instancia cambie a En ejecución y a que las comprobaciones de estado se realicen de forma correcta.
9. Deshabilite las comprobaciones de origen o destino para la instancia NAT (consulte 5. Deshabilitar las comprobaciones de origen/destino).
10. Actualice la tabla de enrutamiento para enviar tráfico a la instancia NAT (consulte 6. Actualización de la tabla de enrutamiento).

5. 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.

Para deshabilitar las comprobaciones de origen o destino

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.
4. Elija Acciones, Redes, Cambiar verificación de origen/destino.
5. Para comprobar el origen o el destino, seleccione Detener.
6. Seleccione Save.
7. 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).

6. Actualización de la tabla de enrutamiento

La tabla de enrutamiento para la subred privada debe tener una ruta que envíe tráfico de Internet a la instancia NAT.

Para actualizar la tabla de enrutamiento

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Tablas de enrutamiento.
3. Seleccione la tabla de enrutamiento de la subred privada.
4. En la pestaña Rutas, elija Editar rutas y luego elija Agregar ruta.
5. Ingrese 0.0.0.0/0 para Destino y el ID de instancia de la instancia NAT para Destino.
6. Seleccione Save changes (Guardar cambios).

Para obtener más información, consulte Configurar tablas de enrutamiento.

7. Pruebe su instancia NAT

Una vez que haya lanzado una instancia NAT y haya completado los pasos de configuración anteriores, puede probar si una instancia en su subred privada puede acceder a Internet a través de la instancia de NAT mediante el uso de la instancia NAT como servidor bastión.

Tareas

- Paso 1: Actualizar el grupo de seguridad de la instancia de NAT
- Paso 2: Lanzar una instancia de prueba en la subred privada
- Paso 3: Realizar un ping a un sitio web compatible con ICMP
- Paso 4: Limpiar

Paso 1: Actualizar el grupo de seguridad de la instancia de NAT

Para permitir que las instancias de la subred privada envíen tráfico de ping a la instancia de NAT, añada una regla que permita el tráfico ICMP entrante y saliente. Para permitir que la instancia de NAT sirva como servidor bastión, agregue una regla que permita el tráfico SSH saliente a la subred privada.

Para actualizar el grupo de seguridad de su instancia de NAT

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

2. En el panel de navegación, elija Grupos de seguridad.
3. Seleccione la casilla de verificación del grupo de seguridad asociado a la instancia NAT.
4. En la pestaña Reglas de entrada, seleccione Editar reglas de entrada.
5. Seleccione Add rule (Agregar regla). Seleccione All ICMP IPv4 (Todos los ICMP IPv4) para Type (Tipo). Elija Personalizado para Origen e ingrese el rango de direcciones IP de su subred privada. Seleccione Guardar reglas.
6. En la pestaña Reglas de salida, elija Editar reglas de salida.
7. Seleccione Add rule (Agregar regla). Seleccione SSH para Type (Tipo). Elija Personalizado para Destino e ingrese el rango de direcciones IP de su subred privada.
8. Seleccione Add rule (Agregar regla). Seleccione All ICMP IPv4 (Todos los ICMP IPv4) para Type (Tipo). Seleccione Anywhere - PIv4 (En cualquier lugar: IPv4) para Destination (Destino). Seleccione Save rules (Guardar reglas).

Paso 2: Lanzar una instancia de prueba en la subred privada

Lance una instancia en su subred privada. Debe permitir el acceso a SSH desde la instancia de NAT y debe utilizar el mismo par de claves que utilizó para la instancia de NAT.

Para lanzar una instancia de prueba en la subred privada

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel, elija Iniciar instancia.
3. Seleccione su subred privada.
4. No asigne una dirección IP pública a esta instancia.
5. Asegúrese de que el grupo de seguridad de esta instancia permita el acceso SSH entrante desde su instancia NAT o desde el rango de direcciones IP de su subred pública y el tráfico ICMP saliente.
6. Seleccione el mismo par de claves que utilizó para la instancia de NAT.

Paso 3: Realizar un ping a un sitio web compatible con ICMP

Para comprobar que la instancia de prueba de la subred privada puede usar la instancia de NAT para comunicarse con Internet, ejecute el comando ping.

Para probar la conexión a Internet desde tu instancia privada

1. Desde su equipo local, configure el reenvío del agente SSH para poder utilizar la instancia de NAT como servidor bastión.

   Linux and macOS

   ```
   ssh-add key.pem
   ```

   Windows

   Descargue e instale Pageant, si aún no está instalado.

   Convierta su clave privada utilizando PuTTYgen.

   Inicie Pageant, abra el menú contextual para el icono de Pageant de la barra de tareas (puede estar oculto) y elija Agregar clave. Seleccione el archivo .ppk que ha creado, escriba la frase de contraseña si es necesario, y elija Abrir.

2. Conéctese a la instancia de NAT desde su equipo local.

   Linux and macOS

   ```
   ssh -A ec2-user@nat-instance-public-ip-address
   ```

   Windows

   Conéctese a la instancia de NAT mediante PuTTY. En Auth, debe seleccionar Allow agent forwarding y deje Private key file for authentication en blanco.

3. Desde la instancia de NAT, ejecute el comando ping y especifique un sitio web que esté habilitado para ICMP.

   ```
   [ec2-user@ip-10-0-4-184]$ ping ietf.org
   ```

   Para confirmar que la instancia de NAT tiene acceso a Internet, compruebe que ha recibido un resultado como el siguiente y, a continuación, pulse Ctrl+C para cancelar el comando ping. De lo contrario, compruebe que la instancia de NAT esté en una subred pública (que su tabla de enrutamiento contenga una ruta a una puerta de enlace de Internet).

   ```
   PING ietf.org (104.16.45.99) 56(84) bytes of data.
   ```

```
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=1 ttl=33 time=7.88 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=2 ttl=33 time=8.09 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=3 ttl=33 time=7.97 ms
...
```

4. Desde su instancia NAT, conéctese a su instancia en su subred privada utilizando su dirección IP privada.

```
[ec2-user@ip-10-0-4-184]$ ssh ec2-user@private-server-private-ip-address
```

5. Desde su instancia privada, pruebe que puede conectarse a Internet ejecutando el comando ping.

```
[ec2-user@ip-10-0-135-25]$ ping ietf.org
```

Para confirmar que la instancia privada tiene acceso a Internet a través de la instancia de NAT, compruebe que ha recibido un resultado como el siguiente y, a continuación, pulse Ctrl+C para cancelar el comando ping.

```
PING ietf.org (104.16.45.99) 56(84) bytes of data.
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=1 ttl=33 time=8.76 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=2 ttl=33 time=8.26 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=3 ttl=33 time=8.27 ms
...
```

Solución de problemas

Si el ping comando falla desde el servidor de la subred privada, siga estos pasos para solucionar el problema:

- Verifique que haya hecho ping a un sitio web que tenga habilitado ICMP. De lo contrario, su servidor no puede recibir paquetes de respuesta. Para probar esto, ejecute el mismo comando ping desde una terminal de línea de comandos en su propia computadora.
- Verifique que el grupo de seguridad de su instancia NAT permita el tráfico ICMP entrante desde su subred privada. De lo contrario, su instancia NAT no puede recibir el comando ping de su instancia privada.
- Verifique que deshabilitó la verificación de origen o destino para su instancia NAT. Para obtener más información, consulte 5. Deshabilitar las comprobaciones de origen/destino.

- Verifique que configuró sus tablas de rutas correctamente. Para obtener más información, consulte 6. Actualización de la tabla de enrutamiento.

Paso 4: Limpiar

Si ya no necesita el servidor de prueba de la subred privada, finalice la instancia para que no se le siga facturando. Para obtener más información, consulte Terminar una instancia en la Guía del usuario de Amazon EC2.

Si ya no necesita la instancia de NAT, puede detenerla o cancelarla para que no se le siga facturando. Si ha creado una AMI de NAT, puede crear una nueva instancia de NAT siempre que la necesite.

Comparar las puertas de enlace NAT con las instancias NAT

A continuación se proporciona un resumen general de las diferencias entre las puertas de enlace 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 100 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
Desempeñ	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.
Direccion es 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 .
Direccion es 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.

Atributo	Gateway NAT	Instancia NAT
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.	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 puerta de enlace 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 puerta de enlace 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).

Asociar direcciones IP elásticas con recursos en la VPC

Una dirección IP elástica es una dirección IPv4 estática y pública diseñada específicamente para la naturaleza dinámica de la computación en la nube. Con esta característica, puede asociar una dirección IP elástica con cualquier instancia o interfaz de red dentro de una nube privada virtual (VPC) en su cuenta de AWS. Al utilizar direcciones IP elásticas, puede acceder a una serie de beneficios que simplifican la administración y la resiliencia de su infraestructura en la nube.

Uno de las ventajas principales de las direcciones IP elásticas es la habilidad de enmascarar los errores de una instancia. En caso de que una instancia sufra una interrupción o necesite un reemplazo, puede reasignar la dirección IP elástica asociada a otra instancia dentro de su VPC. Este proceso de conmutación por error garantiza que el punto de conexión de sus aplicaciones y servicios se mantenga consistente y fiable a la vez que minimiza el tiempo de inactividad y brinda una experiencia del usuario superior.

Además, las direcciones IP elásticas ofrecen flexibilidad a la hora de administrar los recursos de la red. Puede programar la asociación y la desvinculación de estas direcciones según sea necesario, lo que le permite dirigir el tráfico a distintas instancias según sus necesidades empresariales en constante evolución. Esta asignación dinámica de direcciones IP le permite adaptarse a la demanda cambiante, escalar su infraestructura e implementar arquitecturas innovadoras sin las restricciones de las asignaciones de IP estáticas.

Las direcciones IP elásticas se utilizan no solo para la conmutación por error de instancias, sino también como identificadores estables para sus recursos en la nube. Esto puede ser beneficioso al momento de configurar servicios externos, como registros DNS o reglas de firewall, para comunicarse con sus aplicaciones alojadas en AWS. Al asociar una dirección IP pública persistente, puede preparar sus configuraciones de red para el futuro y evitar la necesidad de actualizar las referencias externas cuando las instancias subyacentes se sustituyan o escalen.

Contenido

- Conceptos y reglas de direcciones IP elásticas
- Introducción a las direcciones IP elásticas

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 red 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 principal de su instancia, su dirección IPv4 pública actual (en caso de que la tenga) se liberará al grupo de direcciones IP públicas. Si anula la asociación de la dirección IP elástica, a la interfaz de red principal 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.
- 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.
- 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 puerta de enlace de Internet. Para obtener más información, consulte Grupos de seguridad y ACL de red.
- 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.

- Las direcciones IPv4 públicas admiten las etiquetas de asignación de costos. Si aplica etiquetas a las direcciones IP elásticas, puede usarlas para hacer un seguimiento de los costos de las direcciones IPv4 públicas en AWS Cost Explorer.

  Para poder utilizar las etiquetas como etiquetas de asignación de costos, debe activarlas. Para obtener más información, consulte Activación de etiquetas de asignación de costes definidas por el usuario en la Guía del usuario de AWS Billing. Tenga en cuenta que después de crear y aplicar etiquetas definidas por el usuario a los recursos, las claves de etiqueta pueden tardar hasta 24 horas en aparecer en la página de etiquetas de asignación de costos para su activación.

  Una vez activadas las etiquetas de asignación de costos…

  - Para todas las direcciones IPv4 públicas (incluidas las direcciones IPv4 públicas asignadas a instancias de EC2 y las direcciones IP elásticas) asociadas a una interfaz de red elástica, puede ver los costos asociados a las direcciones IPv4 públicas en el Explorador de costos seleccionando Tipo de uso > PublicIPv4InUseAddress (horas).
  - Si una dirección IP elástica etiquetada no está asociada a una ENI o está asociada a un recurso detenido (como una instancia de EC2 detenida), se considera una dirección IPv4 inactiva. Para ver los costos asociados a las direcciones IPv4 inactivas en el Explorador de costos, seleccione Tipo de uso > PublicIPv4IdleAddress (horas).

  Para obtener más información sobre el Explorador de costos, consulte Analyzing your costs with AWS Cost Explorer en la Guía del usuario de AWS Billing.

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.

Para más información sobre los precios de las direcciones IP elásticas, consulte Dirección IPv4 pública en Precios de Amazon VPC.

Introducción a las direcciones IP elásticas

En las secciones siguientes, se presenta una introducción a las direcciones IP elásticas.

Tareas

- 1. Asignar una dirección IP elástica
- 2. Asociar una dirección IP elástica
- 3. Anulación de la asociación de una dirección IP elástica
- 4. Transferencia de las direcciones IP elásticas
- 5. Liberar una dirección IP elástica
- 6. Recuperar una dirección IP elástica
- Descripción general de la línea de comandos

1. 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 Asignar dirección IP elástica.
4. (Opcional) Si asigna una dirección IP elástica (EIP), elija el Grupo de bordes de red al que desea asignar la EIP. Un grupo de bordes de red es un conjunto de zonas de disponibilidad (AZ), zonas locales o zonas de Wavelength desde las que AWS anuncia una dirección IP pública. Es posible que las zonas locales y las zonas de Wavelength tengan grupos de bordes de red diferentes a los de las AZ de una región para garantizar una latencia o una distancia física mínima entre la red de AWS y los clientes que acceden a los recursos de estas zonas.

> **Important**
>
> Debe asignar una EIP en el mismo grupo de bordes de red que el recurso de AWS que se asociará a la EIP. Una EIP de un grupo de bordes de red solo se puede anunciar en zonas de ese grupo de bordes de red y no en otras zonas representadas por otros grupos de bordes de red.

Si tiene zonas locales o zonas de Wavelength habilitadas (para obtener más información, consulte Habilitar una zona local o Habilitar zonas de Wavelength), puede elegir un grupo de bordes de red para las AZ, las zonas locales o las zonas de Wavelength. Elija el grupo de bordes de red con cuidado, ya que la EIP y el recurso de AWS al que está asociado deben residir en el mismo grupo de bordes de red. Puede utilizar la consola de EC2 para ver el grupo de bordes de red en el que se encuentran las zonas de disponibilidad, las zonas locales o las zonas de Wavelength (consulte Zonas locales). Por lo general, todas las zonas de disponibilidad de una región pertenecen al mismo grupo de bordes de red, mientras que las zonas locales o las zonas de Wavelength pertenecen a sus propios grupos de bordes de red independientes.

Si las zonas locales o las zonas de Wavelength no están habilitadas, cuando asigna una EIP, el grupo de bordes de red que representa a todas las AZ de la región (por ejemplo `us-west-2`) se predefine para usted y no puede cambiarlo. Esto significa que la EIP que asigne a este grupo de bordes de red se anunciará en todas las zonas de disponibilidad de la región en la que usted se encuentre.

5. 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.

6. (Opcional) Añada o elimine una etiqueta.

   [Agregar una etiqueta] Elija Agregar nueva etiqueta y haga lo siguiente:

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

   [Eliminar una etiqueta] Elija Eliminar a la derecha de la clave y del valor de la etiqueta.

7. Elija Asignar.

2. 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.

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.

3. 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).

4. Transferencia de las direcciones IP elásticas

En esta sección se describe cómo transferir las direcciones IP elásticas de una Cuenta de AWS a otra. La transferencia de direcciones IP elásticas puede resultar útil en las siguientes situaciones:

- Reestructuración organizativa: utilice las transferencias de direcciones IP elásticas para mover rápidamente las cargas de trabajo de una Cuenta de AWS a otra. No debe esperar a que se permita incluir nuevas direcciones IP elásticas en sus grupos de seguridad y NACL.
- Administración de seguridad centralizada: utilice una cuenta de seguridad de AWS centralizada para rastrear y transferir direcciones IP elásticas que se hayan examinado y cumplan con las normas de seguridad.
- Recuperación de desastres: utilice las transferencias de direcciones IP elásticas para reasignar rápidamente las IP a las cargas de trabajo de Internet orientadas al público durante eventos de emergencia.

La transferencia de direcciones IP elásticas no implica cargos.

Tareas

- Habilitar la transferencia de direcciones IP elásticas
- Deshabiltar la transferencia de direcciones IP elásticas
- Aceptar una dirección IP elástica transferida

Habilitar la transferencia de direcciones IP elásticas

En esta sección, se describe cómo aceptar una dirección IP elástica que se ha transferido. Tenga en cuenta las siguientes limitaciones relacionadas con la habilitación de direcciones IP elásticas para su transferencia:

- Puede transferir direcciones IP elásticas de cualquier Cuenta de AWS (cuenta de origen) a cualquier otra cuenta de AWS de la misma región de AWS (cuenta de transferencia).
- Al transferir una dirección IP elástica, hay un protocolo de enlace de dos pasos entre Cuentas de AWS. Cuando la cuenta de origen inicie la transferencia, las cuentas de transferencia tienen siete días para aceptar la transferencia de la dirección IP elástica. Durante esos siete días, la cuenta de origen puede ver la transferencia pendiente (por ejemplo, en la consola de AWS o mediante el comando de la AWS CLI describe-address-transfers). Transcurridos siete días, la transferencia caduca y la propiedad de la dirección IP elástica vuelve a la cuenta de origen.
- Las transferencias aceptadas están visibles en la cuenta de origen (por ejemplo, en laAWS consola o mediante elAWS CLI comando describe-address-transfers) durante 14 días después de que se hayan aceptado las transferencias.

- AWS no notifica a las cuentas de transferencia sobre las solicitudes pendientes de transferencia de direcciones IP elásticas. El propietario de la cuenta de origen debe notificar al propietario de la cuenta de transferencia que hay una solicitud de transferencia de direcciones IP elásticas que debe aceptar.
- Todas las etiquetas asociadas a la dirección IP elástica que se transfiere se restablecen cuando se completa la transferencia.
- No puede transferir las direcciones IP elásticas asignadas desde los grupos de direcciones IPv4 públicas que incorpore a su Cuenta de AWS (normalmente denominados grupos de direcciones traiga su propia IP [BYOIP]).
- Si se intenta transferir una dirección IP elástica que tenga un registro DNS inverso asociado, se puede iniciar el proceso de transferencia. Sin embargo, la cuenta de transferencia no puede aceptar la transferencia hasta que se elimine el registro DNS asociado.
- Si ha habilitado y configurado AWS Outposts, es posible que haya asignado direcciones IP elásticas de un grupo de direcciones IP (CoIP) que son propiedad del cliente. No puede transferir direcciones IP elásticas asignadas desde una CoIP. Sin embargo, puede usar AWS RAM para compartir un CoIP con otra cuenta. Para obtener más información, consulte Direcciones IP propiedad del cliente en la Guía del usuario de AWS Outposts.
- Puede utilizar Amazon VPC IPAM para hacer un seguimiento de la transferencia de direcciones IP elásticas a cuentas de una organización desde AWS Organizations. Para obtener más información, consulte Ver historial de direcciones IP. Si se transfiere una dirección IP elástica a una Cuenta de AWS fuera de la organización, se pierde el historial de auditoría de IPAM de la dirección IP elástica.

La cuenta de origen debe completar estos pasos.

Para habilitar la transferencia de direcciones IP elásticas

1. Asegúrese de utilizar la cuenta de AWS de origen.
2. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
3. En el panel de navegación, elija Elastic IPs.
4. Seleccione una o más direcciones IP elásticas para habilitar la transferencia y elija Acciones, Habilitar la transferencia.
5. Si está transfiriendo varias direcciones IP elásticas, verá la opción Tipo de transferencia. Elija una de las siguientes opciones:

- Elija Una sola cuenta si va a transferir las direcciones IP elásticas a una sola cuenta de AWS.
- Elija Varias cuentas si va a transferir las direcciones IP elásticas a varias cuentas de AWS.

6. En Transferir ID de cuenta, ingrese los ID de las cuentas de AWS a las que quiere transferir las direcciones IP elásticas.
7. Para confirmar la transferencia, ingrese **`enable`** en el cuadro de texto.
8. Elija Enviar.
9. Para aceptar la transferencia, consulte Aceptar una dirección IP elástica transferida. Para deshabilitar la transferencia, consulte Deshabiltar la transferencia de direcciones IP elásticas.

Deshabiltar la transferencia de direcciones IP elásticas

En esta sección, se describe cómo deshabilitar una transferencia de una dirección IP elástica una vez se ha habilitado la transferencia.

La cuenta de origen que habilitó la transferencia debe llevar a cabo estos pasos.

Para deshabilitar la transferencia de una dirección IP elástica

1. Asegúrese de utilizar la cuenta de AWS de origen.
2. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
3. En el panel de navegación, elija Elastic IPs.
4. En la lista de recursos de IP elásticas, asegúrese de tener habilitada la propiedad que muestra la columna Estado de la transferencia.
5. Seleccione una o más direcciones IP elásticas que tengan un Estado de la transferencia en Pendiente y elija Acciones, Deshabilitar la transferencia.
6. Para confirmarlo, ingrese **`disable`** en el cuadro de texto.
7. Elija Enviar.

Aceptar una dirección IP elástica transferida

En esta sección, se describe cómo aceptar una dirección IP elástica que se ha transferido.

Al transferir una dirección IP elástica, hay un protocolo de enlace de dos pasos entre Cuentas de AWS. Cuando la cuenta de origen inicie la transferencia, las cuentas de transferencia tienen siete días para aceptar la transferencia de la dirección IP elástica. Durante esos siete días, la cuenta

de origen puede ver la transferencia pendiente (por ejemplo, en la consola de AWS o mediante el comando de la AWS CLI describe-address-transfers). Transcurridos siete días, la transferencia caduca y la propiedad de la dirección IP elástica vuelve a la cuenta de origen.

Al aceptar las transferencias, tenga en cuenta las siguientes excepciones que pueden tener lugar y cómo solucionarlas:

- AddressLimitExceed: si su cuenta de transferencia superó la cuota de direcciones IP elásticas, la cuenta de origen puede habilitar la transferencia de direcciones IP elásticas, pero esta excepción se produce cuando la cuenta de transferencia intenta aceptarla. De forma predeterminada, todas las cuentas de AWS están limitadas a cinco (5) direcciones IP elásticas por región. Consulte Límite de direcciones IP elásticas en la Guía del usuario de Amazon EC2 para obtener instrucciones sobre cómo aumentar el límite.
- InvalidTransfer.AddressCustomPtrSet: la dirección IP elástica que intenta transferir está configurada para utilizar la búsqueda inversa de DNS. La cuenta de origen puede habilitar la transferencia de la dirección IP elástica. No obstante, esta excepción se produce cuando la cuenta de transferencia intenta aceptar la transferencia. Para resolver este problema, la cuenta de origen debe eliminar el registro de DNS de la dirección IP elástica. Para obtener más información, consulte Eliminación de un registro de DNS inverso en la Guía del usuario de Amazon EC2.
- InvalidTransfer.AddressAssociated: si una dirección IP elástica está asociada a una instancia de ENI o EC2, la cuenta de origen puede habilitar la transferencia de la dirección IP elástica, pero esta excepción se produce cuando la cuenta de transferencia intenta aceptarla. Para resolver este problema, la cuenta de origen debe desasociar la dirección IP elástica. Para obtener más información, consulte Desasociar una dirección IP elástica en la Guía del usuario de Amazon EC2.

Para otras excepciones, contacte con Soporte.

La cuenta de transferencia debe completar estos pasos.

Para aceptar la transferencia de una dirección IP elástica

1. Asegúrese de utilizar la cuenta de transferencia.
2. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
3. En el panel de navegación, elija Elastic IP.
4. Elija Acciones, Aceptar la transferencia.
5. No se transfiere ninguna etiqueta asociada a la dirección IP elástica que se transfiere con la dirección IP elástica cuando acepta la transferencia. Si desea definir una etiqueta Nombre de la

dirección IP elástica que acepta, seleccione Crear una etiqueta con la clave “Nombre” y un valor que especifique.

6. Ingrese la dirección IP elástica que quiere transferir.
7. Si acepta la transferencia de varias direcciones IP elásticas, elija Agregar dirección para ingresar una dirección IP elástica adicional.
8. Elija Enviar.

5. Liberar 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 Elastic asignadas para su uso con una VPC incluso si no están 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.

6. Recuperar una dirección IP elástica

Si libera una dirección IP elástica pero cambia de idea, es posible que pueda recuperarla. No podrá recuperar la dirección IP elástica si se ha asignado a otra cuenta de AWS o si recuperarla da como resultado que usted supere 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
```

Descripción general de la línea de comandos

Puede realizar las tareas descritas en esta sección mediante 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 Trabajo con VPC de Amazon.

Acepte la transferencia de direcciones IP elásticas

- accept-address-transfer (AWS CLI)
- Approve-EC2AddressTransfer (AWS Tools for Windows PowerShell)

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)

Describa las transferencias de direcciones IP elásticas

- describe-address-transfers (AWS CLI)
- Get-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Deshabiltar la transferencia de direcciones IP elásticas

- disable-address-transfer (AWS CLI)
- Disable-EC2AddressTransfer (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)

Habiltar la transferencia de direcciones IP elásticas

- enable-address-transfer (AWS CLI)
- Enable-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Liberar una dirección IP elástica

- release-address (AWS CLI)
- Remove-EC2Address (AWS Tools for Windows PowerShell)

Etiquetado de una dirección IP elástica

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Ver las direcciones IP elásticas

- describe-addresses (AWS CLI)
- Get-EC2Address (AWS Tools for Windows PowerShell)

Conectar 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 Direct Connect.

Uno de los beneficios más importantes de la puerta de enlace de tránsito es que centraliza y simplifica la administración de la conectividad entre sus VPC y las redes en las instalaciones. En vez de configurar varias conexiones de VPN o enlaces de Direct Connect, puede utilizar la puerta de enlace de tránsito como un punto único de integración, lo cual puede ayudar a reducir la complejidad general y los costos operativos de su arquitectura de red.

El precio por el uso de la puerta de enlace de tránsito se basa en la cantidad de datos que se transfieran a través de la puerta de enlace. Existe una tarifa por GB para los datos que se transfieren hacia y desde la puerta de enlace de tránsito y otra tarifa por hora por el propio recurso de la puerta

de enlace de tránsito. El precio específico varía según la región de AWS y está sujeto a cambios, por lo que es importante consultar la página de precios de AWS Transit Gateway actual para acceder a la información más actualizada. Al comprender el modelo de precios para las puertas de enlace de tránsito, mejora su planificación y armado de presupuestos para los costos actuales asociados con este producto de red de AWS. Esta característica, más la eficiencia operativa y los beneficios de conectividad, convierten a las puertas de enlace de tránsito en una gran opción para las organizaciones que buscan crear soluciones de nube híbrida que sean escalables y rentables.

En la siguiente tabla, se describen algunos casos de uso comunes de las puertas de enlace de tránsito. Para obtener información sobre cada caso de uso, consulte Ejemplos de escenarios de la puerta de enlace de tránsito en la Guía del usuario de AWS Transit Gateway.

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.
VPC aisladas	Configure la transit gateway como varios enrutadores aislados. Es similar a utilizar varias transit gateways, pero ofrece mayor flexibilidad en aquellos casos en los que es posible que las rutas y las conexiones cambien.
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 AWS Transit Gateway.

Conectar la VPC a redes remotas mediante AWS Virtual Private Network

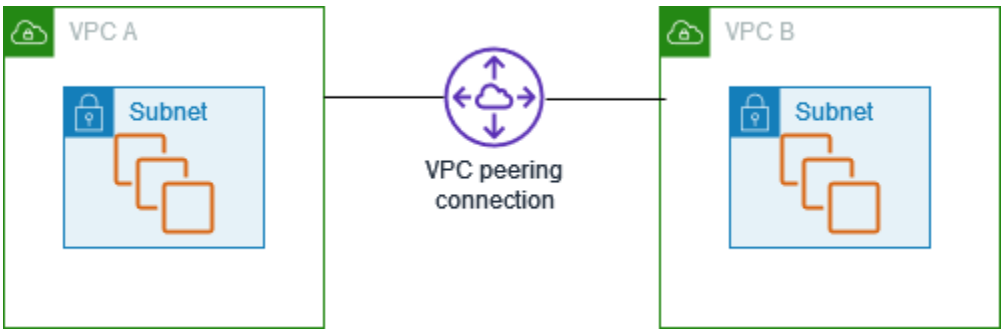
Puede conectar su VPC a redes y usuarios remotos mediante las siguientes opciones de conectividad de VPN.

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), puede crear varias conexiones de AWS Site-to-Site VPN a través de su puerta de enlace 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 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 Direct Connect? en la Guía del usuario de Direct Connect.

Conecte las VPC utilizando el emparejamiento de VPC

Una conexión de emparejamiento de VPC es una característica de redes que permite una comunicación segura y directa entre dos nubes privadas virtuales (VPC) dentro de la infraestructura de AWS. Con esta conexión privada, los recursos de las VPC emparejadas interactúan entre sí como si formaran parte de la misma red, lo que elimina la necesidad de atravesar la Internet pública.



El proceso de creación de una conexión de emparejamiento de VPC utiliza la infraestructura de VPC existente para establecer esta conexión, sin necesidad de una puerta de enlace, de AWS Site-to-Site VPN o de ningún equipo físico adicional. Este diseño garantiza que no existan puntos de error ni cuellos de botella en el ancho de banda.

Una de las ventajas principales de una conexión de emparejamiento de VPC es la posibilidad de conectar las VPC entre varias cuentas de AWS o incluso entre distintas regiones de AWS. Esta flexibilidad permite que las organizaciones integren sin problemas sus recursos en la nube, tanto si se encuentran en la misma cuenta como si están repartidos en varias cuentas y ubicaciones geográficas. La naturaleza privada de la conexión también garantiza que todo el tráfico de datos entre las VPC emparejadas permanezca dentro de la red de AWS, sin atravesar nunca la Internet pública.

Los casos prácticos de las conexiones de emparejamiento de VPC son muy variados. Con esta característica, las organizaciones acceden a una comunicación segura entre los distintos niveles de una aplicación (como los servidores web y los servidores de bases de datos), facilitan el intercambio de recursos entre varios equipos o unidades de negocio o incluso conectan las redes en las instalaciones con sus VPC de AWS para crear una arquitectura de nube híbrida.

Una interconexión de VPC es una conexión de redes entre dos VPC que permite direccionar el tráfico entre ellas de forma privada. Los recursos de VPC emparejadas pueden comunicarse entre sí como si se encontraran en la misma red. Puede crear una conexión de emparejamiento de VPC entre sus VPC, con una VPC de otra Cuenta de AWS o con una VPC de una región de AWS diferente. El tráfico entre las VPC emparejadas nunca atraviesa la Internet pública.

Para obtener más información, consulte la Guía de interconexión de Amazon VPC.

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 CloudWatch Internet Monitor

Puede usar Internet Monitor para tener visibilidad sobre cómo los problemas de Internet afectan al rendimiento y la disponibilidad entre las aplicaciones alojadas en AWS y los usuarios finales. También puede explorar, casi en tiempo real, cómo mejorar la latencia prevista de su aplicación pasando a utilizar otros servicios o redirigiendo el tráfico a su carga de trabajo a través de diferentes Regiones de AWS. Para obtener más información, consulte Uso de Amazon CloudWatch Internet Monitor.

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 IP Address Manager (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.

Analizador de accesibilidad

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 cuando son accesibles e identifica el componente de bloqueo cuando son inaccesibles. Para obtener más información, consulte Reachability Analyzer (Analizador de accesibilidad).

Analizador de acceso a la red

Puede utilizar 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

AWS CloudTrail registra las llamadas a la API de Amazon VPC, como:

- Qué llamadas a la API se realizaron (por ejemplo, acciones como crear o modificar recursos de la VPC)
- La dirección IP de origen de la llamada
- Quién realizó la llamada
- Cuándo se realizó la llamada

Se crean registros por separado para las acciones de `CreateVpc`, `DeleteVpc` y `CreateDefaultVpc`. Estos registros también incluyen los recursos predeterminados (como cualquier puerta de enlace de Internet predeterminada o grupo de seguridad predeterminado) creados y asociados con la VPC.

Para obtener más información, consulte Registro de llamadas a la API de Amazon EC2 mediante AWS CloudTrail en la Guía del usuario 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 las siguientes ubicaciones: Registros de Amazon CloudWatch, Amazon S3 o Amazon Data Firehose. La ruta de entrega configurada y los permisos que permiten enviar los registros de tráfico de red a un destino como Registros de CloudWatch o S3 se denominan suscripciones. Una vez creado un registro de flujo, puede recuperarlo y ver las entradas del registro de flujo en el grupo de registro, el bucket o el flujo de entrega que configuró.

Los logs de flujo pueden ayudarlo en una serie de tareas, tales como:

- Diagnosticar reglas de grupo de seguridad muy restrictivas

- Supervisar 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.

> **Note**
>
> En esta sección solo se trata de los registros de flujo para las VPC. Para obtener información sobre los registros de flujo para las puertas de enlace de tránsito introducidos en la versión 6, consulte Registrar el tráfico de red mediante los registros de flujo de las puertas de enlace de tránsito en la Guía del usuario de puertas de enlace de tránsito de Amazon VPC.

Contenido

- Conceptos básicos de logs de flujo
- Registros de log de flujo
- Ejemplos de registros de log de flujo
- Limitaciones de los logs de flujo
- Precios
- Trabajo con registros de flujo
- Publicar registros de flujo en CloudWatch Logs
- Publicar registros de flujo en Amazon S3
- Publicar registros de flujo a Amazon Data Firehose
- Realizar consultas en los registros de flujo mediante Amazon Athena
- Administración de identidades y accesos en los registros de flujo de VPC
- Solucionar problemas de los registros de flujo de VPC

Conceptos básicos de logs de flujo

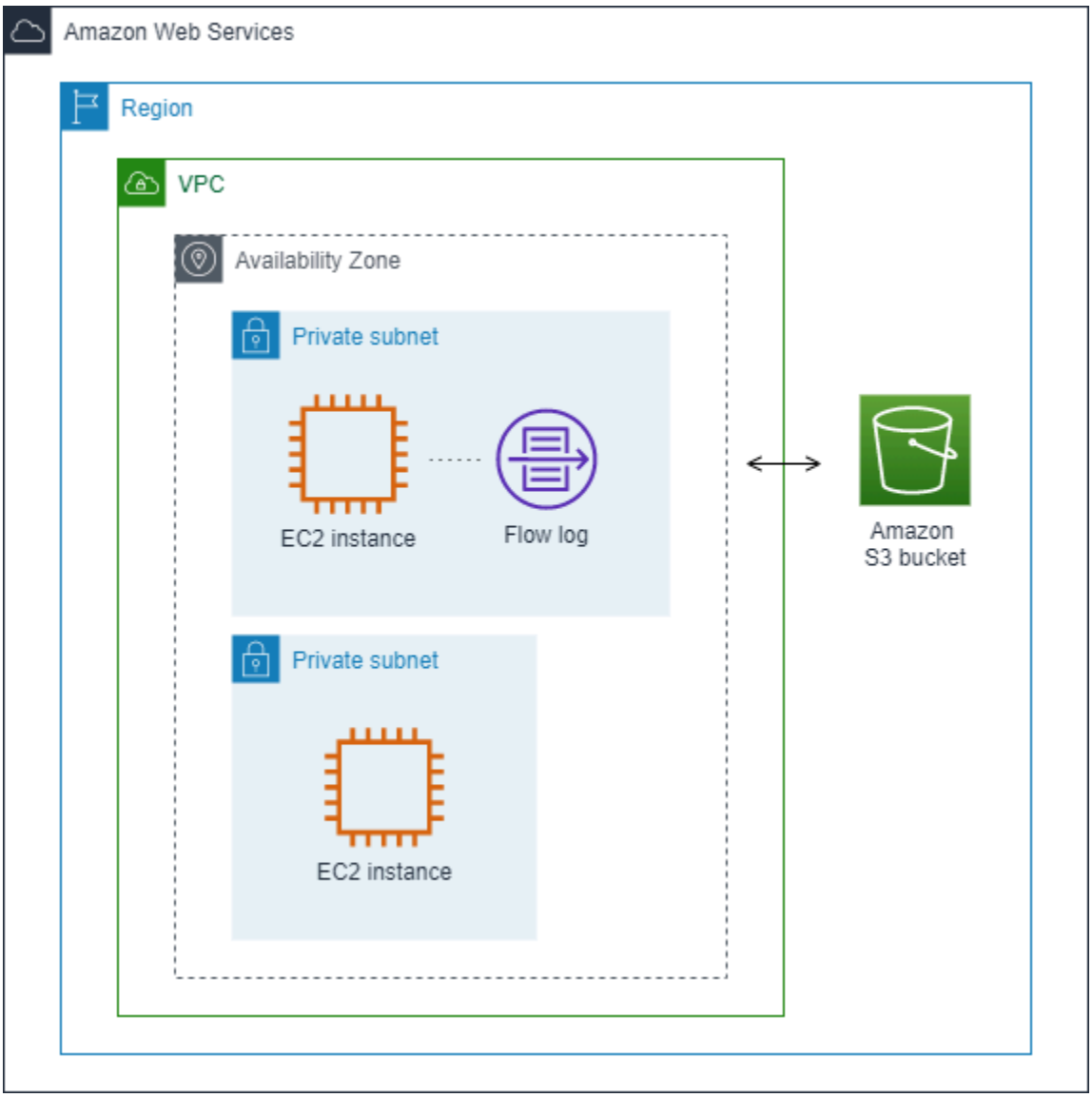
Puede crear un log de flujo para una VPC, una subred o una interfaz de red. Si crea un log de flujo para una subred o VPC, se supervisará cada interfaz de red de la VPC o la subred.

Los datos de logs de flujo de una interfaz de red supervisada 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.

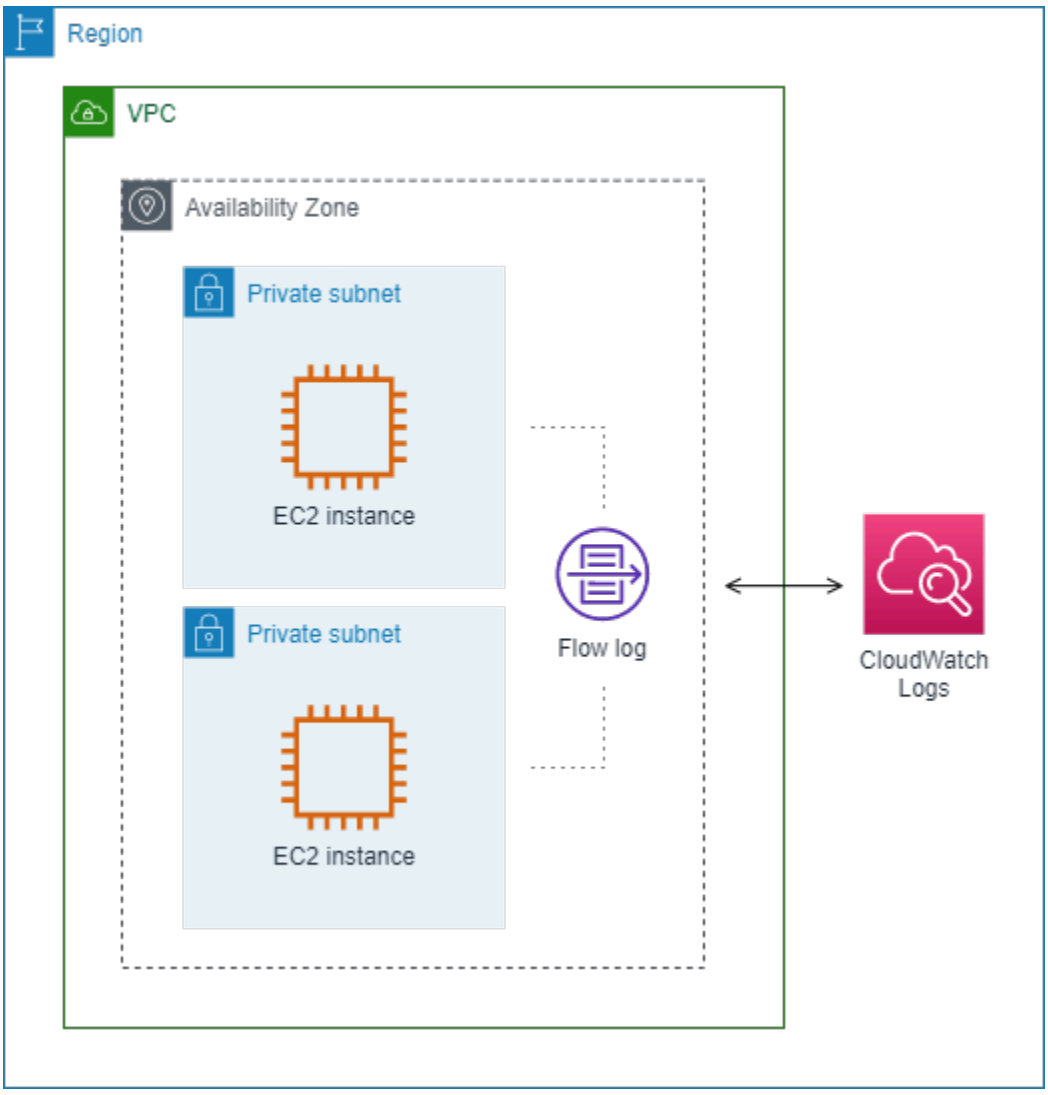
Para crear un registro de flujo, especifique:

- 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 que captura el tráfico aceptado para la interfaz de red de una de las instancias EC2 en una subred privada y publica las entradas de registro de flujo en un bucket de Amazon S3.



En el siguiente ejemplo una entrada de registro de flujo captura todo el tráfico de la subred y publica las entradas de registro de flujo en los Registros de Amazon CloudWatch. El registro de flujo captura el tráfico de todas las interfaces de red de la subred.



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 2. Crear un log de flujo.

Si lanza una instancia en la subred después de haber creado un registro de flujo para la subred o la VPC, se crea un flujo de registros (para CloudWatch Logs) o un objeto de archivo de registros (para Amazon S3) para la nueva interfaz de red. El flujo de registro o el objeto de archivo se crea tan pronto como ocurre tráfico de red en la interfaz.

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
- Puertas de enlace NAT
- Transit puerta de enlaces

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 ayudarlo a organizar los registros de flujo, por ejemplo, por finalidad o propietario.

Si ya no necesita un log de flujo, puede eliminarlo. Al eliminar un registro de flujo, se deshabilita el servicio del registro de flujo para el recurso, de modo que no se creen ni se publiquen nuevas entradas de registros de flujo. La eliminación de un registro de flujo no elimina ningún dato de registro de flujo existente. Tras eliminar un registro de flujo, puede eliminar los datos del registro de flujo directamente desde el destino cuando haya terminado con él. Para obtener más información, consulte 4. Eliminar un registro de flujo.

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
- Formato predeterminado
- Formato personalizado

- Campos disponibles

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. 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 personali zado, 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 un equilibrador de carga de red, 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. Devuelve el símbolo “-” para los flujos asociados a una puerta de enlace NAT regional.	2

Campo	Descripción	Versión
	Tipo de datos de Parquet: STRING	
srcaddr	Para el tráfico entrante, esta es la dirección IP del origen del tráfico. Para tráfico saliente, esta es la dirección IPv4 privada o la dirección IPv6 de la interfaz de red que envía el tráfico. En el caso del tráfico saliente de una puerta de enlace NAT regional, es la misma dirección IP de origen del paquete que en pkt-srcaddr. Consulte 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. En el caso del tráfico entrante hacia una puerta de enlace NAT regional, la dirección IP de destino del paquete es la misma que en pkt-dstaddr. Consulte 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
protocol	El número de protocolo IANA del tráfico. Para obtener más información, consulte Números de protocolo asignados en internet. 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

Campo	Descripción	Versión
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 de hasta 60 segundos antes de que el paquete se recibiera en la interfaz de red o de hasta 60 segundos después de que se transmitiera. 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: • ACCEPT: Se ha aceptado el tráfico. • REJECT: Se ha rechazado el tráfico. Por ejemplo, los grupos de seguridad o las ACL de red no permitían el tráfico, o los paquetes llegaban después de que se cerrara la conexión. Tipo de datos de Parquet: STRING	2

Campo	Descripción	Versión
log-status	El estado de registro del registro de flujo: • 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. Pueden omitirse algunos informes de registros de flujo durante el intervalo de agregación (consulte log-status en Campos disponibles). Esto puede deberse a una restricción de capacidad interna de AWS o a un error interno. Si utiliza AWS Cost Explorer para ver los cargos de los registros de flujo de la VPC y se omitieron algunos registros de flujo durante el intervalo de agregación de estos registros, el número de registros en el informe de AWS Cost Explorer será mayor que el número de registros de flujo que informe Amazon VPC. 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. Devuelve el símbolo “-” para los flujos asociados a una puerta de enlace NAT regional. Tipo de datos de Parquet: STRING	3

Campo	Descripción	Versión
instance-id	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 puerta de enlace NAT. Tipo de datos de Parquet: STRING	3

Campo	Descripción	Versión
tcp-flags	El valor de máscara de bits de las siguientes marcas TCP: • FIN: 1 • SYN: 2 • RST: 4 • SYN-ACK: 18 Si no se registran marcadores compatibles, el valor del marcador TCP es 0. Por ejemplo, dado que tcp-flags no es compatible con el registro de marcadores ACK o PSH, los registros de tráfico con estos marcadores no compatibles darán como resultado un valor 0 de tcp-flags. Sin embargo, si un marcador no compatible va acompañado de un marcador compatible, indicaremos el valor del marcador compatible. Por ejemplo, si ACK forma parte de SYN-ACK, indicará 18. Y si hay un registro como SYN+ECE, dado que SYN es un marcador compatible y ECE no, el valor del marcador TCP es 2. Si por alguna razón la combinación de marcadores no es válida y el valor no se puede calcular, el valor es '-'. Si no se envían marcadores, el valor del marcador TCP es 0. 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. Para obtener información general sobre marcadores TCP (como el significado de marcadores como FIN, SYN y ACK), consulte TCP segment structure (Estructura de segmentos TCP) en Wikipedia. Tipo de datos de Parquet: INT_32	3

Campo	Descripción	Versión
type	El tipo de tráfico. Los valores posibles son: IPv4 | IPv6 | EFA. Para obtener más información, consulte Elastic Fabric Adapter. Tipo de datos de Parquet: STRING	3
pkt-srcaddr	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, el tráfico puede fluir a través de una interfaz de red para una puerta de enlace NAT. Otro caso es cuando 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). Tipo de datos de Parquet: STRING	3
pkt-dstaddr	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, el tráfico puede fluir a través de una interfaz de red para una puerta de enlace NAT. Otro caso es cuando 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). Tipo de datos de Parquet: STRING	3
region	La región que contiene la interfaz de red para la que se registra el tráfico. Tipo de datos de Parquet: STRING	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

Campo	Descripción	Versión
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. Si la dirección IP de origen pertenece a un rango superpuesto, pkt-src-aws-service muestra solo uno de los códigos de servicio de AWS. Los valores posibles son: `AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | AURORA_DSQL | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CLOUDFRONT_ORIGIN_FACING | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | IVS_LOW_LATENCY | IVS_REALTIME | KINESIS_VIDEO_STREAMS | MEDIA_PACKAGE_V2 | 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 campo pkt-src-aws-service. 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	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 -. • 1: a través de otro recurso en la misma VPC, incluida una interfaz de red gestionada por AWS o una puerta de enlace local de Outpost • 2: a través de una puerta de enlace de Internet o un punto de conexión de VPC de puerta de enlace • 3: a través de una puerta de enlace 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 zona local o una zona de Wavelength • 7: a través de un punto de enlace de VPC de puerta de enlace • 8: a través de una puerta de enlace de Internet Tipo de datos de Parquet: INT_32	5
ecs-cluster-arn	AWSNombre de recurso (ARN) de del clúster de ECS si el tráfico proviene de una tarea de ECS en ejecución. Para incluir este campo en su suscripción, necesita permiso para llamar a ecs:ListClusters. Tipo de datos de Parquet: STRING	7
ecs-cluster-name	Nombre del clúster de ECS si el tráfico proviene de una tarea de ECS en ejecución. Para incluir este campo en su suscripción, necesita permiso para llamar a ecs:ListClusters. Tipo de datos de Parquet: STRING	7

Campo	Descripción	Versión
ecs-container-instance-arn	ARN de la instancia de contenedor de ECS si el tráfico proviene de una tarea de ECS en ejecución en una instancia de EC2. Si el proveedor de capacidad lo es AWS Fargate, este campo será '-'. Para incluir este campo en su suscripción, necesita permiso para llamar a ecs:ListClusters y ecs:ListContainerInstances. Tipo de datos de Parquet: STRING	7
ecs-container-instance-id	ID de la instancia de contenedor de ECS si el tráfico proviene de una tarea de ECS en ejecución en una instancia de EC2. Si el proveedor de capacidad lo es AWS Fargate, este campo será '-'. Para incluir este campo en su suscripción, necesita permiso para llamar a ecs:ListClusters y ecs:ListContainerInstances. Tipo de datos de Parquet: STRING	7
ecs-container-id	ID de tiempo de ejecución de Docker del contenedor si el tráfico proviene de una tarea de ECS en ejecución. Si hay uno o más contenedores en la tarea de ECS, este será el ID de tiempo de ejecución de Docker del primer contenedor. Para incluir este campo en su suscripción, necesita permiso para llamar a ecs:ListClusters. Tipo de datos de Parquet: STRING	7
ecs-second-container-id	ID de tiempo de ejecución de Docker del contenedor si el tráfico proviene de una tarea de ECS en ejecución. Si hay más de un contenedor en la tarea de ECS, este será el ID de tiempo de ejecución de Docker del segundo contenedor. Para incluir este campo en su suscripción, necesita permiso para llamar a ecs:ListClusters. Tipo de datos de Parquet: STRING	7
ecs-service-name	Nombre del servicio de ECS si el tráfico proviene de una tarea de ECS en ejecución y esta tarea la inicia un servicio de ECS. Si la tarea de ECS no la inicia un servicio de ECS, este campo será '-'. Para incluir este campo en su suscripción, necesita permiso para llamar a ecs:ListClusters y ecs:ListServices. Tipo de datos de Parquet: STRING	7

Campo	Descripción	Versión
ecs-task-definition-arn	ARN de la definición de la tarea de ECS si el tráfico proviene de una tarea de ECS en ejecución. Para incluir este campo en su suscripción, necesita permiso para llamar a ecs:ListClusters y ecs:ListTaskDefinitions. Tipo de datos de Parquet: STRING	7
ecs-task-arn	ARN de la tarea de ECS si el tráfico proviene de una tarea de ECS en ejecución. Para incluir este campo en su suscripción, necesita permiso para llamar a ecs:ListClusters y ecs:ListTasks. Tipo de datos de Parquet: STRING	7
ecs-task-id	ID de la tarea de ECS si el tráfico proviene de una tarea de ECS en ejecución. Para incluir este campo en su suscripción, necesita permiso para llamar a ecs:ListClusters y ecs:ListTasks. Tipo de datos de Parquet: STRING	7
reject-reason	Motivo por el que se ha rechazado el tráfico. Valores posibles: BPA y EC. Devuelve un '-' por cualquier otro motivo de rechazo. • BPA: para obtener más información sobre el Bloqueo de acceso público de VPC (BPA), consulte Bloqueo de acceso público de las VPC y subredes. • EC: el flujo fue rechazado por el punto de conexión de VPC debido a los controles de cifrado. Para obtener más información sobre los controles de cifrado de VPC, consulte Aplicación del cifrado del tráfico en tránsito en VPC. Tipo de datos de Parquet: STRING	8

Campo	Descripción	Versión
resource-id	El ID de la puerta de enlace NAT regional que contiene la interfaz de red para la cual se registra el tráfico. Devuelve el símbolo “-” para los flujos de tráfico que no están asociados a una puerta de enlace NAT regional. Para obtener más información sobre las puertas de enlace NAT regionales, consulte Puertas de enlace NAT regionales para la expansión automática en varias zonas de disponibilidad. Tipo de datos de Parquet: STRING	9

Campo	Descripción	Versión

encryption-status	Estado de cifrado del flujo. Para obtener más información sobre los controles de cifrado de VPC, consulte Aplicación del cifrado del tráfico en tránsito en VPC. Los valores posibles son:
	• 0: sin cifrar.
	• 1: cifrado por nitro. Está cifrado por el hardware del sistema Nitro.
	• 2: cifrado por la aplicación. Solo se considera cifrado por la aplicación lo siguiente:
	  • flujos en el puerto TCP 443 para puntos de conexión de interfaz hacia servicios de AWS*
	  • flujos en el puerto TCP 443 para puntos de conexión de puerta de enlace*
	  • flujos hacia un clúster de Redshift cifrado a través de un punto de conexión de VPC **
	• 3: cifrado por Nitro y cifrado por la aplicación.
	
	El valor es “-” si los controles de cifrado de VPC no están habilitados o si FlowLog no puede obtener el estado.
	
	Note
	* En el caso de los puntos de conexión de interfaz y de puerta de enlace, AWS no examina los datos de los paquetes para determinar el estado de cifrado; en su lugar, se basa en el puerto utilizado para inferir el estado de cifrado.
	** Para los puntos de conexión administrados por AWS especificados, AWS determina el estado de cifrado en función del requisito de TLS en la configuración del servicio.
	
	Tipo de datos de Parquet: INT_32
		10

Campo	Descripción	Versión
instance-tag	Valor de etiqueta para la primera etiqueta de instancia incluida en las TagFieldSpecifications. Los valores de las etiquetas se muestran convirtiendo todos los caracteres especiales mediante la codificación de porcentaje UTF-8. Para incluir este campo en la suscripción, se necesitan permisos para llamar a ec2:DescribeTags e iam:CreateServiceLinkedRole. Para obtener información sobre el rol vinculado al servicio de etiquetas de Amazon EC2 para registros de flujo, consulte Uso de roles vinculados al servicio para los registros de flujo de VPC. Tipo de datos de Parquet: STRING	11
instance-tag-2	Valor de etiqueta para la segunda etiqueta de instancia incluida en las TagFieldSpecifications. Los valores de las etiquetas se muestran convirtiendo todos los caracteres especiales mediante la codificación de porcentaje UTF-8. Para incluir este campo en la suscripción, se necesitan permisos para llamar a ec2:DescribeTags e iam:CreateServiceLinkedRole. Para obtener información sobre el rol vinculado al servicio de etiquetas de Amazon EC2 para registros de flujo, consulte Uso de roles vinculados al servicio para los registros de flujo de VPC. Tipo de datos de Parquet: STRING	11
interface-tag	Valor de etiqueta para la primera etiqueta network-interface incluida en las TagFieldSpecifications. Los valores de las etiquetas se muestran convirtiendo todos los caracteres especiales mediante la codificación de porcentaje UTF-8. Para incluir este campo en la suscripción, se necesitan permisos para llamar a ec2:DescribeTags e iam:CreateServiceLinkedRole. Para obtener información sobre el rol vinculado al servicio de etiquetas de Amazon EC2 para registros de flujo, consulte Uso de roles vinculados al servicio para los registros de flujo de VPC. Tipo de datos de Parquet: STRING	11

Campo	Descripción	Versión
interface-tag-2	Valor de etiqueta para la segunda etiqueta network-interface incluida en las TagFieldSpecifications. Los valores de las etiquetas se muestran convirtiendo todos los caracteres especiales mediante la codificación de porcentaje UTF-8. Para incluir este campo en la suscripción, se necesitan permisos para llamar a ec2:DescribeTags e iam:CreateServiceLinkedRole. Para obtener información sobre el rol vinculado al servicio de etiquetas de Amazon EC2 para registros de flujo, consulte Uso de roles vinculados al servicio para los registros de flujo de VPC. Tipo de datos de Parquet: STRING	11
asg-tag	Valor de etiqueta para la primera etiqueta auto-scaling-group incluida en las TagFieldSpecifications. Los valores de las etiquetas se muestran convirtiendo todos los caracteres especiales mediante la codificación de porcentaje UTF-8. Para incluir este campo en la suscripción, se necesitan permisos para llamar a autoscaling:DescribeTags e iam:CreateServiceLinkedRole. Debe tener al menos un trail de CloudTrail habilitado en la cuenta para que los valores de las etiquetas de los grupos de escalado automático se registren y actualicen correctamente en tiempo real. Para obtener información sobre el rol vinculado al servicio de etiquetas de Amazon EC2 para registros de flujo, consulte Uso de roles vinculados al servicio para los registros de flujo de VPC. Tipo de datos de Parquet: STRING	11

Campo	Descripción	Versión
asg-tag-2	Valor de etiqueta para la segunda etiqueta auto-scaling-group incluida en las TagFieldSpecifications. Los valores de las etiquetas se muestran convirtiendo todos los caracteres especiales mediante la codificación de porcentaje UTF-8. Para incluir este campo en la suscripción, se necesitan permisos para llamar a autoscaling:DescribeTags e iam:CreateServiceLinkedRole. Debe tener al menos un trail de CloudTrail habilitado en la cuenta para que los valores de las etiquetas de los grupos de escalado automático se registren y actualicen correctamente en tiempo real. Para obtener información sobre el rol vinculado al servicio de etiquetas de Amazon EC2 para registros de flujo, consulte Uso de roles vinculados al servicio para los registros de flujo de VPC. Tipo de datos de Parquet: STRING	11
interface-type	El tipo de interfaz de red local que captura el flujo. Los valores admitidos son: `nat_gateway` | `network_load_balancer` | `regional_nat_gateway` | `transit_gateway` | `vpc_endpoint` . Si la interfaz de red no tiene un servicio asociado o el servicio no es compatible, el valor es '-'. Tipo de datos de Parquet: STRING	11
next-hop-interface-id	El ID de la interfaz de red del siguiente salto. Para el tráfico de salida, esta es la interfaz que recibe el tráfico. Para el tráfico de entrada, esta es la interfaz que envía el tráfico. Tipo de datos de Parquet: STRING	11
next-hop-subnet-id	El ID de la subred que contiene la interfaz de red del siguiente salto. Tipo de datos de Parquet: STRING	11

Campo	Descripción	Versión
next-hop-az-id	El ID de la zona de disponibilidad que contiene la interfaz de red del siguiente salto. Tipo de datos de Parquet: STRING	11
next-hop-vpc-id	El ID de la VPC que contiene la interfaz de red del siguiente salto. Tipo de datos de Parquet: STRING	11
next-hop-interface-type	El tipo de la interfaz de red del siguiente salto. Para obtener una lista de posibles valores, consulte el campo interface-type. Tipo de datos de Parquet: STRING	11

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. Para obtener información sobre cómo crear registros de flujo, consulte Trabajo con registros de flujo.

Contenido

- Tráfico aceptado y rechazado
- Registros sin datos y omitidos
- Reglas de grupos de seguridad y ACL de red
- Tráfico IPv6
- Secuencia de marca TCP
- Tráfico a través de una puerta de enlace NAT zonal
- Tráfico a través de una puerta de enlace NAT regional
- Tráfico a través de una transit puerta de enlace
- Nombre del servicio, ruta de tráfico y dirección del flujo

Tráfico aceptado y rechazado

Los siguientes ejemplos son registros de logs de flujo predeterminados.

En este ejemplo, se permitió el tráfico SSH (puerto de destino 22, protocolo TCP) desde la dirección IP 172.31.16.139 a la interfaz de red con la dirección IP privada 172.31.16.21 y el ID 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
```

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 omita puede representar varios flujos que no se capturaron para la interfaz de red durante el intervalo de integración.

```
2 123456789010 eni-11111111aaaaaaaaa - - - - - - - 1431280876 1431280934 - SKIPDATA
```

> **Note**
>
> Pueden omitirse algunos informes de registros de flujo durante el intervalo de agregación (consulte log-status en Campos disponibles). Esto puede deberse a una restricción de capacidad interna de AWS o a un error interno. Si utiliza AWS Cost Explorer para ver los

cargos de los registros de flujo de la VPC y se omitieron algunos registros de flujo durante el intervalo de agregación de estos registros, el número de registros en el informe de AWS Cost Explorer será mayor que el número de registros de flujo que informe Amazon VPC.

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

Esta sección contiene ejemplos de registros de flujo personalizados que capturan los siguientes campos en el orden que se indica a continuación.

```
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
```

La tcp-flags de los ejemplos de esta sección están representados por el segundo al último valor del registro de flujo. Los marcadores TCP pueden ayudarlo a identificar la dirección del tráfico, por ejemplo, el servidor que inició la conexión.

> **Note**
>
> Para obtener más información sobre las opciones de tcp-flags y una explicación de cada uno de los marcadores TCP, consulte Campos disponibles.

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 servidor envió una marca FIN (1) al cliente para la conexión en el puerto 43418. El cliente respondió con una FIN al servidor en el puerto 43418.

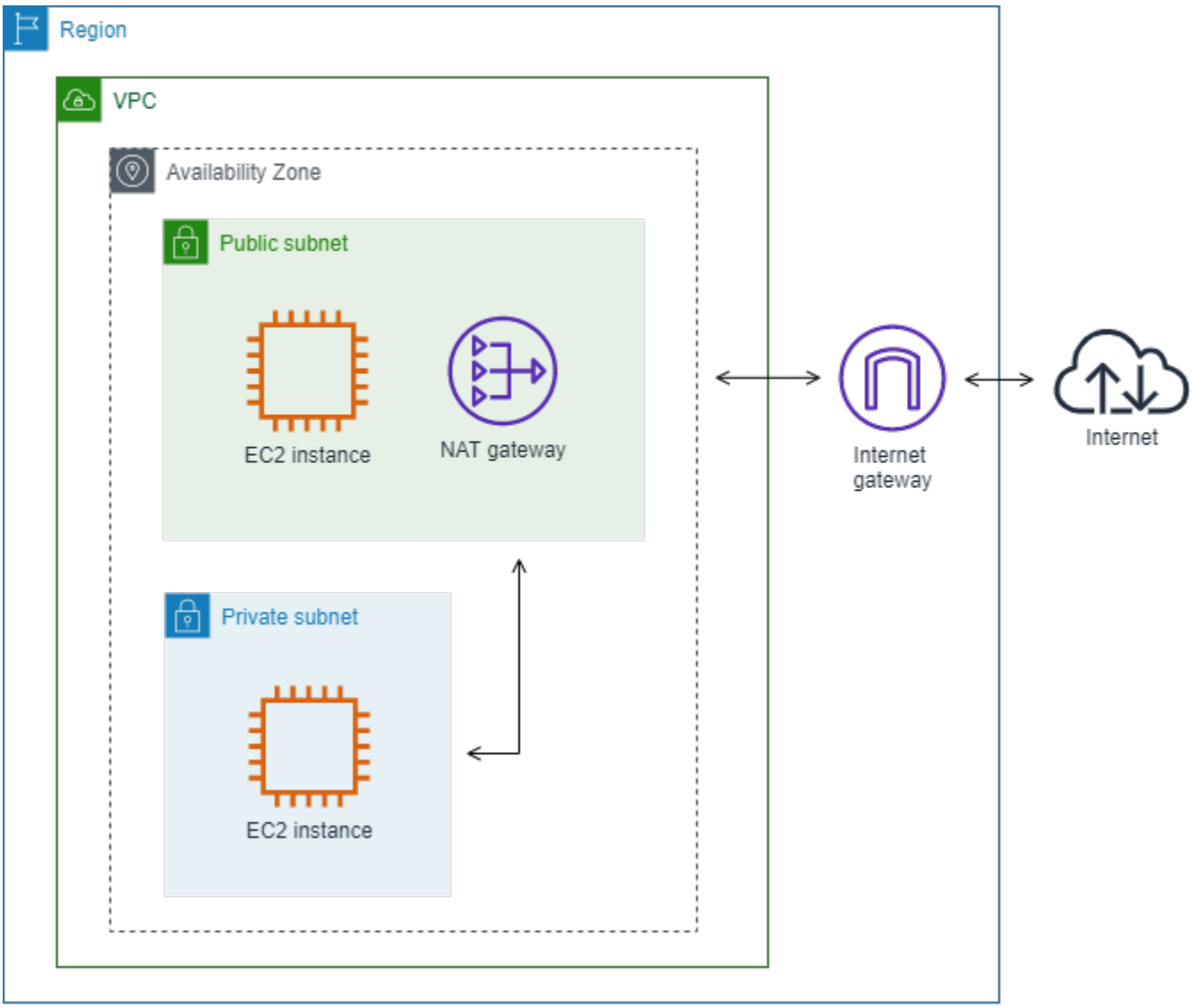
```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 63388 1219 1566848933 1566849113 ACCEPT 1 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 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 que se abren y cierran en un mismo intervalo de agregación, las marcas podrían establecerse en la misma línea de la entrada del registro de flujo para el 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 puerta de enlace NAT zonal

En este ejemplo, una instancia en una subred privada accede a Internet a través de una puerta de enlace NAT zonal que se encuentra en una subred pública.



El siguiente registro de flujo personalizado de la interfaz de red de la puerta de enlace NAT zonal captura los siguientes campos en el siguiente orden.

```
instance-id interface-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

El registro 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 puerta de enlace NAT zonal, hasta un host en Internet (203.0.113.5). La interfaz de red de la puerta de enlace NAT zonal es una interfaz de red administrada por el solicitante; por lo tanto, el registro del flujo muestra el símbolo “-” en el campo instance-id. La siguiente línea muestra el tráfico desde la instancia de origen hacia la interfaz de red de la puerta de enlace NAT zonal. 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 puerta de enlace NAT zonal, 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 muestran el tráfico desde la interfaz de red de la puerta de enlace NAT zonal hacia el host de destino en Internet, así como el tráfico de respuesta del host hacia la interfaz de red de la puerta de enlace 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 siguiente línea muestra el tráfico de respuesta desde la interfaz de red de la puerta de enlace NAT zonal hacia 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 puerta de enlace NAT zonal, y el campo pkt-srcaddr muestra la dirección IP del host en Internet.

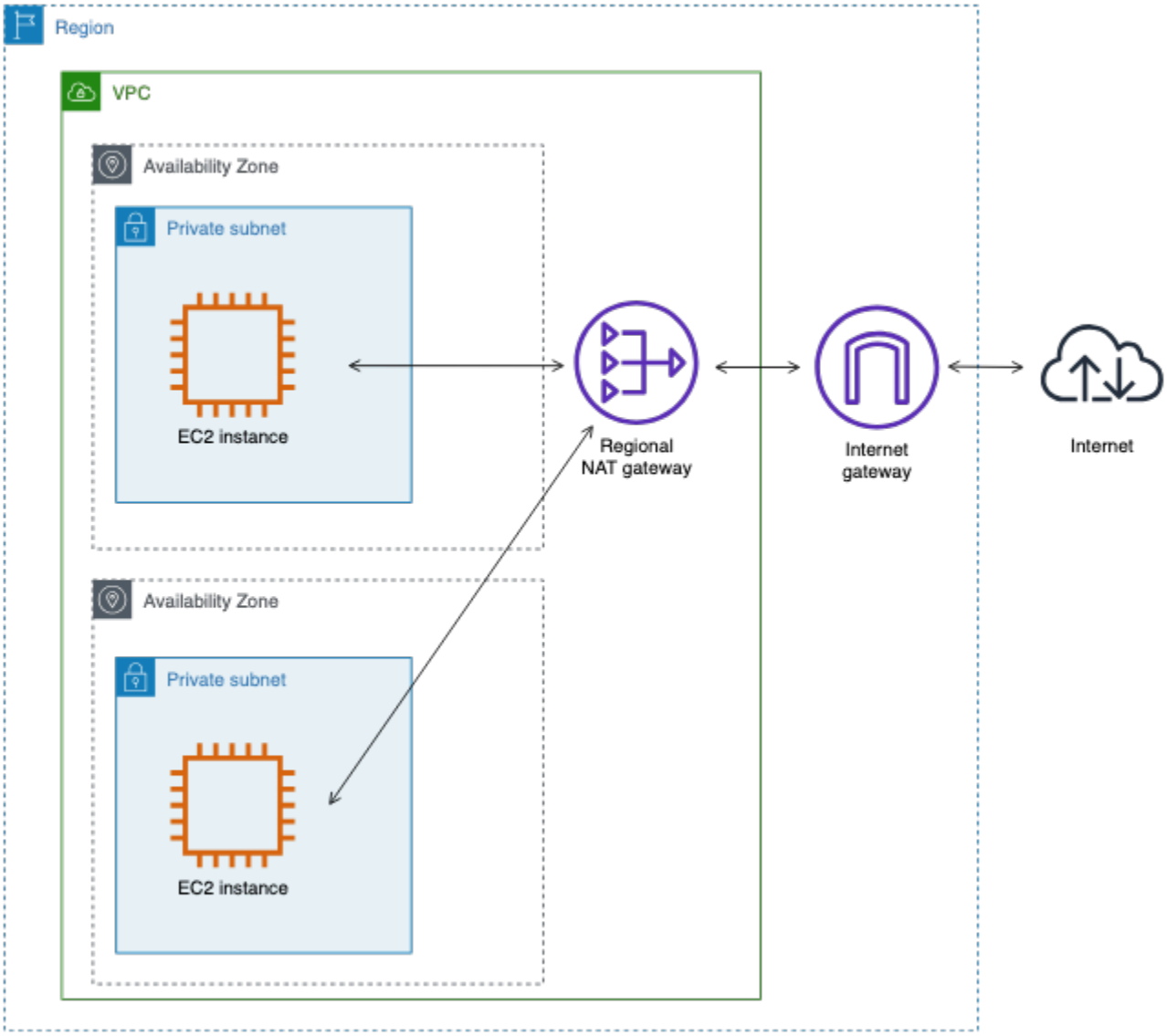
```
- eni-1235b8ca123456789 10.0.0.220 10.0.1.5 203.0.113.5 10.0.1.5
```

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 asociada a la interfaz de red. No existe ninguna diferencia entre los campos dstaddr y pkt-dstaddr y los campos srcaddr y pkt-srcaddr. A diferencia de la interfaz de red de la puerta de enlace NAT zonal, esta interfaz de red no es una interfaz 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 puerta de enlace NAT regional

Una puerta de enlace NAT regional se puede conectar a varias subredes en distintas zonas de disponibilidad. En este ejemplo, dos instancias en subredes privadas de dos zonas de disponibilidad diferentes acceden a Internet a través de la misma puerta de enlace NAT regional. Los siguientes registros de flujo muestran el tráfico desde una de las instancias hacia Internet a través de la puerta de enlace NAT regional.



El siguiente registro de flujo personalizado de la puerta de enlace NAT regional captura los siguientes campos en el siguiente orden.

```
resource-id instance-id interface-id subnet-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

El registro de flujo muestra el flujo de tráfico desde la dirección IP de la instancia (10.0.1.5), a través de la puerta de enlace NAT regional, hasta un host en Internet (203.0.113.5). Los campos instance-id, interface-id y subnet-id no se aplican a la puerta de enlace NAT regional. Por lo tanto, el registro del flujo muestra el símbolo “-” en estos campos. En su lugar, el campo resource-id muestra el ID de la puerta de enlace NAT regional. Los campos dstaddr y pkt-dstaddr muestran la dirección IP de destino final del host en Internet.

```
nat-1234567890abcdef - - - 10.0.1.5 203.0.113.5 10.0.1.5 203.0.113.5
```

Las dos líneas siguientes muestran el tráfico desde la puerta de enlace NAT regional (dirección IP pública 107.22.182.139) hacia el host de destino en Internet. También muestran el tráfico de respuesta desde el host hacia la puerta de enlace NAT regional.

```
nat-1234567890abcdef - - - 107.22.182.139 203.0.113.5 107.22.182.139 203.0.113.5
nat-1234567890abcdef - - - 203.0.113.5 107.22.182.139 203.0.113.5 107.22.182.139
```

La siguiente línea muestra el tráfico de respuesta desde la puerta de enlace NAT regional hacia la instancia de origen. Los campos srcaddr y pkt-srcaddr muestran la dirección IP del host en Internet.

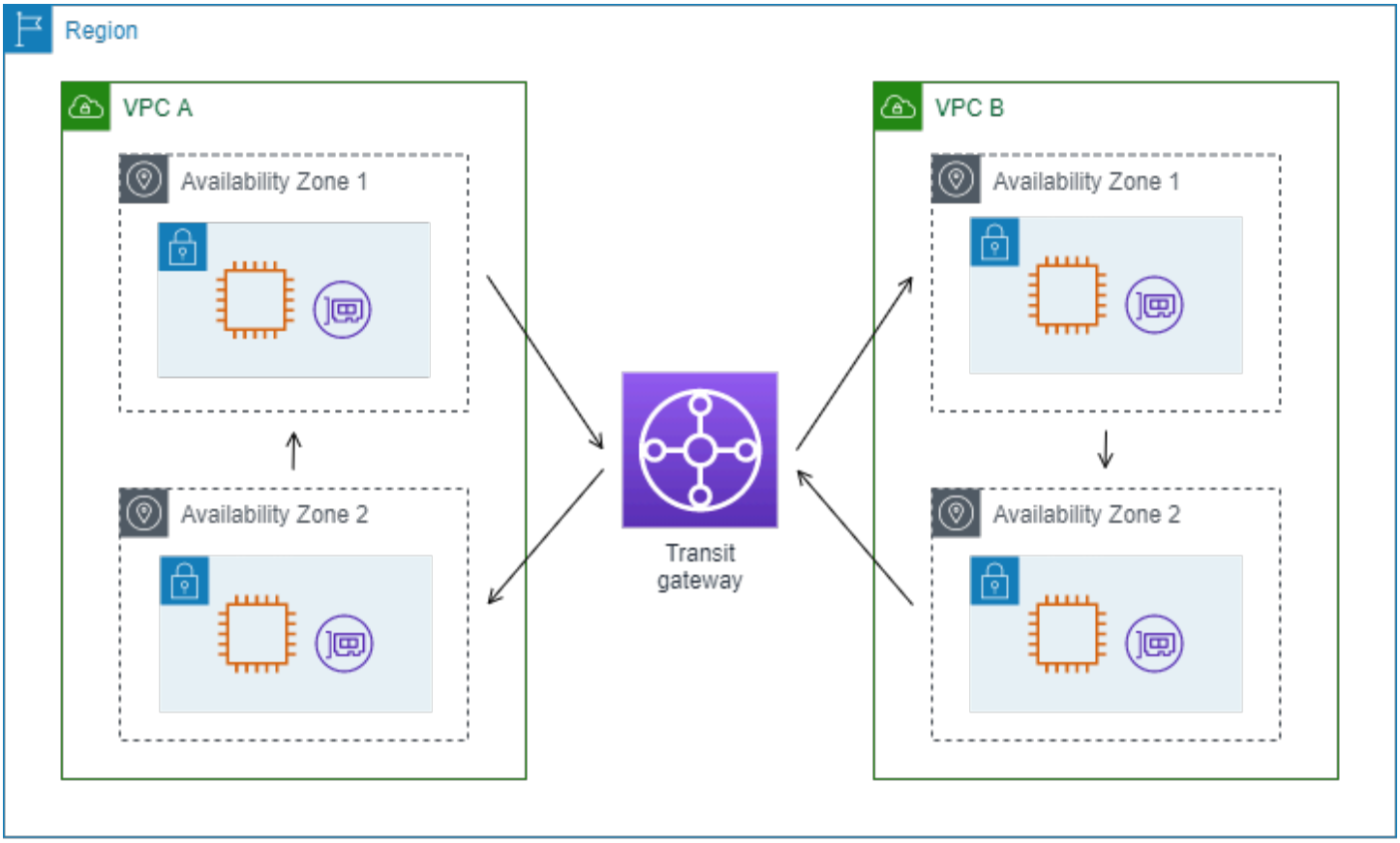
```
nat-1234567890abcdef - - - 203.0.113.5 10.0.1.5 203.0.113.5 10.0.1.5
```

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 asociada a la interfaz de red, y el resource-id es “-”. No existe ninguna diferencia entre los campos dstaddr y pkt-dstaddr y los campos srcaddr y pkt-srcaddr.

```
- i-01234567890123456 eni-1111aaaa2222bbbb3 subnet-aaaaaaaa012345678 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 subnet-aaaaaaaa012345678 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 puerta de enlace

En este ejemplo, un cliente en VPC A se conecta a un servidor web en VPC B a través de una transit puerta de enlace. El cliente y el servidor están en zonas de disponibilidad distintas. El tráfico llega al servidor de la VPC B utilizando un ID de interfaz de red elástica (en este ejemplo, supongamos que el ID es eni-1111111111111111) y deja la VPC B usando otro (por ejemplo, eni-22222222222222222).



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-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 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-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 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-11111111111111111, una interfaz de red administrada el por solicitante para la transit puerta de enlace en la subred

subnet-11111111aaaaaaaaa. 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 puerta de enlace y el campo pkt-srcaddr muestra la dirección IP de origen del cliente en VPC A.

```
3 eni-1111111111111111 123456789010 vpc-abcdefab012345678 subnet-11111111aaaaaaaaa -
 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-22222222222222222, una interfaz de red administrada por el solicitante para la transit puerta de enlace en la subred subnet-22222222bbbbbbbbb. El campo dstaddr muestra la dirección IP privada de la interfaz de red de transit puerta de enlace y el campo pkt-dstaddr muestra la dirección IP del cliente en VPC A.

```
3 eni-22222222222222222 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb -
 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 puerta de enlace 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:

- Después de crear un registro de flujo, no verá los datos del registro de flujo hasta que haya tráfico activo para la interfaz de red, subred o VPC que haya seleccionado.
- 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 crear un registro de flujo, no podrá cambiar su configuración ni su formato de registro. 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 desde una interfaz de red y el origen no es ninguna de las direcciones IP de dicha interfaz de red, entonces el comportamiento depende de la dirección del flujo. Para un flujo saliente, el registro 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 registro es para un flujo de entrada a la interfaz de red, la IP privada principal de la interfaz de red no se mostrará en el campo `srcaddr`.
- 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.
- Para los campos `pkt-srcaddr` y `pkt-dstaddr`, si la capa intermedia tiene habilitada la conservación de la dirección IP del cliente, en este campo se puede mostrar la IP del cliente conservada en lugar de la dirección IP de la capa intermedia.
- En el caso del campo `traffic-path`, el valor es el mismo para los flujos que pasan por los recursos de la misma VPC y los flujos que pasan por una puerta de enlace local de Outpost.
- Pueden omitirse algunos informes de registros de flujo durante el intervalo de agregación (consulte log-status en Campos disponibles). Esto puede deberse a una restricción de capacidad interna

de AWS o a un error interno. Si utiliza AWS Cost Explorer para ver los cargos de los registros de flujo de la VPC y se omitieron algunos registros de flujo durante el intervalo de agregación de estos registros, el número de registros en el informe de AWS Cost Explorer será mayor que el número de registros de flujo que informe Amazon VPC.

- Si utiliza el bloqueo de acceso público (BPA) de la VPC:
  - Los registros de flujo del BPA de la VPC no incluyen los registros omitidos.
  - Los registros de flujo del BPA de la VPC no incluyen `bytes` incluso si incorpora el campo `bytes` en el registro de flujo.
- Los registros de flujo de VPC admiten un máximo de 250 suscripciones por recurso y cuenta. Para crear suscripciones adicionales en un recurso que haya alcanzado este límite, primero se deben eliminar las suscripciones existentes.

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 de sincronización temporal de Amazon.
- Tráfico DHCP.
- Tráfico de origen reflejado. Verá el tráfico reflejado únicamente en el tráfico de destino.
- 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 Equilibrador de carga de red.
- Tráfico del Protocolo de resolución de direcciones (ARP).
- Tráfico en una puerta de enlace NAT regional de corta duración, que se elimina unos minutos después de su creación.

Limitaciones específicas de los campos de ECS disponibles en la versión 7:

- Los campos de ECS no se calculan si las tareas de ECS subyacentes no son propiedad del propietario de la suscripción del registro de flujo.

Por ejemplo, supongamos que se comparte una subred (`SubnetA`) con otra cuenta (`AccountB`) y, a continuación, se crea una suscripción al registro de flujo para `SubnetA`. Si `AccountB` inicia tareas de ECS en la subred compartida, su suscripción recibe los registros de tráfico de esas tareas. Sin embargo, los campos de ECS para estos registros no se calculan por motivos de seguridad.

- Si crea suscripciones de registro de flujo con campos de ECS en el nivel de recursos de VPC/subred, cualquier tráfico generado para las interfaces de red que no sean de ECS también se entregará a sus suscripciones. Los valores de los campos de ECS serán '-' para el tráfico IP que no sea de ECS. Por ejemplo, tiene una subred (`subnet-000000`) y crea una suscripción de registro de flujo para esta subred con campos de ECS (`fl-00000000`). En `subnet-000000`, usted inicia una instancia EC2 (`i-0000000`) que está conectada a Internet y genera tráfico IP de forma activa. También inicia una tarea de ECS en ejecución (`ECS-Task-1`) en la misma subred. Como `i-0000000` y `ECS-Task-1` generan tráfico IP, su suscripción de registros de flujo `fl-00000000` proporcionará los registros de tráfico de ambas entidades. Sin embargo, solo `ECS-Task-1` tendrá metadatos de ECS reales para los campos de ECS que haya incluido en su formato de registro. Para el tráfico relacionado de `i-0000000`, estos campos tendrán un valor de '-'.
- `ecs-container-id` y `ecs-second-container-id` se ordenan a medida que el servicio de registros de flujo de la VPC los recibe del flujo de eventos de ECS. No se garantiza que estén en el mismo orden en que aparecen en la consola ECS o en la llamada a la API DescribetTask. Si un contenedor pasa al estado DETENIDO mientras la tarea aún se está ejecutando, es posible que siga apareciendo en su registro.
- Los metadatos del ECS y los registros de tráfico IP provienen de dos fuentes diferentes. Empezamos a calcular su tráfico de ECS en cuanto obtenemos toda la información necesaria de las dependencias principales.

  Después de iniciar una nueva tarea, se empiezan a calcular los campos de ECS cuando se cumplen las dos condiciones siguientes: se recibe el tráfico IP de la interfaz de red subyacente y se recibe el evento de ECS que contiene los metadatos de la tarea de ECS para indicar que esta se está ejecutando.

  Después de detener una tarea, se dejan de calcular los campos de ECS cuando se cumplen las dos condiciones siguientes: ya no se recibe el tráfico IP de la interfaz de red subyacente (o se recibe tráfico de IP que tiene una demora superior a un día) y se recibe el evento de ECS que contiene los metadatos de la tarea de ECS para indicar que esta ya no se está ejecutando.
- Solo se admiten las tareas de ECS iniciadas en modo de red de `awsvpc`.

Limitaciones específicas del campo `encryption-status`:

- El estado de cifrado puede ser “-” (no disponible) en algunos flujos, debido a la limitación de algunos dispositivos de red para informar el estado de cifrado. Los usuarios pueden ignorar estos flujos en el análisis.
- Que se muestre como cifrado en el modo de supervisión no significa que el flujo se permita en el modo de aplicación. Y viceversa.
  - Si un flujo está cifrado en el modo de supervisión, es posible que no cumpla los requisitos en el modo de aplicación:
    - Si el flujo implica una ENI creada por un servicio de AWS, el servicio debe admitir los controles de cifrado.
    - Si el flujo pasa por el emparejamiento de VPC, la VPC emparejada puede no aplicar los controles de cifrado.
  - Si un flujo no está cifrado en el modo de supervisión, aun así puede cumplir los requisitos en el modo de aplicación, siempre que el servicio relacionado con el flujo se haya agregado como una exclusión.

Limitaciones específicas de los campos de etiquetas de Amazon EC2 para registros de flujo disponibles en la versión 11:

- Los campos de etiquetas no se calculan si las etiquetas de un recurso no pertenecen al propietario de la suscripción de registros de flujo.

  Por ejemplo, supongamos que se comparte una subred (`SubnetA`) con otra cuenta (`AccountB`) y, a continuación, se crea una suscripción al registro de flujo para `SubnetA` con un campo de etiqueta en las interfaces de red. Si `AccountB` inicia una interfaz de red etiquetada con la clave que ha configurado, su suscripción recibe los registros de tráfico de la interfaz de red iniciada por `AccountB`, pero los campos de etiquetas configurados por su suscripción no se calculan por motivos de seguridad. Se puede etiquetar la interfaz de red iniciada por `AccountB` para mostrar las etiquetas si se desea.
- Si crea suscripciones de registros de flujo con campos de etiquetas en el nivel de recursos de VPC/subred, cualquier tráfico generado para las interfaces de red no etiquetadas también se entregará para las suscripciones. Los valores de los campos de etiquetas serán '-' para los recursos no etiquetados.
- Los grupos de escalado automático no podrán mostrar ninguna etiqueta si se denominan '-', ya que se trata de un carácter reservado para indicar un valor ausente o la inexistencia de valor.

- Si se crea cualquier suscripción de registros de flujo de VPC con campos de etiquetas, se crearán algunos recursos en representación del usuario. Para consumir las actualizaciones de los valores de las etiquetas, se crearán reglas administradas de EventBridge para enviar los cambios de las etiquetas al servicio de registros de flujo de VPC. Estas reglas administradas de EventBridge se limpiarán automáticamente si se eliminan todas las suscripciones con campos de etiquetas. No elimine manualmente estas reglas administradas de EventBridge. Si lo hace, se producirán retrasos considerables en la actualización de los valores de las etiquetas. Para controlar esta creación o limpieza y proporcionar acceso a los valores de las etiquetas, se creará un rol vinculado al servicio en la cuenta. Consulte Uso de roles vinculados al servicio para los registros de flujo de VPC para obtener más detalles.
- Debido a las restricciones de análisis de Registros de Amazon CloudWatch y Athena, todos los caracteres especiales de los valores de las etiquetas se codificarán mediante la codificación de porcentaje UTF-8. Esto se puede decodificar de forma nativa en Athena mediante `url_decode` o se puede decodificar con cualquier decodificador de URL o URI.
- Durante la primera hora después de crear una nueva suscripción, es posible que los valores de las etiquetas estén ausentes o no sean precisos. Después de esta primera hora, los valores de las etiquetas reflejarán con precisión los valores de los recursos etiquetados con una granularidad de 1 minuto.
- Si se realizan varios cambios de etiqueta en el mismo recurso en el mismo segundo, existe la posibilidad de que se pierdan las actualizaciones, lo que dará lugar a valores de etiqueta desactualizados durante un máximo de una hora.
- Para los campos de etiquetas de los grupos de escalado automático, debe tener al menos un trail de CloudTrail habilitado en la cuenta. Sin un trail habilitado, los valores de las etiquetas de los grupos de escalado automático pueden estar obsoletos o ser imprecisos.

Limitaciones específicas de los campos `next-hop-`:

- Los campos del siguiente salto no se calculan si la interfaz de red del siguiente salto no pertenece al propietario de la suscripción de registros de flujo, a excepción de `next-hop-az-id`.
- Los campos del siguiente salto no están disponibles si el siguiente salto no tiene una interfaz de red (por ejemplo, el tráfico a la puerta de enlace de Internet).
- Los campos del siguiente salto no están disponibles para el tráfico entre regiones.
- Los campos del siguiente salto no están disponibles para el tráfico de entrada de algunos servicios de red (por ejemplo, puerta de enlace de tránsito y Equilibrador de carga de red).

- Si el tráfico pasa por un dispositivo intermedio (por ejemplo, puerta de enlace de tránsito o equilibrador de carga de red), la interfaz de red del siguiente salto es la interfaz asociada al dispositivo intermedio (como la conexión de puerta de enlace de tránsito), no el destino final del tráfico

Precios

Se aplican costos por archivo e ingesta de datos para los registros distribuidos cuando se publican registros de flujo. Para obtener más información acerca de los precios de publicación de registros distribuidos, abra Precios de Amazon CloudWatch, seleccione Logs (Registros) y busque Vended Logs (Registros distribuidos).

Para realizar un seguimiento de los cargos de publicación de los registros de flujo, puede aplicar etiquetas de asignación de costos al recurso 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 los siguientes temas:

- Uso de etiquetas de asignación de costos en la Guía del usuario de AWS Billing.
- Etiquetado de grupos de registro de Amazon CloudWatch en la Guía del usuario de Registros de Amazon CloudWatch
- Uso de etiquetas de buckets de S3 de asignación de costos en la Guía del usuario de Amazon Simple Storage Service
- Etiquetado de flujos de entrega en la Guía para desarrolladores de Amazon Data Firehose

Trabajo con registros de flujo

Puede trabajar con registros de flujo con las consolas de Amazon EC2 y Amazon VPC.

Tareas

- 1. Control del uso de los registros de flujo con IAM
- 2. Crear un log de flujo
- 3. Etiquetado de un registro de flujo
- 4. Eliminar un registro de flujo

- Descripción general de la línea de comandos

1. Control del uso de los registros de flujo con IAM

De forma predeterminada, los usuarios no tienen permiso para trabajar con registros de flujo. Puede crear un rol de IAM con una política asociada que conceda permisos a los usuarios para crear, describir y eliminar registros de flujo.

A continuación se muestra una política de ejemplo que concede a los usuarios permisos completos para crear, describir y eliminar logs de flujo.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": "*"
    }
  ]
}
```

Para obtener más información, consulte the section called “Cómo funciona Amazon VPC con IAM”.

2. Crear un log de flujo

Puede crear registros de flujo para sus VPC, subredes o interfaces de red. Al crear un registro de flujo, debe especificar un destino para el registro de flujo. Para obtener más información, consulte los siguientes temas:

- the section called “Crear un registro de flujo que se publique en CloudWatch Logs”
- the section called “Crear un registro de flujo que se publique en Amazon S3”
- the section called “Crear un registro de flujo que publique en Amazon Data Firehose”

3. Etiquetado de un registro de flujo

Puede agregar o eliminar etiquetas de un registro de flujo en cualquier momento.

Para administrar las etiquetas de un registro de flujo

1. Realice una de las siguientes acciones:
   - Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/. En el panel de navegación, elija Network Interfaces. Seleccione la casilla de verificación de la interfaz de red.
   - Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. En el panel de navegación, elija Your VPCs (Sus VPC). Seleccione la casilla de verificación de la VPC.
   - Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. En el panel de navegación, elija Subnets (Subredes). Seleccione la casilla de verificación de la subred.
2. Elija Flow Logs (Registros de flujo).
3. Elija Actions (Acciones) y, a continuación, Manage tags (Administrar etiquetas).
4. Para agregar una etiqueta nueva, elija Add new tag (Agregar nueva etiqueta) y, a continuación, ingrese la clave y el valor. Para eliminar una etiqueta, elija Eliminar.
5. Cuando termine de agregar o quitar las etiquetas, elija Save (Guardar).

4. Eliminar un registro de flujo

Puede eliminar un registro de flujo en cualquier momento. Tras haber eliminado un registro de flujo, puede que se necesiten varios minutos para que se dejen de recopilar los datos.

La eliminación de un registro de flujo no elimina los datos del registro del destino ni modifica el recurso de destino. Debe eliminar los datos del registro de flujo existentes directamente desde el destino y borrar el recurso de destino mediante la consola del servicio de destino.

Para eliminar un registro de flujo

1. Realice una de las siguientes acciones:
   - Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/. En el panel de navegación, elija Network Interfaces. Seleccione la casilla de verificación de la interfaz de red.
   - Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. En el panel de navegación, elija Your VPCs (Sus VPC). Seleccione la casilla de verificación de la VPC.

- Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. En el panel de navegación, elija Subnets (Subredes). Seleccione la casilla de verificación de la subred.

2. Elija Flow Logs (Registros de flujo).
3. Elija Actions (Acciones), Delete flow logs (Eliminar registros de flujo).
4. Cuando se le pida confirmación, escriba **`delete`** y elija Delete (Eliminar).

Descripción general de la línea de comandos

Puede utilizar la línea de comandos para realizar las tareas descritas en esta página.

Crear un registro de flujo

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

Describir un registro de flujo

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)

Etiquetado de un registro de flujo

- create-tags y delete-tags (AWS CLI)
- New-EC2Tag y Remove-EC2Tag (AWS Tools for Windows PowerShell)

Eliminar un registro de flujo

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)

Publicar registros de flujo en CloudWatch Logs

Los registros de flujo pueden publicar datos de registro de flujo directamente en Amazon CloudWatch. Amazon CloudWatch es un servicio integral de supervisión y observabilidad. Recopila y rastrea métricas, registros y datos de eventos de varios recursos de AWS, como así también

de las aplicaciones y los servicios propios. CloudWatch brinda información sobre la utilización de los recursos, el rendimiento de las aplicaciones y el estado operacional, lo que permite detectar y responder a los cambios y a los posibles problemas del rendimiento de todo el sistema. Con CloudWatch, puede establecer alarmas, visualizar los registros y las métricas y responder automáticamente para recopilar y optimizar sus recursos en la nube. Es una herramienta esencial para asegurar la fiabilidad, la disponibilidad y el rendimiento de sus aplicaciones e infraestructura en la nube.

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 registro 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 registro combinado capturará todo el tráfico.

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 Registros de Amazon CloudWatch.

Precios

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, abra Precios de Amazon CloudWatch seleccione Logs (Registros) y consulte Vended Logs (Registros distribuidos).

Contenido

- Rol de IAM para publicar registros de flujo en CloudWatch Logs
- Crear un registro de flujo que se publique en CloudWatch Logs
- Visualización de los informes de los registros de flujo con Registros CloudWatch
- Buscar entradas de registros de flujo
- Procesar entradas de registro de flujo en CloudWatch Logs

Rol 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 registro 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.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

Asegúrese de que el rol posee la siguiente política de confianza, la cual permite al servicio de registros de flujo asumir ese rol.

JSON

```
{
  "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"
    }
}
```

Crear un rol de IAM para registros de flujo

Se puede actualizar un rol existente tal como se ha descrito anteriormente. También puede emplear el siguiente procedimiento para crear un nuevo rol y usarlo con los registros de flujo. Especificará esta función al crear el registro 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, seleccione Políticas.
3. Elija Create Policy (Crear política).
4. En la página Create policy (Crear política), haga lo siguiente:
   a. Elija JSON.
   b. Reemplace el contenido de esta ventana por la política de permisos que aparece al principio de esta sección.
   c. Elija Siguiente.

d. Introduzca un nombre para su política y una descripción y etiquetas opcionales y, a continuación, elija Create policy (Crear política).

5. Seleccione Roles en el panel de navegación.
6. Elija Creación de rol.
7. En Trusted entity type (Tipo de entidad de confianza), elija Custom trust policy (Política de confianza personalizada). En Custom trust policy (Política de confianza personalizada), reemplace `"Principal": {},` con lo siguiente y luego elija Next (Siguiente).

```
"Principal": {
   "Service": "vpc-flow-logs.amazonaws.com"
},
```

8. En la página Add permissions (Agregar permisos), seleccione la casilla de verificación de la política que creó anteriormente en este procedimiento y luego elija Next (Siguiente).
9. Ingrese un nombre para el rol y, opcionalmente, especifique una descripción.
10. Elija Create role (Crear rol).

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 sigue estos pasos como usuario empleando un determinado rol de IAM, asegúrese de que el rol tenga permisos para utilizar la acción `iam:PassRole`.

Requisito previo

Compruebe que la entidad principal de IAM que está utilizando para realizar la solicitud tenga los permisos para llamar la acción de `iam:PassRole`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
```

```
            ],
            "Resource": "arn:aws:iam::111122223333:role/flow-log-role-name"
        }
    ]
}
```

Para crear un registro de flujo mediante la consola

1. Realice una de las siguientes acciones:
   - Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/. En el panel de navegación, elija Network Interfaces. Seleccione la casilla de verificación de la interfaz de red.
   - Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. En el panel de navegación, elija Your VPCs (Sus VPC). Seleccione la casilla de verificación de la VPC.
   - Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. En el panel de navegación, elija Subnets (Subredes). Seleccione la casilla de verificación de la subred.
2. Seleccione Actions (Acciones) y, a continuación, Create flow log (Crear registro de flujo).
3. 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.
4. 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.
5. En Destination (Destino), elija Send to CloudWatch Logs (Enviar a CloudWatch Logs).
6. Para el grupo de registro de destino, elija el nombre de un grupo de registro existente o ingrese el nombre de un grupo de registro nuevo. Si ingresa un nombre, crearemos el grupo de registro cuando haya tráfico para registrar.
7. En Acceso al servicio, seleccione un rol de servicio de IAM existente que tenga permisos para publicar registros en Registros de CloudWatch, o bien seleccione la opción para crear un nuevo rol de servicio.
8. Para Log record format (Formato de registro de registro), seleccione el formato para el registro de flujo.
   - Para utilizar el formato predeterminado, elija 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).

9. En Metadatos adicionales, seleccione si desea incluir los metadatos de Amazon ECS en el 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-EC2FlowLog (AWS Tools for Windows PowerShell)

El siguiente ejemplo de la AWS CLI crea un registro de flujo que captura todo el tráfico aceptado para la subred especificada. Los registros de flujo se entregan al grupo de registros especificado. El parámetro `--deliver-logs-permission-arn` especifica el rol de IAM necesario para publicar en CloudWatch Logs.

```
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
```

Visualización de los informes de los registros de flujo con Registros CloudWatch

Puede consultar las entradas de registro de flujo a través de la consola de CloudWatch Logs. 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 mediante la consola

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 registro).
3. Seleccione el nombre del grupo de registro que contiene los registros de flujo para abrir la página de detalles.
4. Seleccione el nombre del flujo de registro que contiene las entradas de registro de flujo. Para obtener más información, consulte Registros de log de flujo.

Para consultar las entradas de registro de flujo publicados en CloudWatch Logs mediante la línea de comandos

- get-log-events (AWS CLI)
- Get-CWLLogEvent (AWS Tools for Windows PowerShell)

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 Logs (Registros), Log groups (Grupos de registro).
3. Seleccione el grupo de registro que contiene el registro de flujo y, a continuación, seleccione el flujo de registro si conoce la interfaz de red que está buscando. De manera alternativa, elija Search log group (Buscar 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 eventos, introduzca la siguiente cadena. Esto supone que el registro de log de flujo utiliza el formato predeterminado.

   ```
   [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]
```

Procesar entradas de registro de flujo en CloudWatch Logs

Puede procesar los registros de flujo de la misma forma que cualquier otro evento de registro que recopile Registros de CloudWatch. Para obtener más información sobre cómo supervisar los datos de registro y los filtros de métricas, consulte Creación de métricas con filtros a partir de eventos de registro en la Guía del usuario de Registros 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), ingrese la siguiente cadena.

```
[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).
6. Cuando esté preparado para continuar, seleccione Next (Siguiente).

7. 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).
8. En el panel de navegación, elija Alarms (Alarmas), Create Alarm (Crear alarma).
9. Elija Crear alarma.
10. Seleccione el nombre de métrica que ha creado y elija Select metric (Seleccionar métrica).
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 TimeSinceLastActive is... (Siempre LaÚltimaVezActivo es…), 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. Elija Siguiente.
13. Para Notification (Notificación), seleccione un tema de SNS existente o elija Create new topic (Crear tema nuevo) para crear uno nuevo. Elija Next (Siguiente).
14. Ingrese un nombre y una descripción para la alarma y, a continuación, elija Next (Siguiente).
15. Cuando haya terminado de obtener una vista previa de 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. Amazon S3 (Simple Storage Service) es un servicio de almacenamiento de objetos altamente escalable y durable. Su diseño permite almacenar y recuperar cualquier cantidad de datos desde cualquier parte de la web. S3 ofrece la durabilidad y la disponibilidad más avanzadas de la industria e incorpora las características de control de versiones, cifrado y control de acceso de los datos.

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 supervisadas 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.

Para crear un bucket de Amazon S3 y utilizarlo con los registros de flujo, consulte Creación de un bucket en la Guía del usuario de Amazon S3.

Para más información sobre cómo mejorar la ingesta, el procesamiento y la visualización de los registros de flujo de la VPC, consulte Registro centralizado con OpenSearch 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 Registros de Amazon CloudWatch.

Precios

Se aplican costos por ingesta y archivo de datos para los registros a la venta cuando se publican registros de flujo en Amazon S3. Para obtener más información, abra Precios de Amazon CloudWatch seleccione Logs (Registros) y consulte Vended Logs (Registros distribuidos).

Contenido

- Archivos de registro de flujo
- Permisos del bucket de Amazon S3 para registros de flujo
- Política de clave requerida para el uso con SSE-KMS
- Permisos de archivos de registro de Amazon S3
- Crear un registro de flujo que se publique en Amazon S3
- Visualización de los informes de los registros de flujo con Amazon S3

Archivos de registro de flujo

Los registros de flujo de VPC recopilan datos sobre el tráfico IP que entra y sale de su VPC en colecciones de registro, agregan esos registros en archivos de registro y, a continuación, publican los archivos de registro en el bucket de Amazon S3 en intervalos de cinco minutos. Se pueden publicar varios archivos y cada registro de archivo puede contener algunos o todos los registros de flujo del tráfico IP registrado en los cinco minutos anteriores.

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.

> **Note**
>
> Si los datos en formato Parquet con compresión Gzip pesan menos de 100 KB por período de agregación, el almacenamiento de los datos en formato Parquet puede ocupar más espacio que el texto sin formato con compresión Gzip debido a los requisitos de memoria de los archivos de Parquet.

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/aws-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/aws-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
```

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.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
                }
            }
        }
    ]
}
```

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 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.

Tenga en cuenta que el servicio de entrega de registros llama a la acción `HeadBucket` de la API de Amazon S3 para verificar la existencia y la ubicación del bucket de S3. No es necesario que se conceda permiso al servicio de entrega de registros para la ejecución de esta acción. El servicio continúa entregando los registros del flujo de la VPC aunque no pueda confirmar la existencia del bucket de S3. Sin embargo, habrá un error `AccessDenied` en la llamada a `HeadBucket` en los registros de CloudTrail.

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) en su bucket de S3. Para obtener más información, consulte Protección de datos mediante cifrado del lado del servidor en la Guía del usuario de Amazon S3.

Si elija SSE-S3, no se requiere ninguna configuración adicional. Amazon S3 se encarga de la clave de cifrado.

Si elige SSE-KMS, debe utilizar un ARN de clave administrada por el cliente. Si utiliza un ID de clave, puede producirse un error LogDestination undeliverable cuando cree un registro de flujo. Además, debe actualizar la política de claves para la clave administrada por el cliente, de manera que la cuenta de entrega de registros pueda escribir en el bucket de S3. Para obtener más información sobre la política clave requerida para usar con SSE-KMS, consulte Cifrado del lado del servidor del bucket de Amazon S3 en la Guía del usuario de Registros de Amazon CloudWatch.

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 registros tiene los permisos `READ` y `WRITE`. Para obtener más información, consulte Información general de las listas de control de acceso (ACL) en la Guía del usuario de Amazon S3.

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.

Requisito previo

La entidad principal de IAM que cree el registro de flujo debe utilizar un rol de IAM que tenga los siguientes permisos, que son necesarios para publicar registros de flujo en el bucket de Amazon S3 de destino.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
```

```
        "logs:DeleteLogDelivery"
      ],
      "Resource": "*"
    }
  ]
}
```

Para crear un registro de flujo mediante la consola

1. Realice una de las siguientes acciones:
   - Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/. En el panel de navegación, elija Network Interfaces. Seleccione la casilla de verificación de la interfaz de red.
   - Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. En el panel de navegación, elija Your VPCs (Sus VPC). Seleccione la casilla de verificación de la VPC.
   - Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. En el panel de navegación, elija Subnets (Subredes). Seleccione la casilla de verificación de la subred.
2. Seleccione Actions (Acciones) y, a continuación, Create flow log (Crear registro de flujo).
3. En Filter (Filtro), especifique el tipo de datos de tráfico IP que desea registrar.
   - Accepted (Aceptado): registrar solo tráfico aceptado.
   - Rejected (Rechazado): registrar solo tráfico rechazado.
   - All (Todo): Tráfico aceptado y rechazado
4. 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.
5. En Destination (Destino), elija Send to an Amazon S3 bucket (Enviar a un bucket de Amazon S3).
6. 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 `AWSLogs` 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.

7. 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 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 flujo.
8. En Metadatos adicionales, seleccione si desea incluir los metadatos de Amazon ECS en el formato de registro.
9. 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.
10. (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).
11. (Opcional) Para particionar los registros de flujo por hora, elija Every 1 hour (60 mins) (Cada 1 hora [60 minutos]).
12. (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.
13. Elija Create flow log (Crear registro de flujo).

Creación de un registro de flujo que publica en Amazon S3 mediante la línea de comandos

Utilice uno de los siguientes comandos:

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

En el siguiente ejemplo de AWS CLI se crea un registro de flujo que captura todo el tráfico de la VPC especificada y entrega los registros de flujo al bucket de Amazon S3 especificado. 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/custom-flow-logs/ --log-format '${version} ${vpc-id} ${subnet-id} ${instance-
id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${tcp-flags} ${type} ${pkt-
srcaddr} ${pkt-dstaddr}'
```

Visualización de los informes de los registros de flujo con Amazon S3

Puede ver las entradas de registro de flujo mediante la consola de Amazon S3. Es posible que, después de crear su registro de flujo, se necesiten unos minutos para que se encuentre visible en la consola.

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 flujo.

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. Seleccione el nombre del bucket para abrir la página de detalles.
3. Diríjase a la carpeta con los archivos de registro. Por ejemplo, *prefijo*/AWSLogs/*account_id*/vpcflowlogs/*región*/*año*/*mes*/*día*/.
4. Seleccione la casilla de verificación junto al nombre del archivo y luego elija Download (Descargar).

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.

Publicar registros de flujo a Amazon Data Firehose

Los registros de flujo pueden publicar datos del registro de flujo directamente en Amazon Data Firehose. Amazon Data Firehose es un servicio completamente administrado que recopila,

transforma y envía flujos de datos en tiempo real a distintos productos de almacenamiento y análisis de datos de AWS. Se encarga de la ingesta de datos.

Firehose puede ser bastante útil al trabajar con los registros de flujo de la VPC. Los registros de flujo de la VPC capturan información sobre el tráfico IP entrante y saliente de las interfaces de red en su VPC. Estos datos pueden ser cruciales para la supervisión de la seguridad, el análisis del rendimiento y el cumplimiento normativo. Sin embargo, la administración del almacenamiento y el procesamiento de este flujo continuo de datos de registro puede ser una tarea compleja y que requiera muchos recursos.

La integración de Firehose con los registros de flujo de la VPC le permite enviar estos datos a su destino de preferencia, como Amazon S3 o Amazon Redshift. Firehose escalará y controlará la ingestión, la transformación y el envío de sus registros de flujo de la VPC, lo cual lo libera de la carga operativa. Gracias a esto, en vez de preocuparse por la infraestructura subyacente, puede enfocarse en el análisis de los datos y el envío de la información.

Además, Firehose ofrece características, como la transformación, la compresión y el cifrado de datos, que pueden mejorar la eficiencia y la seguridad su canalización de procesamiento de los registros de flujo de la VPC. Utilizar Firehose para los registros de flujo de la VPC simplifica la administración de los datos y permite obtener información de los datos del tráfico de su red.

Al publicar en Amazon Data Firehose, los datos del registro de flujo se publican en un flujo de entrega de Amazon Data Firehose en formato de texto sin formato.

Precios

Se aplican los cargos estándar de ingesta y entrega. Para obtener más información, abra Precios de Amazon CloudWatch seleccione Logs (Registros) y consulte Vended Logs (Registros distribuidos).

Contenido

- Roles de IAM para la entrega entre cuentas
- Crear un registro de flujo que publique en Amazon Data Firehose

Roles de IAM para la entrega entre cuentas

Al publicar en Amazon Data Firehose, puede elegir un flujo de entrega que esté en la misma cuenta que el recurso que se va a supervisar (la cuenta de origen) o en una cuenta diferente (la cuenta de destino). Para habilitar la entrega entre cuentas de los registros de flujo a Amazon Data Firehose, debe crear un rol de IAM en la cuenta de origen y un rol de IAM en la cuenta de destino.

Roles

- Rol de cuenta de origen
- Rol de cuenta de destino

Rol de cuenta de origen

En la cuenta de origen, cree un rol que conceda los siguientes permisos. En este ejemplo, el nombre del rol es `mySourceRole`, pero puede elegir un nombre diferente para este rol. La última instrucción permite que el rol de la cuenta de destino asuma este rol. Las instrucciones de condición garantizan que esta función se pase solo al servicio de entrega de registros y solo al supervisar el recurso especificado. Al crear la política, especifique las VPC, las interfaces de red o las subredes que está supervisando con la clave de condición `iam:AssociatedResourceARN`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::123456789012:role/mySourceRole",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "delivery.logs.amazonaws.com"
                },
                "StringLike": {
                    "iam:AssociatedResourceARN": [
                        "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-00112233344556677"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
```

```
                "logs:GetLogDelivery"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::111122223333:role/
AWSLogDeliveryFirehoseCrossAccountRole"
        }
    ]
}
```

Asegúrese de que este rol tenga la siguiente política de confianza, la cual permite que el servicio de entrega de registros asuma el rol.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

En la cuenta de origen, use el siguiente procedimiento para crear el rol.

Para crear el rol de la cuenta de origen

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Políticas.
3. Elija Create Policy (Crear política).
4. En la página Create policy (Crear política), haga lo siguiente:

a. Elija JSON.

b. Reemplace el contenido de esta ventana por la política de permisos que aparece al principio de esta sección.

c. Elija Siguiente.

d. Introduzca un nombre para su política y una descripción y etiquetas opcionales y, a continuación, elija Create policy (Crear política).

5. Seleccione Roles en el panel de navegación.
6. Elija Creación de rol.
7. En Trusted entity type (Tipo de entidad de confianza), elija Custom trust policy (Política de confianza personalizada). En Custom trust policy (Política de confianza personalizada), reemplace `"Principal": {},` con lo siguiente, lo cual especifica el servicio de entrega de registros. Elija Siguiente.

```
"Principal": {
   "Service": "delivery.logs.amazonaws.com"
},
```

8. En la página Add permissions (Agregar permisos), seleccione la casilla de verificación de la política que creó anteriormente en este procedimiento y luego elija Next (Siguiente).
9. Ingrese un nombre para el rol y, opcionalmente, especifique una descripción.
10. Elija Create role (Crear rol).

Rol de cuenta de destino

En la cuenta de destino, cree un rol con un nombre que comience con AWSLogDeliveryFirehoseCrossAccountRole. El rol debe otorgar los siguientes permisos.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iam:CreateServiceLinkedRole",
```

```
            "firehose:TagDeliveryStream"
        ],
        "Resource": "*"
    }
  ]
}
```

Asegúrese de que este rol tenga la siguiente política de confianza, la cual permite que el rol que creó en la cuenta de origen asuma este rol.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/mySourceRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

En la cuenta de destino, use el siguiente procedimiento para crear el rol.

Para crear el rol de cuenta de destino

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Políticas.
3. Elija Create Policy (Crear política).
4. En la página Create policy (Crear política), haga lo siguiente:

    a. Elija JSON.

    b. Reemplace el contenido de esta ventana por la política de permisos que aparece al principio de esta sección.

    c. Elija Siguiente.

d. Ingrese un nombre para la política que comience con AWSLogDeliveryFirehoseCrossAccountRole y, a continuación, elija Create policy (Crear política).

5. Seleccione Roles en el panel de navegación.
6. Elija Creación de rol.
7. En Trusted entity type (Tipo de entidad de confianza), elija Custom trust policy (Política de confianza personalizada). En Custom trust policy (Política de confianza personalizada), reemplace `"Principal": {},` con lo siguiente, lo cual especifica la función de la cuenta de origen. Elija Siguiente.

```
"Principal": {
   "AWS": "arn:aws:iam::source-account:role/mySourceRole"
},
```

8. En la página Add permissions (Agregar permisos), seleccione la casilla de verificación de la política que creó anteriormente en este procedimiento y luego elija Next (Siguiente).
9. Ingrese un nombre para el rol y, opcionalmente, especifique una descripción.
10. Elija Create role (Crear rol).

Crear un registro de flujo que publique en Amazon Data Firehose

Puede crear registros de flujo para sus VPC, subredes o interfaces de red.

Requisitos previos

- Cree el flujo de entrega de Amazon Data Firehose de destino. Use Direct Put (Venta directa) como fuente. Para obtener más información, consulte Creación de un flujo de entrega de Amazon Data Firehose.
- La cuenta que crea el registro de flujo debe utilizar un rol de IAM que conceda los siguientes permisos para publicar registros de flujo en Amazon Data Firehose.

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "iam:CreateServiceLinkedRole",
                "firehose:TagDeliveryStream"
            ],
            "Resource": "*"
        }
    ]
}
```

- Si va a publicar registros de flujo en una cuenta diferente, cree las funciones de IAM necesarias tal como se describe en the section called “Roles de IAM para la entrega entre cuentas”.

Para crear un registro de flujo que publique en Amazon Data Firehose

1. Realice una de las siguientes acciones:
   - Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/. En el panel de navegación, elija Network Interfaces. Seleccione la casilla de verificación de la interfaz de red.
   - Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. En el panel de navegación, elija Your VPCs (Sus VPC). Seleccione la casilla de verificación de la VPC.
   - Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/. En el panel de navegación, elija Subnets (Subredes). Seleccione la casilla de verificación de la subred.
2. Seleccione Actions (Acciones) y, a continuación, Create flow log (Crear registro de flujo).
3. Para Filter (Filtro), especifique el tipo de tráfico que desea registrar.
   - Accepted (Aceptado): registrar solo tráfico aceptado
   - Rejected (Rechazado): registrar solo tráfico rechazado
   - All (Todo): registrar tráfico aceptado y rechazado
4. 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.
5. En Destination (Destino), elija cualquiera de las siguientes opciones:
   - Send to Amazon Data Firehose in the same account (Enviar a Amazon Data Firehose en la misma cuenta): el flujo de entrega y el recurso para supervisar están en la misma cuenta.

- Send to Amazon Data Firehose in a different account (Enviar a Amazon Data Firehose en una cuenta diferente): el flujo de entrega y el recurso para supervisar están en cuentas diferentes.

6. Para el nombre de la secuencia de Amazon Data Firehose, elija la secuencia de entrega que ha creado.
7. [Solo entrega entre cuentas] En Acceso al servicio, seleccione un rol de servicio de IAM para la entrega entre cuentas con permisos para publicar registros. También se puede elegir Configurar permisos para abrir la consola de IAM y crear un rol de servicio.
8. 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 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 flujo.
9. En Metadatos adicionales, seleccione si desea incluir los metadatos de Amazon ECS en el formato de registro.
10. (Opcional) Elija Add tag (Agregar etiqueta) para aplicar etiquetas al registro de flujo.
11. Elija Create flow log (Crear registro de flujo).

Creación de un registro de flujo que publica en Amazon Data Firehose mediante la línea de comandos

Utilice uno de los siguientes comandos:

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

En el siguiente ejemplo de AWS CLI, se crea un registro de flujo que captura todo el tráfico de la VPC especificada y envía los registros de flujo al flujo de entrega de Amazon Data Firehose especificado en la misma cuenta.

```
aws ec2 create-flow-logs --traffic-type ALL \
  --resource-type VPC \
  --resource-ids vpc-00112233344556677 \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream/flowlogs_stream
```

En el siguiente ejemplo de AWS CLI, se crea un registro de flujo que captura todo el tráfico de la VPC especificada y envía los registros de flujo al flujo de entrega de Amazon Data Firehose especificado en una cuenta diferente.

```
aws ec2 create-flow-logs --traffic-type ALL \
  --resource-type VPC \
  --resource-ids vpc-00112233344556677 \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream/flowlogs_stream \
  --deliver-logs-permission-arn arn:aws:iam::source-account:role/mySourceRole \
  --deliver-cross-account-role arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole
```

Como resultado de la creación de los registros de flujo, obtiene los datos de los registros de flujo del destino que configuró para el flujo de envío.

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 nubes privadas virtuales (VPC) son los principales interlocutores o puede identificar las direcciones IP con las conexiones TCP más rechazadas.

Opciones

- Se puede optimizar y automatizar la integración de sus registros de flujo de VPC con Athena. Genere una plantilla de CloudFormation que cree los recursos de AWS necesarios, además de consultas predefinidas para la obtención de 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

Incurre en cargos estándar de Amazon Athena por ejecutar consultas. Incurre 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
- Generar la plantilla de CloudFormation mediante la AWS CLI
- Ejecutar una consulta predefinida

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

- La región seleccionada debe admitir AWS Lambda y Amazon Athena.
- Los buckets de Amazon S3 deben estar en la región seleccionada.
- El formato del registro de registro para el registro de flujo debe incluir los campos utilizados por las consultas predefinidas específicas que desea ejecutar.

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 elija None (Ninguno), debe especificar la fecha de inicio y finalización de la partición, utilizando fechas anteriores. Si elija 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 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.
- 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.
2. En el panel de navegación izquierdo, elija Query Editor (Editor de consultas). En Workgroup (Grupo de trabajo), seleccione el grupo de trabajo creado por la plantilla de CloudFormation.
3. Seleccione Saved queries (Consultas guardadas), seleccione una consulta, modifique los parámetros según sea necesario y, a continuación, ejecute la consulta. Para obtener una lista de las consultas predefinidas disponibles, consulte Predefined queries (Consultas predefinidas).

4. En Query results (Resultados de consulta), consulte los resultados de la consulta.

Consultas predefinidas

La siguiente es la lista completa de consultas llamadas Athena. Las consultas predefinidas que se proporcionan al generar la plantilla dependen de los campos que forman parte del formato de la entrada de registro del registro de flujo. Por lo tanto, es posible que la plantilla no contenga todas estas consultas predefinidas.

- 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.

Administración de identidades y accesos en los registros de flujo de VPC

AWS utiliza credenciales de seguridad para identificarlo y concederle acceso a sus recursos de AWS. Puede utilizar las características de AWS Identity and Access Management (IAM) para permitir que otros usuarios, servicios y aplicaciones usen sus recursos de AWS total o parcialmente, sin necesidad de compartir sus credenciales de seguridad.

En esta sección se describen los roles vinculados a servicios de AWS que se crean específicamente para los registros de flujo de VPC y las políticas administradas adjuntas a los roles vinculados a servicios de los registros de flujo de VPC. Para obtener más información sobre los roles y políticas de AWS IAM, consulte Términos y conceptos de roles en la Guía del usuario de IAM.

Para obtener más información sobre la administración de identidades y accesos para una VPC, consulte Administración de identidades y accesos para Amazon VPC en la Guía del usuario de Amazon VPC.

Contenido

- Uso de roles vinculados al servicio para los registros de flujo de VPC
- Políticas administradas de AWS para registros de flujo de VPC

Uso de roles vinculados al servicio para los registros de flujo de VPC

Los registros de flujo de VPC utilizan roles vinculados al servicio de AWS Identity and Access Management (IAM). Un rol vinculado al servicio es un tipo único de rol de IAM que está vinculado directamente a los registros de flujo de VPC. Los roles vinculados a servicios están predefinidos por los registros de flujo de VPC e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

Un rol vinculado a un servicio simplifica la configuración de los registros de flujo de VPC porque ya no tendrá que añadir manualmente los permisos necesarios. Los registros de flujo de VPC definen los permisos de los roles vinculados al servicio y, salvo que se indique lo contrario, solo los registros de flujo de VPC pueden asumir esos roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege los recursos de los registros de flujo de VPC, ya que no puede eliminar de forma involuntaria los permisos para acceder a dichos recursos.

Para obtener información sobre otros servicios que admiten roles vinculados al servicio, consulte Servicios de AWS que funcionan con IAM y busque los servicios que tengan Sí en la columna Roles vinculados al servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de los roles vinculados al servicio para los registros de flujo de VPC

Los registros de flujo de VPC utilizan el rol vinculado al servicio denominado AWSServiceRoleForVPCFlowLogs – Este rol vinculado al servicio permite a los registros de flujo de VPC crear y administrar reglas administradas de EventBridge y llamar a las API DescribeTag en representación del usuario para realizar un seguimiento automático de las actualizaciones de los valores de las etiquetas de EC2 asociados a los recursos en las suscripciones de registros de flujo que incluyen campos de etiquetas.

El rol vinculado al servicio AWSServiceRoleForVPCFlowLogs confía en los siguientes servicios para asumir el rol:

- `vpc-flow-logs.amazonaws.com`

La política de permisos del rol se denomina AWSVPCFlowLogsServiceRolePolicy y permite que los registros de flujo de VPC puedan realizar las siguientes acciones en los recursos especificados:

- Acción: `autoscaling:DescribeTags` en los grupos de escalado automático de EC2 para validar los valores de las etiquetas.

  Acción: `tag:GetResources` en las instancias de EC2 y las interfaces de red elásticas para validar los valores de las etiquetas.

  Acción: `events:PutRule` en las nuevas reglas administradas a partir de las fuentes `aws.tag` y `aws.autoscaling` para los tipos de detalles relacionados con los eventos de cambio de etiquetas.

  Acción: `events:DeleteRule` en las reglas administradas creadas por los registros de flujo de VPC denominados `VPCFlowLogsEC2TagsManagedRule` y/o `VPCFlowLogsASGTagsManagedRule`.

  Acción: `events:DescribeRule` en las reglas administradas creadas por los registros de flujo de VPC denominados `VPCFlowLogsEC2TagsManagedRule` y/o `VPCFlowLogsASGTagsManagedRule`.

Acción: `events:PutTargets` en las reglas administradas creadas por los registros de flujo de VPC denominados `VPCFlowLogsEC2TagsManagedRule` y/o `VPCFlowLogsASGTagsManagedRule`.

Acción: `events:RemoveTargets` en las reglas administradas creadas por los registros de flujo de VPC denominados `VPCFlowLogsEC2TagsManagedRule` y/o `VPCFlowLogsASGTagsManagedRule`.

Debe configurar los permisos para permitir a sus usuarios, grupos o funciones, crear, editar o eliminar la descripción de un rol vinculado al servicio. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado al servicio para los registros de flujo de VPC

No necesita crear manualmente un rol vinculado a servicios. Cuando crea CreateFlowLogs con campos de etiquetas en su formato de registro y el parámetro TagFieldSpecifications asociado en la API Consola de administración de AWS, AWS CLI, o AWS, los registros de flujo de VPC crean el rol vinculado al servicio por usted.

> **Important**
>
> Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Para obtener más información, consulte Un nuevo rol ha aparecido en mi Cuenta de AWS.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando crea CreateFlowLogs con campos de etiquetas en su formato de registro y el parámetro TagFieldSpecifications asociado, los registros de flujo de VPC crean de nuevo el rol vinculado al servicio por usted.

También puede usar la consola de IAM para crear un rol vinculado a servicios con el caso de uso AWSServiceRoleForVPCFlowLogs. En la AWS CLI o la API de AWS, cree un rol vinculado al servicio con el nombre de servicio `vpc-flow-logs.amazonaws.com`. Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Edición de un rol vinculado al servicio para los registros de flujo de VPC

Los registros de flujo de VPC no permiten que edite el rol vinculado al servicio AWSServiceRoleForVPCFlowLogs. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado al servicio para los registros de flujo de VPC

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar los recursos del rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el servicio de los registros de flujo de VPC usa el rol cuando intenta eliminar los recursos, es posible que la eliminación no se complete correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de los registros de flujo de VPC utilizados por AWSServiceRoleForVPCFlowLogs

1. Elimine todas las suscripciones a los registros de flujo de VPC que usen campos de etiquetas en el formato de registro.
2. Espere al menos una hora a que los registros de flujo de VPC procesen la eliminación de todas las suscripciones de etiquetas de la cuenta y limpien automáticamente las reglas administradas de EventBridge creadas para admitir el enriquecimiento de registros.

Eliminación manual del rol vinculado a servicios mediante IAM

Use la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado al servicio AWSServiceRoleForVPCFlowLogs. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles con roles vinculados al servicio para los registros de flujo de VPC

Los registros de flujo de VPC no admiten el uso de roles vinculados al servicio en todas las regiones en las que el servicio está disponible. Puede usar el rol AWSServiceRoleForVPCFlowLogs en las siguientes regiones.

Nombre de la región	Identidad de la región	Compatibilidad con los registros de flujo de VPC
Este de EE. UU. (Norte de Virginia)	us-east-1	Sí
Este de EE. UU. (Ohio)	us-east-2	Sí
Oeste de EE. UU. (Norte de California)	us-west-1	Sí
Oeste de EE. UU. (Oregón)	us-west-2	Sí
África (Ciudad del Cabo)	af-south-1	Sí
Asia Pacífico (Hong Kong)	ap-east-1	Sí
Asia-Pacífico (Yakarta)	ap-southeast-3	Sí
Asia-Pacífico (Mumbai)	ap-south-1	Sí
Asia-Pacífico (Osaka)	ap-northeast-3	Sí
Asia-Pacífico (Seúl)	ap-northeast-2	Sí
Asia-Pacífico (Singapur)	ap-southeast-1	Sí
Asia-Pacífico (Sídney)	ap-southeast-2	Sí
Asia-Pacífico (Tokio)	ap-northeast-1	Sí
Canadá (centro)	ca-central-1	Sí
Europa (Fráncfort)	eu-central-1	Sí
Europa (Irlanda)	eu-west-1	Sí
Europa (Londres)	eu-west-2	Sí

Nombre de la región	Identidad de la región	Compatibilidad con los registros de flujo de VPC
Europa (Milán)	eu-south-1	Sí
Europa (París)	eu-west-3	Sí
Europa (Estocolmo)	eu-north-1	Sí
Medio Oriente (Baréin)	me-south-1	Sí
Medio Oriente (EAU)	me-central-1	Sí
América del Sur (São Paulo)	sa-east-1	Sí
AWS GovCloud (US-East)	us-gov-east-1	Sí
AWS GovCloud (Oeste de EE. UU.)	us-gov-west-1	Sí

Políticas administradas de AWS para registros de flujo de VPC

Si utiliza registros de flujo de VPC y crea una suscripción con campos de etiquetas y el parámetro TagFieldSpecifications asociado, la política administrada AWSVPCFlowLogsServiceRolePolicy se crea automáticamente en la cuenta de IAM y se asocia al rol vinculado al servicio AWSServiceRoleForVPCFlowLogs.

Esta política administrada permite a los registros de flujo de VPC hacer lo siguiente:

- Crear y administrar reglas administradas de EventBridge para enviar eventos de actualización de etiquetas al servicio de registros de flujo de la VPC.
- Llamar a las API en nombre de los clientes para validar la vigencia de los valores de las etiquetas para el enriquecimiento de registros.

En el ejemplo siguiente, se muestran detalles de la política administrada que se creó.

JSON

```
{
    "Version":"2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowPutRuleOnSpecificSourcesAndDetailTypes",
            "Effect": "Allow",
            "Action": "events:PutRule",
            "Resource": [
                "arn:aws:events:*:*:rule/VPCFlowLogsEC2TagsManagedRule",
                "arn:aws:events:*:*:rule/VPCFlowLogsASGTagsManagedRule"
            ],
            "Condition": {
                "ForAllValues:StringEquals": {
                    "events:source": [
                        "aws.tag",
                        "aws.autoscaling"
                    ],
                    "events:detail-type": [
                        "AWS API Call via CloudTrail",
                        "Tag Change on Resource"
                    ]
                },
                "Null": {
                    "events:source": "false",
                    "events:detail-type": "false"
                },
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AllowOtherOperationsOnRulesManagedByVPCFlowLogs",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:DescribeRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": [
                "arn:aws:events:*:*:rule/VPCFlowLogsEC2TagsManagedRule",
                "arn:aws:events:*:*:rule/VPCFlowLogsASGTagsManagedRule"
            ],
            "Condition": {
                "StringEquals": {
```

```
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
        },
        {
            "Sid": "AllowDescribeTagsOnAllEC2Resources",
            "Effect": "Allow",
            "Action": [
                "tag:GetResources",
                "autoscaling:DescribeTags"
            ],
            "Resource": "*"
        }
    ]
}
```

La primera instrucción del ejemplo anterior permite a los registros de flujo de VPC crear reglas administradas de EventBridge en su cuenta AWS para las fuentes `aws.tag` y `aws.autoscaling` para los tipos de detalles relacionados con los eventos de cambio de etiquetas.

La segunda instrucción del ejemplo anterior permite a los registros de flujo de VPC controlar el ciclo de vida de las reglas administradas creadas en su cuenta AWS para los recursos denominados `VPCFlowLogsEC2TagsManagedRule` y/o `VPCFlowLogsASGTagsManagedRule`.

La tercera instrucción del ejemplo anterior permite a los registros de flujo de VPC llamar a las API de etiquetas en nombre de los clientes para validar la vigencia de los valores de las etiquetas a fin de enriquecer los registros.

Política administrada AWS: AWSVPCFlowLogsServiceRolePolicy

Puede asociar la política `AWSVPCFlowLogsServiceRolePolicy` a las identidades de IAM. Esta política concede permisos que permiten a los registros de flujo de VPC crear y administrar reglas administradas de EventBridge y llamar a las API DescribeTag en representación del usuario para realizar un seguimiento automático de las actualizaciones de los valores de las etiquetas de EC2 asociados a los recursos en las suscripciones de registros de flujo que incluyen campos de etiquetas.

To view the permissions for this policy, see AWSVPCFlowLogsServiceRolePolicy en la AWS Referencia de la política administrada.

Actualizaciones de la política administrada por AWS

Ver los detalles sobre las actualizaciones de las políticas administradas de AWS para los registros de flujo de VPC desde que este servicio comenzó a realizar el seguimiento de estos cambios.

Cambio	Descripción	Fecha
the section called “AWSVPCFlowLogsServiceRolePolicy ”: política nueva	La nueva política AWSVPCFlowLogsServiceRolePolicy permite a los registros de flujo de VPC crear y administrar reglas administradas de EventBridge y llamar a las API DescribeTag en representación del usuario para realizar un seguimiento automático de las actualizaciones de los valores de las etiquetas de EC2 asociados a los recursos en las suscripciones de registros de flujo que incluyen campos de etiquetas.	31 de marzo de 2026
Los registros de flujo de VPC comenzaron a realizar el seguimiento de los cambios	Los registros de flujo de VPC comenzaron a realizar el seguimiento de los cambios de sus políticas administradas de AWS.	31 de marzo de 2026

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
- El log de flujo está activo, pero no hay registros de logs de flujo ni grupo de logs
- Error 'LogDestinationNotFoundException' o 'Access Denied for LogDestination'

- Superación del límite de la política de bucket de Amazon S3
- LogDestination undeliverable
- El tamaño de los datos de los registros de flujo no coincide con los datos de facturación

Registros de logs de flujo incompletos

Problema

Sus registros de flujo están incompletos o ya no se publican.

Causa

Podría haber un problema al entregar los registros de flujo al grupo de registros de CloudWatch Logs o podría haber entradas SkipData presentes.

Solución

Consulte la pestaña Registros de flujo para la VPC, la subred o la interfaz de red. No se pueden describir los registros de flujo de una VPC o subred que se haya compartido con usted. Sin embargo, se pueden describir los registros de flujo de una interfaz de red que se cree en una VPC o subred que se haya compartido con usted. Si hay algún error, aparece en la columna Estado. Otra opción, utilice el comando describe-flow-logs y compruebe el valor devuelto en el campo `DeliverLogsErrorMessage`.

Estos son los posibles valores de error sobre el estado:

- `Rate limited`: este error se puede producir cuando el número de entradas de registro de flujo para una interfaz de red es superior al número máximo 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 Rol de IAM para publicar registros de flujo en CloudWatch Logs.

- `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

Espere 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. También puede indicar que la política de bucket no permite que los registros se envíen al bucket.
- Al crear un registro de flujo que publica datos en Registros de Amazon CloudWatch, 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 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 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.

LogDestination undeliverable

Problema

Cuando intenta crear un registro de flujo, obtiene el siguiente mensaje de error: `LogDestination <bucket name> is undeliverable`.

Causas posibles

El bucket de Amazon S3 de destino se cifra mediante el cifrado del lado del servidor con AWS KMS (SSE-KMS) y el cifrado predeterminado del bucket es un ID de la clave de KMS.

Solución

El valor debe ser un ARN de la clave de KMS. Cambie el tipo de cifrado predeterminado de S3 de ID de la clave de KMS a ARN de la clave de KMS. Para obtener más información, consulte Configuración del cifrado predeterminado en la Guía del usuario de Amazon Simple Storage Service.

El tamaño de los datos de los registros de flujo no coincide con los datos de facturación

Problema

El tamaño total de los datos de sus registros de flujo no coincide con el tamaño indicado en los datos de facturación.

Causas posibles

Es posible que haya entradas de SKIPDATA en sus registros de flujo. Consulte Registros sin datos y omitidos para obtener una explicación de las entradas de SKIPDATA.

Solución

Confirme que las entradas SKIPDATA estén presentes en sus entradas de registro consultando en sus registros distintas entradas en el campo de estado del registro.

Ejemplos de consultas para comprobar la existencia de SKIPDATA:

CW Insights:

```
fields @timestamp, @message, @logStream, @log
| filter interfaceId = 'eni-123'
| stats count(*) by interfaceId, logStatus
| sort by interfaceId, logStatus
```

Athena:

```
SELECT log_status, interface_id, count(1)
FROM vpc_flow_logs
WHERE interface_id IN ('eni-1', 'eni-2', 'eni-3')
GROUP BY log_status, interface_id
```

Métricas de CloudWatch para sus VPC

Amazon VPC publica datos sobre sus VPC en Amazon CloudWatch. Puede recuperar estadísticas sobre sus VPC como un conjunto ordenado de datos de serie temporal, denominados métricas. Una métrica es una variable que hay que supervisar y los datos son los valores de esa variable a lo largo del tiempo. Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch.

Contenido

- Dimensiones y métricas de NAU
- Habilitación o deshabilitación de la supervisión del NAU
- Ejemplo de alarma de CloudWatch para NAU

Dimensiones y métricas de NAU

Uso de direcciones de red (NAU, uso de direcciones de red) es una métrica que se aplica a los recursos de la red virtual para ayudarlo a planificar y supervisar el tamaño de su VPC. Supervisar el NAU no tiene ningún costo. El monitoreo del NAU es útil porque, si agota las cuotas de NAU o NAU emparejadas de su VPC, no podrá lanzar nuevas instancias de EC2 ni aprovisionar nuevos recursos, como los equilibradores de carga de red, los puntos de conexión de VPC las funciones de Lambda, las conexiones de puerta de enlace de tránsito o las puertas de enlace NAT.

Si ha habilitado la supervisión del uso de direcciones de red para una VPC, Amazon VPC envía las métricas relacionadas con el NAU a Amazon CloudWatch. El tamaño de una VPC se mide por la cantidad de unidades de uso de direcciones de red (NAU) que contiene la VPC.

Puede usar estas métricas para entender el ritmo de crecimiento de su VPC, pronosticar cuándo alcanzará su límite de tamaño o crear alarmas cuando se superen los umbrales de tamaño.

El espacio de nombres `AWS/EC2` incluye las siguientes métricas de supervisión de NAU.

Métrica	Descripción
`NetworkAddressUsage`	El recuento de NAU por VPC. Criterios de presentación de informes • Cada 24 horas Dimensiones • Nombre: `Per-VPC Metrics`, valor: el ID de VPC.
`NetworkAddressUsagePeered`	El recuento de NAU para la VPC y todas las VPC con las que está emparejada. Criterios de presentación de informes • Cada 24 horas Dimensiones • Nombre: `Per-VPC Metrics`, valor: el ID de VPC.

El espacio de nombres `AWS/Usage` incluye las siguientes métricas de supervisión de NAU.

Métrica	Descripción
`ResourceCount`	El recuento de NAU por VPC. Criterios de presentación de informes • Cada 24 horas Dimensiones • Nombre: `Service`, valor: `EC2`

Métrica	Descripción
	• Nombre: `Type`, valor: `Resource` • Nombre: `Resource`, valor: el ID de VPC. • Nombre: `Class`, valor: `NetworkAddressUsage`
`ResourceCount`	El recuento de NAU para la VPC y todas las VPC con las que está emparejada. Criterios de presentación de informes • Cada 24 horas Dimensiones • Nombre: `Service`, valor: `EC2` • Nombre: `Type`, valor: `Resource` • Nombre: `Resource`, valor: el ID de VPC. • Nombre: `Class`, valor: `NetworkAddressUsagePeered`
`ResourceCount`	Una vista combinada del uso de NAU en las VPC. Criterios de presentación de informes • Cada 24 horas Dimensiones • Nombre: `Service`, valor: `EC2` • Nombre: `Type`, valor: `Resource` • Nombre: `Resource`, valor: `VPC` • Nombre: `Class`, valor: `NetworkAddressUsage`

Métrica	Descripción
`ResourceCount`	Una vista combinada del uso de NAU en las VPC interconectadas. Criterios de presentación de informes • Cada 24 horas Dimensiones • Nombre: `Service`, valor: `EC2` • Nombre: `Type`, valor: `Resource` • Nombre: `Resource`, valor: `VPC` • Nombre: `Class`, valor: `NetworkAddressUsagePeered`

Habilitación o deshabilitación de la supervisión del NAU

Para ver las métricas del NAU en CloudWatch, primero debe habilitar la supervisión en cada VPC que desee supervisar.

Para habilitar o deshabilitar la supervisión del NAU

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. Seleccione Actions (Acciones), Edit VPC settings (Editar la configuración de VPC).
5. Realice una de las siguientes acciones:

   - Para habilitar la supervisión, seleccione Network mapping units metrics settings (Configuración de métricas de unidades de mapeo de red), Enable network address usage metrics (Habilitar métricas de uso de direcciones de red).
   - Para deshabilitar la supervisión, desmarque Network mapping units metrics settings (Configuración de métricas de unidades de mapeo de red), Enable network address usage metrics (Habilitar métricas de uso de direcciones de red).

Para habilitar o deshabilitar la supervisión mediante la línea de comandos

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

Ejemplo de alarma de CloudWatch para NAU

Puede usar el comando AWS CLI y el ejemplo `.json` siguientes para crear una alarma de Amazon CloudWatch y una notificación de SNS que realice un seguimiento al uso de NAU de la VPC con un umbral de 50 000 NAU. En esta muestra, es necesario crear primero un tema de Amazon SNS. Para obtener más información, consulte Introducción a Amazon SNS en la Guía para desarrolladores de Amazon Simple Notification Service.

```
aws cloudwatch put-metric-alarm --cli-input-json file://nau-alarm.json
```

A continuación se muestra un ejemplo de `nau-alarm.json`.

```
{
    "Namespace": "AWS/EC2",
    "MetricName": "NetworkAddressUsage",
    "Dimensions": [{
        "Name": "Per-VPC Metrics",
        "Value": "vpc-0123456798"
    }],
    "AlarmActions": ["arn:aws:sns:us-west-1:123456789012:my_sns_topic"],
    "ComparisonOperator": "GreaterThanThreshold",
    "Period": 86400,
    "EvaluationPeriods": 1,
    "Threshold": 50000,
    "AlarmDescription": "Tracks NAU utilization of the VPC with 50k NAUs as the
 threshold",
    "AlarmName": "VPC NAU Utilization",
    "Statistic": "Maximum"
}
```

Comprensión de los códigos de Amazon VPC en informes de facturación y de uso

Cuando usa Amazon VPC, incluimos los códigos relacionados en sus informes de facturación y de uso de AWS. La revisión de estos códigos le ayuda a entender sus costos y patrones de uso de Amazon VPC. El seguimiento y la gestión de sus gastos son esenciales para optimizar sus costos.

En las siguientes tablas, se describen los códigos de Amazon VPC que aparecen en sus informes de facturación y de uso. Para obtener una lista de los códigos de región utilizados en los informes de facturación y de uso, consulte Códigos de región para facturación de AWS.

Códigos de facturación para:

- Administración de direcciones IP
- Puntos de conexión de VPC
- Puertas de enlace de tránsito
- Análisis de redes
- Replicación de tráfico
- VPC Lattice
- Recursos entre cuentas/regiones

Recursos relacionados

- Precios de Amazon VPC
- Precios de AWS PrivateLink
- Precios de AWS Transit Gateway
- Precios de Amazon VPC Lattice

Administración de direcciones IP

Código	Descripción	Unidades	Granularity (Grado de detalle)
region-PublicIPv4:InUseAddress	El tiempo durante el cual un recurso utiliza las direcciones IPv4 públicas.	Horas	Por segundo
region-PublicIPv4:IdleAddress	El tiempo durante el cual un recurso no utiliza las direcciones IPv4 públicas.	Horas	Por segundo
region-PublicIPv4:ContiguousBlock	El uso de direcciones IPv4 públicas en un bloque de IPv4 contiguo proporcionado por Amazon.	Horas	Por hora
region-IPAddressManager-IP-Hours	El tiempo durante el cual el nivel avanzado de IPAM administra las direcciones IP.	Horas	Por hora

Puntos de conexión de VPC

Código	Descripción	Unidades	Granularity (Grado de detalle)
region-VpcEndpoint-Hours	El tiempo durante el cual se aprovisionan los puntos de conexión de VPC de la interfaz.	Horas	Por hora

Código	Descripción	Unidades	Granularity (Grado de detalle)
region-VpcEndpoint-Bytes	Los datos procesados por los puntos de conexión de VPC de la interfaz.	GB	Por hora
region-VpcEndpoint-GWLBE-Hours	El tiempo durante el cual se aprovisionan los puntos de conexión del equilibrador de carga de puerta de enlace.	Horas	Por hora
region-VpcEndpoint-GWLBE-Bytes	Los datos procesados por los puntos de conexión del equilibrador de carga de puerta de enlace.	GB	Por hora

Puertas de enlace de tránsito

Código	Descripción	Unidades	Granularity (Grado de detalle)
region-TransitGateway-Hours	El uso de conexiones de puerta de enlace de tránsito.	Horas	Por hora
region-TransitGateway-Bytes	Los datos procesados por las puertas de enlace de tránsito.	GB	Por hora

Código	Descripción	Unidades	Granularity (Grado de detalle)
region-TGW-Multicast-Consumer-Bytes	Los datos procesados por las instancias receptoras de multidifusión.	GB	Por hora

Análisis de redes

Código	Descripción	Unidades	Granularity (Grado de detalle)
region-Analysis-Runs	La cantidad de rutas de red analizadas por Reachability Analyzer.	Recuento	Por análisis
region-NetworkInterface-Assessment	La cantidad de interfaces de red analizadas por el analizador de acceso a la red.	Recuento	Por evaluación

Replicación de tráfico

Código	Descripción	Unidades	Granularity (Grado de detalle)
region-ENI-Mirror	El tiempo durante el cual una interfaz de red está configurada para la duplicación del tráfico.	Horas	Por hora

VPC Lattice

Código	Descripción	Unidades	Granularity (Grado de detalle)
region-VPCLattice-Service-Hourly	El tiempo de ejecución de los servicios de VPC Lattice.	Horas	Por hora
region-VPCLattice-DataProcessing-Bytes	Los datos procesados por los servicios de VPC Lattice.	GB	Por hora
region-VPCLattice-RequestCount-Free	Las solicitudes HTTP y las conexiones TCP gratuitas.	Recuento	Por hora
region-VpcLattice-Service-Network-Resource-Hours	El tiempo de ejecución de las redes de servicio de VPC Lattice.	Horas	Por hora

Recursos entre cuentas/regiones

Código	Descripción	Unidades	Granularity (Grado de detalle)
region-VpcResource-Provider-Bytes	Los datos transferidos desde los recursos de los proveedores entre cuentas o regiones.	GB	Por hora
region-VpcResource-Consumer-Bytes	Los datos transferidos por los recursos de consumo entre cuentas o regiones.	GB	Por hora

Descripción de la arquitectura de red de VPC

Amazon VPC le permite definir una red virtual aislada lógicamente dentro de la nube de AWS, que recibe el nombre de nube privada virtual (VPC). Cree VPC separadas para aislar la infraestructura por carga de trabajo o unidad organizativa. Puede configurar sus VPC seleccionando rangos de direcciones IP, configurando el enrutamiento y agregando puertas de enlace de red para conectar sus VPC entre sí, a Internet o a su propia red corporativa. Usted lanza recursos de AWS, como instancias de EC2 o instancias de RDS, en sus VPC.

La siguiente tabla describe las características clave de una red de VPC. Un administrador de red puede utilizar esta guía para describir la arquitectura y la configuración de su red de VPC. Disponer de esta información les permite configurar una red funcionalmente equivalente en las instalaciones o mediante otro proveedor de nube.

Característica	Descripción
Ubicación geográfica	Amazon VPC está alojado en todas las regiones de AWS del mundo. Puede seleccion

Característica	Descripción
	ar las regiones para su red de VPC que acerquen los recursos de AWS a sus clientes.
Subredes	Las subredes que defina para sus VPC definen los límites de la red y determinan las direcciones IP de sus recursos de AWS. Puede agregar subredes en varias zonas de disponibilidad para aumentar la disponibilidad de los recursos.
Conectividad de red	Las puertas de enlace que debe conectar a las VPC o subredes para proporcionar conectividad entre la red de VPC y otras redes, como otras VPC o subredes, Internet o las redes en las instalaciones.
Controles de seguridad	Los grupos de seguridad que cree para sus VPC controlan el tráfico hacia y desde los recursos asociados, como los recursos informáticos, los recursos de bases de datos y los equilibradores de carga. Cada subred tiene una ACL de red que controla el tráfico entrante y saliente de la subred.
Administración del tráfico	Las reglas de enrutamiento controlan el flujo de tráfico entre las subredes, las VPC y las ubicaciones externas. Los equilibradores de carga proporcionados por Elastic Load Balancing distribuyen el tráfico entrante entre varios destinos, como instancias de EC2, contenedores y funciones de Lambda.

Ubicación geográfica

Amazon VPC está disponible en todas las regiones de AWS del mundo. Cada región es un área geográfica independiente. Puede reducir la latencia de la red al crear VPC para sus recursos en regiones cercanas a la mayoría de sus usuarios.

Puede utilizar Amazon EC2 Global View para enumerar las VPC en todas las regiones mediante una interfaz gráfica de usuario (no hay una interfaz de programación equivalente). Con la consola de Amazon VPC, la API de AWS y las interfaces de línea de comandos de AWS, debe enumerar las VPC y los recursos de VPC de cada región de forma individual.

Por qué es importante

Una vez que determine dónde están ubicadas sus VPC, puede decidir si desea configurar una red funcionalmente equivalente en las mismas ubicaciones o en ubicaciones diferentes, según sus necesidades.

Obtención de un resumen de sus VPC en todas las regiones

1. Abra la consola de Amazon EC2 Global View en https://console.aws.amazon.com/ec2globalview/home.
2. En la pestaña Region explorer (Explorador de regiones), en Summary (Resumen), compruebe el recuento de recursos de las VPC, que incluye la cantidad de VPC y la cantidad de regiones. Esto incluye tanto las VPC predeterminadas que crea AWS en su nombre como las VPC no predeterminadas que usted crea. Elija el texto subrayado para ver cómo se distribuye el recuento de VPC entre regiones. Si una región tiene solo una VPC, lo más probable es que sea la predeterminada de la región.
3. En la pestaña Búsqueda global (Global search), seleccione el filtro de cliente Resource type = Vpc (Tipo de recurso = Vpc). Puede filtrar aún más los resultados especificando una región o una etiqueta.

Obtención de las VPC de una región mediante la AWS CLI

Utilice el siguiente comando describe-images. Debe ejecutarlo en cada región en la que tenga VPC. El parámetro `--query` solo incluye los ID de la VPC en la salida. Puede incluir cualquier campos adicionales según sea necesario.

```
aws ec2 describe-vpcs \
```

```
    --region us-east-2 \
    --query "Vpcs[*].VpcId"
```

Cada región incluye una VPC predeterminada. Si no utiliza las VPC predeterminadas, puede excluirlas de los resultados añadiendo el siguiente filtro.

```
--filters Name=is-default,Values=false
```

Subredes

Una subred es un límite de red lógico en una VPC. Al crear una subred, asigna un bloque de direcciones IP. A los recursos que lanza a una subred se les asignan direcciones IP del bloque de direcciones IP de la subred. Las direcciones IP permiten que los recursos se comuniquen entre sí a través de una red local o Internet.

El mapa de recursos de la consola de Amazon VPC proporciona una representación visual de las subredes de la VPC.

Por qué son importantes

Las subredes permiten a los administradores de red implementar límites de seguridad y controlar el tráfico entre los niveles de aplicaciones. Al anotar las direcciones IP de las subredes, puede ayudar a garantizar que los recursos en una red funcionalmente equivalente puedan comunicarse con los mismos clientes o aplicaciones que en su red de VPC.

Visualización de las subredes de una VPC mediante el mapa de recursos

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 casilla de verificación de la VPC.
4. Elija la pestaña Resource map (Mapa de recursos).
5. En el panel de VPC, seleccione Show details (Mostrar detalles). En el panel Subnets (Subredes), se presentan todas las subredes de la VPC y sus rangos de direcciones IP. Coloque el cursor sobre una subred para resaltar la tabla de enrutamiento y las conexiones de red asociadas. Para obtener más información, elija el enlace para abrir la página de detalles de la subred.

Descripción de las subredes de una VPC mediante la AWS CLI

Utilice el siguiente comando describe-subnets. El parámetro `--filters` abarca la búsqueda para describir las subredes de la VPC especificada. El parámetro `--query` solo incluye los campos especificados en la salida. Puede incluir cualquier campos adicionales según sea necesario.

```
aws ec2 describe-subnets \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query Subnets[*].
[SubnetId,AvailabilityZoneId,CidrBlock,Ipv6CidrBlockAssociationSet[0].Ipv6CidrBlock] \
    --output table
```

A continuación, se muestra un ejemplo del resultado. Las columnas son el ID de la subred, el ID de la zona de disponibilidad, el rango de direcciones IPv4 y el primer rango de direcciones IPv6 (si lo hubiera).

```
-------------------------------------------------------------------------------
|                                DescribeSubnets                              |
+--------------------------+-----------+---------------+--------------------------+
|  subnet-0d2d1b81e0bc9c6d4 |  usw2-az1 |  10.0.144.0/20 |  2600:1f14:1e6e:a003::/64  |
|  subnet-0e01d500780bb7468 |  usw2-az1 |  10.0.16.0/20  |  2600:1f14:1e6e:a001::/64  |
|  subnet-0eb17d85f5dfd33b1 |  usw2-az2 |  10.0.128.0/20 |  2600:1f14:1e6e:a002::/64  |
|  subnet-0e990c67809773b19 |  usw2-az2 |  10.0.0.0/20   |  2600:1f14:1e6e:a000::/64  |
+--------------------------+-----------+---------------+--------------------------+
```

La conectividad de red

Las opciones de conectividad que ofrece Amazon VPC le permiten crear una red que abarque las VPC de varias cuentas y regiones y redes remotas.

Puede utilizar el mapa de recursos de la consola de Amazon VPC para descubrir si sus VPC utilizan puertas de enlace de Internet, puertas de enlace de Internet de solo salida, puertas de enlace NAT o puntos de conexión de VPC de las puertas de enlace. El mapa de recursos no muestra ninguna puerta de enlace de tránsito, conexión de pares, puerta de enlace privada virtual ni ningún otro tipo de punto de conexión de VPC que esté en uso. Puede obtener la lista completa de puertas de enlace y conexiones de red de una VPC describiéndolas mediante la consola, la API o una interfaz de línea de comando de un tipo a la vez.

Por qué es importante

Una vez que comprenda la conectividad que proporciona su red de VPC, puede asegurarse de que los recursos de una red funcionalmente equivalente puedan comunicarse con los mismos recursos locales y remotos.

Visualización de las conexiones de red de una VPC mediante el mapa de recursos

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 casilla de verificación de la VPC.
4. Elija la pestaña Resource map (Mapa de recursos).
5. En el panel de VPC, seleccione Show details (Mostrar detalles). En el panel Network connections (Conexiones de red), se presentan las puertas de enlace de Internet, las puertas de enlace de Internet de solo salida, las puertas de enlace NAT y los puntos de conexión de VPC de las puertas de enlace. Si el tipo de recurso no está claro, coloque el cursor sobre el icono de enlace de la conexión de red y examine la URL resultante. Esta URL es un enlace al recurso en la consola y contiene el tipo y el ID del recurso (por ejemplo, internetGatewayId=igw-0123456780abcdef).

Obtención de las conexiones de red de sus VPC mediante la AWS CLI

1. Utilice el comando describe-internet-gateways para obtener las puertas de enlace de Internet de la región especificada. El parámetro `--query` solo incluye los campos especificados en la salida. Puede incluir cualquier campos adicionales según sea necesario.

```
aws ec2 describe-internet-gateways \
    --region us-east-2 \
    --query InternetGateways[*].[Attachments[0].VpcId,InternetGatewayId] \
    --output table
```

   A continuación, se muestra un ejemplo del resultado. Las columnas muestran los ID de la VPC y los ID de la puerta de enlace de Internet.

```
-------------------------------------------------------
|             DescribeInternetGateways              |
+-------------------------+-------------------------+
|  None                   |  igw-04c61dba10EXAMPLE  |
|  vpc-0bf4c2739bEXAMPLE  |  igw-09737a4029EXAMPLE  |
|  vpc-060415a18fEXAMPLE  |  igw-0c562bd22aEXAMPLE  |
```

```
|  vpc-0ea9d41094EXAMPLE |  igw-0e06f7033dEXAMPLE  |
|  vpc-03b86de356EXAMPLE |  igw-0a9ff72d05EXAMPLE  |
+------------------------+-------------------------+
```

2. Utilice el comando describe-egress-only-internet-gateways para obtener las puertas de enlace de Internet de solo salida de la región especificada. El parámetro `--query` solo incluye los campos especificados en la salida. Puede incluir cualquier campos adicionales según sea necesario.

```
aws ec2 describe-egress-only-internet-gateways \
    --region us-east-2 \
    --query EgressOnlyInternetGateways[*].
[Attachments[0].VpcId,EgressOnlyInternetGatewayId] \
    --output table
```

A continuación, se muestra un ejemplo del resultado. Las columnas muestran los ID de la VPC y los ID de las puertas de enlace de Internet de solo salida.

```
-----------------------------------------------------
|        DescribeEgressOnlyInternetGateways         |
+------------------------+--------------------------+
|  vpc-060415a18fEXAMPLE |  eigw-0b8ca558acEXAMPLE  |
+------------------------+--------------------------+
```

3. Utilice el comando describe-nat-gateways para obtener las puertas de enlace NAT de la región especificada. El parámetro `--query` solo incluye los campos especificados en la salida. Puede incluir cualquier campos adicionales según sea necesario.

```
aws ec2 describe-nat-gateways \
    --region us-east-2 \
    --query NatGateways[*].[VpcId,NatGatewayId,SubnetId] \
    --output table
```

A continuación, se muestra un ejemplo del resultado. Las columnas muestran los ID de la VPC, los ID de la puerta de enlace NAT y los ID de la subred.

```
-------------------------------------------------------------------------------
|                            DescribeNatGateways                              |
+------------------------+-------------------------+---------------------------+
|  vpc-060415a18fEXAMPLE |  nat-026316334aEXAMPLE  |  subnet-0eb17d85f5EXAMPLE  |
```

```
|  vpc-060415a18fEXAMPLE |  nat-0f08bc5f52EXAMPLE  |  subnet-0d2d1b81e0EXAMPLE  |
+------------------------+-------------------------+----------------------------+
```

4. Utilice el comando describe-transit-gateway-vpc-attachments para obtener los adjuntos de VPC de la puerta de enlace de tránsito de la región especificada. El parámetro `--query` solo incluye los campos especificados en la salida. Puede incluir cualquier campos adicionales según sea necesario.

```
aws ec2 describe-transit-gateway-vpc-attachments \
    --region us-east-2 \
    --query TransitGatewayVpcAttachments[*].
[VpcId,TransitGatewayId,length(SubnetIds[])] \
    --output table
```

A continuación, se muestra un ejemplo del resultado. Las columnas muestran los ID de la VPC, los ID de las puertas de enlace de tránsito y el recuento de subredes.

```
-------------------------------------------------------
|         DescribeTransitGatewayVpcAttachments          |
+------------------------+------------------------+----+
|  vpc-0bf4c2739bEXAMPLE |  tgw-055dc4e47bEXAMPLE  |  4 |
|  vpc-0ea9d41094EXAMPLE |  tgw-055dc4e47bEXAMPLE  |  2 |
+------------------------+------------------------+----+
```

5. Utilice el comando describe-vpc-peering-connections para obtener las conexiones de emparejamiento de las VPC de la región especificada. El parámetro `--query` solo incluye los campos especificados en la salida. Puede incluir cualquier campos adicionales según sea necesario.

```
aws ec2 describe-vpc-peering-connections \
    --region us-east-2 \
    --query VpcPeeringConnections[*].[AccepterVpcInfo.VpcId,RequesterVpcInfo.VpcId]
 \
    --output table
```

A continuación, se muestra un ejemplo del resultado. Las columnas muestran los ID de las VPC que aceptan, los propietarios de las VPC que aceptan, los ID de las VPC que solicitan y los propietarios de las VPC que solicitan.

```
-------------------------------------------------------------------------------
```

```
|                          DescribeVpcPeeringConnections
 |
+-------------------------+--------------+-------------------------+---------------
+
|  vpc-0ea9d41094EXAMPLE |  123456789012 |  vpc-03b86de356EXAMPLE |  123456789012
 |
+-------------------------+--------------+-------------------------+---------------
+
```

6. Use el comando describe-vpn-gateways para obtener las puertas de enlace privadas virtuales de la región especificada. El parámetro `--query` solo incluye los campos especificados en la salida. Puede incluir cualquier campos adicionales según sea necesario.

```
aws ec2 describe-vpn-gateways \
    --region us-east-2 \
    --query VpnGateways[*].[VpcAttachments[0].VpcId,VpnGatewayId] \
    --output table
```

A continuación, se muestra un ejemplo del resultado. Las columnas muestran los ID de la VPC y los ID de puerta de enlace privada virtual.

```
-------------------------------------------------
|               DescribeVpnGateways             |
+-------------------------+-----------------------+
|  vpc-0bf4c2739bEXAMPLE |  vgw-0cb3226c4aEXAMPLE  |
+-------------------------+-----------------------+
```

7. Utilice el comando describe-vpc-endpoints para obtener los puntos de enlace de VPC de la región especificada. El parámetro `--query` solo incluye los campos especificados en la salida. Puede incluir cualquier campos adicionales según sea necesario.

```
aws ec2 describe-vpc-endpoints \
    --region us-east-2 \
    --query 'VpcEndpoints[*].[VpcId,VpcEndpointType,ServiceName||
ServiceNetworkArn||ResourceConfigurationArn]' \
    --output table
```

A continuación, se muestra un ejemplo del resultado. La primera columna muestra el ID de la VPC, y la segunda columna muestra el tipo de punto de conexión de VPC. La tercera columna depende del tipo de punto de conexión y muestra el nombre del servicio, el ARN de la configuración del recurso o el ARN de la red de servicio.

```
----------------------------------------------------------------------------------------
|                                                    DescribeVpcEndpoints
                                                 |
+------------------------+-----------------
+-------------------------------------------------------------------------------------
+
|  vpc-060415a18fcc9afde |  Interface      |  com.amazonaws.vpce.us-west-2.vpce-
svc-007832a03d60fc387                                |
|  vpc-060415a18fcc9afde |  Interface      |  com.amazonaws.vpce.us-west-2.vpce-
svc-007832a03d60fc387                                |
|  vpc-0bf4c2739bc05a694 |  Gateway        |  com.amazonaws.us-west-2.s3
                                                 |
|  vpc-0ea9d410947d27b7d |  Interface      |  com.amazonaws.us-west-2.logs
                                                 |
|  vpc-0bf4c2739bc05a694 |  Resource       |  arn:aws:vpc-lattice:us-
east-2:123456789012:resourceconfiguration/rcfg-07129f3acded87625  |
|  vpc-0bf4c2739bc05a694 |  ServiceNetwork |  arn:aws:vpc-lattice:us-
east-2:123456789012:servicenetwork/sn-0808d1748faee0c1e           |
|  vpc-0bf4c2739bc05a694 |  ServiceNetwork |  arn:aws:vpc-lattice:us-
east-2:123456789012:servicenetwork/sn-0808d1748faee0c1e           |
+------------------------+-----------------
+-------------------------------------------------------------------------------------
+
```

Controles de seguridad

Los controles de seguridad proporcionados por Amazon VPC determinan el acceso de red a sus VPC y los recursos desplegados allí.

Por qué es importante

Después de determinar el tráfico entrante permitido para llegar a sus subredes y recursos y el tráfico de salida permitido para dejar sus subredes y recursos, puede planificar las reglas de firewall necesarias para una red funcionalmente equivalente.

Controles de seguridad

- Grupos de seguridad
- ACL de red

Grupos de seguridad

Un grupo de seguridad permite el tráfico entrante y saliente específico a nivel de recursos. Los grupos de seguridad son el mecanismo principal para controlar el acceso a los recursos de su VPC.

Obtención de grupos de seguridad para sus VPC

Utilice el comando describe-security-groups para mostrar los grupos de seguridad de la VPC especificada.

```
aws ec2 describe-security-groups \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query SecurityGroups[*].GroupId
```

Obtención de reglas de entrada para un grupo de seguridad

Utilice el comando describe-security-group-rules para mostrar las reglas del grupo de seguridad especificado, donde `IsEgress` es `false`.

```
aws ec2 describe-security-group-rules \
    --filters Name=group-id,Values=sg-0abcdef1234567890 \
    --query 'SecurityGroupRules[?IsEgress==`false`]'
```

Obtención de reglas de salida para un grupo de seguridad

Utilice el comando describe-security-group-rules para mostrar las reglas del grupo de seguridad especificado, donde `IsEgress` es `true`.

```
aws ec2 describe-security-group-rules \
    --filters Name=group-id,Values=sg-0abcdef1234567890 \
    --query 'SecurityGroupRules[?IsEgress==`true`]'
```

ACL de red

Una lista de control de acceso (ACL) de red permite o deniega el tráfico entrante y saliente específico en el nivel de subred. Puede utilizar las ACL de red como defensa en profundidad en caso de que un recurso se implemente sin el grupo de seguridad correcto.

Obtención de las ACL de red para sus subredes

Utilice el comando describe-network-acls para mostrar las ACL de red para la VPC especificada y sus asociaciones de subredes.

```
aws ec2 describe-network-acls \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query "NetworkAcls[*].{ID:NetworkAclId,Subnets:Associations[].SubnetId}"
```

Obtención de las reglas de entrada para una ACL de red

Utilice el comando describe-network-acls para mostrar las reglas de la ACL de red especificada, donde `Egress` es `false`.

```
aws ec2 describe-network-acls \
    --network-acl-ids acl-0abcdef1234567890 \
    --query 'NetworkAcls[*].Entries[?Egress==`false`]'
```

Obtención de las reglas de salida para una ACL de red

Utilice el comando describe-network-acls para mostrar las reglas de la ACL de red especificada, donde `Egress` es `true`.

```
aws ec2 describe-network-acls \
    --network-acl-ids acl-0abcdef1234567890 \
    --query 'NetworkAcls[*].Entries[?Egress==`true`]'
```

Administración del tráfico

La administración eficaz del tráfico combina las decisiones de enrutamiento a nivel de red proporcionadas por las tablas de enrutamiento con las estrategias de distribución a nivel de aplicación proporcionadas por el equilibrio de carga.

Por qué es importante

Los administradores de red deben diseñar subredes, enrutamiento, resolución DNS y equilibrador de carga para optimizar el flujo de tráfico, al mismo tiempo que mantienen los límites de seguridad y requisitos de rendimiento. Al observar la configuración de estos componentes en la red de VPC, puede garantizar que los recursos de una red funcionalmente equivalente se comuniquen con los mismos clientes o dispositivos que en la red de VPC.

Administración del tráfico

- Tablas de enrutamiento
- Conjunto de opciones de DHCP
- Equilibradores de carga

Tablas de enrutamiento

Las tablas de enrutamiento determinan cómo fluye el tráfico de red a través de los límites de la red, como las subredes, las VPC, las redes en las instalaciones e Internet.

El mapa de recursos de la consola de Amazon VPC proporciona una representación visual de las tablas de enrutamiento de la VPC.

Visualización de las tablas de enrutamiento de una VPC mediante el mapa de recursos

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 casilla de verificación de la VPC.
4. Elija la pestaña Resource map (Mapa de recursos).
5. En el panel Route tables (Tablas de enrutamiento), se presentan todas las tablas de enrutamiento de la VPC. Coloque el cursor sobre una tabla de enrutamiento para resaltar las subredes y las conexiones de red asociadas. Para obtener más información, elija el enlace para abrir la página de detalles de la tabla de enrutamiento.

Para describir las tablas de enrutamiento

Use el comando describe-route-tables para describir las tablas de enrutamiento de la VPC especificada y sus asociaciones de subred.

```
aws ec2 describe-route-tables \
    --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
    --query "RouteTables[*].{ID:RouteTableId,Subnets:Associations[].SubnetId}"
```

Obtención de las rutas de una tabla de enrutamiento

Use el comando describe-route-tables para describir las rutas de la tabla de enrutamiento especificada.

```
aws ec2 describe-route-tables \
```

```
    --route-table-ids rtb-02ec01715bEXAMPLE \
    --query RouteTables[*].Routes
```

Conjunto de opciones de DHCP

La VPC posee un conjunto de opciones de DHCP para configurar diversos ajustes de red. Por ejemplo, los servidores DNS personalizados se pueden configurar para que las instancias EC2 resuelvan los nombres de host internos con la infraestructura de DNS existente. Para obtener más información, consulte the section called “Conceptos de conjuntos de opciones de DHCP”.

Para describir las opciones de DHCP para la VPC

Use el comando describe-dhcp-options para describir las opciones de DHCP especificadas. El ejemplo también obtiene el ID de las opciones de DHCP para la VPC especificada con el comando describe-vpcs.

```
aws ec2 describe-dhcp-options \
    --dhcp-options-id "$(aws ec2 describe-vpcs \
        --vpc-id vpc-1234567890abcdef0 \
        --query Vpcs[].DhcpOptionsId --output text)"
```

A continuación, se muestra un ejemplo de salida para una VPC que usa las opciones de DHCP que vienen por defecto.

```
{
    "DhcpOptions": [
        {
            "OwnerId": "415546850671",
            "Tags": [],
            "DhcpOptionsId": "dopt-1234567890abcdef0",
            "DhcpConfigurations": [
                {
                    "Key": "domain-name",
                    "Values": [
                        {
                            "Value": "us-west-2.compute.internal"
                        }
                    ]
                },
                {
                    "Key": "domain-name-servers",
```

```
                    "Values": [
                        {
                            "Value": "AmazonProvidedDNS"
                        }
                    ]
                }
            ]
        }
    ]
}
```

Equilibradores de carga

El equilibrador de carga distribuye el tráfico entrante de los clientes entre varios destinos. Los equilibradores de carga supervisan el estado de los destinos y eliminan automáticamente los que no están en buen estado de la distribución del tráfico, lo que garantiza que solo se utilicen destinos en buen estado. Esto mejora la disponibilidad y el rendimiento de sus aplicaciones para optimizar el uso de los recursos. Para obtener más información, consulte la Guía del usuario de Elastic Load Balancing.

Para describir sus equilibradores de carga

Use el comando describe-load-balancers para mostrar los equilibradores de carga de la VPC especificada.

```
aws elbv2 describe-load-balancers \
    --query 'LoadBalancers[?VpcId==`vpc-1234567890abcdef0`].LoadBalancerArn'
```

Recursos relacionados

Los siguientes son servicios o características opcionales que podría estar utilizando en su red de VPC:

- Direct Connect
- AWS Network Firewall
- IPAM
- Replicación de tráfico
- Logs de flujo de VPC

Administración de las responsabilidades de seguridad para Amazon Virtual Private Cloud

La seguridad en la nube de AWS es la máxima prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida aborda tanto la seguridad de la nube como la 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 AWSProgramas 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 viene determinada por 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 vigentes.

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

- Garantice de la protección de datos en Amazon Virtual Private Cloud
- Aplicación del cifrado del tráfico en tránsito en VPC
- Identity and Access Management para Amazon VPC
- Seguridad de la infraestructura en Amazon VPC
- Controlar el tráfico hacia los recursos de AWS mediante grupos de seguridad
- Control del tráfico de la subred con listas de control de acceso a la red
- Resiliencia en Amazon Virtual Private Cloud
- Validación de conformidad para Amazon Virtual Private Cloud

- Bloqueo de acceso público de las VPC y subredes
- Prácticas recomendadas de seguridad de la VPC

Garantice de la 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. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de datos, consulte Preguntas frecuentes sobre la privacidad de datos. Para obtener más información sobre la protección de datos en Europa, consulte el Centro del Reglamento General de Protección de Datos (RGPD).

Con fines de protección de datos, recomendamos proteger las credenciales de la Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Utiliza SSL/TLS para comunicarse con los recursos de AWS. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure los registros de API y de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre cómo utilizar registros de seguimiento de CloudTrail para capturar actividades de AWS, consulte Working with CloudTrail trails en la Guía del usuario de AWS CloudTrail.
- Utiliza las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-3 al acceder a AWS a través de una interfaz de la línea de comandos o una API, utiliza un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Amazon VPC u otros Servicios de AWS mediante la consola, la API, la AWS CLI o los SDK de AWS. Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Garantice la privacidad del tráfico entre redes en Amazon VPC

Amazon Virtual Private Cloud ofrece características que puede utilizar para aumentar y supervisar la seguridad de la nube privada virtual (VPC):

- Grupos de seguridad: los grupos de seguridad permiten el tráfico entrante y saliente específico a nivel de recursos (como una instancia de EC2). Cuando lanza una instancia, puede asociarla a uno o varios grupos de seguridad. 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, se asocia automáticamente al grupo de seguridad predeterminado de la VPC. Para obtener más información, consulte Grupos de seguridad.
- Listas de control de acceso (ACL) de red: las ACL de red permiten o deniegan el tráfico entrante y saliente específico en el ámbito de la subred. Para obtener más información, consulte Control del tráfico de la subred con listas de control de acceso a la red.
- 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 ayudarlo 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.
- 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.

Aplicación del cifrado del tráfico en tránsito en VPC

Controles de cifrado de VPC es una característica de seguridad y cumplimiento que proporciona un control centralizado y autorizado para supervisar el estado de cifrado de los flujos de tráfico, ayuda a identificar recursos que permiten comunicaciones en texto sin cifrar y ofrece mecanismos para aplicar el cifrado del tráfico en tránsito dentro de las VPC y entre ellas en una región.

Controles de cifrado de VPC usa tanto cifrado en la capa de aplicación como la capacidad integrada de cifrado en tránsito del hardware del sistema Nitro de AWS para garantizar la aplicación del cifrado. Esta característica también extiende el cifrado nativo a nivel de hardware, más allá de las instancias modernas basadas en Nitro, a otros servicios de AWS, incluidos Fargate, Equilibrador de carga de aplicación, Transit Gateway y muchos otros.

La característica está diseñada para cualquier persona que desee garantizar visibilidad y control sobre el estado de cifrado de todo su tráfico. Resulta especialmente útil en sectores donde el cifrado de datos es fundamental para cumplir estándares normativos como HIPAA, FedRAMP y PCI DSS. Los administradores de seguridad y los arquitectos en la nube pueden usarla para aplicar de forma centralizada políticas de cifrado del tráfico en tránsito en todo su entorno de AWS.

Esta característica se puede utilizar en dos modos: modo de supervisión y modo de aplicación obligatoria.

Modos de control de cifrado

Modo monitoreado

En modo de supervisión, Controles de cifrado proporciona visibilidad sobre el estado de cifrado de los flujos de tráfico entre los recursos de AWS, tanto dentro de una VPC como entre VPC. También ayuda a identificar recursos de VPC que no aplican el cifrado del tráfico en tránsito. Puede configurar los registros de flujo de VPC para que emitan el campo enriquecido `encryption-status`, que indica si el tráfico está cifrado. También puede usar la consola o el comando `GetVpcResourcesBlockingEncryptionEnforcement` para identificar los recursos que no aplican el cifrado del tráfico en tránsito.

> **Note**
>
> Las VPC existentes solo se pueden habilitar inicialmente en modo de supervisión. Esto proporciona visibilidad sobre los recursos que permiten o podrían permitir tráfico en texto

sin cifrar. Solo puede activar el modo de aplicación obligatoria en la VPC una vez que estos recursos comiencen a aplicar el cifrado (o cuando cree exclusiones para ellos).

Modo de aplicación obligatoria

En el modo de aplicación obligatoria, los controles de cifrado de VPC impiden el uso de cualquier característica o servicio que permita tráfico sin cifrar dentro del límite de la VPC. No puede habilitar los controles de cifrado de VPC en el modo de aplicación obligatoria directamente en las VPC existentes. Primero debe activar los controles de cifrado de VPC en el modo de supervisión, identificar y modificar los recursos que no cumplan los requisitos para aplicar el cifrado en tránsito y, a continuación, activar el modo de aplicación obligatoria. Sin embargo, puede habilitar los controles de cifrado de VPC en el modo de aplicación obligatoria para VPC nuevas durante su creación.

Cuando está habilitado, el modo de aplicación obligatoria impide crear o asociar recursos de VPC sin cifrar, como instancias de EC2 antiguas que no admiten cifrado nativo integrado o puertas de enlace de Internet, entre otros. Si desea ejecutar un recurso que no cumple los requisitos en una VPC con cifrado aplicado, debe crear una exclusión para ese recurso.

Supervisión del estado de cifrado de los flujos de tráfico

Puede auditar el estado de cifrado de los flujos de tráfico dentro de la VPC mediante el campo `encryption-status` en los registros de flujo de la VPC. Puede tener los siguientes valores:

- `0` = sin cifrar
- `1` = cifrado con Nitro (administrado por Controles de cifrado de VPC)
- `2` = cifrado a nivel de aplicación
  - flujos en el puerto TCP 443 para un punto de conexión de interfaz a un servicio de AWS *
  - flujos en el puerto TCP 443 para puntos de conexión de puerta de enlace *
  - flujos hacia un clúster de Redshift cifrado a través de un punto de conexión de VPC **
- `3` = cifrados tanto con Nitro como a nivel de aplicación
- `(-)` = estado de cifrado desconocido o Controles de cifrado de VPC desactivados

Nota:

* En el caso de los puntos de conexión de interfaz y de puerta de enlace, AWS no examina los datos de los paquetes para determinar el estado de cifrado; en su lugar, se basa en el puerto utilizado para inferir el estado de cifrado.

** Para los puntos de conexión administrados por AWS especificados, AWS determina el estado de cifrado en función del requisito de TLS en la configuración del servicio.

Limitaciones de los registros de flujo de VPC

- Para habilitar los registros de flujo para Controles de cifrado de VPC, debe crear manualmente registros de flujo nuevos que incluyan el campo de estado de cifrado. El campo de estado de cifrado no se agrega automáticamente a los registros de flujo existentes.
- Se recomienda agregar los campos ${traffic-path} y ${flow-direction} a los registros de flujo para obtener información más detallada.

  Ejemplo:

```
aws ec2 create-flow-logs \
--resource-type VPC \
--resource-ids vpc-12345678901234567 \
--traffic-type ALL \
--log-group-name my-flow-logs \
--deliver-logs-permission-arn arn:aws:iam::123456789101:role/publishFlowLogs
--log-format '${encryption-status} ${srcaddr} ${dstaddr} ${srcport} ${dstport}
 ${protocol} ${traffic-path} ${flow-direction} ${reject-reason}'
```

Exclusiones de Controles de cifrado de VPC

El modo de aplicación obligatoria de los controles de cifrado de VPC requiere que todos los recursos de la VPC apliquen el cifrado. Esto garantiza el cifrado dentro de AWS en una región. Sin embargo, puede tener recursos como puerta de enlace de Internet, puerta de enlace NAT o puerta de enlace privada virtual que permiten conectividad fuera de las redes de AWS, donde deberá asumir la responsabildiad de configurar y mantener el cifrado de extremo a extremo. Para ejecutar estos recursos en VPC con cifrado aplicado, puede crear exclusiones de recursos. Una exclusión crea una excepción auditable para los recursos en los que el cliente es responsable de mantener el cifrado (por lo general, en la capa de aplicación).

Solo hay 8 exclusiones compatibles con Controles de cifrado de VPC. Si tiene estos recursos en la VPC y desea pasar al modo de aplicación obligatoria, debe agregar estas exclusiones al cambiar

del modo de supervisión al modo de aplicación obligatoria. No se puede excluir ningún otro recurso. Puede migrar la VPC al modo de aplicación obligatoria mediante la creación de exclusiones para estos recursos. Debe encargarse de garantizar el cifrado de los flujos de tráfico hacia y desde estos recursos

- Puerta de enlace de Internet
- Puerta de enlace NAT
- Puerta de enlace de Internet solo de salida
- Conexiones de emparejamiento de VPC con VPC en las que no se aplica el cifrado (consulte la sección de compatibilidad de emparejamiento de VPC para ver escenarios detallados)
- Puerta de enlace privada virtual
- Funciones de Lambda dentro de la VPC
- VPC Lattice
- Elastic File System

Flujo de trabajo de implementación

1. Habilitar la supervisión: cree un control de cifrado de VPC en modo de supervisión
2. Analizar el tráfico: revise los registros de flujo para supervisar el estado de cifrado de los flujos de tráfico
3. Analizar recursos: use la consola o el comando `GetVpcResourcesBlockingEncryptionEnforcement` para identificar los recursos que no aplican el cifrado del tráfico en tránsito.
4. Preparación [opcional]: planifique las migraciones de recursos y las exclusiones necesarias si desea activar el modo de aplicación obligatoria
5. Aplicación obligatoria [opcional]: cambie al modo de aplicación obligatoria con las exclusiones necesarias configuradas
6. Auditoría: supervisión continua del cumplimiento mediante los registros de flujo

Para obtener instrucciones detalladas de configuración, consulte el blog Introducción a los controles de cifrado de VPC: aplicar el cifrado del tráfico en tránsito dentro de las VPC y entre ellas en una región

Estados de Controles de cifrado de VPC

Los Controles de cifrado de VPC se pueden encontrar en uno de los siguientes estados:

crear

Los Controles de cifrado de VPC están en proceso de ser creados en la VPC.

modify-in-progress

Los Controles de cifrado de VPC están en proceso de ser modificados en la VPC

deleting

Los Controles de cifrado de VPC están en proceso de ser eliminados en la VPC

available

Los controles de cifrado de VPC se implementaron correctamente en la VPC en el modo de supervisión o en el modo de aplicación obligatoria

AWSSoporte y compatibilidad con servicios de

Para cumplir los requisitos de cifrado, un recurso debe aplicar siempre el cifrado del tráfico en tránsito, ya sea a nivel de hardware o a nivel de aplicación. Para la mayoría de los recursos, no se requiere ninguna acción por su parte.

Servicios con cumplimiento automático

La mayoría de los servicios de AWS compatibles con PrivateLink, incluidos los PrivateLink entre regiones, aceptan tráfico cifrado a nivel de aplicación. No es necesario que realice ningún cambio en estos recursos. AWS descarta automáticamente cualquier tráfico que no esté cifrado a nivel de aplicación. Algunas excepciones incluyen los clústeres de Redshift (tanto aprovisionados como sin servidor), en los que debe migrar manualmente los recursos subyacentes.

Recursos que se migran automáticamente

Los equilibradores de carga de red, equilibradores de carga de aplicaciones, los clústeres de Fargate y el plano de control de EKS se migran automáticamente a hardware que admite cifrado de forma nativa una vez que se habilita el modo de supervisión. No es necesario que modifique estos recursos. AWS se encarga de la migración automáticamente.

Recursos que requieren migración manual

Determinados recursos y servicios de VPC requieren que seleccione los tipos de instancia subyacentes. Todas las instancias modernas de EC2 admiten el cifrado del tráfico en tránsito No es necesario que realice ningún cambio si los servicios ya usan instancias modernas de EC2. Puede usar la consola o el comando GetVpcResourcesBlockingEncryptionEnforcement para identificar si alguno de estos servicios usa instancias anteriores. Si identifica recursos de este tipo, debe actualizarlos a instancias modernas de EC2 que admitan cifrado nativo del hardware del sistema Nitro. Estos servicios incluyen instancias de EC2, grupos de escalado automático, RDS (todas las bases de datos y Amazon DocumentDB), ElastiCache aprovisionado, clústeres aprovisionados de Amazon Redshift, EKS, ECS en EC2, OpenSearch aprovisionado y EMR.

Recursos compatibles:

Los siguientes recursos son compatibles con Controles de cifrado de VPC:

- Instancias de EC2 basadas en Nitro
- Equilibradores de carga de red (con limitaciones)
- Equilibradores de carga de aplicación
- AWSClústeres de Fargate
- Amazon Elastic Kubernetes Service (EKS)
- Grupos de Amazon EC2 Auto Scaling
- Amazon Relational Database Service (RDS) (todas las bases de datos)
- Clústeres basados en nodos de Amazon ElastiCache
- Clústeres de Amazon Redshift, tanto aprovisionados como sin servidor
- Amazon Elastic Container Service (ECS) con instancias de contenedores de EC2
- Amazon OpenSearch Service
- Amazon Elastic MapReduce (EMR)
- Amazon Managed Streaming para Apache Kafka (Amazon MSK)
- Los controles de cifrado de VPC aplican la obligatoriedad del cifrado a nivel de aplicación para todos los servicios de AWS a los que se accede mediante PrivateLink. Cualquier tráfico que no esté cifrado a nivel de aplicación se descarta automáticamente en los puntos de conexión de PrivateLink alojados en una VPC con Controles de cifrado de VPC en modo de aplicación obligatoria

Limitaciones específicas del servicio

Limitaciones de equilibrador de carga de red

Configuración de TLS: no puede usar un oyente TLS para delegar el cifrado y el descifrado en el equilibrador de carga cuando se aplican Controles de cifrado en la VPC que lo contiene. No obstante, puede configurar los destinos para que realicen el cifrado y descifrado TLS

Amazon Redshift (aprovisionado y sin servidor)

Los clientes no pueden pasar al modo de aplicación obligatoria en una VPC que tenga un clúster o un punto de conexión existentes. Para usar Controles de cifrado de VPC con Amazon Redshift, debe restaurar el clúster o el espacio de nombres desde una instantánea. En el caso de los clústeres aprovisionados, cree una instantánea del clúster de Redshift existente y, a continuación, restáurelo desde esa instantánea mediante la operación restaurar desde instantánea de clúster. En el caso de Redshift sin servidor, cree una instantánea del espacio de nombres existente y, a continuación, restáurelo desde esa instantánea mediante la operación restaurar desde instantánea en el grupo de trabajo sin servidor. Tenga en cuenta que no es posible habilitar Controles de cifrado de VPC en clústeres o espacios de nombres existentes sin realizar el proceso de creación de instantánea y restauración. Consulte la documentación de Amazon Redshift para obtener instrucciones sobre la creación de instantáneas.

Amazon MSK (Managed Streaming para Apache Kafka)

Esta funcionalidad es compatible con clústeres nuevos que usan la versión 4.1 y que se crean en su propia VPC. Los pasos siguientes ayudarán a usar el cifrado de VPC con MSK.

- El cliente habilita el cifrado de VPC en una VPC que no tenga ningún otro clúster de MSK
- El cliente crea un clúster con Kafka versión 4.1 y con el tipo de instancia M7g

Gateway Load Balancer y AWS Network Firewall

Gateway Load Balancer y AWS Network Firewall no son compatibles con las VPC en modo de aplicación. Si estos recursos están presentes en su VPC, debe ejecutar la VPC en modo de supervisión.

Limitaciones regionales y de zona

- Subredes de zonas locales: no se admiten en el modo de aplicación obligatoria; se deben eliminar de la VPC

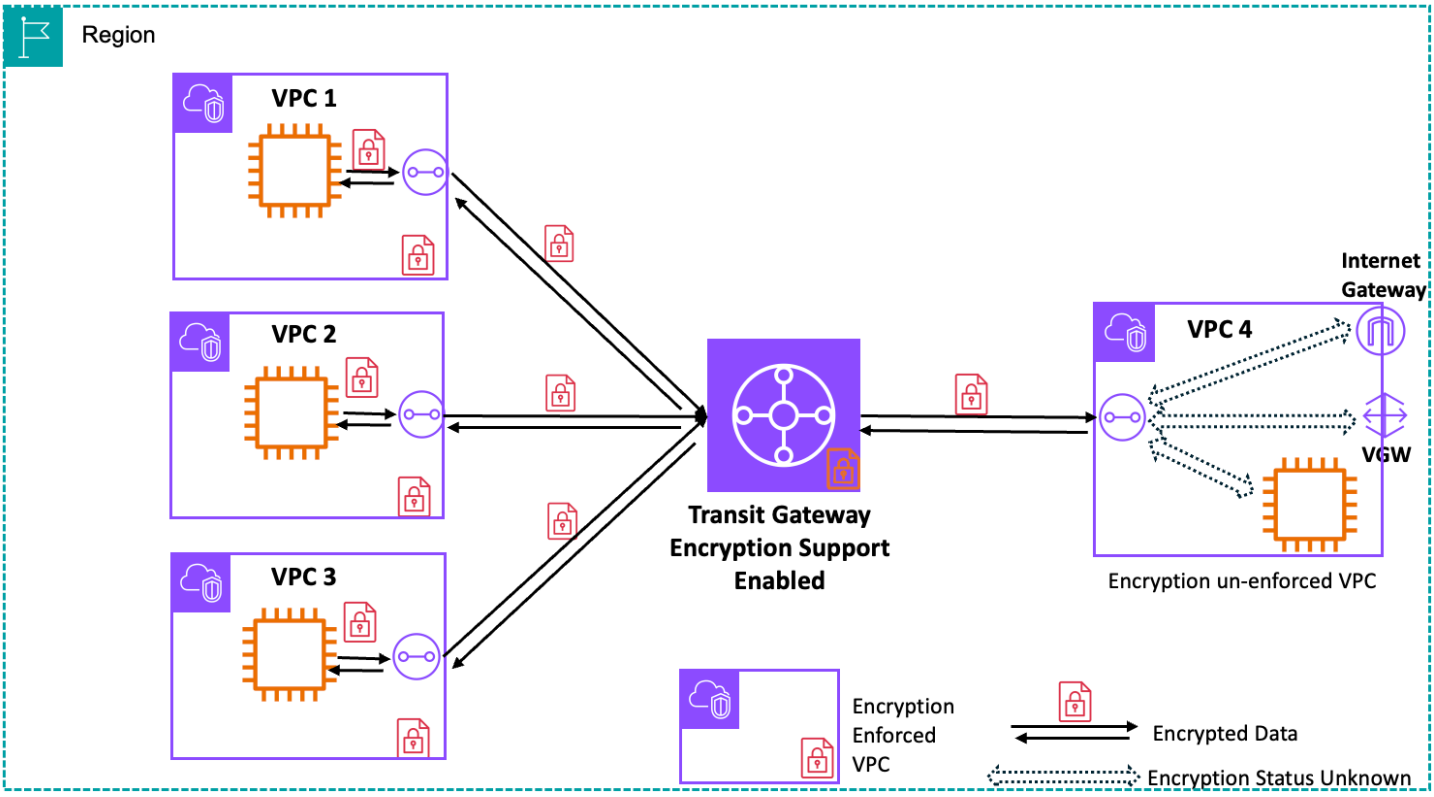
Compatibilidad con emparejamiento de VPC

Para garantizar el cifrado en tránsito con el emparejamiento de VPC entre dos VPC, ambas VPC deben residir en la misma región y tener los controles de cifrado habilitados en el modo de aplicación obligatoria, sin ninguna exclusión. Debe crear una exclusión de emparejamiento si desea emparejar una VPC con cifrado aplicado con otra VPC que resida en una región diferente o que no tenga los controles de cifrado habilitados en el modo de aplicación obligatoria (sin exclusiones).

Si dos VPC están en el modo de aplicación obligatoria y están emparejadas entre sí, no puede cambiar el modo de aplicación obligatoria al modo de supervisión. Debe crear primero una exclusión de emparejamiento, antes de cambiar el modo de Controles de cifrado de VPC a supervisión.

Compatibilidad de cifrado con la puerta de enlace de tránsito

Debe habilitar explícitamente la compatibilidad de cifrado en la puerta de enlace de tránsito para cifrar el tráfico entre las VPC que tengan controles de cifrado habilitados. Habilitar el cifrado en una puerta de enlace de tránsito existente no interrumpe los flujos de tráfico actuales, y la migración de los adjuntos de VPC a canales cifrados se realizará de forma transparente y automática. El tráfico entre dos VPC en el modo de aplicación obligatoria (sin exclusiones) a través de la puerta de enlace de tránsito recorre canales cifrados al 100 %. El cifrado en la puerta de enlace de tránsito también permite conectar dos VPC que se encuentran en distintos modos de controles de cifrado. Debe usarlo cuando desee aplicar controles de cifrado en una VPC que está conectada a una VPC en la que no se exige el cifrado. En un caso de este tipo, todo el tráfico dentro de la VPC con cifrado exigido, incluido el tráfico entre VPC, está cifrado. El tráfico entre VPC se cifra entre los recursos de la VPC con cifrado obligatorio y la puerta de enlace de tránsito. Más allá de eso, el cifrado depende de los recursos a los que se dirige el tráfico en la VPC sin aplicación obligatoria y no se garantiza que esté cifrado (dado que la VPC no está en el modo de aplicación obligatoria). Todas las VPC deben estar en la misma región (consulte los detalles aquí).



- En este diagrama, la VPC 1, la VPC 2 y la VPC 3 tienen los controles de cifrado en el modo de aplicación obligatoria y están conectadas a la VPC 4, que tiene los controles de cifrado en ejecución en el modo de supervisión.
- Se cifrará todo el tráfico entre VPC1, VPC2 y VPC3.
- Para mayor claridad, cualquier tráfico entre un recurso de la VPC 1 y un recurso de la VPC 4 se cifrará hasta la puerta de enlace de tránsito mediante el cifrado que ofrece el hardware del sistema Nitro. Más allá de eso, el estado del cifrado depende del recurso en la VPC 4 y no se garantiza que esté cifrado.

Para obtener más información sobre la compatibilidad de cifrado de la puerta de enlace de tránsito, consulte la documentación de la puerta de enlace de tránsito.

Habilite los controles de cifrado de VPC a nivel de cuenta.

Los controles de cifrado de VPC a nivel de cuenta le permiten configurar el modo de control del cifrado y las exclusiones de recursos que se aplican a todas las VPC de su cuenta. Esto proporciona una administración centralizada de las políticas de cifrado sin necesidad de configurar cada VPC de forma individual.

Los controles de cifrado a nivel de cuenta admiten las mismas ocho exclusiones de recursos que los controles a nivel de VPC: Internet Gateway, NAT Gateway, Egress-only Internet Gateway, VPC Peering, Virtual Private Gateway, Lambda, VPC Lattice y Elastic File System.

Modos de los controles de cifrado a nivel de cuenta

Puede establecer los siguientes modos a nivel de cuenta:

No administrada

Los controles de cifrado de VPC permanecen en su modo actual y se pueden gestionar a nivel de la VPC.

Monitor de intentos

Intenta cambiar todas las VPC de la cuenta al modo de supervisión. Identifica los recursos no cifrados sin bloquear su creación.

Aplicación tentativa

Intenta cambiar todas las VPC de la cuenta al modo de aplicación. Bloquea la creación de recursos no cifrados.

Estados de los controles de cifrado a nivel de cuenta

Los controles de cifrado de VPC a nivel de cuenta pueden tener uno de los siguientes estados:

default-state

El control de cifrado de VPC a nivel de cuenta no se ha habilitado.

transitions-in-progress

Las VPC de la cuenta están cambiando al modo especificado.

transitions-partially-successful

Una o más VPC no cambiaron al modo esperado.

transitions-successful

Todas las VPC cambiaron correctamente al modo esperado.

transitions-failed

Ninguna VPC cambió al modo esperado.

Habilitar los controles de cifrado de VPC a nivel de la organización

Si utiliza AWS Organizations para administrar las cuentas de su organización, puede utilizar una política declarativa de AWS Organizations para aplicar los Controles de cifrado de VPC en las cuentas de la organización. Para obtener más información sobre la política declarativa de los Controles de cifrado de VPC, consulte Políticas declarativas compatibles en la Guía del usuario de AWS Organizations.

Precios

Para obtener información sobre los precios, consulte Precios de Amazon VPC.

AWS CLIReferencia de comandos de

Ajustes y configuración

- aws ec2 create-vpc-encryption-control
- aws ec2 modify-vpc-encryption-control
- aws ec2 modify-account-vpc-encryption-control
- aws ec2 describe-account-vpc-encryption-control
- aws ec2 tgw modify-transit-gateway

Supervisión y solución de problemas

- aws ec2 describe-vpc-encryption-controls
- aws ec2 get-vpc-resources-blocking-encryption-enforcement
- aws ec2 create-flow-logs
- aws ec2 describe-flow-logs
- aws logs query

Eliminación

- aws ec2 delete-vpc-encryption-control

Recursos adicionales

Para obtener instrucciones detalladas de configuración, consulte el blog Introducción a los controles de cifrado de VPC: aplicar el cifrado del tráfico en tránsito dentro de las VPC y entre ellas en una región

Para obtener información más detallada sobre la API, consulte la Guía de referencia de la API de EC2.

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
- Autenticarse con identidades
- Administrar el acceso con políticas
- Cómo funciona Amazon VPC con IAM
- Ejemplos de políticas de Amazon VPC
- Solucionar problemas de identidad y acceso de Amazon VPC
- AWSPolíticas administradas por para Amazon Virtual Private Cloud
- Uso de roles vinculados al servicio para VPC

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 ayudarlo 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.

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.

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.

Autenticarse con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe autenticarse como el Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

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

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

Cuenta de AWSUsuario raíz de la

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario raíz de la Cuenta de AWS que tiene acceso completo a todos los Servicios de AWS y recursos. Se recomiendaencarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver la lista completa de las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Usuarios y grupos de IAM

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

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

Roles de IAM

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

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

Administrar el acceso con políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política define los permisos cuando se asocia a una identidad o un recurso. AWS evalúa estas políticas cuando una entidad principal realiza una solicitud. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte Información general de políticas de JSON en la Guía del usuario de IAM.

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

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

Políticas basadas en identidades

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

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

Políticas basadas en recursos

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

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se puede utilizar políticas de IAM administradas de 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 políticas JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulta 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 tipos de políticas adicionales que pueden establecer el máximo de permisos concedidos por los tipos de políticas más frecuentes:

- Límites de permisos: establecen los permisos máximos que una política basada en identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations.
- Políticas de control de recursos (RCP): definen los permisos máximos disponibles para los recursos de las cuentas. Para obtener más información, consulte Políticas de control de recursos (RCP) en la Guía del usuario de AWS Organizations.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. Para obtener más información, consulte Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para 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
- Recursos
- Claves de condición
- Políticas basadas en recursos de Amazon VPC
- Autorización basada en etiquetas
- Roles de IAM

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 más información acerca de los elementos que utiliza en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Acciones

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

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. 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 un usuario permiso para crear una VPC mediante la operación de la API `CreateVpc`, se concede acceso a la acción `ec2:CreateVpc`. 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 ver una lista de las acciones de Amazon VPC, consulte Acciones definidas por Amazon EC2 en la Referencia de autorizaciones de servicio.

Recursos

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

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

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

El recurso de VPC tiene el ARN que se muestra en el ejemplo siguiente.

```
arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}
```

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 sus ARN, consulte Tipos de recursos definidos por Amazon EC2 en la Referencia de autorizaciones de servicio.

Claves de condición

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

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

Amazon VPC define su propio conjunto de claves de condición y también admite el uso de algunas claves de condición globales. Para ver una lista de las claves de condición de Amazon VPC, consulte Claves de condición para Amazon EC2 en la Referencia de autorizaciones de servicio. 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 acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM 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 Condition de una política mediante las claves de condición. Para obtener más información, consulte Conceder permisos para etiquetar recursos durante la creación 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.

Roles de IAM

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 puertas de enlaces 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 the section called “Rol de IAM para publicar registros de flujo en CloudWatch Logs”.

Ejemplos de políticas de Amazon VPC

De manera predeterminada, los roles de IAM no tienen permiso para crear ni modificar recursos de VPC. Tampoco pueden realizar tareas mediante la Consola de administración de AWS, la AWS CLI o la API de AWS. Un administrador de IAM debe crear políticas de IAM que concedan permiso a los roles para realizar operaciones de API concretas en los recursos especificados que necesiten. El administrador debe asociar esas políticas a los roles 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 de IAM en la Guía del usuario de IAM.

Contenido

- Prácticas recomendadas sobre las políticas
- Utilizar la consola de Amazon VPC
- Crear una VPC con una subred pública
- Modificar y eliminar recursos de VPC
- Administrar grupos de seguridad
- Administración de reglas de grupos de seguridad
- Lanzar instancias en una subred específica
- Lanzar instancias en una VPC específica
- Bloqueo de acceso público de las VPC y subredes
- Ejemplos de políticas de Amazon VPC adicionales

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, eliminar o acceder a los recursos de Amazon VPC de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience a utilizar las políticas administradas de AWS y avance hacia permisos de privilegios mínimos. Para empezar a conceder permisos a los usuarios y cargas de trabajo, utilice las políticas administradas de AWS que otorgan permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de tarea en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía del usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado como, por ejemplo, CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte Validación de políticas con el Analizador de acceso de IAM en la Guía del usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesite usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para obtener una mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía del usuario de IAM.

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

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 se crea una política basada en identidad que es más restrictiva que los permisos necesarios mínimos, la consola no funcionará del modo esperado para las entidades (roles de IAM) que tengan esa política.

La siguiente política concede permiso a un rol para enumerar los recursos en la consola de la VPC, pero no para crearlos, actualizarlos ni eliminarlos.

JSON

```
{
    "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 conceder permisos mínimos para la consola a los roles que solo realizan llamadas a la AWS CLI o a la API de AWS. En lugar de ello, conceda acceso únicamente a las acciones que coincidan con la operación de API que el rol necesite ejecutar.

Crear una VPC con una subred pública

En el siguiente ejemplo se permite a los roles crear VPC, subredes, tablas de enrutamiento y puertas de enlace de Internet. Los roles también pueden asociar una puerta de enlace de Internet a una VPC y crear enrutamientos en tablas de enrutamiento. La acción `ec2:ModifyVpcAttribute` permite a los roles habilitar nombres de host de DNS para la VPC, con el fin de que cada instancia lanzada en una VPC reciba un nombre de host de DNS.

JSON

```
{
   "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 roles crear una VPC en la consola de Amazon VPC.

Modificar y eliminar recursos de VPC

Es posible que desee controlar los recursos de VPC que los roles pueden modificar o eliminar. Por ejemplo, la siguiente política permite a los roles utilizar y eliminar tablas de enrutamiento que tengan la etiqueta `Purpose=Test`. La política también especifica que los roles solo pueden eliminar puertas de enlace de Internet que tengan la etiqueta `Purpose=Test`. Los roles no pueden utilizar tablas de enrutamiento ni puertas de enlace de Internet que no tengan esta etiqueta.

JSON

```
{
    "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

La siguiente política permite a los roles administrar grupos de seguridad. La primera instrucción permite a los roles 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 segunda instrucción exige que los roles etiqueten todos los grupos de seguridad que creen con la etiqueta `Stack=Test`. La tercera instrucción permite a los roles crear etiquetas cuando creen un grupo de seguridad. La cuarta instrucción permite a los roles ver cualquier grupo de seguridad y cualquier regla de grupo de seguridad. La quinta instrucción permite a los roles crear un grupo de seguridad en una VPC.

> **Note**
>
> AWS CloudFormation no puede utilizar esta política para crear un grupo de seguridad con las etiquetas necesarias. Si elimina la condición de la acción `ec2:CreateSecurityGroup` que requiere la etiqueta, la política funcionará.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup",
                "ec2:ModifySecurityGroupRules",
                "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
            ],
            "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"
                },
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": "Stack"
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSecurityGroup"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeVpcs",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        }
    ]
}
```

Para permitir que los roles cambien el grupo de seguridad que está asociado a una instancia, agregue la acción `ec2:ModifyInstanceAttribute` a la política.

Para permitir que los roles cambien los grupos de seguridad de 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 roles permiso para ver todos los grupos de seguridad y las reglas de los grupos de seguridad, agregar y quitar reglas de entrada y salida para los grupos de seguridad de una VPC específica, y modificar las descripciones de las reglas de esa VPC específica. En la primera instrucción, se utiliza la clave de condición `ec2:Vpc` a fin de obtener permisos para una VPC específica.

La segunda instrucción concede a los roles permisos para describir todos los grupos de seguridad, reglas de grupos de seguridad y etiquetas. Esto permite a los roles ver las reglas de los grupos de seguridad para modificarlas.

JSON

```
{
    "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:us-east-1:123456789012:security-group/*",
            "Condition": {
                "ArnEquals": {
                    "ec2:Vpc": "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-1234567890abcdef0"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:ModifySecurityGroupRules"
            ],
```

```
            "Resource": "arn:aws:ec2:us-east-1:123456789012:security-group-rule/
*"
        }
    ]
}
```

Lanzar instancias en una subred específica

La siguiente política concede a los roles 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. Si los roles intentan lanzar una instancia en una subred distinta o 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 roles permiso para realizar tales acciones).

La política también concede permiso para utilizar el recurso de interfaz de red. Cuando se realiza el lanzamiento en una subred, la solicitud `RunInstances` crea una interfaz de red principal de manera predeterminada, de modo que el rol necesita permiso para crear este recurso cuando lanza la instancia.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:us-east-1::image/ami-*",
                "arn:aws:ec2:us-east-1:123456789012:instance/*",
                "arn:aws:ec2:us-
east-1:123456789012:subnet/subnet-1234567890abcdef0",
                "arn:aws:ec2:us-east-1:123456789012:network-interface/*",
                "arn:aws:ec2:us-east-1:123456789012:volume/*",
                "arn:aws:ec2:us-east-1:123456789012:key-pair/*",
                "arn:aws:ec2:us-east-1:123456789012:security-
group/sg-0abcdef1234567890"
            ]
        }
```

```
    ]
}
```

Lanzar instancias en una VPC específica

La siguiente política concede a los roles 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 roles permiso para lanzar instancias utilizando solo AMI que tengan la etiqueta "`department=dev`".

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:subnet/*",
            "Condition": {
                "ArnEquals": {
                    "ec2:Vpc": "arn:aws:ec2:us-
east-1:123456789012:vpc/vpc-1234567890abcdef0"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/department": "dev"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
```

```
            "Resource": [
                "arn:aws:ec2:us-east-1:123456789012:instance/*",
                "arn:aws:ec2:us-east-1:123456789012:volume/*",
                "arn:aws:ec2:us-east-1:123456789012:network-interface/*",
                "arn:aws:ec2:us-east-1:123456789012:key-pair/*",
                "arn:aws:ec2:us-east-1:123456789012:security-group/*"
            ]
        }
    ]
}
```

Bloqueo de acceso público de las VPC y subredes

Los siguientes ejemplos de políticas otorgan permiso a los roles para trabajar con la característica Bloqueo de acceso público (BPA) de las VPC para bloquear el acceso público a los recursos en las VPC y las subredes.

Ejemplo 1: permitir el acceso de solo lectura a la configuración de toda la cuenta de BPA de la VPC y a las exclusiones de BPA de la VPC.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "VPCBPAReadOnlyAccess",
      "Action": [
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcBlockPublicAccessExclusions"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Ejemplo 2: permitir el acceso completo de lectura y escritura a la configuración de toda la cuenta de BPA de la VPC y a las exclusiones de BPA de la VPC.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "VPCBPAFullAccess",
      "Action": [
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcBlockPublicAccessExclusions",
        "ec2:ModifyVpcBlockPublicAccessOptions",
        "ec2:CreateVpcBlockPublicAccessExclusion",
        "ec2:ModifyVpcBlockPublicAccessExclusion",
        "ec2:DeleteVpcBlockPublicAccessExclusion"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Ejemplo 3: Permitir el acceso a todas las API de EC2, excepto modificar la configuración de BPA de la VPC y crear exclusiones.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "EC2FullAccess",
            "Action": [
                "ec2:*"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Sid": "VPCBPAPartialAccess",
            "Action": [
```

```
                "ec2:ModifyVpcBlockPublicAccessOptions",
                "ec2:CreateVpcBlockPublicAccessExclusion"
            ],
            "Effect": "Deny",
            "Resource": "*"
        }
    ]
}
```

Ejemplos de políticas de Amazon VPC adicionales

Puede encontrar otras políticas de IAM de ejemplo relacionadas con Amazon VPC en la siguiente documentación:

- Listas de prefijos administradas
- Replicación de tráfico
- Puertas de enlace de tránsito
- Puntos de conexión de VPC y servicios de punto de conexión de VPC (AWS PrivateLink)
- Emparejamiento de VPC de

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
- No tengo autorización para realizar la operación iam:PassRole
- Quiero permitir que personas ajenas a mi cuenta de AWS accedan a mis recursos de Amazon VPC.

No tengo autorización para realizar una acción en Amazon VPC

Si la Consola de administración de AWS le indica que no está autorizado para llevar a cabo una acción, debe ponerse en contacto con su gestionador para recibir ayuda. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

El siguiente ejemplo de error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar detalles sobre una subred pero su rol de IAM 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 la política para poder acceder a la subred.

No tengo autorización para realizar la operación iam:PassRole

Si recibe un error que indica que no tiene autorización para llevar a cabo la acción `iam:PassRole`, sus políticas deben actualizarse para permitirle pasar un rol a Amazon VPC.

Algunos Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado 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 que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

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. Se 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.
- 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 Cuenta de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a sus 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 federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

AWSPolíticas administradas por para Amazon Virtual Private Cloud

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes, por lo que puede empezar a asignar permisos a los usuarios, grupos y roles.

Considere que es posible que las políticas administradas por AWS no concedan permisos de privilegio mínimo para los casos de uso concretos, ya que están disponibles para que las utilicen todos los clientes de AWS. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

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

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

AWSPolítica 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 Referencia de políticas administradas por AWS.

AWSPolítica 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 Referencia de políticas administradas por AWS.

AWSpolítica administrada : AmazonVPCCrossAccountNetworkInterfaceOperations

Puede asociar la política `AmazonVPCCrossAccountNetworkInterfaceOperations` a las identidades de IAM. Esta política otorga permisos que permiten a la identidad crear interfaces de red y adjuntarlas a recursos multicuenta.

Para ver los permisos de esta política, consulte AmazonVPCCrossAccountNetworkInterfaceOperations en la Referencia de políticas administradas por AWS.

AWSPolítica administrada por : AWSServiceRoleForNATGateway

Puede asociar la política `AWSServiceRoleForNATGateway` a las identidades de IAM. Esta política concede permisos que permiten que la identidad actúe en su nombre para escalar automáticamente las puertas de enlace NAT regionales.

Para ver los permisos de esta política, consulte AWSServiceRoleForNATGateway en la Referencia de la política administrada de AWS.

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 “AmazonVPCFullAccess”: actualización de una política actual	Se agregaron acciones a la política administrada AWSIPAMServiceRolePolicy (ec2:ModifyManagedPrefixList, ec2:DescribeManagedPrefixLists y ec2:GetManagedPrefixListEntries) para permitir que IPAM lea y modifique las listas de prefijos administradas.	31 de octubre de 2025
the section called “AWSServiceRoleForNATGateway ”: política nueva	La nueva política AWSServiceRoleForNATGateway permite que la identidad escale automáticamente las puertas de enlace NAT regionales.	19 de noviembre de 2025
the section called “AmazonVPCFullAccess”: actualización de una política actual	Se agregaron las acciones AssociateSecurityGroupVpc, DescribeSecurityGroupVpcAssociations y DisassociateSecurityGroupVpc, las cuales permiten asociar, desasociar y ver las asociaciones de grupos de seguridad con las VPC.	9 de diciembre de 2024
the section called “AmazonVPCReadOnlyAccess”: actualización de una política actual	Se agregó la acción DescribeSecurityGroupVpcAssociations, la cual permite ver las asociaciones de los grupos de seguridad con las VPC.	9 de diciembre de 2024

Cambio	Descripción	Fecha
the section called “AmazonVPCFullAccess”: actualización de una política actual	Se agregó la acción GetSecurityGroupsForVpc, que le permite obtener grupos de seguridad que se pueden usar en su VPC.	8 de febrero de 2024
the section called “AmazonVPCReadOnlyAccess”: actualización de una política actual	Se agregó la acción GetSecurityGroupsForVpc, que le permite obtener grupos de seguridad que se pueden usar en su VPC.	8 de febrero de 2024
the section called “AmazonVPCCrossAccountNetworkInterfaceOperations”: actualización de una política actual	Se agregaron las acciones AssignIpv6Addresses y UnassignIpv6Addresses, que permiten administrar las direcciones IPv6 asociadas a las interfaces de red.	25 de septiembre de 2023
the section called “AmazonVPCReadOnlyAccess”: actualización de una política actual	Se agregó la acción DescribeSecurityGroupRules, que le permite ver las reglas de los grupos de seguridad.	2 de agosto de 2021
the section called “AmazonVPCFullAccess”: actualización de una política actual	Se agregaron las acciones DescribeSecurityGroupRules y ModifySecurityGroupRules, que permiten ver y modificar las reglas de los grupos de seguridad.	2 de agosto de 2021

Cambio	Descripción	Fecha
the section called “AmazonVPCFullAccess”: actualización de una política actual	Se agregaron acciones para las puertas de enlace de operador, los grupos IPv6, las gateways locales y las tablas de enrutamiento de puertas de enlace locales.	23 de junio de 2021
the section called “AmazonVPCReadOnlyAccess”: actualización de una política actual	Se agregaron acciones para las puertas de enlace de operador, los grupos IPv6, las gateways locales y las tablas de enrutamiento de puertas de enlace locales.	23 de junio de 2021

Uso de roles vinculados al servicio para VPC

Amazon VPC utiliza roles vinculados al servicio de AWS Identity and Access Management (IAM). Un rol vinculado al servicio es un tipo único de rol de IAM que está vinculado directamente a VPC. Los roles vinculados al servicio están predefinidos por VPC e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

Un rol vinculado al servicio facilita la configuración de VPC, ya que no es necesario agregar manualmente los permisos necesarios. VPC define los permisos de los roles vinculados al servicio y, salvo que se indique lo contrario, solo VPC puede asumir esos roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege los recursos de la VPC, ya que no puede eliminar de forma involuntaria los permisos para acceder a dichos recursos.

Para obtener información sobre otros servicios que admiten roles vinculados al servicio, consulte Servicios de AWS que funcionan con IAM y busque los servicios que tengan Sí en la columna Roles vinculados al servicio. Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de los roles vinculados al servicio para VPC

VPC utiliza el rol vinculado al servicio denominado AWSServiceRoleForNATGateway. Este rol vinculado al servicio permite que Amazon VPC asigne direcciones IP elásticas en su nombre para escalar automáticamente las puertas de enlace NAT regionales, asociar y desasociar las direcciones IP elásticas existentes a las puertas de enlace NAT regionales cuando lo solicite, y describir interfaces de red para identificar la infraestructura existente y ampliarla automáticamente a nuevas zonas de disponibilidad.

El rol vinculado al servicio AWSServiceRoleForNATGateway confía en los siguientes servicios para asumir el rol:

- `ec2-nat-gateway.amazonaws.com`

La política de permisos del rol denominada AWSNATGatewayServiceRolePolicy permite que VPC realice las siguientes acciones sobre los recursos especificados:

- Acción: `AllocateAddress` sobre direcciones IP elásticas administradas por el servicio, para asignar direcciones IP elásticas en su nombre. Las direcciones IP elásticas administradas por el servicio se encargan automáticamente del etiquetado posterior con etiquetas administradas por el servicio y de la acción ReleaseAddress.
- Acción: `AssociateAddress` sobre las direcciones IP elásticas existentes previamente, para asociarlas manualmente a la puerta de enlace NAT regional cuando lo solicite.
- Acción: `DisassociateAddress` sobre las direcciones IP elásticas existentes previamente, para quitarlas de la puerta de enlace NAT regional cuando lo solicite.
- Acción: `DescribeAddresses` para obtener información de direcciones IP públicas a partir de direcciones IP elásticas proporcionadas por el cliente durante la asociación.
- Acción: `DescribeNetworkInterface` sobre las interfaces de red existentes, para identificar automáticamente las zonas de disponibilidad en las que reside la infraestructura y escalar horizontalmente de forma automática a nuevas zonas.

Debe configurar los permisos para permitir a sus usuarios, grupos o funciones, crear, editar o eliminar la descripción de un rol vinculado al servicio. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación de un rol vinculado al servicio para VPC

No necesita crear manualmente un rol vinculado a servicios. Cuando crea una puerta de enlace NAT con un modo de disponibilidad “regional” en la Consola de administración de AWS, la AWS CLI o la API de AWS, VPC crea el rol vinculado al servicio en su nombre.

> **Important**
>
> Este rol vinculado a servicios puede aparecer en su cuenta si se ha completado una acción en otro servicio que utilice las características compatibles con este rol. Además, si utilizaba el servicio VPC antes del 1 de enero de 2017, cuando comenzó a admitir roles vinculados al servicio, VPC creó el rol AWSServiceRoleForNATGateway en la cuenta. Para obtener más información, consulte Un nuevo rol ha aparecido en mi Cuenta de AWS.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Cuando crea una puerta de enlace NAT con un modo de disponibilidad “regional”, VPC crea de nuevo el rol vinculado al servicio en su nombre.

También puede usar la consola de IAM para crear un rol vinculado al servicio con el caso de uso AWSServiceRoleForNATGateway. En la AWS CLI o la API de AWS, cree un rol vinculado al servicio con el nombre de servicio `ec2-nat-gateway.amazonaws.com`. Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Edición de un rol vinculado al servicio para VPC

VPC no permite que edite el rol vinculado al servicio AWSServiceRoleForNATGateway. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación de un rol vinculado al servicio para VPC

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar los recursos del rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el servicio VPC usa el rol cuando intenta eliminar los recursos, es posible que la eliminación no se complete correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de VPC utilizados por AWSServiceRoleForNATGateway

- Elimine todas las puertas de enlace NAT regionales en todas las regiones en las que estén implementadas.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Use la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado al servicio AWSServiceRoleForNATGateway. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Regiones compatibles con roles vinculados al servicio para VPC

VPC admite el uso de roles vinculados al servicio en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte Puntos de conexión y Regiones de AWS.

VPC no admite el uso de roles vinculados al servicio en todas las regiones en las que el servicio está disponible. Puede usar el rol AWSServiceRoleForNATGateway en las siguientes regiones.

Nombre de la región	Identidad de la región	Compatibilidad en VPC
Este de EE. UU. (Norte de Virginia)	us-east-1	Sí
Este de EE. UU. (Ohio)	us-east-2	Sí
Oeste de EE. UU. (Norte de California)	us-west-1	Sí
Oeste de EE. UU. (Oregón)	us-west-2	Sí
África (Ciudad del Cabo)	af-south-1	Sí
Asia Pacífico (Hong Kong)	ap-east-1	Sí

Nombre de la región	Identidad de la región	Compatibilidad en VPC
Asia-Pacífico (Taipéi)	ap-east-2	Sí
Asia-Pacífico (Yakarta)	ap-southeast-3	Sí
Asia-Pacífico (Mumbai)	ap-south-1	Sí
Asia-Pacífico (Hyderabad)	ap-south-2	Sí
Asia-Pacífico (Osaka)	ap-northeast-3	Sí
Asia-Pacífico (Seúl)	ap-northeast-2	Sí
Asia-Pacífico (Singapur)	ap-southeast-1	Sí
Asia-Pacífico (Sídney)	ap-southeast-2	Sí
Asia-Pacífico (Tokio)	ap-northeast-1	Sí
Asia-Pacífico (Melbourne)	ap-southeast-4	Sí
Asia-Pacífico (Malasia)	ap-southeast-5	Sí
Asia-Pacífico (Nueva Zelanda)	ap-southeast-6	Sí
Asia-Pacífico (Tailandia)	ap-southeast-7	Sí
Canadá (centro)	ca-central-1	Sí
Oeste de Canadá (Calgary)	ca-west-1	Sí
Europa (Fráncfort)	eu-central-1	Sí
Europa (Zúrich)	eu-central-2	Sí
Europa (Irlanda)	eu-west-1	Sí
Europa (Londres)	eu-west-2	Sí
Europa (Milán)	eu-south-1	Sí

Nombre de la región	Identidad de la región	Compatibilidad en VPC
Europa (España)	eu-south-2	Sí
Europa (París)	eu-west-3	Sí
Europa (Estocolmo)	eu-north-1	Sí
Israel (Tel Aviv)	il-central-1	Sí
Medio Oriente (Baréin)	me-south-1	Sí
Medio Oriente (EAU)	me-central-1	Sí
Medio Oriente (Arabia Saudí)	me-west-1	Sí
México (centro)	mx-central-1	Sí
América del Sur (São Paulo)	sa-east-1	Sí
AWS GovCloud (US-East)	us-gov-east-1	No
AWS GovCloud (Oeste de EE. UU.)	us-gov-west-1	No

Seguridad de la infraestructura en Amazon VPC

Como se trata de un servicio administrado, Amazon Virtual Private Cloud está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y sobre cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS siguiendo las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Puede utilizar llamadas a la API publicadas de AWS para acceder a Amazon VPC a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Aislamiento de red

Una nube privada virtual (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 iniciar 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.

Puede utilizar AWS PrivateLink para permitir que los recursos de la VPC se conecten a Servicios de AWS mediante direcciones IP privadas, como si los servicios estuvieran alojados directamente en la VPC. Por lo tanto, no es necesario utilizar una puerta de enlace de Internet o un dispositivo NAT para acceder a los Servicios de AWS.

Controlar el tráfico de red

Tenga en cuenta las siguientes opciones para controlar el tráfico de red a los recursos en la VPC, como las instancias EC2:

- Utilice grupos de seguridad como mecanismo principal para controlar el acceso de red a las VPC. Cuando sea necesario, utilice las ACL de red 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. Las ACL de red pueden ser efectivas como control secundario (por ejemplo, para denegar un subconjunto específico de tráfico) o como 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 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 una puerta de enlace NAT para acceder a Internet desde las instancias en subredes privadas.
- Configure tablas de enrutamiento de subred con las rutas de red mínimas para cumplir con los requisitos de conectividad.
- 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. Así, puede implementar políticas de IAM especiales para el control de cambios, lo que facilita auditar los cambios de las reglas de los grupos de seguridad o

en los scripts de verificación de reglas automatizados. 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 utilizar diferentes reglas de direccionamiento de la subred de la VPC basadas en interfaces de red asignadas a una subred.

- Utilice AWS Virtual Private Network o 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 CSPM para verificar la accesibilidad accidental a la red desde sus instancias.
- Utilice AWS Network Firewall para proteger las subredes de la VPC de amenazas de red comunes.

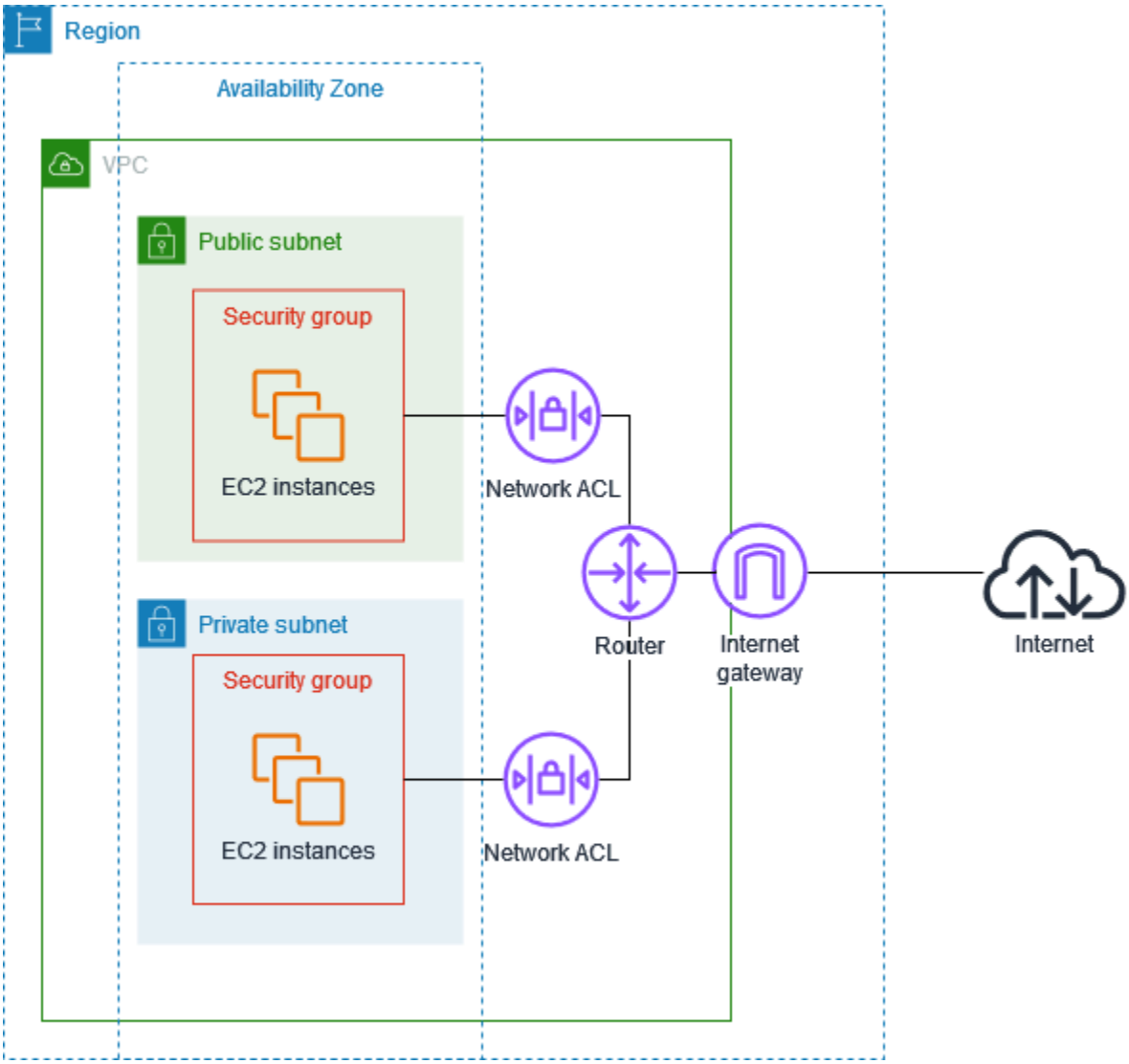
Comparar grupos de seguridad y ACL de red

La siguiente tabla resume las diferencias básicas entre grupos de seguridad y ACL de red.

Característica	Grupo de seguridad	ACL de red
Nivel de operación	Nivel de instancia	Nivel de subred
Ámbito	Se aplica a todas las instancias asociadas al grupo de seguridad	Se aplica a todas las instancias en las subredes asociadas
Tipo de regla	Solo reglas de permiso	Reglas de permiso y denegación
Evaluación de reglas	Evalúa todas las normas antes de decidir si permitir el tráfico	Evalúa las reglas en orden ascendente hasta encontrar una coincidencia con el tráfico
Tráfico de retorno	Permitido automáticamente (con estado)	Debe estar permitido de forma explícita (sin estado)

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.



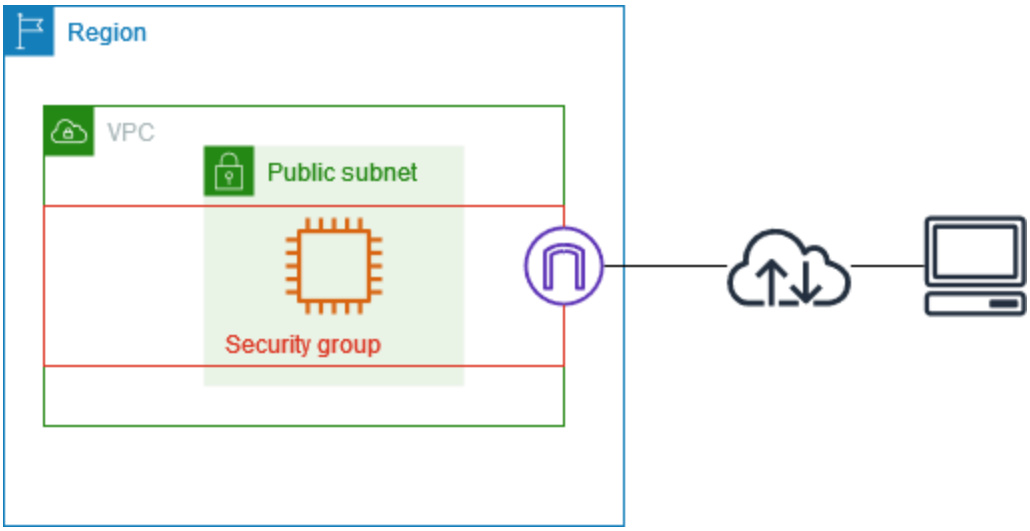
Puede proteger sus instancias utilizando sólo grupos de seguridad. Sin embargo, puede añadir ACL de red como una capa adicional de defensa. Para obtener más información, consulte Ejemplo: controlar el acceso a las instancias de una subred.

Controlar el tráfico hacia los recursos de AWS mediante grupos de seguridad

Un grupo de seguridad 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 una VPC, cada uno con sus propias reglas de entrada y salida. Puede especificar el origen, el rango de puertos y el protocolo de cada regla de entrada. Puede especificar el destino, el rango de puertos y el protocolo de cada regla de salida.

En el siguiente diagrama se muestra una VPC con una subred, una puerta de enlace de Internet y un grupo de seguridad. La subred contiene una instancia de EC2. El grupo de seguridad se asigna a la instancia. El grupo de seguridad actúa como un firewall virtual. El único tráfico que llega a la instancia es el permitido por las reglas del grupo de seguridad. Por ejemplo, si el grupo de seguridad contiene una regla que permite el tráfico ICMP a la instancia desde su red, puede hacer ping a la instancia desde su equipo. Si el grupo de seguridad no contiene una regla que permita el tráfico SSH, no podrá conectarse a la instancia mediante SSH.



Contenido

- Conceptos básicos de los grupos de seguridad
- Ejemplo de grupo de seguridad
- Reglas del grupo de seguridad
- Grupos de seguridad predeterminados para las VPC
- Create a security group for your VPC (Crear un grupo de seguridad para la VPC)
- Configuración de reglas de grupos de seguridad
- Eliminación de un grupo de seguridad
- Asociación de grupos de seguridad a varias VPC
- Compartir grupos de seguridad con AWS Organizations

Precios

El uso de grupos de seguridad no supone ningún cargo adicional.

Conceptos básicos de los grupos de seguridad

- Puede asignar un grupo de seguridad a los recursos creados en la misma VPC que el grupo de seguridad o a los recursos de otras VPC si utiliza la característica de asociación de VPC de grupos de seguridad para asociar el grupo de seguridad a otras VPC de la misma región. También puede asignar varios grupos de seguridad a un único recurso.
- 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.
  - En los nombres de los grupos de seguridad no se distingue entre mayúsculas y minúsculas.
  - 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.
- Los grupos de seguridad no filtran el tráfico destinado a los siguientes servicios ni desde estos:
  - Servicios de nombres de dominio de Amazon (DNS)
  - Protocolo de configuración dinámica de host de Amazon (DHCP)
  - Metadatos de la instancia de Amazon EC2
  - Puntos de conexión de metadatos de tareas de Amazon ECS
  - Activación de licencias para instancias de Windows
  - Servicio de sincronización temporal de Amazon
  - Direcciones IP reservadas del enrutador de la VPC predeterminado

- 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.

Prácticas recomendadas

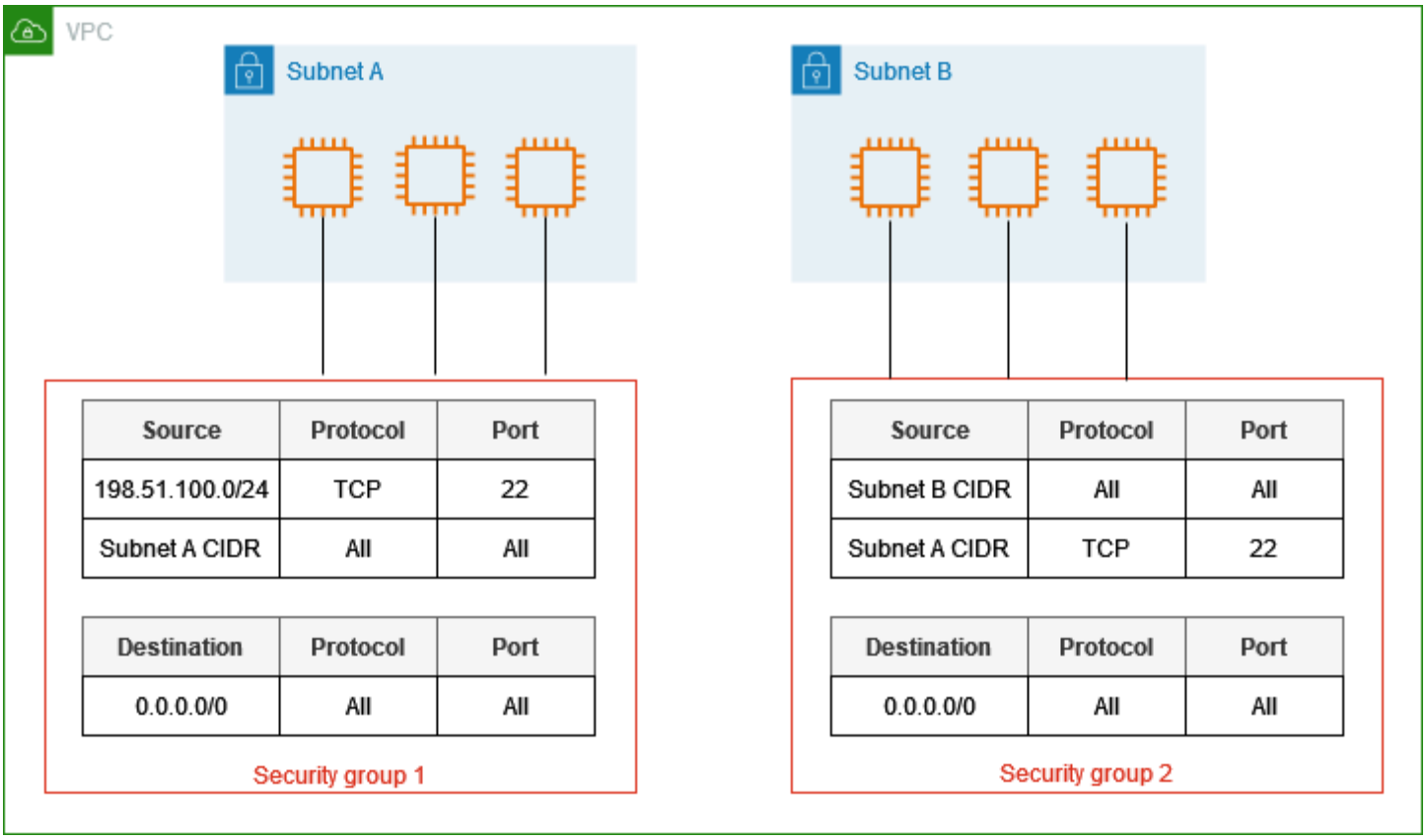
- Autorice solo a entidades principales de IAM específicas a crear y modificar grupos de seguridad.
- Cree el número mínimo de grupos de seguridad que necesite para reducir el riesgo de error. Use cada grupo de seguridad para administrar el acceso a los recursos que tienen funciones y requisitos de seguridad similares.
- Al agregar reglas entrantes para los puertos 22 (SSH) o 3389 (RDP) para acceder a sus instancias de EC2, autorice solo rangos de direcciones IP específicas. Si especifica 0.0.0.0/0 (IPv4) y ::/ (IPv6), esto permite a cualquier persona acceder a sus instancias desde cualquier dirección IP mediante el protocolo especificado.
- No abra rangos de puertos grandes. Asegúrese de que el acceso a través de cada puerto esté restringido a las fuentes o destinos que lo requieran.
- Considere crear ACL de red con reglas similares a sus grupos de seguridad para agregar 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.

Ejemplo de grupo de seguridad

En el siguiente diagrama se muestra una VPC con dos grupos de seguridad y dos subredes. Las instancias de la subred A tienen los mismos requisitos de conectividad; por lo tanto, están asociadas al grupo de seguridad 1. Las instancias de la subred B tienen los mismos requisitos de conectividad; por lo tanto, están asociadas al grupo de seguridad 2. Las reglas del grupo de seguridad permiten el tráfico de la siguiente manera:

- La primera regla de entrada del grupo de seguridad 1 permite el tráfico SSH a las instancias de la subred A desde el rango de direcciones especificado (por ejemplo, un rango de su propia red).
- La segunda regla de entrada del grupo de seguridad 1 permite que las instancias de la subred A se comuniquen entre sí mediante cualquier protocolo o puerto.

- La primera regla de entrada del grupo de seguridad 2 permite que las instancias de la subred B se comuniquen entre sí mediante cualquier protocolo o puerto.
- La segunda regla de entrada del grupo de seguridad 2 permite que las instancias de la subred A se comuniquen con las instancias de la subred B mediante SSH.
- Ambos grupos de seguridad utilizan la regla de salida predeterminada, la cual permite todo el tráfico.



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 origen o destino específicos.

Contenido

- Conceptos básicos de las reglas de los grupos de seguridad
- Componentes de una regla de grupo de seguridad
- Referencia a grupos de seguridad
- Tamaño del grupo de seguridad
- Reglas antiguas de los grupos de seguridad

Conceptos básicos de las reglas de los grupos de seguridad

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. Para obtener instrucciones, consulte Configuración de reglas de grupos 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.
- 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.

Limitación

Los grupos de seguridad no pueden bloquear las solicitudes de DNS hacia Route 53 Resolver o desde este, a veces denominado “dirección IP de VPC+2” (consulte Amazon Route 53 Resolver en la Guía para desarrolladores de Amazon Route 53) o AmazonProvidedDNS. Para filtrar las solicitudes de DNS a través de Route 53 Resolver, utilice el Firewall de DNS de Route 53 Resolver.

Componentes de una regla de grupo de seguridad

Los siguientes son componentes de las reglas del grupo de seguridad de entrada y salida:

- 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. Para obtener más información, consulte Reglas del grupo de seguridad en la Guía del usuario de Amazon EC2.
- 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 de prefijo `/32`. Por ejemplo, `203.0.113.1/32`.
  - Una única dirección IPv6. Debe utilizar la longitud de 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, `pl-1234abc1234abc123`. Para obtener más información, consulte Listas de prefijos administradas.
  - El ID de un grupo de seguridad. Por ejemplo, `sg-1234567890abcdef0`. Para obtener más información, consulte the section called “Referencia a grupos de seguridad”.
- (Opcional) Descripción: puede agregar una descripción a la regla, que puede ayudarlo 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 ._-:/()#,@[]+=;{}!$*.

Para ver ejemplos, consulte las reglas de los grupos de seguridad para diferentes casos de uso en la Guía del usuario de Amazon EC2.

Referencia a grupos de seguridad

Al especificar un grupo de seguridad como origen o destino de una regla, la regla afecta a todas las instancias que están asociadas a los grupos de seguridad. Las instancias se pueden comunicar en la dirección que se determine, mediante las direcciones IP privadas de las instancias, a través del protocolo y el puerto especificados.

Por ejemplo, a continuación, se representa una regla de entrada para un grupo de seguridad que hace referencia al grupo de seguridad sg-0abcdef1234567890. Esta regla permite el tráfico SSH entrante desde las instancias asociadas a sg-0abcdef1234567890.

Origen	Protocolo	Rango de puerto
sg-0abcdef1234567890	TCP	22

Al hacer referencia a un grupo de seguridad en una regla de grupo de seguridad, tenga en cuenta lo siguiente:

- Puede hacer referencia a un grupo de seguridad en la regla de entrada de otro grupo de seguridad si se cumple alguna de las siguientes condiciones:
  - Los grupos de seguridad están asociados con la misma VPC.
  - Existe una conexión de emparejamiento entre las VPC a las que están asociados los grupos de seguridad.
  - Hay una puerta de enlace de tránsito entre las VPC a las que están asociados los grupos de seguridad.
- Puede hacer referencia a un grupo de seguridad en la regla de salida si se cumple alguna de las siguientes condiciones:
  - Los grupos de seguridad están asociados con la misma VPC.
  - Existe una conexión de emparejamiento entre las VPC a las que están asociados los grupos de seguridad.
- No se agrega ninguna regla del grupo de seguridad al que se hace referencia al grupo de seguridad que hace referencia a él.
- En el caso de las reglas de entrada, las instancias de EC2 asociadas a un grupo de seguridad pueden recibir tráfico entrante desde las direcciones IP privadas de las interfaces de red de las instancias de EC2 asociadas al grupo de seguridad de referencia.

- En el caso de las reglas de salida, las instancias de EC2 asociadas al grupo de seguridad pueden enviar tráfico saliente a las direcciones IP privadas de las instancias de EC2 asociadas al grupo de seguridad al que se hace referencia.
- No verificamos los grupos de seguridad a los que se hace referencia para dar autorización en las siguientes acciones: `AuthorizeSecurityGroupIngress`, `AuthorizeSecurityGroupEgress`, `RevokeSecurityGroupIngress` y `RevokeSecurityGroupEgress`. Solo comprobamos si el grupo de seguridad existe. Se obtiene el siguiente resultado:
  - Especificar el grupo de seguridad al que se hace referencia en las políticas de IAM para estas acciones no tiene ningún efecto.
  - Cuando un grupo de seguridad al que se hace referencia es propiedad de otra cuenta, la cuenta propietaria no recibe eventos de CloudTrail para estas acciones.

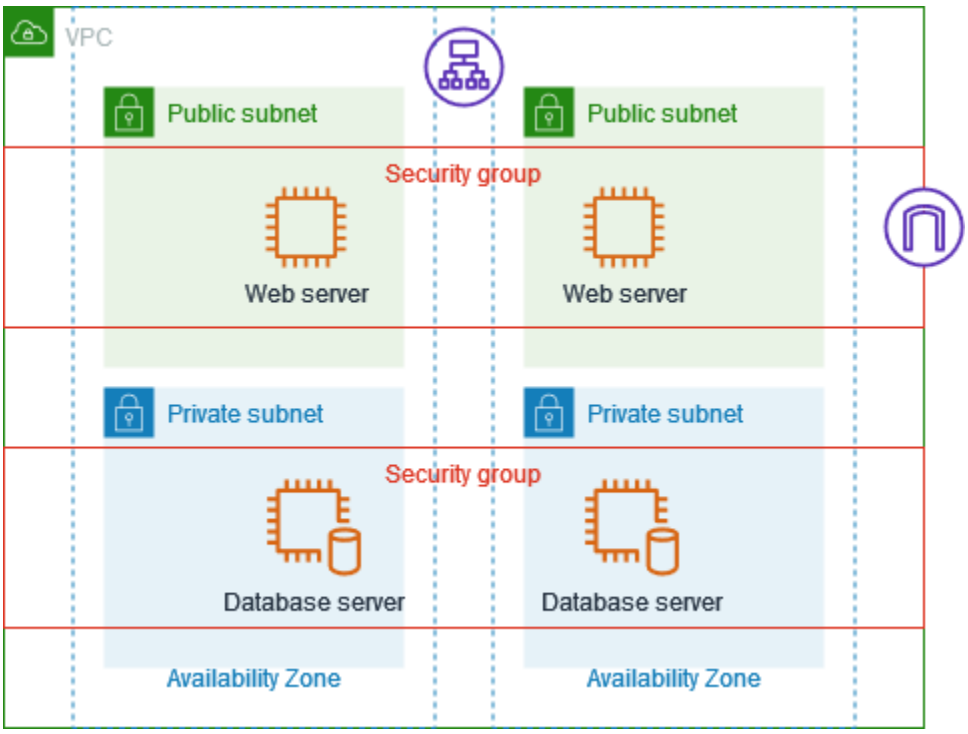
Limitación

Si configura rutas para reenviar el tráfico entre dos instancias en subredes diferentes a través de un dispositivo de middlebox, debe asegurarse de que los grupos de seguridad de ambas instancias permiten 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.

Ejemplo

En el siguiente diagrama se muestra una VPC con subredes en dos zonas de disponibilidad, una puerta de enlace de Internet y un equilibrador de carga de aplicación. Cada zona de disponibilidad tiene una subred pública para servidores web y una subred privada para servidores de bases de datos. Hay grupos de seguridad independientes para el equilibrador de carga, los servidores web y los servidores de bases de datos. Cree las siguientes reglas de grupo de seguridad para permitir el tráfico.

- Agregue reglas al grupo de seguridad del equilibrador de carga para permitir el tráfico HTTP y HTTPS de Internet. El origen es 0.0.0.0/0.
- Agregue reglas al grupo de seguridad para servidores web para permitir solo el tráfico HTTP y HTTPS del equilibrador de carga. El origen es el grupo de seguridad para el equilibrador de carga.
- Agregue reglas al grupo de seguridad para servidores de bases de datos para permitir solicitudes de bases de datos de servidores web. El origen es el grupo de seguridad para los servidores web.



Tamaño del grupo de seguridad

El tipo de origen o destino determina la forma en que cada regla cuenta para el número máximo de reglas que puede tener por grupo de seguridad.

- Una regla que hace referencia a un bloque de CIDR cuenta como una regla.
- Una regla que hace referencia a otro grupo de seguridad cuenta como una regla, independientemente del tamaño del grupo de seguridad al que se hace referencia.
- Una regla que hace referencia a una lista de prefijos administrada por el cliente cuenta como el tamaño máximo de la lista de prefijos. Por ejemplo, si el tamaño máximo de la lista de prefijos es 20, una regla que haga referencia a esta lista de prefijos cuenta como 20 reglas.
- Una regla que hace referencia a una lista de prefijos administrados por AWS cuenta como el peso de la lista de prefijos. Por ejemplo, si el peso de la lista de prefijos es 10, una regla que haga referencia a esta lista de prefijos cuenta como 10 reglas. Para obtener más información, consulte the section called “Listas de prefijos administradas por AWS disponibles”.

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. 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.

Si tiene una regla del grupo de seguridad que hace referencia a un grupo de seguridad en una VPC emparejada o compartida, la regla se marca como obsoleta cuando el grupo de seguridad referenciado se elimina o la conexión de emparejamiento de VPC se elimina. Las reglas obsoletas de los grupos de seguridad se pueden eliminar de la misma manera que cualquier otra regla del grupo de seguridad.

Grupos de seguridad predeterminados para las VPC

Las VPC predeterminadas y las VPC que cree incluyen un grupo de seguridad predeterminado. El nombre del grupo de seguridad predeterminado es “default”.

Se recomienda crear grupos de seguridad para recursos o grupos de recursos específicos en lugar de utilizar el grupo de seguridad predeterminado. Sin embargo, si no asocia un grupo de seguridad con algunos recursos en el momento de la creación, los asociamos con el grupo de seguridad predeterminado. Por ejemplo, si no especifica un grupo de seguridad cuando lanza una instancia EC2, asociamos la instancia con el grupo de seguridad predeterminado para su VPC.

Conceptos básicos de un 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, devolveremos el siguiente código de error: `Client.CannotDelete`.

Reglas predeterminadas

En la tabla siguiente se describen las reglas de entrada predeterminadas del grupo de seguridad predeterminado.

Origen	Protocolo	Rango de puerto	Descripción
sg-1234567890abcdef0	Todos	Todos	Permite el tráfico entrante de todos los recursos asignados

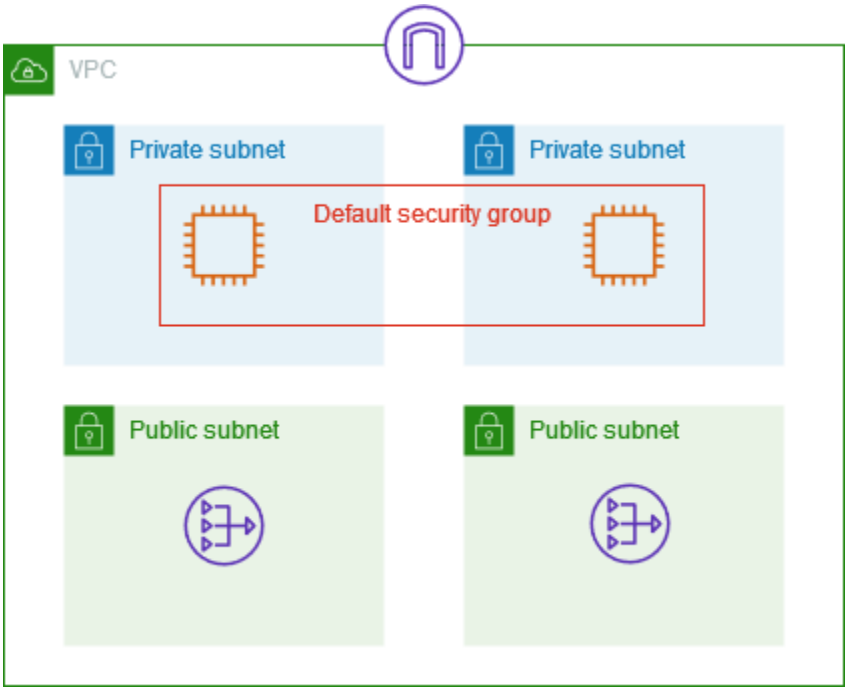
Origen	Protocolo	Rango de puerto	Descripción
			a este grupo de seguridad. El origen es el ID de este grupo de seguridad.

En la tabla siguiente se describen las reglas de salida predeterminadas del grupo de seguridad predeterminado.

Destino	Protocolo	Rango de puerto	Descripción
0.0.0.0/0	Todos	Todos	Permite todo el tráfico IPv4 saliente.
::/0	Todos	Todos	Permite todo el tráfico IPv6 saliente. Esta regla se agrega solo si su VPC tiene un bloque de CIDR IPv6 asociado.

Ejemplo

En el siguiente diagrama se muestra una VPC con un grupo de seguridad predeterminado, una puerta de enlace de Internet y una puerta de enlace de NAT. La seguridad predeterminada contiene solo sus reglas predeterminadas y está asociada con dos instancias de EC2 que se ejecutan en la VPC. En este escenario, cada instancia puede recibir tráfico entrante de la otra instancia en todos los puertos y protocolos. Las reglas predeterminadas no permiten que las instancias reciban tráfico de la puerta de enlace de Internet ni de la puerta de enlace de NAT. Si las instancias deben recibir tráfico adicional, se recomienda crear un grupo de seguridad con las reglas necesarias y asociar el grupo de seguridad nuevo a las instancias en lugar del grupo de seguridad predeterminado.



Create a security group for your VPC (Crear un grupo de seguridad para la VPC)

Tu nube privada virtual (VPC) incluye un grupo de seguridad predeterminado. Puede crear grupos de seguridad adicionales para cada VPC. Los grupos de seguridad solo se pueden utilizar en la VPC para la que se creó.

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. Puede añadir reglas al crear un grupo de seguridad o más adelante. Para obtener más información, consulte Reglas del grupo de seguridad.

Permisos necesarios

Antes de comenzar, asegúrese de tener los permisos necesarios. Para obtener más información, consulte los siguientes temas:

- Administrar grupos de seguridad
- Administración de reglas de grupos de seguridad

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 Grupos de seguridad.
3. Elija Create Security Group (Creación de 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 en la que desea crear los recursos a los que desea asociar el grupo de seguridad.
6. (Opcional) Para añadir reglas de entrada, elija Reglas de entrada. Para cada regla, elija Agregar regla y especifique el protocolo, el puerto y la fuente. Para obtener más información, consulte Configuración de reglas de grupos de seguridad.
7. (Opcional) Para añadir reglas de salida, seleccione Reglas de salida. Para cada regla, elija Agregar regla y especifique el protocolo, el puerto y el destino.
8. (Opcional) Para agregar una etiqueta, elija Agregar etiqueta nueva e ingrese la clave y el valor de la etiqueta.
9. Elija Creación de grupo de seguridad.

Para crear un grupo de seguridad con AWS CLI

Utilice el comando create-security-group.

Alternativamente, puede crear un nuevo grupo de seguridad creando una copia de uno existente. Al copiar un grupo de seguridad, agregamos automáticamente las mismas reglas de entrada y salida que el grupo de seguridad original y usamos la misma VPC que el grupo de seguridad original. Escriba un nombre y una descripción para el nuevo grupo de seguridad. Si lo desea, puede elegir una VPC diferente y modificar las reglas de entrada y salida según sea necesario. Sin embargo, no puede copiar un grupo de seguridad de una región a otra.

Para crear un grupo de seguridad basado en uno existente

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Grupos de seguridad.
3. Seleccione un grupo de seguridad.
4. Seleccione Acciones y, a continuación, Copiar al nuevo grupo de seguridad.
5. Ingrese un nombre y una descripción para el grupo de seguridad.
6. (Opcional) Elija una VPC diferente si es necesario.
7. (Opcional) Agregue, elimine o edite las reglas del grupo de seguridad según sea necesario.

8. Elija Creación de grupo de seguridad.

Configuración de reglas de grupos de seguridad

Después de crear un grupo de seguridad, puede agregar, actualizar y eliminar sus reglas de grupo de seguridad. Cuando agrega, actualiza o elimina una regla, esta se aplica automáticamente a todos los recursos asociados al grupo de seguridad.

Permisos necesarios

Antes de comenzar, asegúrese de tener los permisos necesarios. Para obtener más información, consulte Administración de reglas de grupos de seguridad.

Protocolos y puertos

- Con la consola, si selecciona un tipo predefinido, el Protocolo y el Rango de puertos se especifican automáticamente. Para introducir un rango de puertos, debe seleccionar uno de los siguientes tipos personalizados: TCP personalizado o UDP personalizado.
- Con la AWS CLI, puede agregar una sola regla con un solo puerto mediante las opciones `--protocol` y `--port`. Para añadir varias reglas, o una regla con un rango de puertos, utilice la opción `--ip-permissions`.

Orígenes y destinos

- Con la consola, puede especificar lo siguiente como origen de las reglas de entrada o como destino de las reglas de salida:
  - Personalizado: un bloque de CIDR de IPv4 y un bloque de CIDR de IPv6, un grupo de seguridad o una lista de prefijos.
  - Anywhere-IPv4: el bloque de CIDR IPv4 0.0.0.0/0.
  - Anywhere-IPv6: el bloque de CIDR ::/0 IPv6.
  - Mi IP: la dirección IPv4 pública de su equipo local.
- Con la AWS CLI, puede especificar un bloque de CIDR de IPv4 mediante la opción `--cidr` o un grupo de seguridad mediante la opción `--source-group`. Para especificar una lista de prefijos o un bloque de CIDR de IPv6, utilice la opción `--ip-permissions`.

> **Warning**
>
> Si elige Anywhere-IPv4, permite el tráfico desde todas las direcciones IPv4. Si elige Anywhere-IPv6, permite el tráfico desde todas las direcciones IPv6. Se recomienda autorizar solo los rangos de direcciones IP específicos que necesitan acceso a sus recursos.

Para añadir reglas a 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 Grupos de seguridad.
3. Seleccione el grupo de seguridad.
4. Para editar las reglas de entrada, seleccione Editar reglas de entrada en Acciones o en la pestaña Reglas de entrada.

   a. Para agregar una regla, elija Agregar regla e ingrese el tipo, el protocolo, el puerto y la fuente de la regla.

      Si el tipo es 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 en su nombre.

   b. Para actualizar una regla, cambie su protocolo, descripción y fuente según sea necesario. Sin embargo, no puede cambiar el tipo de fuente. Por ejemplo, si el origen es un bloque CIDR de IPv4, no puede especificar un bloque de CIDR de IPv6, una lista de prefijos o un grupo de seguridad.

   c. Para eliminar una regla, pulse el botón Eliminar.

5. Para editar las reglas de salida, selecciona Editar reglas de salida en Acciones o en la pestaña Reglas de salida.

   a. Para agregar una regla, elija Agregar regla e ingrese el tipo, el protocolo, el puerto y el destino de la regla. También puede introducir una descripción opcional.

      Si el tipo es 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 en su nombre.

b. Para actualizar una regla, cambie su protocolo, descripción y fuente según sea necesario. Sin embargo, no puede cambiar el tipo de fuente. Por ejemplo, si el origen es un bloque CIDR de IPv4, no puede especificar un bloque de CIDR de IPv6, una lista de prefijos o un grupo de seguridad.

c. Para eliminar una regla, pulse el botón Eliminar.

6. Seleccione Guardar reglas.

Para configurar reglas del grupo de seguridad mediante la AWS CLI

- Agregar: utilice los comandos authorize-security-group-ingress y authorize-security-group-egress.
- Eliminar: utilice los comandos revoke-security-group-ingress y revoke-security-group-egress.
- Modificar: utilice los comandos modify-security-group-rules, update-security-group-rule-descriptions-ingress, y update-security-group-rule-descriptions-egress.

Eliminación de un grupo de seguridad

Cuando ya no necesite un grupo de seguridad creado, puede eliminarlo.

Requisitos

- El grupo de seguridad no se puede asociar a ningún recurso.
- Una regla no puede hacer referencia al grupo de seguridad en otro grupo de seguridad.
- El grupo de seguridad no puede ser el grupo de seguridad predeterminado para una VPC.

Para eliminar un grupo de seguridad con la consola

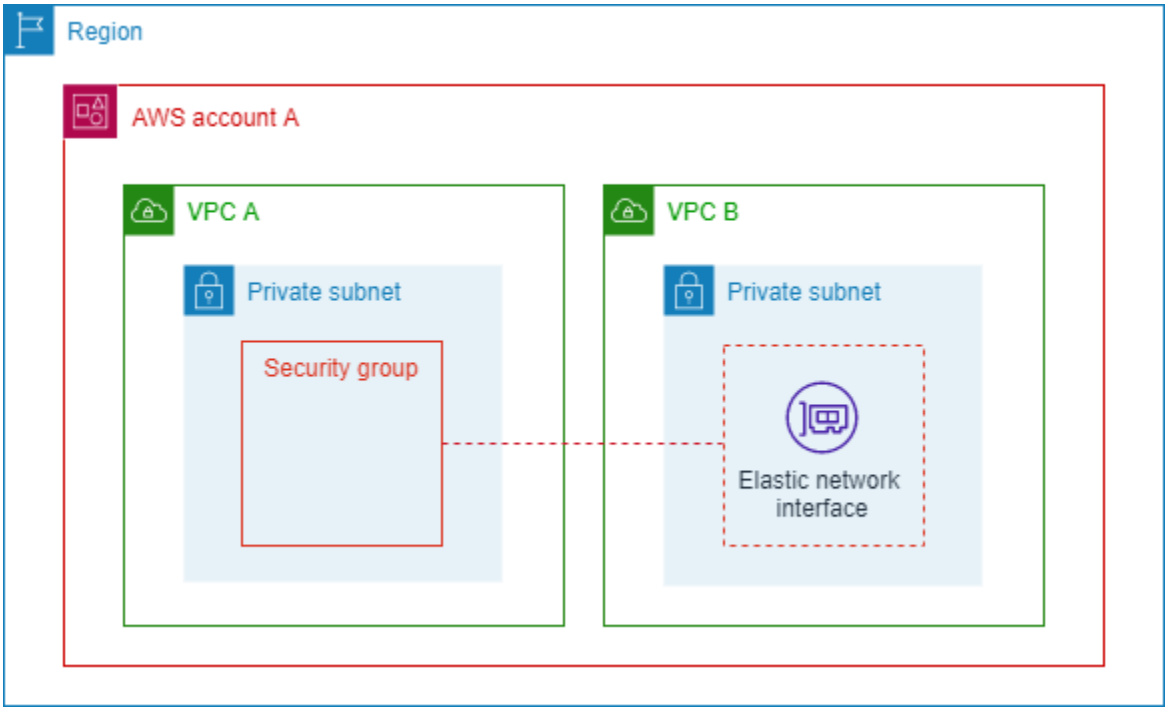
1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Security Groups (Grupos de seguridad).
3. Seleccione un grupo de seguridad y elija Acciones, Eliminar grupo de seguridad.
4. Si ha seleccionado más de un grupo de seguridad, se le solicitará que lo confirme. Si algunos de los grupos de seguridad no se pueden eliminar, mostramos el estado de cada grupo de seguridad, que indica si se eliminará. Para confirmar la eliminación, use Eliminar.
5. Elija Eliminar.

Para eliminar un grupo de seguridad mediante la AWS CLI

Utilice el comando delete-security-group.

Asociación de grupos de seguridad a varias VPC

Si tiene cargas de trabajo que se ejecutan en varias VPC que comparten requisitos de seguridad de red, puede utilizar la característica de Asociaciones de VPC a grupos de seguridad para asociar un grupo de seguridad a varias VPC de la misma región. Esto le permite administrar y mantener los grupos de seguridad en un solo lugar para varias VPC de su cuenta.



En el diagrama anterior, se muestra la cuenta A de AWS con dos VPC. Cada una de las VPC tiene cargas de trabajo que se ejecutan en una subred privada. En este caso, las cargas de trabajo de las subredes de la VPC A y B comparten los mismos requisitos de tráfico de red, por lo que la cuenta A puede usar la característica de asociación de VPC al grupo de seguridad para asociar el grupo de seguridad de la VPC A con la VPC B. Cualquier actualización realizada en el grupo de seguridad asociado se aplica automáticamente al tráfico de las cargas de trabajo de la subred de la VPC B.

Requisitos de la característica de Asociación de VPC a grupos de seguridad

- Debe ser propietario de la VPC o tener una de las subredes de la VPC compartida con usted para asociar un grupo de seguridad a esta.
- La VPC y los grupos de seguridad deben estar en la misma región de AWS.
- No se puede asociar un grupo de seguridad predeterminado con otra VPC ni asociar un grupo de seguridad con una VPC predeterminada.

- Tanto el propietario del grupo de seguridad como el propietario de la VPC pueden ver las asociaciones de la VPC al grupo de seguridad.

Servicios que admiten esta característica

- Amazon API Gateway (solo API de REST)
- AWS Auto Scaling
- CloudFormation
- Amazon EC2
- Amazon EFS
- Amazon EKS
- Amazon FSx
- AWS PrivateLink
- Amazon Route 53
- Elastic Load Balancing
  - Equilibrador de carga de aplicación
  - Equilibrador de carga de red

Asociación de un grupo de seguridad a otra VPC

En esta sección, se explica cómo utilizar Consola de administración de AWS y AWS CLI para asociar un grupo de seguridad a las VPC.

AWS Management Console

Para asociar un grupo de seguridad a otra VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Grupos de seguridad.
3. Elija un grupo de seguridad para ver sus detalles.
4. Elija la pestaña Asociaciones de VPC.
5. Elija Asociar VPC.
6. En ID de la VPC, elija una VPC para asociarla con el grupo de seguridad.

7. Elija Asociar VPC.

Command line

Para asociar un grupo de seguridad a otra VPC

1. Cree una asociación de VPC con associate-security-group-vpc.
2. Compruebe el estado de una asociación de VPC con describe-security-group-vpc-associations y espere a que aparezca el estado `associated`.

La VPC ya está asociada al grupo de seguridad.

Una vez que se haya asociado la VPC al grupo de seguridad, puede, por ejemplo, lanzar una instancia en la VPC y elegir este nuevo grupo de seguridad o hacer referencia a este grupo de seguridad en una regla de grupo de seguridad existente.

Disociación de un grupo de seguridad de otra VPC

En esta sección, se explica cómo usar la Consola de administración de AWS y la AWS CLI para disociar un grupo de seguridad de las VPC. Puede que desee hacerlo si su objetivo es eliminar el grupo de seguridad. Los grupos de seguridad no se pueden eliminar si están asociados. Solo puede disociar un grupo de seguridad si no hay interfaces de red en la VPC asociada que utilice ese grupo de seguridad.

AWS Management Console

Para disociar un grupo de seguridad de una VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Grupos de seguridad.
3. Elija un grupo de seguridad para ver sus detalles.
4. Elija la pestaña Asociaciones de VPC.
5. Elija Disociar VPC.
6. En ID de la VPC, elija una VPC para disociarla del grupo de seguridad.
7. Elija Disociar VPC.
8. Consulte el Estado de la disociación en la pestaña de asociaciones de la VPC y espere a que aparezca el estado `disassociated`.

Command line

Cómo disociar un grupo de seguridad de una VPC

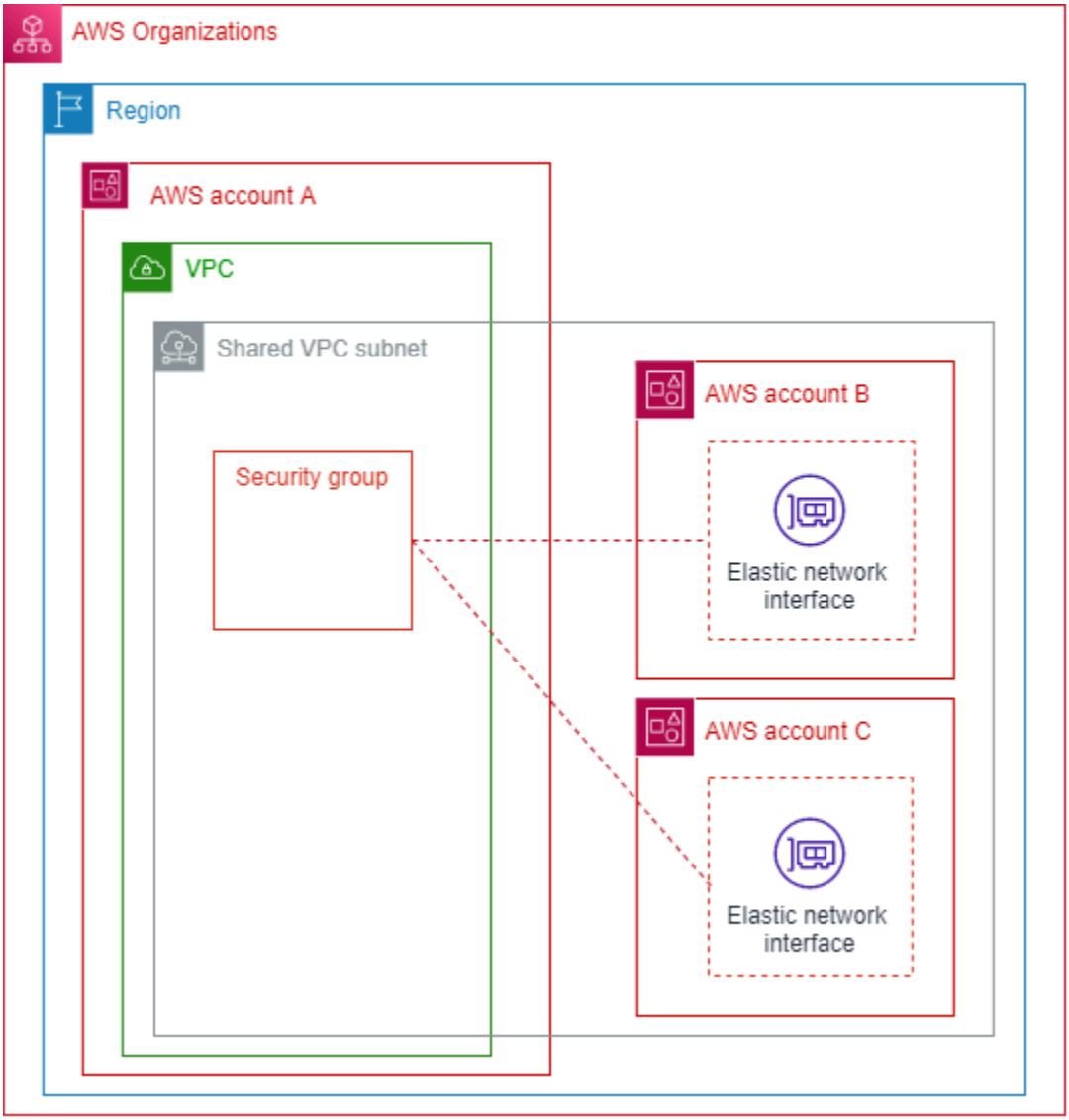
1. Disocie una asociación de VPC con disassociate-security-group-vpc.
2. Compruebe el estado de una disociación de la VPC con describe-security-group-vpc-associations y espere a que aparezca el estado `disassociated`.

La VPC ya se disoció del grupo de seguridad.

Compartir grupos de seguridad con AWS Organizations

La característica Grupo de seguridad compartido le permite compartir un grupo de seguridad con otras cuentas de AWS Organizations dentro de la misma región de AWS y hacer que el grupo de seguridad esté disponible para que lo utilicen esas cuentas.

En el siguiente diagrama, se muestra cómo puede utilizar la característica Grupo de seguridad compartido para simplificar la administración de los grupos de seguridad en todas las cuentas de su AWS Organizations:



En este diagrama, se muestran tres cuentas que forman parte de la misma organización. La cuenta A comparte una subred de VPC con las cuentas B y C. La cuenta A comparte el grupo de seguridad con las cuentas B y C mediante la característica de Grupos de seguridad compartidos. A continuación, las cuentas B y C utilizan ese grupo de seguridad cuando lanzan instancias en la subred compartida. Esto permite a la cuenta A administrar el grupo de seguridad; cualquier actualización del grupo de seguridad se aplica a los recursos que las cuentas B y C tienen en ejecución en la subred de VPC compartida.

Requisitos de la característica de Grupos de seguridad compartidos

- Esta característica solo está disponible para las cuentas de la misma organización en AWS Organizations. Debe habilitar el uso compartido de recursos en AWS Organizations.

- La cuenta que comparte el grupo de seguridad debe ser propietaria tanto de la VPC como del grupo de seguridad.
- No puede compartir los grupos de seguridad predeterminados.
- No puede compartir grupos de seguridad que estén en una VPC predeterminada.
- Las cuentas participantes pueden crear grupos de seguridad en una VPC compartida, pero no pueden compartir esos grupos de seguridad.
- Se requiere un conjunto mínimo de permisos para que una entidad principal de IAM comparta un grupo de seguridad con AWS RAM. Use las política de IAM administradas `AmazonEC2FullAccess` y `AWSResourceAccessManagerFullAccess` para garantizar que las entidades principales de IAM dispongan de los permisos necesarios para compartir y utilizar los grupos de seguridad compartidos. Si utiliza una política de IAM personalizada, las acciones `c2:PutResourcePolicy` y `ec2:DeleteResourcePolicy` son obligatorias. Estas son acciones de IAM solo de permiso. Si a una entidad principal de IAM no se le conceden estos permisos, se producirá un error al intentar compartir el grupo de seguridad mediante la AWS RAM.

Servicios que admiten esta característica

- Amazon API Gateway
- Amazon EC2
- Amazon ECS
- Amazon EFS
- Amazon EKS
- Amazon EMR
- Amazon FSx
- Amazon ElastiCache
- AWS Elastic Beanstalk
- AWS Glue
- Amazon MQ
- Amazon SageMaker AI
- Elastic Load Balancing
  - Equilibrador de carga de aplicación
  - Equilibrador de carga de red

Cómo afecta esta característica a las cuotas existentes

Se aplican cuotas de los grupos de seguridad. Sin embargo, para la cuota “Grupos de seguridad por interfaz de red”, si un participante utiliza grupos propios y compartidos en una interfaz de red elástica (ENI), se aplica la cuota mínima de propietario y participante.

Ejemplo para demostrar cómo esta característica afecta a la cuota:

- Cuota de cuentas de propietarios: 4 grupos de seguridad por interfaz
- Cuota de cuentas de participantes: 5 grupos de seguridad por interfaz.
- El propietario comparte los grupos SG-O1, SG-O2, SG-O3, SG-O4 y SG-O5 con el participante. El participante ya tiene sus propios grupos en la VPC: SG-P1, SG-P2, SG-P3, SG-P4, SG-P5.
- Si el participante crea una ENI y utiliza solo sus propios grupos, puede asociar los 5 grupos de seguridad (SG-P1, SG-P2, SG-P3, SG-P4 y SG-P5), ya que esa es su cuota.
- Si el participante crea una ENI y utiliza algún grupo compartido en ella, solo podrá asociar hasta 4 grupos. En este caso, la cuota de una ENI de este tipo es la cuota mínima de propietarios y participantes. Las posibles configuraciones válidas tendrán el siguiente aspecto:
  - SG-O1, SG-P1, SG-P2, SG-P3
  - SG-O1, SG-O2, SG-O3, SG-O4

Cómo compartir un grupo de seguridad

En esta sección, se explica cómo usar la Consola de administración de AWS y la AWS CLI para compartir un grupo de seguridad con otras cuentas de su organización.

AWS Management Console

Para compartir un grupo de seguridad

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Grupos de seguridad.
3. Elija un grupo de seguridad para ver sus detalles.
4. Elija la pestaña Sharing (Compartir) .
5. Elija Compartir grupo de seguridad.
6. Elija Crear recurso compartido. Como resultado, se abre la consola de AWS RAM, donde se creará el recurso compartido para el grupo de seguridad.

7. Ingrese un Nombre para el recurso compartido.
8. En Recursos (opcional), elija Grupos de seguridad.
9. Elija un grupo de seguridad. El grupo de seguridad no puede ser un grupo de seguridad predeterminado ni estar asociado a la VPC predeterminada.
10. Elija Siguiente.
11. Revise las acciones que las entidades principales podrán realizar y seleccione Siguiente.
12. En Entidades principales (opcional), seleccione Permitir compartir solo dentro de la organización.
13. En Entidades principales, seleccione uno de los siguientes tipos de entidades principales e introduzca los números correspondientes:

    - Cuenta de AWS: el número de una cuenta de su organización.
    - Organización: el ID de AWS Organizations.
    - Unidad organizativa (OU): el ID de una OU de la organización.
    - Rol de IAM: el ARN de un rol de IAM. La cuenta que creó el rol debe ser miembro de la misma organización que la cuenta que creó este recurso compartido.
    - Usuario de IAM: el ARN de un usuario de IAM. La cuenta que creó el usuario debe ser miembro de la misma organización que la cuenta que creó este recurso compartido.
    - Entidad principal del servicio: no puede compartir un grupo de seguridad con una entidad principal del servicio.
14. Seleccione Añadir.
15. Elija Siguiente.
16. Elija Crear recurso compartido.
17. En Recursos compartidos, espere que el Estado sea `Associated`. Si se produce un error en la asociación de grupos de seguridad puede deberse a una de las limitaciones que se han indicado anteriormente. Consulte los detalles del grupo de seguridad y la pestaña Compartir de la página de detalles para ver cualquier mensaje relacionado con los motivos por los que un grupo de seguridad no se puede compartir.
18. Vuelva a la lista de grupos de seguridad de la consola de la VPC.
19. Elija el grupo de seguridad que compartió.
20. Elija la pestaña Sharing (Compartir) . Su recurso de AWS RAM debería aparecer allí. Si no es así, es posible que se haya producido un error al crear el recurso compartido y que tenga que volver a crearlo.

Command line

Para compartir un grupo de seguridad

1. En primer lugar, debe crear un recurso compartido para el grupo de seguridad que desee compartir con AWS RAM. Consulte Crear un recurso compartido en AWS RAM en la Guía del usuario de AWS RAM para conocer los pasos para crear un recurso compartido con AWS RAM usando la AWS CLI
2. Para ver las asociaciones de recursos compartidos creadas, utilice get-resource-share-associations.

El grupo de seguridad ya está compartido. Puede seleccionar el grupo de seguridad cuando lanza una instancia de EC2 en una subred compartida dentro de la misma VPC.

Detención de la compartición de un grupo de seguridad

En esta sección, se explica cómo utilizar la Consola de administración de AWS y la AWS CLI para dejar de compartir un grupo de seguridad con otras cuentas de la organización.

AWS Management Console

Cómo dejar de compartir un grupo de seguridad

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Grupos de seguridad.
3. Elija un grupo de seguridad para ver sus detalles.
4. Elija la pestaña Sharing (Compartir) .
5. Elija un recurso compartido de un grupo de seguridad y elija Dejar de compartir.
6. Seleccione Sí, dejar de compartir.

Command line

Cómo dejar de compartir un grupo de seguridad

Elimine el recurso compartido con delete-resource-share.

El grupo de seguridad ya no está compartido. Cuando el propietario deja de compartir un grupo de seguridad, se aplican las siguientes reglas:

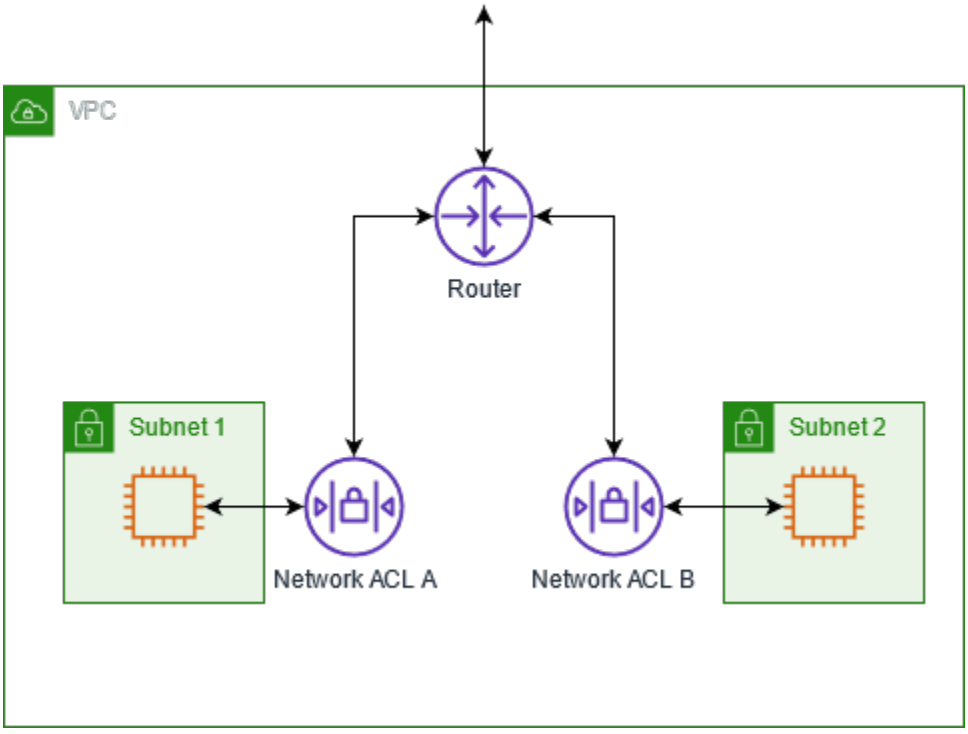
- Las interfaces de red elásticas (ENI) existentes participantes siguen recibiendo las actualizaciones de reglas de los grupos de seguridad que se realicen en los grupos de seguridad no compartidos. Dejar de compartir solo impide que el participante cree nuevas asociaciones con el grupo no compartido.
- Los participantes ya no pueden asociar el grupo de seguridad no compartido a ninguna ENI de su propiedad.
- Los participantes pueden describir y eliminar las ENI que siguen asociadas a los grupos de seguridad no compartidos.
- Si los participantes siguen teniendo ENI asociadas al grupo de seguridad no compartido, el propietario no puede eliminarlo. El propietario solo puede eliminar el grupo de seguridad después de que los participantes disocien (eliminen) el grupo de seguridad de todas sus ENI.
- Los participantes no pueden lanzar nuevas instancias de EC2 utilizando una ENI asociada a un grupo de seguridad no compartido.

Control del tráfico de la subred con listas de control de acceso a la red

Una lista de control de acceso (ACL) de red permite o deniega el tráfico entrante o saliente específico en el nivel de subred. Puede usar la ACL de red predeterminada para su VPC o puede crear una ACL de red personalizada para su VPC con reglas similares a las de sus grupos de seguridad. Las ACL de red personalizadas añaden una capa adicional de seguridad a su VPC.

El uso de ACL de red no supone ningún cargo adicional.

En el siguiente diagrama se muestra una VPC con dos subredes. Cada subred tiene una ACL de red. Cuando el tráfico entra en la VPC (por ejemplo, desde una VPC interconectada, una conexión VPN o Internet), el enrutador envía el tráfico a su destino. La ACL de red A determina qué tráfico destinado a la subred 1 puede entrar en la subred 1, y qué tráfico destinado a una ubicación fuera de la subred 1 puede salir de la subred 1. Del mismo modo, la ACL de red B determina qué tráfico puede entrar y salir de la subred 2.



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.

Contenido

- Conceptos básicos de la ACL de red
- Reglas de ACL de red
- ACL de red predeterminada para una VPC
- ACL de red personalizadas para su VPC
- Detección de la MTU de la ruta y las ACL de red
- Creación de una ACL de red para su VPC
- Administración de las asociaciones de ACL de red para su VPC
- Eliminación de una ACL de red para su VPC
- Ejemplo: controlar el acceso a las instancias de una subred

Conceptos básicos de la ACL de red

A continuación se describen los conceptos básicos que debe saber acerca de las ACL de red antes de comenzar.

Asociaciones de ACL de red

- 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 de manera automática a la ACL de red predeterminada.
- Puede crear una ACL de red personalizada y asociarla a una subred para permitir o denegar el tráfico entrante o saliente específico a nivel de subred.
- 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.

Reglas de ACL de red

- Una ACL de red tiene reglas de entrada y reglas de salida. Hay cuotas (o límites) en cuanto al número de reglas que puede tener por cada ACL de red. Cada regla puede permitir o denegar el tráfico. Cada regla tiene un número del 1 al 32 766. Evaluamos las reglas en orden, empezando por la regla numerada más baja, al decidir permitir o denegar el tráfico. Si el tráfico coincide con una regla, se aplica la regla y no evaluamos ninguna regla adicional. Le recomendamos que, para empezar, cree reglas en incrementos (por ejemplo, incrementos de 10 o 100), de forma que pueda insertar reglas nuevas más adelante de ser necesario.
- Evaluamos las reglas de ACL de red cuando el tráfico entra y sale de la subred, no cuando se enruta dentro de una subred.
- Las NACL no tienen estado, lo que significa que no se guarda la información sobre el tráfico enviado o recibido anteriormente. Si, por ejemplo, crea una regla de NACL para permitir que cierto tráfico entrante específico llegue a una subred, no se permitirán las respuestas a ese tráfico automáticamente. Esto contrasta con la forma en que funcionan los grupos de seguridad. Los grupos de seguridad tienen estado, lo que significa que se guarda la información sobre el tráfico enviado o recibido anteriormente. Si, por ejemplo, un grupo de seguridad permite el tráfico entrante a una instancia EC2, las respuestas se permiten de forma automática independientemente de las reglas de salida del grupo de seguridad.

Limitaciones

- Existen cuotas (también conocidas como límites) para ACL de red. Para obtener más información, consulte ACL de red.

- Las ACL de red no pueden bloquear las solicitudes de DNS hacia Route 53 Resolver (también conocido como dirección IP VPC+2 o AmazonProvidedDNS) ni desde este. Para filtrar las solicitudes de DNS a través de Route 53 Resolver, puede activar el Firewall de DNS de Route 53 Resolver.
- Las ACL de red no pueden bloquear el tráfico hacia el Servicio de metadatos de la instancia (IMDS). Para administrar el acceso al IMDS, consulte Configurar las opciones de metadatos de la instancia en la Guía del usuario de Amazon EC2.
- Las ACL de red de Amazon no filtran el tráfico destinado a los siguientes servicios ni desde estos:
  - Servicios de nombres de dominio de Amazon (DNS)
  - Protocolo de configuración dinámica de host de Amazon (DHCP)
  - Metadatos de la instancia de Amazon EC2
  - Puntos de conexión de metadatos de tareas de Amazon ECS
  - Activación de licencias para instancias de Windows
  - Servicio de sincronización temporal de Amazon
  - Direcciones IP reservadas del enrutador de la VPC predeterminado

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.
- Intervalo 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.

Para ver ejemplos de reglas, consulte the section called “Ejemplo: controlar el acceso a las instancias de una subred”.

Consideraciones

- Existen cuotas (también conocidas como límites) para el número de reglas por ACL de red. Para obtener más información, consulte Cuotas de Amazon VPC.
- Al añadir o eliminar una regla de una ACL, las subredes asociadas a la ACL estarán sujetas a ese cambio. Los cambios surten efecto después de un corto período de tiempo.
- 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`.
- Puede que desee agregar una regla de denegación en caso de que deba abrir un amplio rango de puertos, pero haya ciertos puertos dentro de ese rango que quiera denegar. Asegúrese de asignar a la regla de denegación un número inferior que la regla que permite el tráfico en el rango más amplio de puertos.
- Si agrega y elimina reglas de una ACL de red al mismo tiempo, tenga cuidado. Si elimina reglas de entrada o de salida y, a continuación, agrega más entradas nuevas de las permitidas (consulte Cuotas de Amazon VPC), se quitarán las entradas seleccionadas para eliminación y las nuevas entradas no se agregarán. Esto puede provocar problemas de conectividad inesperados e impedir involuntariamente el acceso a su VPC y desde esta.

ACL de red predeterminada para una VPC

Su nube privada virtual (VPC) incluye de forma automática una ACL de red predeterminada. Una 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 reglas cuyo número de regla es un asterisco (*). Estas reglas garantizan que si un paquete no coincide con ninguna de las reglas numeradas, se denegará.

Puede modificar una ACL de red predeterminada si agrega reglas o elimina las reglas numeradas predeterminadas. No puede eliminar una regla cuyo número de regla es un asterisco.

Reglas de entrada predeterminadas

En la tabla siguiente, se muestran las reglas de entrada predeterminadas para una ACL de red predeterminada. Las reglas para IPv6 se agregan solo si crea la VPC con un bloque de CIDR IPv6 asociado o asocia un bloque de CIDR IPv6 a la VPC. Sin embargo, si ha modificado las reglas de entrada de la ACL de red predeterminada, no se agregará la una regla que permite todo el tráfico IPv6 entrante cuando asocie un bloque de IPv6 con su VPC.

Regla n.º	Tipo	Protocolo	Intervalo de puertos	Fuente	Permitir/ Denegar
100	Todo el tráfico IPv4	Todos	Todos	0.0.0.0/0	PERMITIR
101	Todo el tráfico IPv6	Todos	Todos	::/0	PERMITIR
*	Todo el tráfico	Todos	Todos	0.0.0.0/0	DENY
*	Todo el tráfico IPv6	Todos	Todos	::/0	DENY

Reglas de salida predeterminadas

En la tabla siguiente, se muestran las reglas de salida predeterminadas para una ACL de red predeterminada. Las reglas para IPv6 se agregan solo si crea la VPC con un bloque de CIDR IPv6 asociado o asocia un bloque de CIDR IPv6 a la VPC. Sin embargo, si ha modificado las reglas de salida de la ACL de red predeterminada, no se agregará la una regla que permite todo el tráfico IPv6 de salida cuando asocie un bloque de IPv6 con su VPC.

Regla n.º	Tipo	Protocolo	Rango de puerto	Destino	Permitir/ Denegar
100	Todo el tráfico	Todos	Todos	0.0.0.0/0	PERMITIR
101	Todo el tráfico IPv6	Todos	Todos	::/0	PERMITIR
*	Todo el tráfico	Todos	Todos	0.0.0.0/0	DENY
*	Todo el tráfico IPv6	Todos	Todos	::/0	DENY

ACL de red personalizadas para su VPC

Puede crear una ACL de red personalizada y asociarla a una subred para permitir o denegar el tráfico entrante o saliente específico a nivel de subred. Para obtener más información, consulte the section called “Crear una ACL de red”.

Cada ACL de red incluye una regla de entrada y una regla de salida predeterminadas cuyo número de regla es un asterisco (*). Estas reglas garantizan que si un paquete no coincide con ninguna de las reglas, se denegará.

Puede modificar una ACL de red predeterminada si agrega o elimina reglas. No puede eliminar una regla cuyo número de regla es un asterisco.

Para todas las reglas que agregue, debe haber una regla de entrada o salida que permita el tráfico de respuesta. Para obtener más información acerca de cómo seleccionar el rango de puerto efímero correcto, consulte Puertos efímeros.

Ejemplo de reglas de entrada

En la tabla siguiente, se muestran las reglas de entrada para una ACL de red. Las reglas para IPv6 se agregan solo si la VPC tiene un bloque de CIDR IPv6 asociado. El tráfico IPv4 e IPv6 se evalúan por separado. Por lo tanto, ninguna de las reglas para el tráfico IPv4 se aplican a las del tráfico IPv6. Puede agregar reglas de IPv6 junto a las reglas de IPv4 correspondientes o agregar las reglas de IPv6 después de la última regla de IPv4.

Cuando un paquete llega a la subred, lo evaluamos según las reglas de entrada de la ACL de red con la que está asociada la subred, comenzando desde la regla con el número inferior. Por ejemplo, supongamos que hay tráfico IPv4 destinado al puerto HTTPS (443). El paquete no coincide con las reglas 100 o 105. Cumple con la regla 110, que permite que el tráfico entre en la subred. Si el paquete se ha destinado al puerto 139 (NetBIOS), no se le aplica ninguna de las reglas numeradas, así que la regla * para el tráfico IPv4 termina por rechazar el paquete.

Regla n.º	Tipo	Protocolo	Intervalo de puertos	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 de direcciones IPv4 públicas de su red doméstica (a través de la puerta de enlace de Internet).

Regla n.º	Tipo	Protocolo	Intervalo de puertos	Fuente	Permitir/ Denegar	Comentarios
140	TCP personalizada	TCP	32768-65535	0.0.0.0/0	PERMITIR	Permite el tráfico IPv4 de retorno de entrada de Internet (para solicitudes que se originan en la subred).
145	TCP personalizada	TCP	32768-65535	::/0	PERMITIR	Permite el tráfico IPv6 de retorno entrante de Internet (para solicitudes que se originan en la subred).
*	Todo el tráfico	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).

Ejemplo de reglas de salida

En la tabla siguiente, se muestran reglas de salida de ejemplo para una ACL de red personalizada. Las reglas para IPv6 se agregan solo si la VPC tiene un bloque de CIDR IPv6 asociado. El tráfico IPv4 e IPv6 se evalúan por separado. Por lo tanto, ninguna de las reglas para el tráfico IPv4 se aplican a las del tráfico IPv6. Puede agregar reglas de IPv6 junto a las reglas de IPv4 correspondientes o agregar las reglas de IPv6 después de la última regla de IPv4.

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.
120	TCP personalizada	TCP	*1024-655 5*	*192.0.2.(/24*	PERMITIR	Permite las respuestas de salida al tráfico SSH desde su red doméstica.
140	TCP personalizada	TCP	*32768-65 35*	0.0.0.0/0	PERMITIR	Permite las respuestas IPv4 de salida a clientes de Internet (por ejemplo, ofrecer páginas web).
145	TCP personalizada	TCP	*32768-65 35*	::/0	PERMITIR	Permite las respuestas IPv6 de salida a clientes de Internet

Regla n.º	Tipo	Protocolo	Rango de puerto	Destino	Permitir/ Denegar	Comentarios
						(por ejemplo, ofrecer páginas web).
*	Todo el tráfico	Todos	Todos	0.0.0.0/0	DENY	Deniega todo el tráfico IPv4 de salida no controlado por ninguna regla precedente.
*	Todo el tráfico	Todos	Todos	::/0	DENY	Deniega todo el tráfico IPv6 de salida no controlado por ninguna regla precedente.

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 puerta de enlace 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 su VPC es el cliente que inicia una solicitud, su ACL de red deberá tener una regla de entrada para permitir el tráfico destinado a los puertos efímeros específicos del sistema operativo de la instancia.

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.

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 sus balanceadores de carga e instancias del backend, consulte los siguientes:

- ACL de red para el equilibrador de carga de aplicación
- ACL de red para el equilibrador de carga de red
- ACL de red para el equilibrador de carga clásico

Solución de problemas de accesibilidad

Reachability Analyzer es una herramienta de análisis de configuración estática. Utilice Reachability Analyzer para analizar y depurar la accesibilidad de la red entre dos recursos en la VPC. Reachability Analyzer produce detalles salto a salto de la ruta virtual entre estos recursos cuando son accesibles y, en caso contrario, identifica el componente de bloqueo. Por ejemplo, puede identificar reglas de ACL de red faltantes o mal configuradas.

Para obtener más información, consulte la Guía del Analizador de accesibilidad.

Detección de la MTU de la ruta y las ACL de red

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.

En el caso de IPv4, cuando un host envía un paquete mayor que la MTU del host receptor o de un dispositivo a lo largo de la ruta, el host o el dispositivo receptor descarta el paquete. 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 de un dispositivo a lo largo de la ruta, el host o dispositivo receptor descarta el paquete. 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.

Creación de una ACL de red para su VPC

Las siguientes tareas muestran cómo crear una ACL de red, agregar reglas a la ACL de red y, a continuación, asociar la ACL de red a una subred.

Tareas

- Paso 1: cree una ACL de red
- Paso 2: agregue reglas
- Paso 3: asocie una subred a una ACL de red
- (Opcional) Administración de las ACL de red con Firewall Manager

Paso 1: cree una ACL de red

Puede crear una ACL de red personalizada para su VPC. Las reglas iniciales de una ACL de red personalizada bloquean el tráfico de entrada y de salida. De manera predeterminada, su nueva ACL de red personalizada no está asociada a una subred y debe asociarse de manera explícita a las subredes.

Creación de una ACL de red mediante la consola

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 Crear ACL de red.
4. (Opcional) En Nombre, ingrese un nombre para su ACL de red.
5. En VPC, seleccione la VPC.
6. (Opcional) En Etiquetas, elija Agregar etiqueta y especifique una clave y un valor de etiqueta.
7. Elija Crear ACL de red.

Creación de una ACL de red mediante la línea de comandos

- create-network-acl (AWS CLI)
- New-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Paso 2: agregue reglas

Puede agregar reglas que permitan o denieguen el tráfico de entrada o salida.

Las reglas se procesan por orden; se empieza por la regla con 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.

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.

Incorporación de una regla a una ACL de red mediante la consola

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.
4. Para agregar una regla de entrada, haga lo siguiente:
    a. Elija la pestaña Reglas de entrada.
    b. Elija Editar reglas de entrada, Agregar nueva regla.
    c. Ingrese un número de regla que aún no esté en uso, un tipo, protocolo, intervalo de puertos, origen y si desea permitir o denegar el tráfico. Para algunos tipos, completaremos el protocolo y el puerto por usted. Si se le solicita un rango de puertos, escriba un número de puerto o un rango de puertos (por ejemplo, 49152-65535).

        Para utilizar un protocolo que no aparezca en la lista, elija Protocolo personalizado para el tipo y, a continuación, seleccione el protocolo. Para obtener más información, consulte Números de protocolo.
    d. Seleccione Save changes (Guardar cambios).
5. Para agregar una regla de salida, haga lo siguiente:
    a. Elija la pestaña Outbound rules (Reglas de salida).
    b. Elija Editar reglas de salida, Agregar nueva regla.
    c. Ingrese un número de regla que aún no esté en uso, un tipo, protocolo, intervalo de puertos, origen y si desea permitir o denegar el tráfico. Para algunos tipos, completaremos el protocolo y el puerto por usted. Si se le solicita un rango de puertos, escriba un número de puerto o un rango de puertos (por ejemplo, 49152-65535).

Para utilizar un protocolo que no aparezca en la lista, elija Protocolo personalizado para el tipo y, a continuación, seleccione el protocolo. Para obtener más información, consulte Números de protocolo.

d. Seleccione Save changes (Guardar cambios).

Incorporación de una regla a una ACL de red mediante la línea de comandos

- create-network-acl-entry (AWS CLI)
- New-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Sustitución de una regla en una ACL de red mediante la línea de comandos

- replace-network-acl-entry (AWS CLI)
- Set-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Eliminación de una regla desde una ACL de red mediante la línea de comandos

- delete-network-acl-entry (AWS CLI)
- Remove-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Paso 3: asocie 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.

(Opcional) Administración de las ACL de red con Firewall Manager

AWS Firewall Manager simplifica las tareas de administración y mantenimiento de las ACL de red en varias cuentas y subredes. Puede utilizar Firewall Manager para supervisar las cuentas y las subredes de la organización y para aplicar de manera automática las configuraciones de las ACL de red que se hayan definido. Firewall Manager es especialmente útil cuando se desea proteger la organización en su totalidad o si se agregan con frecuencia nuevas subredes que se desea proteger de manera automática desde una cuenta de administrador central.

Con una política de Firewall Manager para las ACL de red, y desde una cuenta de administrador única, puede configurar, supervisar y administrar el conjunto de reglas mínimo que desea definir en las ACL de red utilizadas en la organización. Usted especifica las cuentas y las subredes de la organización que estén dentro del alcance de la política de Firewall Manager. Firewall Manager informa del estado de cumplimiento de las ACL de red de las subredes dentro del alcance; también se puede configurar Firewall Manager para que corrija de manera automática las ACL de red no conformes.

Si desea obtener más información, consulte los siguientes recursos en la Guía para desarrolladores de AWS Firewall Manager:

- AWS Firewall Manager Requisitos previos de
- Configuración de políticas de ACL de red de AWS Firewall Manager
- Uso de políticas de ACL de red con Firewall Manager

Administración de las asociaciones de ACL de red para su VPC

Cada subred está asociada a una ACL de red. Al crear una subred por primera vez, esta se asocia inicialmente a la ACL de red predeterminada de la VPC. Puede crear una ACL de red personalizada y asociarla a una o más subredes, en sustitución de la asociación de ACL de red anterior.

Tareas

- Descripción de las asociaciones de ACL de red
- Cambio de las subredes asociadas a una ACL de red
- Cambio de la ACL de red asociada a una subred

Descripción de las asociaciones de ACL de red

Puede describir la ACL de red asociada a una subred y también puede describir las subredes asociadas a una ACL de red.

Descripción de la ACL de red asociada 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 Subnets (Subredes).
3. Seleccione la subred.
4. Seleccione la pestaña ACL de red.

Descripción de la ACL de red asociada a una subred mediante la AWS CLI

Utilice el siguiente comando describe-network-acls para enumerar las ACL de red asociadas a la subred especificada.

```
aws ec2 describe-network-acls --filters Name=association.subnet-
id,Values=subnet-0d2d1b81e0bc9c6d4 --query NetworkAcls[*].NetworkAclId
```

A continuación, se muestra un ejemplo del resultado.

```
[
    "acl-03701d1f82d8c3fd6"
]
```

Descripción de las subredes asociadas a una ACL de red mediante la consola

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.
4. Seleccione la pestaña Asociaciones de subredes.

Descripción de las subredes asociadas a una ACL de red mediante la AWS CLI

Utilice el siguiente comando describe-network-acls para enumerar las subredes asociadas a la ACL de red especificada.

```
aws ec2 describe-network-acls --network-acl-ids acl-060415a18fcc9afde --query
 NetworkAcls[*].Associations[].SubnetId
```

A continuación, se muestra un ejemplo del resultado.

```
[
    "subnet-0d2d1b81e0bc9c6d4",
    "subnet-0e990c67809773b19",
    "subnet-0eb17d85f5dfd33b1",
    "subnet-0e01d500780bb7468"
]
```

Cambio de las subredes asociadas a una ACL de red

Puede desasociar una ACL de red personalizada de una subred. Cuando se ha desasociado una subred de la ACL de red personalizada, la subred se asocia automáticamente a la ACL de red predeterminada de la VPC. Los cambios surten efecto después de un corto período de tiempo.

Cambio de las subredes 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.
3. Seleccione la ACL de red.
4. En el menú Acciones, elija Editar asociaciones de subred.
5. Elimine la subred de Subredes seleccionadas.
6. Seleccione Save changes (Guardar cambios).

Cambio de la ACL de red asociada a 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 de la VPC. Si crea una ACL de red personalizada, asocie la ACL de red a una o más subredes para aplicar las reglas de la ACL de red.

Después de cambiar la ACL de red de una subred, los cambios surten efecto al cabo de un breve período de tiempo.

Cambio de la ACL de red 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 (Subredes).
3. Seleccione la subred.
4. Elija Acciones, Editar asociación de ACL de red.
5. Para el ID de ACL de red, seleccione la ACL de red que desee asociar a la subred y revise las reglas de entrada y salida de la ACL de red seleccionada.
6. Seleccione Save.

Sustitución de una ACL de red con la línea de comandos

- replace-network-acl-association (AWS CLI)
- Set-EC2NetworkAclAssociation (AWS Tools for Windows PowerShell)

Eliminación de una ACL de red para su VPC

Cuando ya no necesite una ACL de red, puede eliminarla. La ACL de red no se puede eliminar si tiene subredes asociadas. La ACL de red predeterminada no se puede eliminar.

Eliminación de las asociaciones de una ACL de red mediante la consola

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 Asociada con indica el número de subredes asociadas a cada ACL de red. Esta columna es - si no hay subredes asociadas.
3. Seleccione la ACL de red.
4. En el menú Acciones, elija Editar asociaciones de subred.
5. Elimine las asociaciones de subredes.
6. Seleccione Save changes (Guardar cambios).

Descripción de las ACL de la red, incluidas las asociaciones, mediante la línea de comandos

- describe-network-acls (AWS CLI)
- Get-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Sustitución de una ACL de red mediante la línea de comandos

- replace-network-acl-association (AWS CLI)

- Set-EC2NetworkAclAssociation (AWS Tools for Windows PowerShell)

Eliminación de una ACL de red mediante la consola

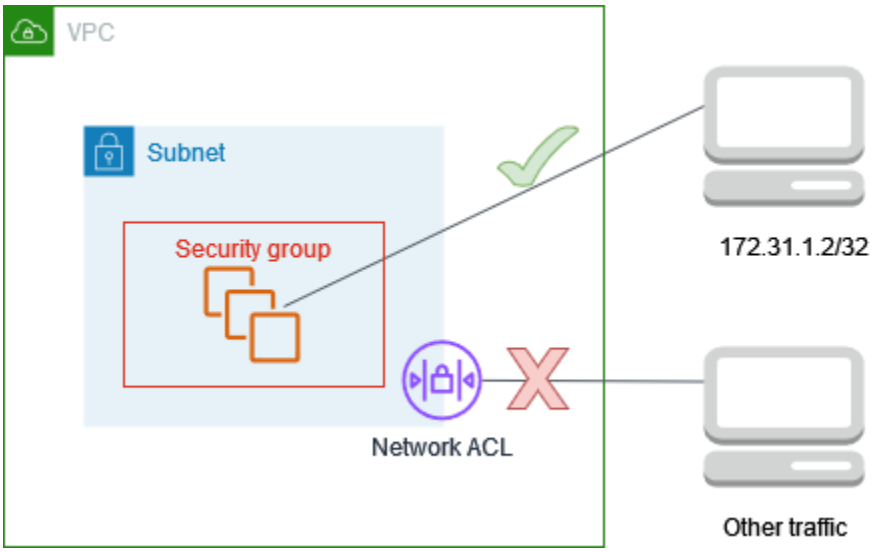
1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Network ACLs.
3. Seleccione la ACL de red.
4. Seleccione Acciones y Eliminar las ACL de red.
5. Cuando le pidan confirmación, escriba **`delete`** y elija Eliminar.

Eliminación de una ACL de red mediante la línea de comandos

- 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 para realizar tareas administrativas. El equipo remoto puede ser un equipo en la red local, tal como se muestra en el diagrama, o puede ser una instancia en una subred o VPC diferente. Las reglas de ACL de red para la subred y las reglas del grupo de seguridad para las instancias permiten el acceso desde la dirección IP de su equipo remoto. El resto del tráfico de Internet u otras redes se deniega.



Usar una ACL de red 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.

Por ejemplo, si se actualiza accidentalmente el grupo de seguridad para permitir el acceso SSH entrante desde cualquier lugar, la ACL de red restringe el acceso a únicamente el rango de direcciones IP del equipo remoto. La ACL de red deniega el tráfico SSH entrante desde cualquier otra dirección IP.

Reglas de ACL de red

A continuación se muestran reglas de entrada de ejemplo para la ACL de red asociada a la subred. Estas reglas se aplican a todas las instancias de la subred.

Regla n.º	Tipo	Protocolo	Intervalo de puertos	Fuente	Permitir/ Denegar	Comentarios
100	SSH	TCP	22	*172.31.1.2/32*	PERMITIR	Permita el tráfico de entrada desde el equipo remoto.
*	Todo el tráfico	Todos	Todos	0.0.0.0/0	DENY	Deniegue todo el resto de tráfico de entrada.

A continuación se muestran reglas de salida de ejemplo para la ACL de red asociada a la subred. Las ACL de red son sin estado. Por lo tanto, debe incluir una regla que permita respuestas al tráfico de entrada.

Regla n.º	Tipo	Protocolo	Rango de puerto	Destino	Permitir/ Denegar	Comentarios
100	TCP personalizada	TCP	1024-65535	*172.31.1.2/32*	PERMITIR	Permite las respuestas salientes al equipo remoto.
*	Todo el tráfico	Todos	Todos	0.0.0.0/0	DENEGAR	Deniega todo el resto de tráfico saliente.

Reglas del grupo de seguridad

A continuación, se muestran las reglas de entrada de ejemplo de un grupo de seguridad asociado a las instancias. Estas reglas se aplican a todas las instancias asociadas al grupo de seguridad. Un usuario con la clave privada de par de claves asociado a las instancias puede conectarse a las instancias desde el equipo remoto mediante SSH.

Tipo de protocolo	Protocolo	Intervalo de puertos	Fuente	Comentarios
Todo el tráfico	Todos	Todos	*sg-1234567890abcdef0*	Permita la comunicación entre las instancias asociadas a este grupo de seguridad.
SSH	TCP	22	*172.31.1.2/32*	Permita el acceso SSH de

Tipo de protocolo	Protocolo	Intervalo de puertos	Fuente	Comentarios
				entrada desde el equipo remoto.

A continuación, se muestran las reglas de salida de ejemplo de un grupo de seguridad asociado a las instancias. Los grupos de seguridad son grupos con estado. Por lo tanto, no necesita una regla que permita respuestas al tráfico entrante.

Tipo de protocolo	Protocolo	Rango de puerto	Destino	Comentarios
Todo el tráfico	Todos	Todos	*sg-1234567890abcdef0*	Permita la comunicación entre las instancias asociadas a este grupo de seguridad.

Diferencias entre las ACL de red y los grupos de seguridad

La siguiente tabla resume las diferencias básicas entre ACL de red y grupos de seguridad.

Característica	ACL de red	Grupo de seguridad
Nivel de operación	Nivel de subred	Nivel de instancia
Ámbito	Se aplica a todas las instancias en las subredes asociadas	Se aplica a todas las instancias asociadas al grupo de seguridad
Tipo de regla	Reglas de permiso y denegación	Solo reglas de permiso

Característica	ACL de red	Grupo de seguridad
Evaluación de reglas	Evalúa las reglas en orden ascendente hasta encontrar una coincidencia con el tráfico	Evalúa todas las normas antes de decidir si permitir el tráfico
Tráfico de retorno	Debe estar permitido de forma explícita (sin estado)	Permitido automáticamente (con estado)

Resiliencia en Amazon Virtual Private Cloud

La infraestructura global de AWS se divide en Regiones de AWS y zonas de disponibilidad. Las Regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes de baja latencia, con 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 uno o varios centros de datos.

Regiones de AWSLas son los componentes principales y cada una representa una ubicación geográfica distinta que aloja varias zonas de disponibilidad físicamente separadas y aisladas. Estas zonas de disponibilidad se encuentran conectadas a través de un entramado de red con un alto nivel de rendimiento y redundancia, además de baja latencia, lo que da lugar a una comunicación y una transferencia de datos fluida entre ellas.

La arquitectura de las zonas de disponibilidad es un elemento diferenciador clave, ya que están diseñadas para ser mucho más robustas y tolerantes a los fallos que las infraestructuras tradicionales de centros de datos únicos o múltiples. Al distribuir los recursos entre varias zonas de disponibilidad dentro de una región, las aplicaciones y las bases de datos pueden configurarse para que, en caso de un error, conmuten de una zona a la otra sin ninguna interrupción en el servicio. Este nivel de redundancia y alta disponibilidad es un requisito fundamental para las cargas de trabajo esenciales y permite a las organizaciones crear soluciones resilientes nativas en la nube.

Además, la escala y alcance mundial de la infraestructura AWS permite que los clientes desplieguen sus aplicaciones más cerca de los usuarios finales, lo que reduce la latencia y mejora la experiencia general del usuario. La disponibilidad de varias regiones en todo el mundo también permite una soberanía y un cumplimiento efectivos de los datos, ya que los clientes pueden almacenar y procesar

los datos dentro de los límites geográficos que exijan sus necesidades regulatorias y comerciales específicas.

Con la infraestructura mundial AWS, las organizaciones pueden diseñar sus entornos de nube para que tengan una alta disponibilidad, sean tolerantes a errores y sean escalables, con la flexibilidad necesaria para adaptarse a los requisitos cambiantes y a las distintas necesidades empresariales. Esta base robusta es un factor clave para la implementación exitosa de aplicaciones y servicios modernos en la nube.

Para obtener más información sobre las Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global de AWS.

Puede configurar las VPC para cumplir con los requisitos de resiliencia de las cargas de trabajo. Para obtener más información, consulte los siguientes temas:

- Comprensión de los patrones de resiliencia y las compensaciones (Blog de arquitectura de AWS)
- Planificación de la topología de red (Marco de AWS Well-Architected)
- Opciones de conectividad de Amazon Virtual Private Cloud (Documentos técnicos de AWS)

Validación de conformidad para Amazon Virtual Private Cloud

Nuestra nueva experiencia de registro de AWS no está diseñada para cargas de trabajo reguladas. Si está utilizando nuestra nueva experiencia de registro de AWS, pero quiere utilizar AWS para cargas de trabajo reguladas, puede registrarse en AWS (avanzado) o activar características avanzadas para su entorno de AWS.

Para saber si un Servicio de AWS está incluido en el alcance de programas de cumplimiento específicos, consulte Servicios de AWS incluidos por programa de cumplimiento y se elige el programa de cumplimiento de su interés. 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 confidencialidad de los datos, los objetivos de conformidad de la empresa, así como de la legislación y los reglamentos aplicables. Para obtener más información sobre la responsabilidad de cumplimiento al usar Servicios de AWS, consulte la Documentación de seguridad de AWS.

Bloqueo de acceso público de las VPC y subredes

La característica de bloqueo de acceso público (BPA) de la VPC es una característica de seguridad centralizada que impide con autoridad el acceso público de Internet a los recursos de la VPC en toda una cuenta de AWS. Garantiza el cumplimiento con los requisitos de seguridad y, al mismo tiempo, proporciona flexibilidad para excepciones específicas y capacidades de auditoría.

La característica de BPA de la VPC tiene los siguientes modos:

- Bidireccional: se bloquea todo el tráfico hacia y desde las puertas de enlace de Internet y las puertas de enlace de Internet de solo salida de esta región (excepto las VPC y las subredes excluidas).
- Solo de entrada: se bloquea todo el tráfico de Internet a las VPC de esta región (excepto las VPC o subredes excluidas). Solo se permite el tráfico hacia y desde las puertas de enlace NAT y las puertas de enlace de Internet solo de salida, ya que estas puertas de enlace solo permiten establecer conexiones salientes.

También puede crear “exclusiones” para esta característica para el tráfico que no desee bloquear. Una exclusión es un modo que se puede aplicar a una sola VPC o subred y que la exime del modo BPA de la VPC de la cuenta y permitirá el acceso bidireccional o solo de salida.

Las exclusiones pueden tener cualquiera de los siguientes modos:

- Bidireccional: se permite todo el tráfico de Internet hacia y desde las VPC y subredes excluidas.
- Solo de salida: se permite el tráfico de Internet saliente desde las VPC y subredes excluidas. Se bloquea el tráfico de Internet entrante a las VPC y subredes excluidas. Esto solo se aplica cuando el BPA de la VPC está establecido en modo bidireccional.

Contenido

- Conceptos básicos del BPA de la VPC
- Evaluación del impacto y monitoreo del BPA de la VPC
- Ejemplo avanzado

Conceptos básicos del BPA de la VPC

En esta sección, se describen detalles importantes sobre el BPA de la VPC, incluidos los servicios que lo admiten y cómo puede trabajar con él.

Contenido

- Disponibilidad en las regiones
- AWSImpacto en los servicios de y cuáles lo admiten
- Limitaciones del BPA de la VPC
- Control del acceso al BPA de la VPC con una política de IAM
- Activación del modo bidireccional del BPA de la VPC para su cuenta
- Cambiar el modo del BPA de la VPC a modo de solo entrada
- Crear y eliminar exclusiones
- Habilite el BPA de la VPC a nivel de Organization

Disponibilidad en las regiones

El BPA de la VPC está disponible en todas las regiones de AWS comerciales, incluso GovCloud y las regiones de China.

En esta guía, también encontrará información sobre el uso del Analizador de acceso a la red y el Analizador de accesibilidad con el BPA de la VPC. Tenga en cuenta que el Analizador de acceso a la red y el Analizador de accesibilidad no están disponibles en todas las regiones comerciales. Para obtener información sobre la disponibilidad regional del Analizador de acceso a la red y el Analizador de accesibilidad, consulte Limitaciones en la Guía del Analizador de acceso a la red y Consideraciones de la Guía del Analizador de accesibilidad.

AWSImpacto en los servicios de y cuáles lo admiten

Los siguientes recursos y servicios admiten el BPA de la VPC y el tráfico a estos servicios y recursos se ve afectado por el BPA de la VPC:

- Puerta de enlace de Internet: se bloquea todo el tráfico entrante y saliente.
- Puerta de enlace de Internet solo de salida: se bloquea todo el tráfico saliente. Las puertas de enlace de Internet de solo salida no permiten el tráfico entrante.

- Equilibrador de carga de puerta de enlace (GWLB): se bloquea todo el tráfico entrante y saliente, excepto que se excluya la subred que contiene los punto de conexión de GWLB.
- Puerta de enlace NAT: se bloquea todo el tráfico entrante y saliente. Las puertas de enlace NAT requieren una puerta de enlace de Internet para la conectividad a Internet.
- Equilibrador de carga de red orientado a Internet: se bloquea todo el tráfico entrante y saliente. Los equilibradores de carga de red orientados a Internet requieren una puerta de enlace de Internet para conectarse a la Internet.
- Equilibrador de carga de aplicación orientado a Internet: se bloquea todo el tráfico entrante y saliente. Los equilibradores de carga de aplicaciones orientados a Internet requieren una puerta de enlace de Internet para conectarse a la Internet.
- Orígenes de la VPC de Amazon CloudFront: se bloquea todo el tráfico entrante y saliente.
- Direct Connect: se bloquea todo el tráfico entrante y saliente que utiliza interfaces virtuales públicas (direcciones IPv4 públicas o IPv6 de unidifusión global). Este tráfico utiliza la puerta de enlace de Internet (o la puerta de enlace de Internet de solo salida) para establecer la conectividad.
- AWS Global Accelerator: se bloquea el tráfico entrante a las VPC, independientemente de que se pueda acceder al objetivo desde Internet o no.
- AWS Network Firewall: se bloquea todo el tráfico entrante y saliente, a menos que se excluya la subred que contiene los puntos de conexión del firewall.
- Puerta de enlace de operador de AWS Wavelength: se bloquea todo el tráfico entrante y saliente.

El BPA de la VPC no bloquea ni afecta al tráfico relacionado con la conectividad privada, como el tráfico de los siguientes servicios y recursos:

- AWS Client VPN
- AWS CloudWAN
- AWS OutpostsPuerta de enlace local de
- AWS Site-to-Site VPN
- Puerta de enlace de tránsito
- Acceso verificado de AWS

Important

- Si se enruta el tráfico entrante y saliente a través de un dispositivo (como una herramienta de seguridad o la supervisión de terceros) que se ejecuta en una instancia EC2 de una subred mediante el enrutamiento de entrada de la VPC, se debe excluir la subred de la carga de trabajo del Bloqueo del acceso público de la VPC. La subred de carga de trabajo es la subred que contiene las instancias cuyo tráfico se enruta a través del dispositivo. No es necesario excluir la subred donde se encuentra el dispositivo.
- El tráfico que se envía de forma privada desde los recursos de la VPC a otros servicios que se ejecutan en la VPC, como Route 53 Resolver, está permitido incluso cuando el BPA de la VPC está activado, ya que no pasa a través de una puerta de enlace de Internet de la VPC. Es posible que estos servicios realicen solicitudes a recursos externos a la VPC en su nombre, por ejemplo, para resolver una consulta de DNS, y que expongan información sobre la actividad de los recursos de la VPC si no se mitigan mediante otros controles de seguridad.
- Si se tiene un equilibrador de carga con acceso a Internet y se crea una exclusión de BPA de VPC solo para una de sus subredes, el equilibrador de carga puede seguir recibiendo tráfico público en la subred excluida y enrutarlo de forma privada a los destinos de las subredes que no estén excluidas. Para garantizar que el BPA de VPC bloquee por completo el acceso público a sus objetivos, asegúrese de que no se excluya ninguna de las subredes del equilibrador de carga.

Limitaciones del BPA de la VPC

El modo de solo entrada del BPA de VPC no se admite en las zonas locales (LZ) donde no se permiten las puertas de enlace NAT ni las puertas de enlace de Internet de solo salida.

Control del acceso al BPA de la VPC con una política de IAM

Para ver ejemplos de políticas de IAM que permiten o deniegan el acceso a la característica de BPA de la VPC, consulte Bloqueo de acceso público de las VPC y subredes.

Activación del modo bidireccional del BPA de la VPC para su cuenta

El modo bidireccional del BPA de la VPC bloquea todo el tráfico hacia y desde las puertas de enlace de Internet y las puertas de enlace de Internet de solo salida en esta región (excepto las VPC y las

subredes excluidas). Para obtener más información acerca de las exclusiones, consulte Crear y eliminar exclusiones.

> **Important**
>
> Se recomienda encarecidamente que revise con detenimiento las cargas de trabajo que requieren acceso a Internet antes de habilitar el BPA de la VPC en sus cuentas de producción.

> **Note**
>
> - Para habilitar el BPA de la VPC en las VPC y las subredes de su cuenta, debe ser propietario de las VPC y las subredes.
> - Si actualmente comparte subredes de VPC con otras cuentas, el modo del BPA de la VPC impuesto por el propietario de la subred también se aplica al tráfico de los participantes, pero los participantes no pueden controlar la configuración del BPA de la VPC que afecta a la subred compartida.

Consola de administración de AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Configuración.
3. Elija Editar la configuración del acceso público.
4. Seleccione Activar el bloqueo del acceso público y Bidireccional y, a continuación, seleccione Guardar cambios.
5. Espere a que el Estado cambie a Activado. La aplicación de las configuraciones del BPA de la VPC y la actualización del estado pueden tardar unos minutos.

El modo bidireccional del BPA de la VPC ya está activado.

AWS CLI

1. Activar el BPA de la VPC:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-bidirectional
```

La aplicación de las configuraciones del BPA de la VPC y la actualización del estado pueden tardar unos minutos.

2. Ver el estado del BPA de la VPC:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

Cambiar el modo del BPA de la VPC a modo de solo entrada

El modo del BPA de la VPC de solo entrada bloquea todo el tráfico de Internet a las VPC de esta región (excepto las VPC o subredes que están excluidas). Solo se permite el tráfico hacia y desde las puertas de enlace NAT y las puertas de enlace de Internet solo de salida, ya que estas puertas de enlace solo permiten establecer conexiones salientes.

Consola de administración de AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Configuración.
3. Elija Editar la configuración del acceso público.
4. Cambie la dirección a Ingress-only.
5. Guarde los cambios y espere a que se actualice el estado. La aplicación de las configuraciones del BPA de la VPC y la actualización del estado pueden tardar unos minutos.

AWS CLI

1. Modifique la dirección del bloqueo del BPA de la VPC:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-ingress
```

La aplicación de las configuraciones del BPA de la VPC y la actualización del estado pueden tardar unos minutos.

2. Ver el estado del BPA de la VPC:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

Crear y eliminar exclusiones

Una exclusión del BPA de la VPC es un modo que se puede aplicar a una sola VPC o subred y que la exime del modo BPA de la VPC de la cuenta y permitirá el acceso bidireccional o solo de salida. Puede crear exclusiones del BPA de la VPC para las VPC y las subredes incluso cuando el BPA de la VPC no esté habilitado en la cuenta para garantizar que no se interrumpa el tráfico en las exclusiones cuando se active el BPA de la VPC. Se aplica automáticamente una exclusión para una VPC a todas las subredes de la VPC.

Puede crear un máximo de 50 exclusiones. Para obtener información acerca de cómo solicitar un aumento del límite, consulte Exclusiones de BPA de la VPC por cuenta en Cuotas de Amazon VPC.

Consola de administración de AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la pestaña Bloqueo de acceso público, en Exclusiones, realice una de las siguientes acciones:
   - Para eliminar una exclusión, selecciónela y, a continuación, elija Acciones > Eliminar exclusiones.
   - Para crear una exclusión, seleccione Crear exclusiones y siga con los siguientes pasos.
4. Seleccione una dirección del bloque:
   - Bidireccional: permite que todo el tráfico de Internet entre y salga de las VPC y subredes excluidas.
   - Solo de salida: permite el tráfico de Internet saliente desde las VPC y subredes excluidas. Bloquea el tráfico de Internet entrante a las VPC y subredes excluidas. Esta configuración se aplica cuando el BPA de la VPC está establecido en modo bidireccional.
5. Elija una VPC o una subred.
6. Seleccione Crear exclusiones.
7. Espere a que el Estado de exclusión cambie a Activo. Puede que tenga que actualizar la tabla de exclusión para ver el cambio.

Se ha creado la exclusión.

AWS CLI

1. Modifique la dirección permitida de la exclusión:

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-
id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. El estado de exclusión puede tardar un tiempo en actualizarse. Para ver el estado de la exclusión:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusions --
exclusion-ids exclusion-id
```

Habilite el BPA de la VPC a nivel de Organization

Si utiliza AWS Organizations para administrar las cuentas de su organización, puede utilizar una política declarativa de AWS Organizations para aplicar el BPA de la VPC en las cuentas de la organización. Para obtener más información sobre la política declarativa del BPA de la VPC, consulte Políticas declarativas compatibles en la Guía del usuario de AWS Organizations.

> **Note**
>
> - Puede usar la política declarativa del BPA de la VPC para configurar si se permiten las exclusiones, pero no puede crear exclusiones con la política. Para crear exclusiones, aún debe crearlas en la cuenta propietaria de la VPC. Para obtener más información sobre la creación de exclusiones del BPA de la VPC, consulte Crear y eliminar exclusiones.
> - Si la política declarativa del BPA de la VPC está habilitada, en las configuraciones de Bloqueo de acceso público verá la leyenda Administrado por la política declarativa y no podrá modificar las configuraciones del BPA de la VPC a nivel de cuenta.

Evaluación del impacto y monitoreo del BPA de la VPC

Esta sección contiene información sobre cómo evaluar el impacto del BPA de la VPC antes de activarla y cómo supervisar si el tráfico se bloquea después de activarla.

Contenido

- Evaluación del impacto del BPA de la VPC con el Analizador de acceso a la red
- Monitoreo del impacto del BPA de la VPC con registros de flujo
- Seguimiento de la eliminación de exclusiones con CloudTrail
- Verificar que la conectividad esté bloqueada con el Analizador de accesibilidad

Evaluación del impacto del BPA de la VPC con el Analizador de acceso a la red

En esta sección, utilizará el Analizador de acceso a la red para ver los recursos de su cuenta que utilizan una puerta de enlace de Internet antes de habilitar el BPA de la VPC y bloquear el acceso. Utilice este análisis para comprender el impacto de activar el BPA de la VPC en su cuenta y bloquear el tráfico.

> **Note**
>
> - El Analizador de acceso a la red no es compatible con IPv6, por lo que no podrá utilizarlo para ver el posible impacto del BPA de la VPC en el tráfico de IPv6 saliente de las puertas de enlace de Internet de solo salida.
> - Se le cobrará por los análisis que realice con el analizador de acceso a la red. Para obtener más información, consulte la sección Pricing en la Guía del usuario del Analizador de acceso a la red.
> - Para obtener información sobre la disponibilidad regional del analizador de acceso a la red, consulte Limitaciones en la Guía del analizador de acceso a la red.

Consola de administración de AWS

1. Abra la consola de AWS Network Insights en https://console.aws.amazon.com/networkinsights/.
2. Seleccione Analizador de acceso a la red.
3. Seleccione Crear alcance de acceso a la red.
4. Seleccione Evaluar el impacto del bloqueo de acceso público de la VPC y, a continuación, Siguiente.
5. La plantilla ya está configurada para analizar el tráfico hacia y desde las puertas de enlace de Internet de su cuenta. Puede verlo en Origen y Destino.
6. Elija Siguiente.

7. Seleccione Crear alcance de acceso a la red.
8. Elija el alcance que acaba de crear y seleccione Analizar.
9. Espere a que el análisis finalice.
10. Visualice los resultados del análisis. Cada fila de la sección Resultados muestra la ruta de red que un paquete puede recorrer en una red hacia o desde una puerta de enlace de Internet de su cuenta. En este caso, si activa el BPA de la VPC y ninguna de las VPC ni subredes que aparecen en estos resultados está configurada como exclusión del BPA de la VPC, se restringirá el tráfico a esas VPC y subredes.
11. Analice cada resultado para comprender el impacto del BPA de la VPC en los recursos de sus VPC.

El análisis de impacto está completo.

AWS CLI

1. Crear un alcance de acceso a la red:

```
aws ec2 create-network-insights-access-scope --region us-east-2 --match-paths
 "Source={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 "Destination={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
```

2. Comenzar el análisis del alcance:

```
aws ec2 start-network-insights-access-scope-analysis  --region us-east-2 --
network-insights-access-scope-id nis-id
```

3. Obtener los resultados del análisis:

```
aws ec2 get-network-insights-access-scope-analysis-findings  --region us-east-2
 --network-insights-access-scope-analysis-id nisa-0aa383a1938f94cd1 --max-items
 1
```

Los resultados muestran el tráfico hacia y desde las puertas de enlace de Internet en todas las VPC de su cuenta. Los resultados se organizan como “hallazgos”. “FindingID”: “AnalysisFinding-1” indica que este es el primer resultado del análisis. Tenga en cuenta que hay varios resultados y cada uno indica un flujo de tráfico que se verá afectado por la activación del BPA de la VPC. El primer resultado mostrará que el tráfico comenzó en una puerta de enlace de Internet (“SequenceNumber”: 1), pasó a una NACL

(“SequenceNumber”: 2) a un grupo de seguridad (“SequenceNumber”: 3) y terminó en una instancia (“SequenceNumber”: 4).

4. Analice los resultados para comprender el impacto del BPA de la VPC en los recursos de sus VPC.

El análisis de impacto está completo.

Monitoreo del impacto del BPA de la VPC con registros de flujo

Los registros de flujo de la VPC son una característica que permite capturar información acerca del tráfico de la IP que entra y sale de las interfaces de red Elastic en la VPC. Puede usar esta característica para supervisar el tráfico que el BPA de la VPC bloquea para que no llegue a las interfaces de red de la instancia.

Cree un registro de flujo para su VPC siguiendo los pasos que se indican en Trabajo con registros de flujo.

Al crear el registro de flujo, asegúrese de utilizar un formato personalizado que incluya el campo `reject-reason`.

Al ver los registros de flujo, si el tráfico a una ENI se rechaza por el BPA de la VPC, verá una `reject-reason` del BPA en la entrada del registro de flujo.

Además de las limitaciones estándar para los registros de flujo de la VPC, tenga en cuenta las siguientes limitaciones específicas del BPA de la VPC:

- Los registros de flujo del BPA de la VPC no incluyen los registros omitidos.
- Los registros de flujo del BPA de la VPC no incluyen `bytes` incluso si incorpora el campo `bytes` en el registro de flujo.

Seguimiento de la eliminación de exclusiones con CloudTrail

En esta sección, se explica cómo puede usar AWS CloudTrail para supervisar y realizar un seguimiento de la eliminación de las exclusiones del BPA de la VPC.

Consola de administración de AWS

Para ver las exclusiones eliminadas en el historial de eventos de CloudTrail, consulte Tipo de recurso > `AWS::EC2::VPCBlockPublicAccessExclusion` en la consola de AWS CloudTrail, en https://console.aws.amazon.com/cloudtrailv2/.

AWS CLI

Puede usar el comando `lookup-events` para ver los eventos relacionados con la eliminación de exclusiones:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCBlockPublicAccessExclusion
```

Verificar que la conectividad esté bloqueada con el Analizador de accesibilidad

El Analizador de accesibilidad de la VPC se puede utilizar para evaluar si se puede acceder o no a determinadas rutas de red según la configuración de la red, incluida la configuración del BPA de la VPC.

Para obtener información sobre la disponibilidad regional del Analizador de accesibilidad, consulte Consideraciones en la Guía del Analizador de accesibilidad.

Consola de administración de AWS

1. Abra la consola de AWS Network Insights en https://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer.
2. Elija Crear y analizar ruta.
3. Para el Tipo de origen, elija Puertas de enlace de Internet y seleccione la puerta de enlace de Internet en la que desea bloquear el tráfico en el menú desplegable Origen.
4. Para el Tipo de destino, elija Instancias y seleccione la instancia desde la que quiere bloquear el tráfico en el menú desplegable Destino.
5. Elija Crear y analizar ruta.
6. Espere a que el análisis finalice. Puede demorar unos minutos.
7. Una vez completado, verá que el Estado de accesibilidad es No alcanzable y que los Detalles de la ruta muestran que `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` es la causa de este problema de accesibilidad.

AWS CLI

1. Cree una ruta de red con el ID de la puerta de enlace de Internet desde la que desea bloquear el tráfico (origen) y el ID de la instancia a la que desea bloquear el tráfico (destino):

```
aws ec2 --region us-east-2 create-network-insights-path --source igw-id --
destination instance-id --protocol TCP
```

2. Iniciar un análisis de la ruta de la red:

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-
path-id nip-id
```

3. Recuperar los resultados del análisis:

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-
insights-analysis-ids nia-id
```

4. Compruebe que `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` es el `ExplanationCode` por la falta de accesibilidad.

Ejemplo avanzado

Esta sección contiene un ejemplo avanzado que lo ayudará a entender cómo funciona la característica de bloqueo del acceso público de la VPC en diferentes situaciones. Cada situación se basa en la anterior, por eso es importante completar los pasos en orden.

Important

No utilice este ejemplo en una cuenta de producción. Se recomienda encarecidamente que revise con detenimiento las cargas de trabajo que requieren acceso a Internet antes de habilitar el BPA de la VPC en sus cuentas de producción.

Note

Para comprender por completo la característica del BPA de la VPC, necesitará disponer de determinados recursos en la cuenta. En esta sección, proporcionamos una plantilla de CloudFormation que puede utilizar para aprovisionar los recursos que necesita para

comprender bien el funcionamiento de esta característica. Hay costos asociados a los recursos que aprovisiona con la plantilla de CloudFormation y a los análisis que realiza con el Analizador de acceso a la red y el Analizador de accesibilidad. Si usa la plantilla de esta sección, asegúrese de completar los pasos de limpieza cuando termine con este ejemplo.

Contenido

- Implementación de plantillas de CloudFormation (opcional)
- Ver el impacto del BPA de la VPC con el analizador de acceso a la red
- Escenario 1: conexión a instancias sin el BPA de la VPC activado
- Escenario 2: activación del BPA de la VPC en modo bidireccional
- Escenario 3: cambio del BPA de la VPC al modo de solo entrada
- Escenario 4: creación de una exclusión
- Escenario 5: modificación del modo de exclusión
- Escenario 6: modificación del modo del BPA de la VPC
- Eliminación

Implementación de plantillas de CloudFormation (opcional)

Para demostrar cómo funciona esta característica, necesita una VPC, subredes, instancias y otros recursos. Para facilitar la realización de esta demostración, a continuación incluimos una plantilla de CloudFormation que puede utilizar para disponer rápidamente de los recursos necesarios para las situaciones de esta demostración. Este paso es opcional y es posible que solo desee ver los diagramas de los escenarios de esta sección.

Note

- Hay costos asociados a los recursos que cree en esta sección con la plantilla de CloudFormation, como el costo de la puerta de enlace NAT y las direcciones IPv4 públicas. Para evitar costos excesivos, asegúrese de completar los pasos de limpieza para eliminar todos los recursos creados para los fines de este ejemplo.
- Esta plantilla de CloudFormation crea los recursos subyacentes necesarios para el BPA de la VPC, pero no habilita la característica del BPA de la VPC en sí misma. Los recursos

que se implementan aquí tienen como objetivo ayudar a comprender y poner a prueba la funcionalidad del BPA de la VPC una vez que decida habilitarlo por separado.

La plantilla crea los siguientes recursos en su cuenta:

- Puerta de enlace de Internet de solo salida
- Puerta de enlace de Internet
- Puerta de enlace de NAT
- Dos subredes públicas
- Una subred privada
- Dos instancias EC2 con direcciones IPv4 privadas y públicas
- Una instancia EC2 con una dirección IPv6 y una dirección IPv4 privada
- Una instancia EC2 con una dirección IPv4 privada únicamente
- Se permite un grupo de seguridad con tráfico entrante SSH e ICMP y se permite TODO el tráfico saliente
- Registro de flujo de VPC
- Un punto de conexión de EC2 Instance Connect en la subred B

Copie la siguiente plantilla y guárdela en un archivo .yaml.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Creates a VPC with public and private subnets, NAT gateway, and EC2
 instances for VPC BPA.

Parameters:
  InstanceAMI:
    Description: ID of the Amazone Machine Image (AMI) to use with the instances
 launched by this template
    Type: AWS::EC2::Image::Id
  InstanceType:
    Description: EC2 Instance type to use with the instances launched by this template
    Type: String
    Default: t2.micro

Resources:
```

```
  # VPC
  VPCBPA:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.0.0.0/16
      EnableDnsHostnames: true
      EnableDnsSupport: true
      InstanceTenancy: default
      Tags:
        - Key: Name
          Value: VPC BPA

  # VPC IPv6 CIDR
  VPCBPAIpv6CidrBlock:
    Type: AWS::EC2::VPCCidrBlock
    Properties:
      VpcId: !Ref VPCBPA
      AmazonProvidedIpv6CidrBlock: true

  # EC2 Key Pair
  VPCBPAKeyPair:
    Type: AWS::EC2::KeyPair
    Properties:
      KeyName: vpc-bpa-key

  # Internet Gateway
  VPCBPAInternetGateway:
    Type: AWS::EC2::InternetGateway
    Properties:
      Tags:
        - Key: Name
          Value: VPC BPA Internet Gateway

  VPCBPAInternetGatewayAttachment:
    Type: AWS::EC2::VPCGatewayAttachment
    Properties:
      VpcId: !Ref VPCBPA
      InternetGatewayId: !Ref VPCBPAInternetGateway

  # Egress-Only Internet Gateway
  VPCBPAEgressOnlyInternetGateway:
    Type: AWS::EC2::EgressOnlyInternetGateway
    Properties:
      VpcId: !Ref VPCBPA
```

```
# Subnets
VPCBPAPublicSubnetA:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref VPCBPA
    CidrBlock: 10.0.1.0/24
    MapPublicIpOnLaunch: true
    Tags:
      - Key: Name
        Value: VPC BPA Public Subnet A

VPCBPAPublicSubnetB:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref VPCBPA
    CidrBlock: 10.0.2.0/24
    MapPublicIpOnLaunch: true
    Tags:
      - Key: Name
        Value: VPC BPA Public Subnet B

VPCBPAPrivateSubnetC:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref VPCBPA
    CidrBlock: 10.0.3.0/24
    MapPublicIpOnLaunch: false
    Ipv6CidrBlock: !Select [0, !GetAtt VPCBPA.Ipv6CidrBlocks]
    AssignIpv6AddressOnCreation: true
    Tags:
      - Key: Name
        Value: VPC BPA Private Subnet C

# NAT Gateway
VPCBPANATGateway:
  Type: AWS::EC2::NatGateway
  Properties:
    AllocationId: !GetAtt VPCBPANATGatewayEIP.AllocationId
    SubnetId: !Ref VPCBPAPublicSubnetB
    Tags:
      - Key: Name
        Value: VPC BPA NAT Gateway
```

```
  VPCBPANATGatewayEIP:
    Type: AWS::EC2::EIP
    Properties:
      Domain: vpc
      Tags:
        - Key: Name
          Value: VPC BPA NAT Gateway EIP

  # Route Tables
  VPCBPAPublicRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref VPCBPA
      Tags:
        - Key: Name
          Value: VPC BPA Public Route Table

  VPCBPAPublicRoute:
    Type: AWS::EC2::Route
    DependsOn: VPCBPAInternetGatewayAttachment
    Properties:
      RouteTableId: !Ref VPCBPAPublicRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      GatewayId: !Ref VPCBPAInternetGateway

  VPCBPAPublicSubnetARouteTableAssoc:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPublicSubnetA
      RouteTableId: !Ref VPCBPAPublicRouteTable

  VPCBPAPublicSubnetBRouteTableAssoc:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPublicSubnetB
      RouteTableId: !Ref VPCBPAPublicRouteTable

  VPCBPAPrivateRouteTable:
    Type: AWS::EC2::RouteTable
    Properties:
      VpcId: !Ref VPCBPA
      Tags:
        - Key: Name
          Value: VPC BPA Private Route Table
```

```
  VPCBPAPrivateRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref VPCBPAPrivateRouteTable
      DestinationCidrBlock: 0.0.0.0/0
      NatGatewayId: !Ref VPCBPANATGateway

  VPCBPAPrivateSubnetCRoute:
    Type: AWS::EC2::Route
    Properties:
      RouteTableId: !Ref VPCBPAPrivateRouteTable
      DestinationIpv6CidrBlock: ::/0
      EgressOnlyInternetGatewayId: !Ref VPCBPAEgressOnlyInternetGateway

  VPCBPAPrivateSubnetCRouteTableAssociation:
    Type: AWS::EC2::SubnetRouteTableAssociation
    Properties:
      SubnetId: !Ref VPCBPAPrivateSubnetC
      RouteTableId: !Ref VPCBPAPrivateRouteTable

  # EC2 Instances Security Group
  VPCBPAInstancesSecurityGroup:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupName: VPC BPA Instances Security Group
      GroupDescription: Allow SSH and ICMP access
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 22
          ToPort: 22
          CidrIp: 0.0.0.0/0
        - IpProtocol: icmp
          FromPort: -1
          ToPort: -1
          CidrIp: 0.0.0.0/0
      VpcId: !Ref VPCBPA
      Tags:
        - Key: Name
          Value: VPC BPA Instances Security Group

  # EC2 Instances
  VPCBPAInstanceA:
    Type: AWS::EC2::Instance
```

```
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: t2.micro
      KeyName: !Ref VPCBPAKeyPair
      SubnetId: !Ref VPCBPAPublicSubnetA
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      Tags:
        - Key: Name
          Value: VPC BPA Instance A

  VPCBPAInstanceB:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: !Ref InstanceType
      KeyName: !Ref VPCBPAKeyPair
      SubnetId: !Ref VPCBPAPublicSubnetB
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      Tags:
        - Key: Name
          Value: VPC BPA Instance B

  VPCBPAInstanceC:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: !Ref InstanceType
      KeyName: !Ref VPCBPAKeyPair
      SubnetId: !Ref VPCBPAPrivateSubnetC
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      Tags:
        - Key: Name
          Value: VPC BPA Instance C

  VPCBPAInstanceD:
    Type: AWS::EC2::Instance
    Properties:
      ImageId: !Ref InstanceAMI
      InstanceType: !Ref InstanceType
      KeyName: !Ref VPCBPAKeyPair
      NetworkInterfaces:
```

```
      - DeviceIndex: '0'
        GroupSet:
          - !Ref VPCBPAInstancesSecurityGroup
        SubnetId: !Ref VPCBPAPrivateSubnetC
        Ipv6AddressCount: 1
    Tags:
      - Key: Name
        Value: VPC BPA Instance D

# Flow Logs IAM Role
VPCBPAFlowLogRole:
  Type: AWS::IAM::Role
  Properties:
    AssumeRolePolicyDocument:
      Version: '2012-10-17'
      Statement:
        - Effect: Allow
          Principal:
            Service: vpc-flow-logs.amazonaws.com
          Action: 'sts:AssumeRole'
    Tags:
      - Key: Name
        Value: VPC BPA Flow Logs Role

VPCBPAFlowLogPolicy:
  Type: AWS::IAM::Policy
  Properties:
    PolicyName: VPC-BPA-FlowLogsPolicy
    PolicyDocument:
      Version: '2012-10-17'
      Statement:
        - Effect: Allow
          Action:
            - 'logs:CreateLogGroup'
            - 'logs:CreateLogStream'
            - 'logs:PutLogEvents'
            - 'logs:DescribeLogGroups'
            - 'logs:DescribeLogStreams'
          Resource: '*'
    Roles:
      - !Ref VPCBPAFlowLogRole

# Flow Logs
VPCBPAFlowLog:
```

```
    Type: AWS::EC2::FlowLog
    Properties:
      ResourceId: !Ref VPCBPA
      ResourceType: VPC
      TrafficType: ALL
      LogDestinationType: cloud-watch-logs
      LogGroupName: /aws/vpc-flow-logs/VPC-BPA
      DeliverLogsPermissionArn: !GetAtt VPCBPAFlowLogRole.Arn
      LogFormat: '${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr}
 ${srcport} ${dstport} ${protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-
status} ${vpc-id} ${subnet-id} ${instance-id} ${tcp-flags} ${type} ${pkt-srcaddr}
 ${pkt-dstaddr} ${region} ${az-id} ${sublocation-type} ${sublocation-id} ${pkt-src-aws-
service} ${pkt-dst-aws-service} ${flow-direction} ${traffic-path} ${reject-reason}'
      Tags:
        - Key: Name
          Value: VPC BPA Flow Logs

  # EC2 Instance Connect Endpoint
  VPCBPAEC2InstanceConnectEndpoint:
    Type: AWS::EC2::InstanceConnectEndpoint
    Properties:
      SecurityGroupIds:
        - !Ref VPCBPAInstancesSecurityGroup
      SubnetId: !Ref VPCBPAPublicSubnetB

Outputs:
  VPCBPAVPCId:
    Description: A reference to the created VPC
    Value: !Ref VPCBPA
    Export:
      Name: vpc-id

  VPCBPAPublicSubnetAId:
    Description: The ID of the public subnet A
    Value: !Ref VPCBPAPublicSubnetA

  VPCBPAPublicSubnetAName:
    Description: The name of the public subnet A
    Value: VPC BPA Public Subnet A

  VPCBPAPublicSubnetBId:
    Description: The ID of the public subnet B
    Value: !Ref VPCBPAPublicSubnetB
```

```
  VPCBPAPublicSubnetBName:
    Description: The name of the public subnet B
    Value: VPC BPA Public Subnet B

  VPCBPAPrivateSubnetCId:
    Description: The ID of the private subnet C
    Value: !Ref VPCBPAPrivateSubnetC

  VPCBPAPrivateSubnetCName:
    Description: The name of the private subnet C
    Value: VPC BPA Private Subnet C

  VPCBPAInstanceAId:
    Description: The ID of instance A
    Value: !Ref VPCBPAInstanceA

  VPCBPAInstanceBId:
    Description: The ID of instance B
    Value: !Ref VPCBPAInstanceB

  VPCBPAInstanceCId:
    Description: The ID of instance C
    Value: !Ref VPCBPAInstanceC

  VPCBPAInstanceDId:
    Description: The ID of instance D
    Value: !Ref VPCBPAInstanceD
```

Consola de administración de AWS

1. Abra la consola de CloudFormation en https://console.aws.amazon.com/cloudformation/.
2. Seleccione Crear pila y cargue el archivo de plantilla .yaml.
3. Siga los pasos para usar la plantilla. Deberá introducir un ID de imagen y un tipo de instancia (como t2.micro). También tendrá que permitir que CloudFormation cree un rol de IAM para crear el registro de flujo y obtener permiso para iniciar sesión en CloudWatch.
4. Una vez que haya lanzado la pila, consulte la pestaña Eventos para ver el progreso y asegurarse de que la pila se complete antes de continuar.

AWS CLI

1. Para crear una pila de CloudFormation, ejecute el siguiente comando:

```
aws cloudformation create-stack --stack-name VPC-BPA-stack --template-body
 file://sampletemplate.yaml --capabilities CAPABILITY_IAM --region us-east-2
```

Salida:

```
{
    "StackId": "arn:aws:cloudformation:us-east-2:470889052923:stack/VPC-BPA-
stack/8a7a2cc0-8001-11ef-b196-06386a84b72f"
}
```

2. Consulte el progreso y asegúrese de que la pila se complete antes de continuar:

```
aws cloudformation describe-stack-events --stack-name VPC-BPA-stack --region us-
east-2
```

Ver el impacto del BPA de la VPC con el analizador de acceso a la red

En esta sección, utilizará el analizador de acceso a la red para ver los recursos de su cuenta que utilizan la puerta de enlace de Internet. Utilice este análisis para comprender el impacto de activar el BPA de la VPC en su cuenta y bloquear el tráfico.

Para obtener información sobre la disponibilidad regional del analizador de acceso a la red, consulte Limitaciones en la Guía del analizador de acceso a la red.

Consola de administración de AWS

1. Abra la consola de AWS Network Insights en https://console.aws.amazon.com/networkinsights/.
2. Seleccione Analizador de acceso a la red.
3. Seleccione Crear alcance de acceso a la red.
4. Seleccione Evaluar el impacto del bloqueo de acceso público de la VPC y, a continuación, Siguiente.
5. La plantilla ya está configurada para analizar el tráfico hacia y desde las puertas de enlace de Internet de su cuenta. Puede verlo en Origen y Destino.
6. Elija Siguiente.
7. Seleccione Crear alcance de acceso a la red.

8. Elija el alcance que acaba de crear y seleccione Analizar.
9. Espere a que el análisis finalice.
10. Visualice los resultados del análisis. Cada fila de la sección Resultados muestra la ruta de red que un paquete puede recorrer en una red hacia o desde una puerta de enlace de Internet de su cuenta. En este caso, si activa el BPA de la VPC y ninguna de las VPC ni subredes que aparecen en estos resultados está configurada como exclusión del BPA de la VPC, se restringirá el tráfico a esas VPC y subredes.
11. Analice cada resultado para comprender el impacto del BPA de la VPC en los recursos de sus VPC.

El análisis de impacto está completo.

AWS CLI

1. Crear un alcance de acceso a la red:

```
aws ec2 create-network-insights-access-scope --match-paths
 "Source={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 "Destination={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
 --region us-east-2
```

Salida:

```
{
  "NetworkInsightsAccessScope": {
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "NetworkInsightsAccessScopeArn": "arn:aws:ec2:us-
east-2:470889052923:network-insights-access-scope/nis-04cad3c4b3a1d5e3e",
    "CreatedDate": "2024-09-30T15:55:53.171000+00:00",
    "UpdatedDate": "2024-09-30T15:55:53.171000+00:00"
  },
  "NetworkInsightsAccessScopeContent": {
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "MatchPaths": [
      {
        "Source": {
          "ResourceStatement": {
            "ResourceTypes": [
              "AWS::EC2::InternetGateway"
            ]
```

```
          }
        }
      },
      {
        "Destination": {
          "ResourceStatement": {
            "ResourceTypes": [
              "AWS::EC2::InternetGateway"
            ]
          }
        }
      }
    ]
  }
}
```

2. Comenzar el análisis del alcance:

```
aws ec2 start-network-insights-access-scope-analysis --network-insights-access-
scope-id nis-04cad3c4b3a1d5e3e --region us-east-2
```

Salida:

```
{
  "NetworkInsightsAccessScopeAnalysis": {
    "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
    "NetworkInsightsAccessScopeAnalysisArn": "arn:aws:ec2:us-
east-2:470889052923:network-insights-access-scope-analysis/
nisa-0aa383a1938f94cd",
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "Status": "running",
    "StartDate": "2024-09-30T15:56:59.109000+00:00",
    "AnalyzedEniCount": 0
  }
}
```

3. Obtener los resultados del análisis:

```
aws ec2 get-network-insights-access-scope-analysis-findings --network-insights-
access-scope-analysis-id nisa-0aa383a1938f94cd1 --region us-east-2 --max-items 1
```

Salida:

```
{
  "AnalysisFindings": [
    {
      "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
      "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
      "FindingId": "AnalysisFinding-1",
      "FindingComponents": [
        {
          "SequenceNumber": 1,
          "Component": {
            "Id": "igw-04a5344b4e30486f1",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:internet-gateway/
igw-04a5344b4e30486f1",
            "Name": "VPC BPA Internet Gateway"
          },
          "OutboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ]
          },
          "InboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ],
            "DestinationPortRanges": [
              {
                "From": 22,
                "To": 22
              }
            ],
            "Protocol": "6",
            "SourceAddresses": [
              "0.0.0.0/5",
              "100.0.0.0/10",
              "96.0.0.0/6"
            ],
            "SourcePortRanges": [
              {
                "From": 0,
                "To": 65535
              }
            ]
          },
```

```
          "Vpc": {
            "Id": "vpc-0762547ec48b6888d",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:vpc/
vpc-0762547ec48b6888d",
            "Name": "VPC BPA"
          }
        },
        {
          "SequenceNumber": 2,
          "AclRule": {
            "Cidr": "0.0.0.0/0",
            "Egress": false,
            "Protocol": "all",
            "RuleAction": "allow",
            "RuleNumber": 100
          },
          "Component": {
            "Id": "acl-06194fc3a4a03040b",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:network-acl/
acl-06194fc3a4a03040b"
          }
        },
        {
          "SequenceNumber": 3,
          "Component": {
            "Id": "sg-093dde06415d03924",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:security-group/
sg-093dde06415d03924",
            "Name": "VPC BPA Instances Security Group"
          },
          "SecurityGroupRule": {
            "Cidr": "0.0.0.0/0",
            "Direction": "ingress",
            "PortRange": {
              "From": 22,
              "To": 22
            },
            "Protocol": "tcp"
          }
        },
        {
          "SequenceNumber": 4,
          "AttachedTo": {
            "Id": "i-058db34f9a0997895",
```

```
            "Arn": "arn:aws:ec2:us-east-2:470889052923:instance/
i-058db34f9a0997895",
            "Name": "VPC BPA Instance A"
          },
          "Component": {
            "Id": "eni-0fa23f2766f03b286",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:network-interface/
eni-0fa23f2766f03b286"
          },
          "InboundHeader": {
            "DestinationAddresses": [
              "10.0.1.85/32"
            ],
            "DestinationPortRanges": [
              {
                "From": 22,
                "To": 22
              }
            ],
            "Protocol": "6",
            "SourceAddresses": [
              "0.0.0.0/5",
              "100.0.0.0/10",
              "96.0.0.0/6"
            ],
            "SourcePortRanges": [
              {
                "From": 0,
                "To": 65535
              }
            ]
          },
          "Subnet": {
            "Id": "subnet-035d235a762eeed04",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:subnet/
subnet-035d235a762eeed04",
            "Name": "VPC BPA Public Subnet A"
          },
          "Vpc": {
            "Id": "vpc-0762547ec48b6888d",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:vpc/
vpc-0762547ec48b6888d",
            "Name": "VPC BPA"
          }
```

```
        }
      ]
    }
  ],
  "AnalysisStatus": "succeeded",
  "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
  "NextToken":
 "eyJOZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ=="
}
```


Los resultados muestran el tráfico hacia y desde las puertas de enlace de Internet en todas las VPC de su cuenta. Los resultados se organizan como “hallazgos”. “FindingID”: “AnalysisFinding-1” indica que este es el primer resultado del análisis. Tenga en cuenta que hay varios resultados y cada uno indica un flujo de tráfico que se verá afectado por la activación del BPA de la VPC. El primer resultado mostrará que el tráfico comenzó en una puerta de enlace de Internet (“SequenceNumber”: 1), pasó a una NACL (“SequenceNumber”: 2) a un grupo de seguridad (“SequenceNumber”: 3) y terminó en una instancia (“SequenceNumber”: 4).

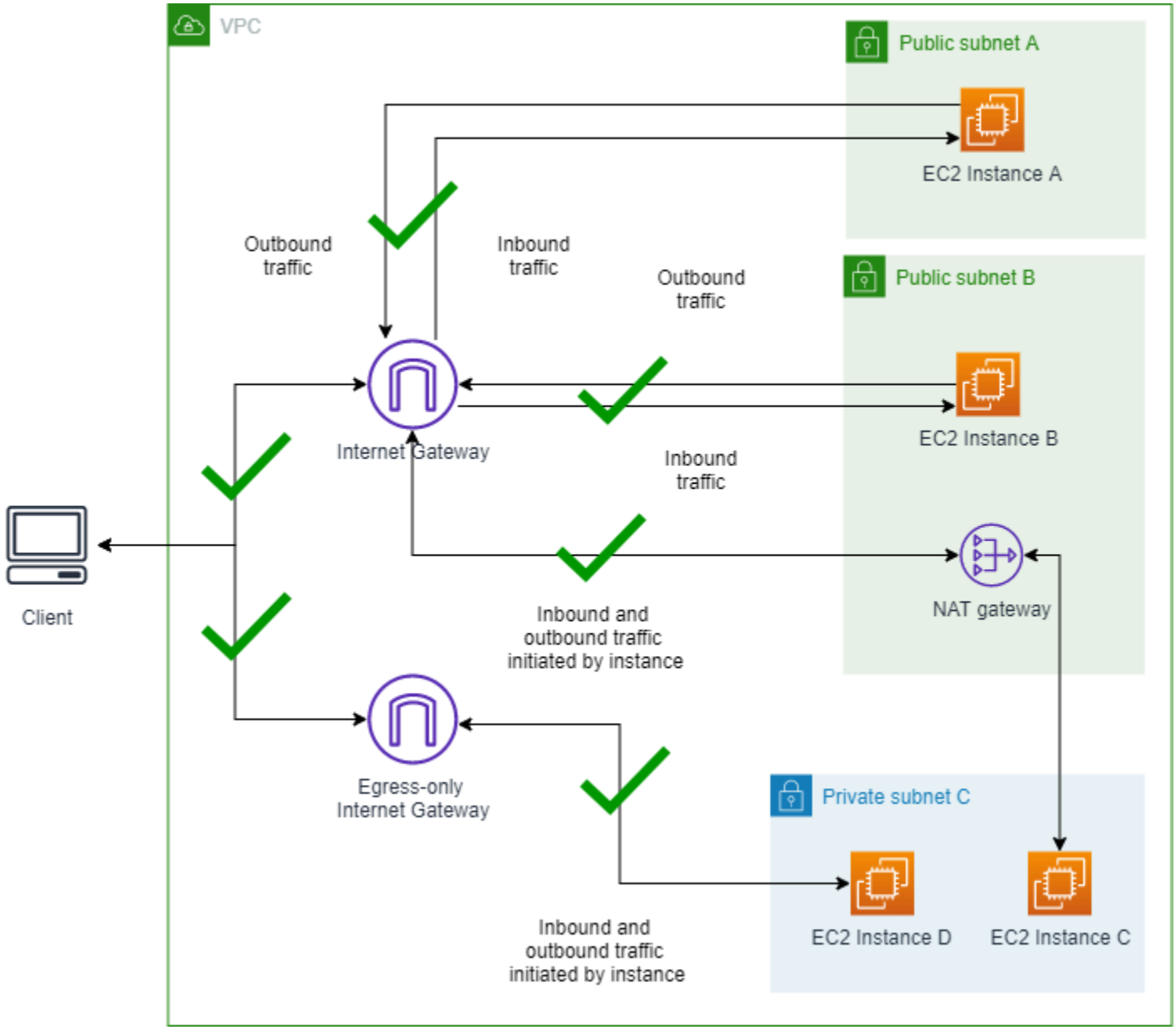
4. Analice los resultados para comprender el impacto del BPA de la VPC en los recursos de sus VPC.

El análisis de impacto está completo.

Escenario 1: conexión a instancias sin el BPA de la VPC activado

En esta sección, se puede acceder a las instancias de EC2 de las subredes públicas A y B desde Internet a través de la puerta de enlace de Internet, que permite el tráfico entrante y saliente. Las instancias C y D de la subred privada pueden iniciar el tráfico saliente a través de la puerta de enlace NAT o la puerta de enlace de Internet de solo salida, pero no se puede acceder a ellas directamente desde Internet. Esta configuración proporciona acceso a Internet a algunos recursos mientras protege otros. El objetivo de esta configuración es establecer una referencia y garantizar que, antes de activar el BPA de la VPC, se pueda acceder a todas las instancias y que se conectará a todas las instancias y hará ping a una dirección IP pública.

Diagrama de una VPC sin el BPA de la VPC activado:



1.1 Conexión a instancias

Complete esta sección para conectarse a sus instancias con el BPA de la VPC desactivado y asegurarse de que puede hacerlo sin problemas. Todas las instancias creadas con CloudFormation para este ejemplo tienen nombres como “Instancia A del BPA de la VPC”.

Consola de administración de AWS

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. Abra los detalles de la instancia A.

3. Conéctese a la instancia A mediante la opción Conexión de instancia EC2 > Conexión mediante el punto de conexión de EC2 Instance Connect.
4. Elija Conectar. Una vez que se haya conectado correctamente a la instancia, haga ping a www.amazon.com para comprobar que puede enviar las solicitudes salientes a Internet.
5. Para conectarse a las instancia B, C y D, use el mismo método que usó para la A. Desde cada instancia, haga ping a www.amazon.com para verificar si puede enviar solicitudes salientes a Internet.

AWS CLI

1. Haga ping a la instancia A mediante la dirección IPv4 pública para comprobar el tráfico entrante:

```
ping 18.225.8.244
```

Salida:

```
Pinging 18.225.8.244 with 32 bytes of data:

Reply from 18.225.8.244: bytes=32 time=51ms TTL=110
Reply from 18.225.8.244: bytes=32 time=61ms TTL=110
```

Advierta que el ping se ha realizado correctamente y que el tráfico no está bloqueado.

2. Utilice la dirección IPv4 privada para conectarse y comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
```

```
/ /
/m/'
Last login: Fri Sep 27 18:27:57 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING www-amazon-com.customer.fastly.net (18.65.233.187) 56(84) bytes of data.
64 bytes from 18.65.233.187 (18.65.233.187): icmp_seq=15 ttl=58 time=2.06 ms
64 bytes from 18.65.233.187 (18.65.233.187): icmp_seq=16 ttl=58 time=2.26 ms
```

Advierta que el ping se ha realizado correctamente y que el tráfico no está bloqueado.

3. Haga ping a la instancia B mediante la dirección IPv4 pública para comprobar el tráfico entrante:

```
ping 3.18.106.198
```

Salida:

```
Pinging 3.18.106.198 with 32 bytes of data:
Reply from 3.18.106.198: bytes=32 time=83ms TTL=110
Reply from 3.18.106.198: bytes=32 time=54ms TTL=110
```

Advierta que el ping se ha realizado correctamente y que el tráfico no está bloqueado.

4. Utilice la dirección IPv4 privada para conectarse y comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id  i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.
Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Fri Sep 27 18:12:27 2024 from 3.16.146.5
```

```
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=249 time=1.55 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=249 time=1.67 ms
```

Advierta que el ping se ha realizado correctamente y que el tráfico no está bloqueado.

5. Conéctese a la instancia C. Como no hay una dirección IP pública a la que hacer ping, utilice EC2 Instance Connect para conectarse y, a continuación, haga ping a una IP pública desde la instancia para comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.
Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Thu Sep 19 20:31:26 2024 from 10.0.2.86
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.75 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.97 ms
64 bytes from server-3-160-24-26.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=3 ttl=248 time=1.08 ms
```

Advierta que el ping se ha realizado correctamente y que el tráfico no está bloqueado.

6. Conéctese a la instancia D. Como no hay una dirección IP pública a la que hacer ping, utilice EC2 Instance Connect para conectarse y, a continuación, haga ping a una IP pública desde la instancia para comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Salida:

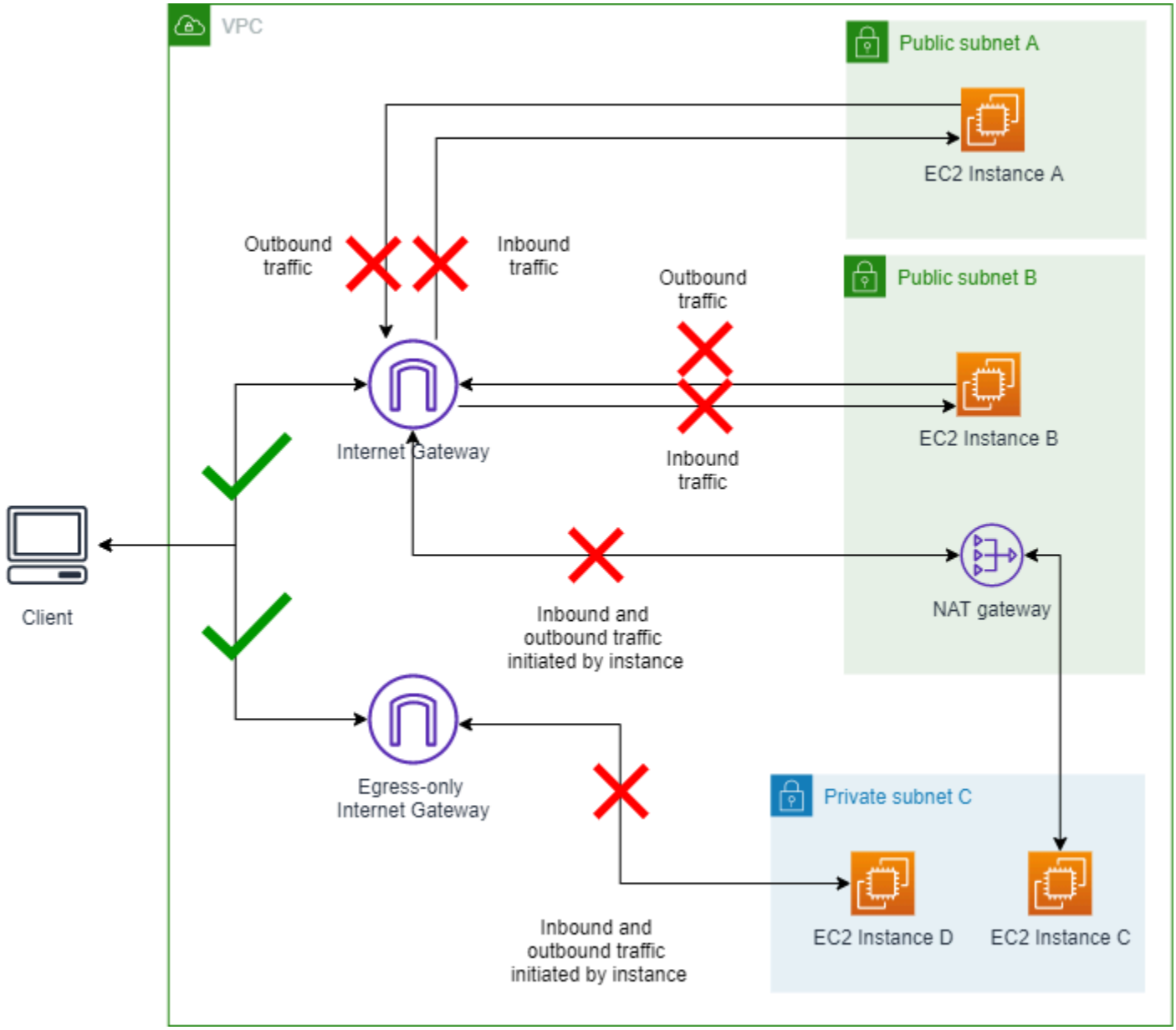
```
The authenticity of host '10.0.3.59 can't be established.
ECDSA key fingerprint is SHA256:c4naBCqbC61/cExDyccEproNU+1HHSpMSzl2J6cOtIZA8g.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.59' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ _/
_/m/'
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121): icmp_seq=1 ttl=58 time=1.19 ms
64 bytes from 2600:9000:25f3:ee00:7:49a5:5fd4:b121
 (2600:9000:25f3:ee00:7:49a5:5fd4:b121): icmp_seq=2 ttl=58 time=1.38 ms
```

Advierta que el ping se ha realizado correctamente y que el tráfico no está bloqueado.

Escenario 2: activación del BPA de la VPC en modo bidireccional

En esta sección, activará el BPA de la VPC y bloqueará el tráfico hacia y desde las puertas de enlace de Internet de su cuenta.

Diagrama donde se muestra el modo bidireccional del BPA de la VPC activado:



2.1 Activación del modo bidireccional del BPA de la VPC

Complete esta sección para habilitar el BPA de la VPC. El modo bidireccional del BPA de la VPC bloquea todo el tráfico hacia y desde las puertas de enlace de Internet y las puertas de enlace de Internet de solo salida en esta región (excepto las VPC y las subredes excluidas).

Consola de administración de AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Configuración.
3. Elija Editar la configuración del acceso público.

4. Seleccione Activar el bloqueo del acceso público y Bidireccional y, a continuación, seleccione Guardar cambios.
5. Espere a que el Estado cambie a Activado. La aplicación de las configuraciones del BPA de la VPC y la actualización del estado pueden tardar unos minutos.

El BPA de la VPC ya está activado.

AWS CLI

1. Use el comando modify-vpc-block-public-access-options para activar el BPA de la VPC:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-bidirectional
```

La aplicación de las configuraciones del BPA de la VPC y la actualización del estado pueden tardar unos minutos.

2. Ver el estado del BPA de la VPC:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

2.2 Conexión a instancias

Complete esta sección para conectarse a sus instancias.

Consola de administración de AWS

1. Haga ping a la dirección IPv4 pública de las instancias A y B, tal y como hizo en el escenario 1. Advierta que el tráfico está bloqueado.
2. Conéctese a la instancia A mediante la opción Conexión de instancia EC2 > Conexión mediante el punto de conexión de EC2 Instance Connect, como lo hizo en el escenario 1. Asegúrese de utilizar la opción de punto de conexión.
3. Elija Conectar. Una vez que se haya conectado correctamente a la instancia, haga ping a www.amazon.com. Advierta que todo el tráfico de salida está bloqueado.
4. Para conectarse a las instancia B, C y D, use el mismo método que usó para la A, y luego verifique las solicitudes salientes a Internet. Advierta que todo el tráfico de salida está bloqueado.

AWS CLI

1. Haga ping a la instancia A mediante la dirección IPv4 pública para comprobar el tráfico entrante:

```
ping 18.225.8.244
```

Salida:

```
Pinging 18.225.8.244 with 32 bytes of data:

Request timed out.
```

Advierta que el ping falla y el tráfico está bloqueado.

2. Utilice la dirección IPv4 privada para conectarse y comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Salida:

```
The authenticity of host '10.0.1.85' can't be established.
ECDSA key fingerprint is SHA256:3zo/gSss+HAZ+7eTyWlOB/Ke04IM+hadjsoLJeRTWBk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.85' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 14:16:53 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Advierta que el ping falla y el tráfico está bloqueado.

3. Haga ping a la instancia B mediante la dirección IPv4 pública para comprobar el tráfico entrante:

```
ping 3.18.106.198
```

Salida:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Advierta que el ping falla y el tráfico está bloqueado.

4. Utilice la dirección IPv4 privada para conectarse y comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id  i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Salida:

```
The authenticity of host '10.0.2.98' can't be established.
ECDSA key fingerprint is SHA256:0IjXKKyVlDthcCfI0IPIJMUiItAOLYKRNLGTYURnFXo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.98' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Fri Sep 27 14:18:16 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Advierta que el ping falla y el tráfico está bloqueado.

5. Conéctese a la instancia C. Como no hay una dirección IP pública a la que hacer ping, utilice EC2 Instance Connect para conectarse y, a continuación, haga ping a una IP pública desde la instancia para comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
/ /
/m/'
Last login: Tue Sep 24 15:17:56 2024 from 10.0.2.86
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Advierta que el ping falla y el tráfico está bloqueado.

6. Conéctese a la instancia D. Como no hay una dirección IP pública a la que hacer ping, utilice EC2 Instance Connect para conectarse y, a continuación, haga ping a una IP pública desde la instancia para comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
```

```
~~..   _/
_/ _/
_/m/'
Last login: Fri Sep 27 16:42:01 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:8200:7:49a5:5fd4:b121
 (2600:9000:25f3:8200:7:49a5:5fd4:b121)) 56 data bytes
```

Advierta que el ping falla y el tráfico está bloqueado.

2.3: Opcional: Verificar que la conectividad esté bloqueada con el analizador de accesibilidad

El analizador de accesibilidad de la VPC se puede utilizar para comprender si se puede acceder o no a determinadas rutas de red según la configuración de la red, incluida la configuración del BPA de la VPC. En este ejemplo, analizará la misma ruta de red que se intentó anteriormente para confirmar que el BPA de la VPC es el motivo por el que falla la conectividad.

Consola de administración de AWS

1. Vaya a la consola de Network Insights en https://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer.
2. Elija Crear y analizar ruta.
3. En Tipo de origen, elija Puertas de enlace de Internet y seleccione la puerta de enlace de Internet etiquetada Puerta de enlace de internet del BPA de la VPC en el menú desplegable Origen.
4. En Tipo de destino, elija Instancias y seleccione la instancia etiquetada como Instancia A del BPA de la VPC en el menú desplegable Destino.
5. Elija Crear y analizar ruta.
6. Espere a que el análisis finalice. Puede demorar unos minutos.
7. Una vez completado, verá que el Estado de accesibilidad es No alcanzable y que los Detalles de la ruta muestran que `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` es la causa.

AWS CLI

1. Cree una ruta de red con el ID de la puerta de enlace de Internet con la etiqueta Puerta de enlace de internet del BPA de la VPC y el ID de la instancia con la etiqueta Instancia A del BPA de la VPC:

```
aws ec2 --region us-east-2 create-network-insights-path --source igw-id --
destination instance-id --protocol TCP
```

2. Iniciar un análisis de la ruta de la red:

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-
path-id nip-id
```

3. Recuperar los resultados del análisis:

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-
insights-analysis-ids nia-id
```

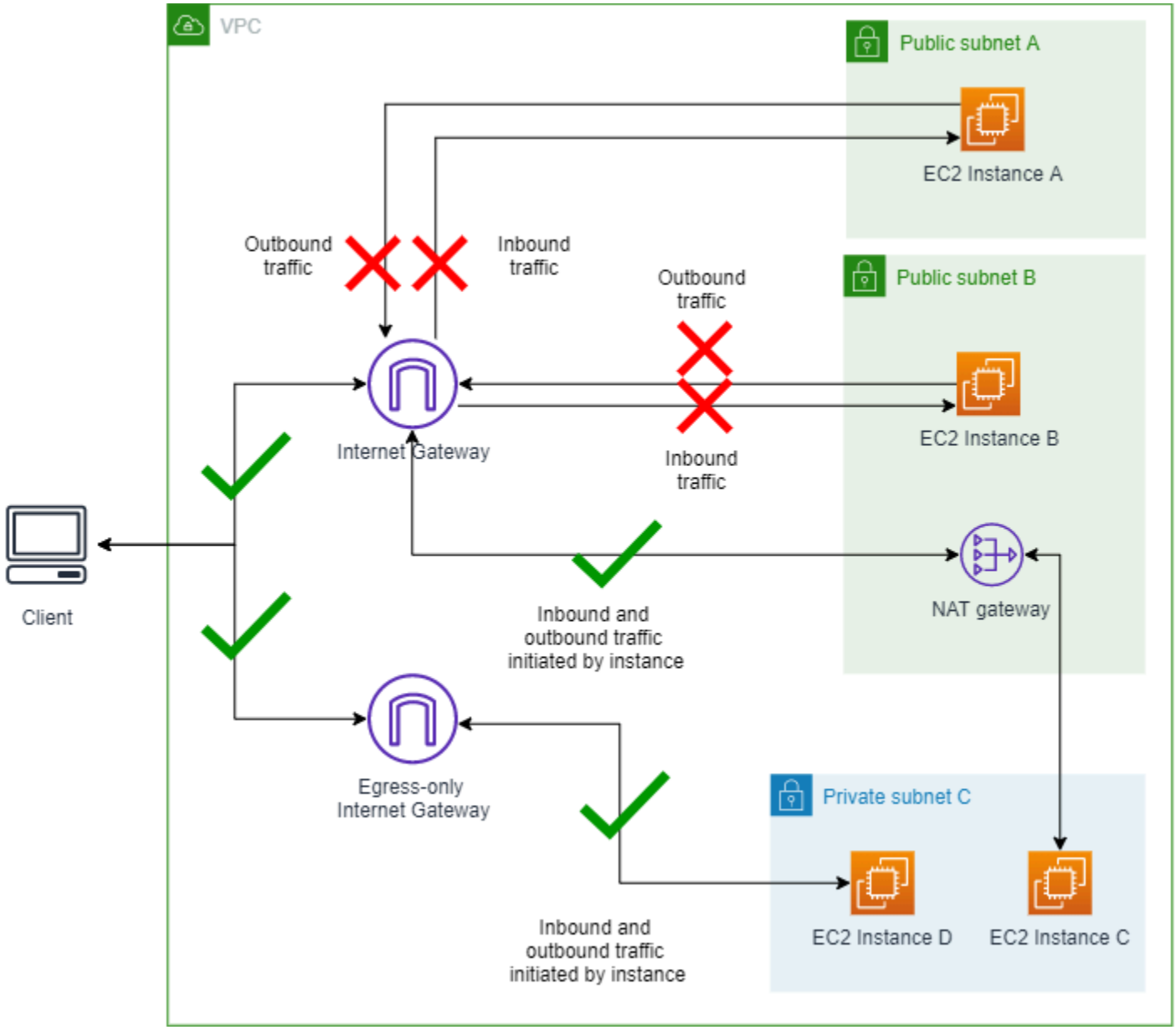
4. Compruebe que `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` es el `ExplanationCode` por la falta de accesibilidad.

Tenga en cuenta que también puede hacer un Monitoreo del impacto del BPA de la VPC con registros de flujo.

Escenario 3: cambio del BPA de la VPC al modo de solo entrada

En esta sección, cambiará la dirección del tráfico del BPA de la VPC y permitirá solo el tráfico que utilice una puerta de enlace NAT o una puerta de enlace de Internet de solo salida. No se podrá acceder a las instancias de EC2 A y B de las subredes públicas desde Internet porque el BPA bloquea el tráfico entrante a través de la puerta de enlace de Internet. Las instancias C y D de la subred privada seguirán pudiendo iniciar el tráfico saliente a través de la puerta de enlace NAT y la puerta de enlace de Internet de solo salida y, por lo tanto, podrán seguir accediendo a Internet.

Diagrama del modo de solo ingreso del BPA de la VPC activado:



3.1 Cambiar el modo al de solo entrada

Complete esta sección para cambiar el modo.

Consola de administración de AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Configuración.
3. En la pestaña Bloqueo de acceso público, seleccione Editar la configuración del acceso público.

4. Modifique la configuración de acceso público en la consola de la VPC y cambie la dirección a Solo entrada.
5. Guarde los cambios y espere a que se actualice el estado. La aplicación de las configuraciones del BPA de la VPC y la actualización del estado pueden tardar unos minutos.

AWS CLI

1. Modifique el modo del BPA de la VPC:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-
gateway-block-mode block-ingress
```

   La aplicación de las configuraciones del BPA de la VPC y la actualización del estado pueden tardar unos minutos.
2. Ver el estado del BPA de la VPC:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

3.2 Conexión a instancias

Complete esta sección para conectarse a las instancias.

Consola de administración de AWS

1. Haga ping a la dirección IPv4 pública de las instancias A y B, tal y como hizo en el escenario 1. Advierta que el tráfico está bloqueado.
2. Conéctese a las instancias A y B mediante EC2 Instance Connect como lo hizo en el escenario 1 y haga ping a www.amazon.com desde allí. Advierta que no puede hacer ping a un sitio público de Internet desde las instancias A o B, ya que el tráfico está bloqueado.
3. Conéctese a las instancias C y D mediante EC2 Instance Connect como lo hizo en el escenario 1 y haga ping a www.amazon.com desde allí. Advierta que puede hacer ping a un sitio público de Internet desde la instancia C o D y que el tráfico está permitido.

AWS CLI

1. Haga ping a la instancia A mediante la dirección IPv4 pública para comprobar el tráfico entrante:

```
ping 18.225.8.244
```

Salida:

```
Pinging 18.225.8.244 with 32 bytes of data:

Request timed out.
```

Advierta que el ping falla y el tráfico está bloqueado.

2. Utilice la dirección IPv4 privada para conectarse y comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Salida:

```
The authenticity of host '10.0.1.85' can't be established.
ECDSA key fingerprint is SHA256:3zo/gSss+HAZ+7eTyWlOB/Ke04IM+hadjsoLJeRTWBk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.1.85' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 14:16:53 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Advierta que el ping falla y el tráfico está bloqueado.

3. Haga ping a la instancia B mediante la dirección IPv4 pública para comprobar el tráfico entrante:

```
ping 3.18.106.198
```

Salida:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Advierta que el ping falla y el tráfico está bloqueado.

4. Utilice la dirección IPv4 privada para conectarse y comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Salida:

```
The authenticity of host '10.0.2.98 ' can't be established.
ECDSA key fingerprint is SHA256:0IjXKKyVlDthcCfI0IPIJMUiItAOLYKRNLGTYURnFXo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.98' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'
Last login: Fri Sep 27 14:18:16 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Advierta que el ping falla y el tráfico está bloqueado.

5. Conéctese a la instancia C. Como no hay una dirección IP pública a la que hacer ping, utilice EC2 Instance Connect para conectarse y, a continuación, haga ping a una IP pública desde la instancia para comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'

Last login: Tue Sep 24 15:28:09 2024 from 10.0.2.86

[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com

PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.84 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.40 ms
```

Advierta que el ping se ha realizado correctamente y que el tráfico no está bloqueado.

6. Conéctese a la instancia D. Como no hay una dirección IP pública a la que hacer ping, utilice EC2 Instance Connect para conectarse y, a continuación, haga ping a una IP pública desde la instancia para comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 16:48:38 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121): icmp_seq=14 ttl=58 time=1.47 ms
64 bytes from 2600:9000:25f3:5800:7:49a5:5fd4:b121
 (2600:9000:25f3:5800:7:49a5:5fd4:b121): icmp_seq=16 ttl=58 time=1.59 ms
```

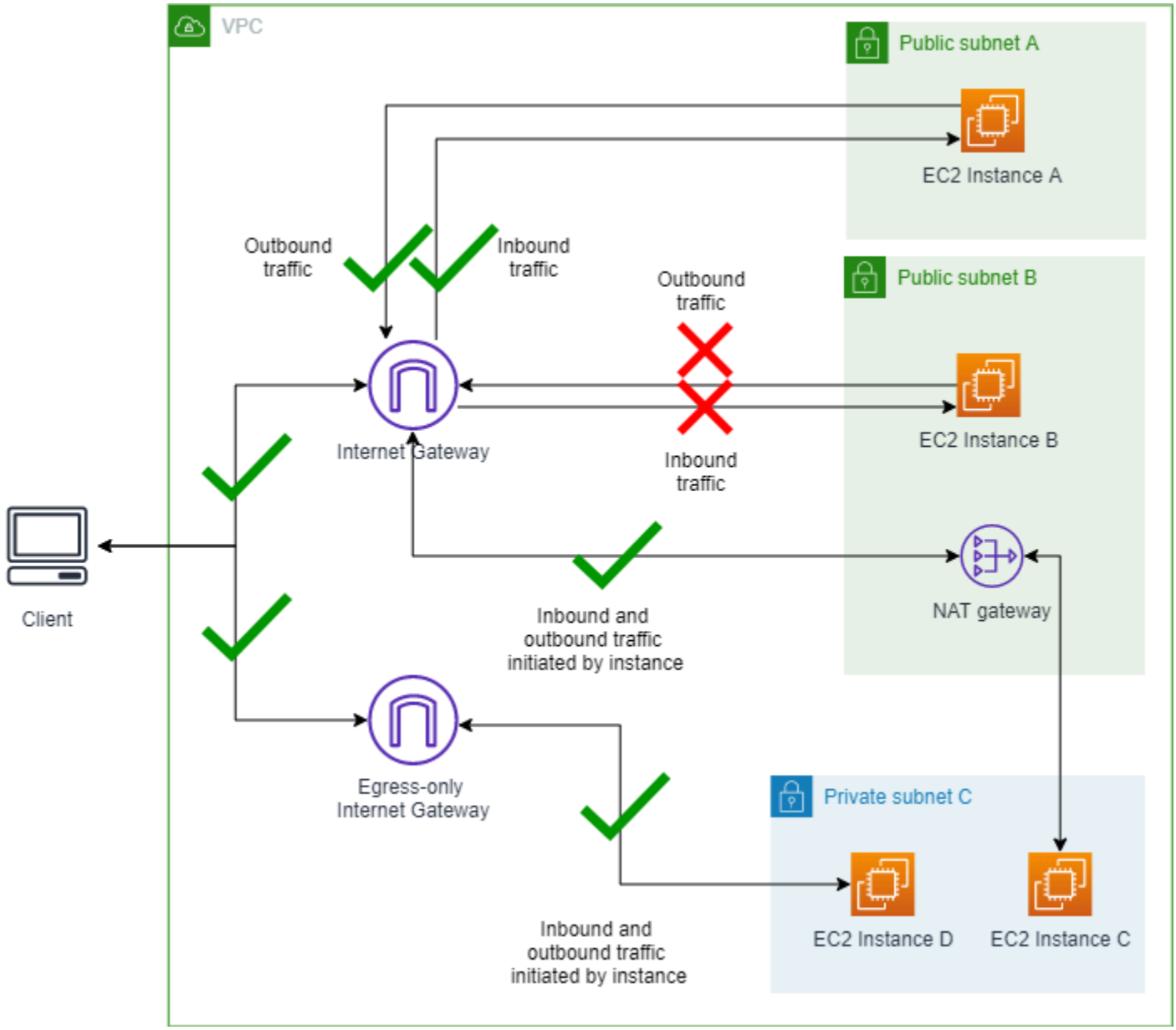
Advierta que el ping se ha realizado correctamente y que el tráfico no está bloqueado.

Escenario 4: creación de una exclusión

En esta sección, creará una exclusión. En ese caso, el BPA de la VPC solo bloqueará el tráfico en las subredes que no tengan una exclusión. Una exclusión del BPA de la VPC es un modo que se puede aplicar a una sola VPC o subred y que la exime del modo BPA de la VPC de la cuenta y permitirá el acceso bidireccional o solo de salida. Puede crear exclusiones del BPA de la VPC para las VPC y las subredes incluso cuando el BPA de la VPC no esté habilitado en la cuenta para garantizar que no se interrumpa el tráfico en las exclusiones cuando se active el BPA de la VPC.

En este ejemplo, crearemos una exclusión para la subred A para mostrar cómo afecta el BPA de la VPC al tráfico a las exclusiones.

Diagrama del modo de solo entrada del BPA de la VPC activado y de la exclusión de la subred A con el modo bidireccional activado:



4.1 Crear una exclusión para la subred A

Complete esta sección para crear una exclusión. Una exclusión del BPA de la VPC es un modo que se puede aplicar a una sola VPC o subred y que la exime del modo BPA de la VPC de la cuenta y permitirá el acceso bidireccional o solo de salida. Puede crear exclusiones del BPA de la VPC para las VPC y las subredes incluso cuando el BPA de la VPC no esté habilitado en la cuenta para garantizar que no se interrumpa el tráfico en las exclusiones cuando se active el BPA de la VPC.

Consola de administración de AWS

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

2. En el panel de navegación izquierdo, elija Configuración.
3. En la pestaña Bloquear el acceso público, en Exclusiones, seleccione Crear exclusiones.
4. Seleccione Subred pública A del BPA de la VPC, asegúrese de que esté seleccionada la opción de dirección Bidireccional permitida y elija Crear exclusiones.
5. Espere a que el Estado de exclusión cambie a Activo. Puede que tenga que actualizar la tabla de exclusión para ver el cambio.

Se ha creado la exclusión.

AWS CLI

1. Modifique la dirección permitida de la exclusión:

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-
id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. El estado de exclusión puede tardar un tiempo en actualizarse. Para ver el estado de la exclusión:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusions --
exclusion-ids exclusion-id
```

4.2 Conexión a instancias

Complete esta sección para conectarse a las instancias.

Consola de administración de AWS

1. Haga ping a la dirección IPv4 pública de la instancia A. Advierta que el tráfico está permitido.
2. Haga ping a la dirección IPv4 pública de la instancia B. Advierta que el tráfico está bloqueado.
3. Conéctese a la instancia A mediante EC2 Instance Connect como lo hizo en el escenario 1 y haga ping a www.amazon.com. Advierta que puede hacer ping a un sitio público de Internet desde la instancia A. El tráfico está permitido.
4. Conéctese a la instancia B mediante EC2 Instance Connect como lo hizo en el escenario 1 y haga ping a www.amazon.com desde allí. Advierta que no puede hacer ping a un sitio público de Internet desde la instancia B. El tráfico está bloqueado.

5. Conéctese a las instancias C y D mediante EC2 Instance Connect como lo hizo en el escenario 1 y haga ping a www.amazon.com desde allí. Advierta que puede hacer ping a un sitio público de Internet desde la instancia C o D. El tráfico está permitido.

AWS CLI

1. Haga ping a la instancia A mediante la dirección IPv4 pública para comprobar el tráfico entrante:

```
ping 18.225.8.244
```

Salida:

```
Pinging 18.225.8.244 with 32 bytes of data:

Reply from 18.225.8.244: bytes=32 time=51ms TTL=110
Reply from 18.225.8.244: bytes=32 time=61ms TTL=110
```

Advierta que el ping se ha realizado correctamente y que el tráfico no está bloqueado.

2. Utilice la dirección IPv4 privada para conectarse y comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #_   ~_  ####_        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~._.   _/
/ /
/m/'
Last login: Fri Sep 27 17:58:12 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

```
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=249 time=1.03 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=249 time=1.72 ms
```

Advierta que el ping se ha realizado correctamente y que el tráfico no está bloqueado.

3. Haga ping a la instancia B mediante la dirección IPv4 pública para comprobar el tráfico entrante:

```
ping 3.18.106.198
```

Salida:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Advierta que el ping falla y el tráfico está bloqueado.

4. Utilice la dirección IPv4 privada para conectarse y comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'
Last login: Fri Sep 27 18:12:03 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Advierta que el ping falla y el tráfico está bloqueado.

5. Conéctese a la instancia C. Como no hay una dirección IP pública a la que hacer ping, utilice EC2 Instance Connect para conectarse y, a continuación, haga ping a una IP pública desde la instancia para comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Output

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,     #   ~_  ####        Amazon Linux 2023
~~  _#####\  ~~     ###|
~~       #/ ___   https://aws.amazon.com/linux/amazon-linux-2023
~~       V~' '->
~~~         /
~~..   _/
_/ /
/m/'

Last login: Tue Sep 24 15:28:09 2024 from 10.0.2.86

[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com

PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=1 ttl=248 time=1.84 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
 icmp_seq=2 ttl=248 time=1.40 ms
```

Advierta que el ping se ha realizado correctamente y que el tráfico no está bloqueado.

6. Conéctese a la instancia D. Como no hay una dirección IP pública a la que hacer ping, utilice EC2 Instance Connect para conectarse y, a continuación, haga ping a una IP pública desde la instancia para comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Output

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:00:52 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING
 www.amazon.com(g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologie
 (2600:141f:4000:59a::3bd4)) 56 data bytes
64 bytes from
 g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologies.com
 (2600:141f:4000:59a::3bd4): icmp_seq=1 ttl=48 time=15.9 ms
64 bytes from
 g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologies.com
 (2600:141f:4000:59a::3bd4): icmp_seq=2 ttl=48 time=15.8 ms
```

Advierta que el ping se ha realizado correctamente y que el tráfico no está bloqueado.

4.3: Opcional: Verificar la conectividad con el analizador de accesibilidad

Con la misma ruta de red creada en el analizador de accesibilidad en el escenario 2, ahora puede ejecutar un nuevo análisis y confirmar que se puede acceder a la ruta ahora que se ha creado una exclusión para la subred pública A.

Para obtener información sobre la disponibilidad regional del Analizador de accesibilidad, consulte Consideraciones en la Guía del Analizador de accesibilidad.

Consola de administración de AWS

1. En la ruta de red que creó anteriormente en la consola de Network Insights, seleccione Volver a ejecutar el análisis.
2. Espere a que el análisis finalice. Esta operación puede tardar varios minutos.
3. Confirme que ahora la ruta está Accesible.

AWS CLI

1. Con el ID de ruta de red creado anteriormente, inicie un nuevo análisis:

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-path-id nip-id
```

2. Recuperar los resultados del análisis:

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-insights-analysis-ids nia-id
```

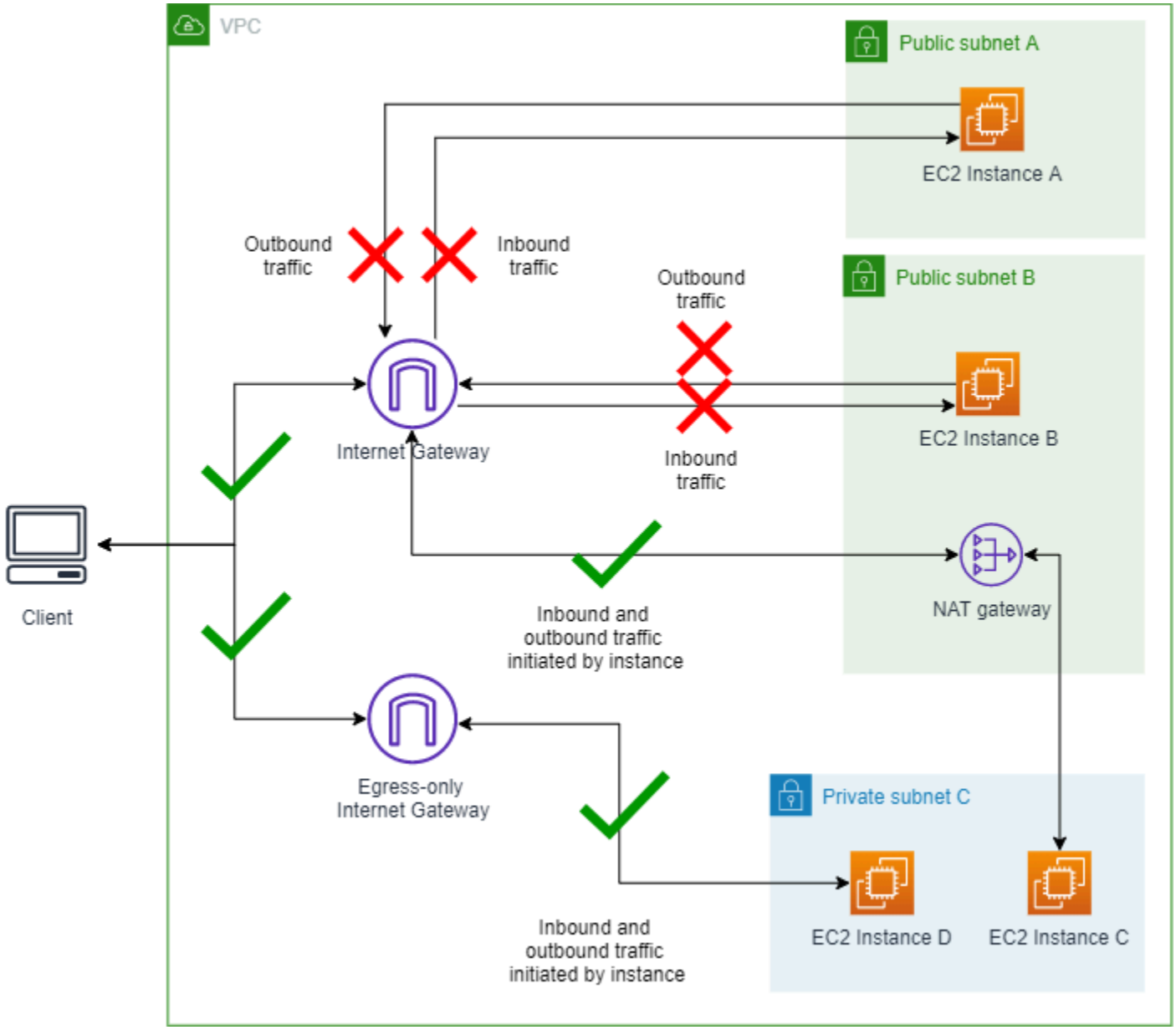
3. Confirme que el código de explicación `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` ya no está presente.

Escenario 5: modificación del modo de exclusión

En esta sección, cambiará la dirección del tráfico permitida en la exclusión para ver cómo afecta al BPA de la VPC.

> **Note**
>
> En este escenario, cambiará el modo de exclusión a solo salida. Tenga en cuenta que, cuando hace esto, la exclusión de solo salida en la subred A no permite el tráfico saliente, lo cual es contraintuitivo, ya que uno esperaría que permitiera el tráfico saliente. Sin embargo, dado que el BPA a nivel de cuenta es de solo entrada, se ignoran las exclusiones de solo salida y el BPA de la VPC restringe el enrutamiento de la subred A a una puerta de enlace de Internet, lo cual bloquea el tráfico saliente. Para habilitar el tráfico saliente en la subred A, tendría que cambiar el BPA de la VPC al modo bidireccional.

Diagrama del modo de solo entrada del BPA de la VPC activado y de la exclusión de la subred A con el modo de solo salida activado:



5.1 Cambiar la dirección permitida de la exclusión a solo salida

Complete esta sección para cambiar la dirección de la exclusión permitida.

Consola de administración de AWS

1. Edite la exclusión que creó en el escenario 4 y cambie la dirección permitida a Solo salida.
2. Seleccione Save changes (Guardar cambios).
3. Espere a que el Estado de exclusión cambie a Activo. La aplicación de las configuraciones del BPA de la VPC y la actualización del estado pueden tardar unos minutos. Puede que tenga que actualizar la tabla de exclusión para ver el cambio.

AWS CLI

1. Modifique la dirección permitida de la exclusión:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-exclusion --exclusion-
id exclusion-id --internet-gateway-exclusion-mode allow-egress
```

   La aplicación de las configuraciones del BPA de la VPC y la actualización del estado pueden tardar unos minutos.
2. El estado de exclusión puede tardar un tiempo en actualizarse. Para ver el estado de la exclusión:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusion
```

5.2 Conexión a instancias

Complete esta sección para conectarse a las instancias.

Consola de administración de AWS

1. Haga ping a la dirección IPv4 pública de las instancias A y B. Advierta que el tráfico está bloqueado.
2. Conéctese a la instancia A y B mediante EC2 Instance Connect como lo hizo en el escenario 1 y haga ping a www.amazon.com. Advierta que no puede hacer ping a un sitio público de Internet desde la instancia A o B. El tráfico está bloqueado.
3. Conéctese a las instancias C y D mediante EC2 Instance Connect como lo hizo en el escenario 1 y haga ping a www.amazon.com desde allí. Advierta que puede hacer ping a un sitio público de Internet desde la instancia C o D. El tráfico está permitido.

AWS CLI

1. Haga ping a la instancia A mediante la dirección IPv4 pública para comprobar el tráfico entrante:

```
ping 18.225.8.244
```

   Salida:

```
Pinging 18.225.8.244 with 32 bytes of data:
Request timed out.
```

Advierta que el ping falla y el tráfico está bloqueado.

2. Utilice la dirección IPv4 privada para conectarse y comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Advierta que el ping falla y el tráfico está bloqueado.

3. Haga ping a la instancia B mediante la dirección IPv4 pública para comprobar el tráfico entrante:

```
ping 3.18.106.198
```

Salida:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Advierta que el ping falla y el tráfico está bloqueado.

4. Utilice la dirección IPv4 privada para conectarse y comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Advierta que el ping falla y el tráfico está bloqueado.

5. Conéctese a la instancia C. Como no hay una dirección IP pública a la que hacer ping, utilice EC2 Instance Connect para conectarse y, a continuación, haga ping a una IP pública desde la instancia para comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:00:31 2024 from 3.16.146.5
```

```
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121): icmp_seq=1 ttl=58 time=1.51 ms
64 bytes from 2600:9000:25f3:a600:7:49a5:5fd4:b121
 (2600:9000:25f3:a600:7:49a5:5fd4:b121): icmp_seq=2 ttl=58 time=1.49 ms
```

Advierta que el ping se ha realizado correctamente y que el tráfico no está bloqueado.

6. Conéctese a la instancia D. Como no hay una dirección IP pública a la que hacer ping, utilice EC2 Instance Connect para conectarse y, a continuación, haga ping a una IP pública desde la instancia para comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:13:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2606:2cc0::374 (2606:2cc0::374)) 56 data bytes
64 bytes from 2606:2cc0::374 (2606:2cc0::374): icmp_seq=1 ttl=58 time=1.21 ms
64 bytes from 2606:2cc0::374 (2606:2cc0::374): icmp_seq=2 ttl=58 time=1.51 ms
```

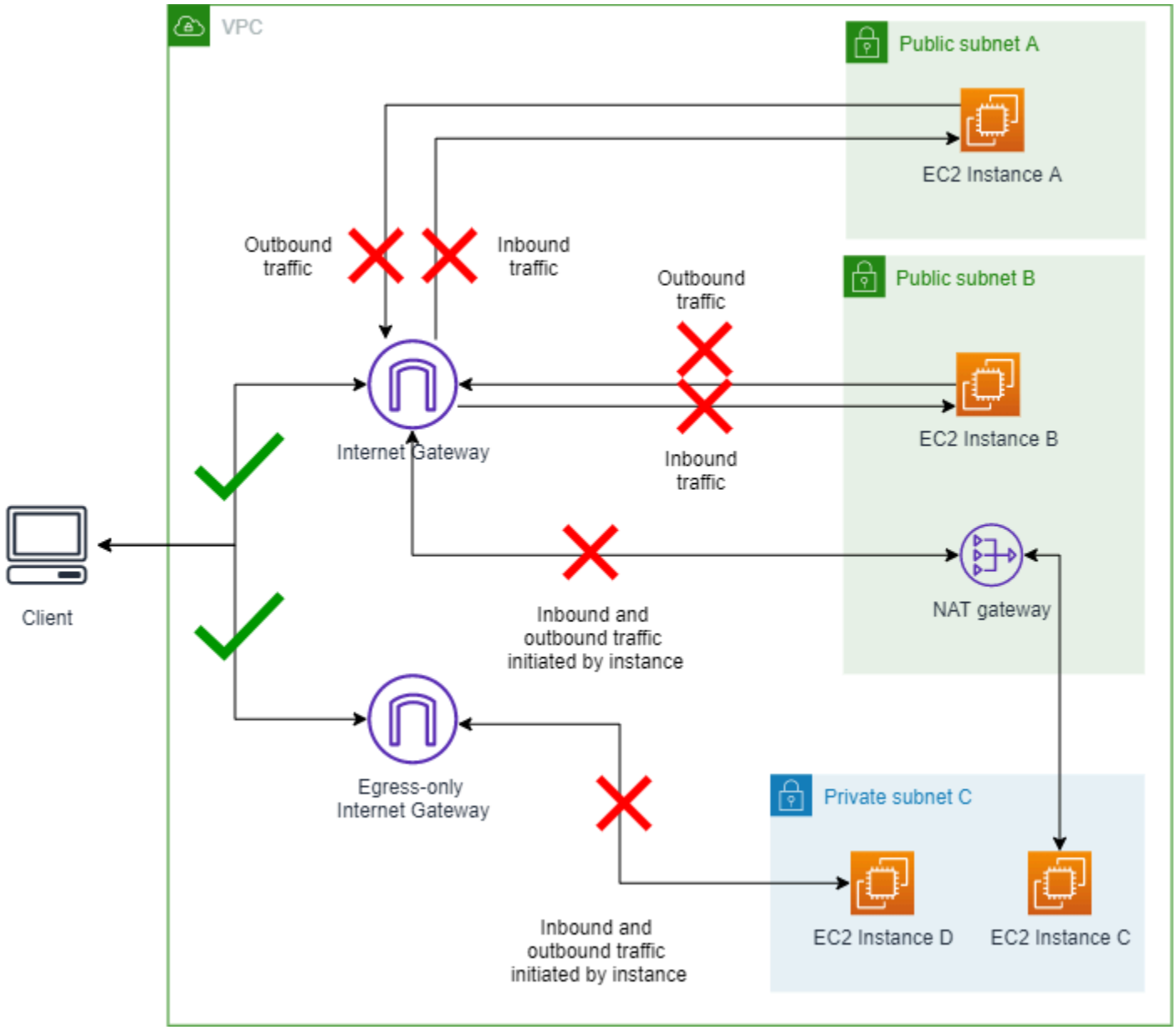
Advierta que el ping se ha realizado correctamente y que el tráfico no está bloqueado.

Escenario 6: modificación del modo del BPA de la VPC

En esta sección, cambiará la dirección del bloque de BPA de la VPC para ver cómo afecta al tráfico. En este escenario, el BPA de la VPC habilitado en modo bidireccional bloquea todo el tráfico igual

que en el escenario 1. A menos que una exclusión tenga acceso a una puerta de enlace NAT o a una puerta de enlace de Internet de solo salida, el tráfico se bloquea.

Diagrama del modo bidireccional del BPA de la VPC activado y de la exclusión de subred A con el modo de solo salida activado:



6.1 Cambiar el BPA de la VPC al modo bidireccional

Complete esta sección para cambiar el modo del BPA de la VPC.

Consola de administración de AWS

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

2. En el panel de navegación izquierdo, elija Configuración.
3. Elija Editar la configuración del acceso público.
4. Cambie la dirección del bloque a Bidireccional y, a continuación, seleccione Guardar cambios.
5. Espere a que el Estado cambie a Activado. La aplicación de las configuraciones del BPA de la VPC y la actualización del estado pueden tardar unos minutos.

AWS CLI

1. Modifique la dirección del bloqueo del BPA de la VPC:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-bidirectional
```

   La aplicación de las configuraciones del BPA de la VPC y la actualización del estado pueden tardar unos minutos.
2. Ver el estado del BPA de la VPC:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

6.2 Conexión a instancias

Complete esta sección para conectarse a las instancias.

Consola de administración de AWS

1. Haga ping a la dirección IPv4 pública de las instancias A y B. Advierta que el tráfico está bloqueado.
2. Conéctese a la instancia A y B mediante EC2 Instance Connect como lo hizo en el escenario 1 y haga ping a www.amazon.com. Advierta que no puede hacer ping a un sitio público de Internet desde la instancia A o B. El tráfico está bloqueado.
3. Conéctese a las instancias C y D mediante EC2 Instance Connect como lo hizo en el escenario 1 y haga ping a www.amazon.com desde allí. Advierta que no puede hacer ping a un sitio público de Internet desde la instancia C o D. El tráfico está bloqueado.

AWS CLI

1. Haga ping a la instancia A mediante la dirección IPv4 pública para comprobar el tráfico entrante:

```
ping 18.225.8.244
```

Salida:

```
Pinging 18.225.8.244 with 32 bytes of data:
Request timed out.
```

Advierta que el ping falla y el tráfico está bloqueado.

2. Utilice la dirección IPv4 privada para conectarse y comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:17:44 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Advierta que el ping falla y el tráfico está bloqueado.

3. Haga ping a la instancia A mediante la dirección IPv4 pública para comprobar el tráfico entrante:

```
ping 3.18.106.198
```

Salida:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Advierta que el ping falla y el tráfico está bloqueado.

4. Utilice la dirección IPv4 privada para conectarse y comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Advierta que el ping falla y el tráfico está bloqueado.

5. Conéctese a la instancia C. Como no hay una dirección IP pública a la que hacer ping, utilice EC2 Instance Connect para conectarse y, a continuación, haga ping a una IP pública desde la instancia para comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
```

```
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:19:45 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:6200:7:49a5:5fd4:b121
 (2600:9000:25f3:6200:7:49a5:5fd4:b121)) 56 data bytes
```

Advierta que el ping falla y el tráfico está bloqueado.

6. Conéctese a la instancia D. Como no hay una dirección IP pública a la que hacer ping, utilice EC2 Instance Connect para conectarse y, a continuación, haga ping a una IP pública desde la instancia para comprobar el tráfico saliente:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-
east-2 --connection-type eice
```

Salida:

```
A newer release of "Amazon Linux" is available.  Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
Last login: Fri Sep 27 18:20:58 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:b400:7:49a5:5fd4:b121
 (2600:9000:25f3:b400:7:49a5:5fd4:b121)) 56 data bytes
```

Advierta que el ping falla y el tráfico está bloqueado.

Eliminación

En esta sección, eliminará todos los recursos que ha creado para este ejemplo avanzado. Es importante limpiar los recursos para evitar cargos adicionales excesivos por los recursos creados en su cuenta.

Eliminar los recursos de CloudFormation

Complete esta sección para eliminar los recursos que ha creado con la plantilla CloudFormation.

Consola de administración de AWS

1. Abra la consola de CloudFormation en https://console.aws.amazon.com/cloudformation/.
2. Elija la pila del BPA de la VPC.
3. Elija Eliminar.
4. Cuando empiece a eliminar la pila, consulte la pestaña Eventos para ver el progreso y asegurarse de que la pila se haya eliminado. Puede que deba forzar la eliminación de la pila para que se elimine por completo.

AWS CLI

1. Crear la pila de CloudFormation. Puede que deba forzar la eliminación de la pila para que se elimine por completo.

```
aws cloudformation delete-stack --stack-name VPC-BPA-stack --region us-east-2
```

2. Verifique el progreso y asegúrese de que la pila se ha eliminado.

```
aws cloudformation describe-stack-events --stack-name VPC-BPA-stack --region us-east-2
```

Seguimiento de la eliminación de exclusiones con CloudTrail

Complete esta sección para realizar un seguimiento de la eliminación de exclusiones con AWS CloudTrail. Las entradas de CloudTrail aparecen al eliminar una exclusión.

Consola de administración de AWS

Para ver las exclusiones eliminadas en el historial de eventos de CloudTrail, consulte Tipo de recurso > AWS::EC2::VPCBlockPublicAccessExclusion en la consola de AWSCloudTrail en https://console.aws.amazon.com/cloudtrailv2/.

AWS CLI

Puede usar el comando lookup-events para ver los eventos relacionados con la eliminación de exclusiones:

```
aws cloudtrail lookup-events --lookup-attributes
 AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCBlockPublicAccessExclusion
```

El ejemplo avanzado está completo.

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, plantéeselas como consideraciones útiles en lugar de como normas.

- Cuando agregue subredes a la VPC para alojar la aplicación, créelas en varias zonas de disponibilidad. Una zona de disponibilidad consiste en uno o varios centros de datos discretos con alimentación, redes y conectividad redundantes en una región de AWS. Usar varias zonas de disponibilidad permite que las aplicaciones de producción estén altamente disponibles, sean tolerantes a errores y tengan escalabilidad.
- Utilice grupos de seguridad para controlar el acceso del tráfico a instancias EC2 en sus subredes. Para obtener más información, consulte Grupos de seguridad.
- Use las ACL de red para controlar el tráfico entrante y saliente en el nivel de subred. Para obtener más información, consulte Control del tráfico de la subred con listas de control de acceso a la red.
- Administre el acceso a los recursos de AWS de la VPC mediante federación de identidades, usuarios y roles de AWS Identity and Access Management (IAM). Para obtener más información, consulte Identity and Access Management para Amazon VPC.
- Use VPC Flow Logs para supervisar el tráfico IP entrante y saliente de una VPC, subred o interfaz de red. Para obtener más información, consulte Logs de flujo de VPC.

- Utilice el Analizador de acceso a la red para identificar acceso no deseado a la red con destino a recursos de nuestras VPC. Para obtener más información, consulte la Guía del usuario del Analizador de acceso a la red.
- Use AWS Network Firewall para supervisar y proteger su VPC mediante el filtrado de tráfico entrante y saliente. Para obtener más información, consulte la Guía de AWS Network Firewall.
- Utilice Amazon GuardDuty para detectar posibles amenazas en las cuentas, los contenedores, las cargas de trabajo y los datos dentro del entorno de AWS. La detección de amenazas fundacional incluye la supervisión de los registros de flujos de la VPC asociados a las instancias de Amazon EC2. Para más información, consulte Registros de flujos de la VPC en la Guía del usuario de Amazon GuardDuty.

Para obtener respuestas a las preguntas frecuentes relacionadas con la seguridad de las VPC, consulte Seguridad y filtrado en las Preguntas frecuentes sobre Amazon VPC.

Uso de Amazon VPC con otros Servicios de AWS

Amazon Virtual Private Cloud (VPC) es un producto básico de AWS que ofrece un entorno de red seguro y personalizable para su infraestructura en la nube. Además de crear y administrar su propia VPC, puede utilizar la integración entre la VPC y otros productos de AWS para crear soluciones integrales que se ajusten a sus necesidades específicas.

Con AWS PrivateLink, puede conectar su VPC a varios servicios de AWS. Esto da lugar a la conexión privada entre su VPC y los servicios compatibles de AWS o las aplicaciones en las instalaciones, lo que mantiene el tráfico de la red dentro de la red de AWS y evita su exposición a la Internet pública. Esto resulta particularmente práctico para mantener límites de seguridad y requisitos de cumplimiento estrictos.

Para reforzar aún más la seguridad de su VPC, puede utilizar AWS Network Firewall. Este servicio de firewall administrado permite definir políticas de seguridad para la red, aplicarlas y filtrar el tráfico tanto de norte a sur como de este a oeste dentro de la VPC. Al emparejar Network Firewall con su VPC, puede mejorar su estrategia de defensa y proteger sus recursos de la nube contra el acceso sin autorización o la actividad malintencionada.

También, puede filtrar el tráfico de DNS dentro de su VPC con DNS Firewall de Route 53 Resolver. Con esta capacidad, puede crear reglas personalizadas de filtrado de DNS para controlar cuáles son los dominios que sus recursos de VPC pueden resolver, lo cual brinda una capa adicional de seguridad y aplicación de la conformidad.

Si detecta problemas de accesibilidad entre los recursos que están dentro de su VPC o conectados a ella, puede utilizar el Analizador de accesibilidad. El Analizador de accesibilidad realiza pruebas de conectividad virtuales, lo que ofrece información de la ruta detallada de cada salto e identifica cualquier componente que cree un bloqueo. Con esta herramienta de solución de problemas, puede identificar y resolver rápidamente problemas de conectividad en la red.

Al integrar estos productos complementarios de AWS con su VPC, puede construir soluciones en la nube potentes, seguras y resilientes para cumplir con sus necesidades empresariales y de arquitectura únicas.

Contenido

- Conectar la VPC a los servicios mediante AWS PrivateLink
- Filtrado del tráfico de red utilizando AWS Network Firewall

- Filtrar el tráfico de DNS utilizando Route 53 Resolver DNS Firewall
- Solucione problemas de accesibilidad con Reachability Analyzer

Conectar la VPC a los servicios mediante AWS PrivateLink

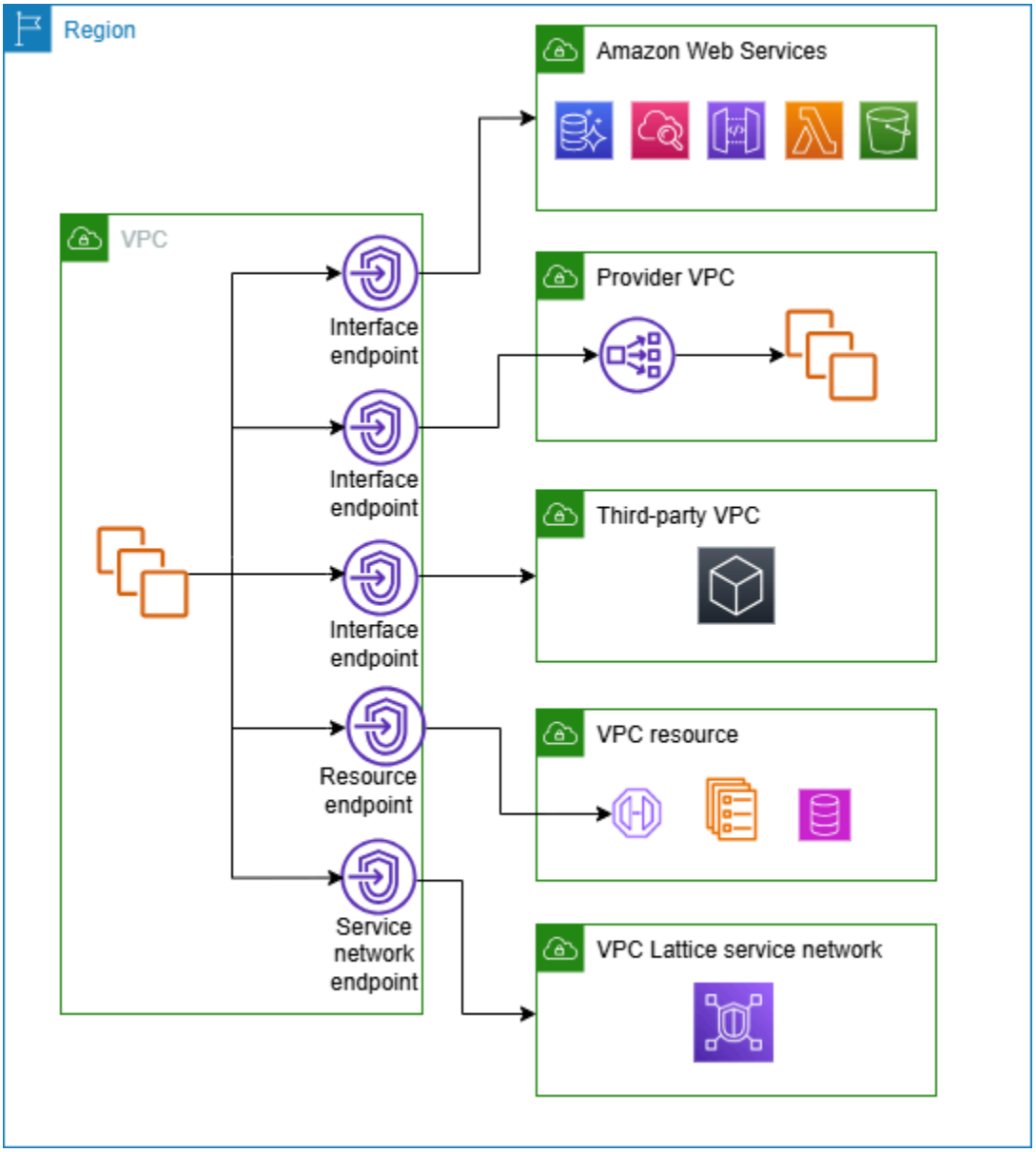
AWS PrivateLink establece conectividad privada entre nubes virtuales privadas (VPC) y Servicios de AWS compatibles, servicios alojados por otras Cuentas de AWS, servicios de AWS Marketplace compatibles y recursos compatibles. Para comunicarse con el servicio o recurso, no necesita una puerta de enlace de Internet, dispositivo NAT, conexión a Direct Connect ni conexión de AWS Site-to-Site VPN.

Para utilizar AWS PrivateLink, cree un punto de conexión de VPC en la subred desde la que necesita acceder al servicio o recurso. De este modo, crea interfaces de red elásticas en las subredes específicas que funcionan como puntos de entrada para el tráfico dirigido al servicio o recurso.

También, puede crear su propio servicio de punto de conexión de VPC, con tecnología de AWS PrivateLink, y permitir que otros usuarios de AWS puedan acceder a su servicio. PrivateLink habilita la creación de puntos de conexión privados de API, lo que le permite a las organizaciones exponer sus servicios de manera segura a otros clientes de AWS. Gracias a esto, las empresas monetizan sus capacidades internas, fomentan los ecosistemas de colaboración y mantienen el control sobre el acceso y el consumo de sus servicios.

Uno de los beneficios más importantes de AWS PrivateLink es la posibilidad de establecer una conectividad segura y privada sin constructos de red tradicionales, como las puertas de enlace de Internet, los dispositivos de NAT o las conexiones de VPC. Esto simplifica la arquitectura de la red, reduce la superficie expuesta a ataques y mejora la seguridad general mediante el confinamiento de los tráficos de datos dentro de la red de AWS.

En el siguiente diagrama, se muestran casos prácticos comunes de AWS PrivateLink. La VPC cuenta con varias instancias de EC2 en una subred privada con acceso a recursos mediante cinco puntos de conexión de VPC. Hay tres puntos de conexión de VPC de interfaz, un punto de conexión de VPC de recurso y un punto de conexión de VPC de la red de servicio.



Para obtener más información, consulte AWS PrivateLink.

Filtrado del tráfico de red utilizando 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	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. Para obtener más información, consulte Firewall en AWS Network Firewall.
Directiva de firewall	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. Para obtener más información, consulte Políticas de firewall en AWS Network Firewall.
Grupo de reglas	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. Para obtener más información, consulte Grupos de reglas en AWS Network Firewall.

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	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. 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 personali zadas para las consultas bloqueadas. Para obtener más información, consulte Grupos de reglas y reglas en DNS Firewall de Route 53 Resolver.

Recurso de DNS Firewall	Descripción
Lista de dominios	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. Para obtener más información, consulte Listas de dominios en DNS Firewall de Route 53 Resolver.

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.

Solucione problemas de accesibilidad con Reachability Analyzer

Reachability Analyzer es una herramienta de análisis de configuración estática. Utilice Reachability Analyzer para analizar y depurar la accesibilidad de la red entre dos recursos en la VPC. Reachability Analyzer produce detalles salto a salto de la ruta virtual entre estos recursos cuando son accesibles y, en caso contrario, identifica el componente de bloqueo.

Puede usar Reachability Analyzer para analizar la accesibilidad entre los siguientes recursos:

- instancias
- Gateways de Internet
- Interfaces de red
- Puertas de enlace de tránsito
- Conexiones de puerta de enlace de tránsito
- Servicios de punto de conexión de VPC
- Puntos de conexión de VPC
- Interconexiones de VPC
- Puertas de enlace de VPN

Para obtener más información, consulte la Guía del Analizador de accesibilidad.

Ejemplos de VPC

Amazon Virtual Private Cloud (VPC) es un componente fundamental dentro del ecosistema de AWS, lo que permite un aprovisionamiento de redes virtuales aisladas que se ajusten a sus necesidades en específico. Al crear y administrar sus propias VPC, obtiene control total sobre el entorno de red, incluida la capacidad de definir rangos de direcciones IP, subredes, tablas de enrutamiento y opciones de conectividad.

En esta sección, se presentan tres ejemplos de configuraciones para su nube privada virtual (VPC), cada uno diseñado para tratar un conjunto de necesidades distinto:

- VPC para el entorno de pruebas: en esta configuración, se muestra cómo crear una VPC para un entorno de desarrollo o de pruebas.
- VPC para servidores web y de base de datos: en esta configuración, se muestra cómo crear una VPC para una arquitectura resiliente en un entorno de producción.
- VPC con servidores en subredes privadas y NAT: en esta configuración más avanzada, todas las instancias de EC2 están aprovisionadas dentro de subredes privadas y un puerta de enlace de NAT facilita el acceso saliente seguro de internet. En este ejemplo, necesita limitar la conectividad directa a internet de sus recursos y, al mismo tiempo, habilitar la comunicación saliente necesaria.

Con estos ejemplos de configuraciones de VPC, esperamos ilustrar las opciones de flexibilidad y personalización disponibles para diseñar su entorno de red en la nube. La configuración de VPC específica que elija debe basarse en la arquitectura de la aplicación, los requisitos de seguridad y los objetivos empresariales generales. Planificar cuidadosamente su infraestructura de VPC ayuda a crear una red virtual robusta, escalable y segura que respalde el crecimiento y la evolución de sus cargas de trabajo en la nube.

Ejemplos

- Ejemplo: VPC para un entorno de prueba
- Ejemplo: una VPC para servidores web y de bases de datos
- Ejemplo: una VPC con servidores en subredes privadas y NAT

Ejemplos relacionados

- Para conectar las VPC entre sí, consulte Configuraciones de emparejamiento de VPC en la Guía de emparejamiento de VPC de Amazon.

- Para conectar las VPC a su propia red, consulte Ejemplos de Site-to-Site VPN en la Guía del usuario de AWS Site-to-Site VPN.
- Para conectar las VPC entre sí y a su propia red, consulte Ejemplos de escenarios de la puerta de enlace de tránsito en Puertas de enlace de tránsito de Amazon VPC.

Recursos adicionales

- Comprensión de los patrones de resiliencia y las compensaciones (Blog de arquitectura de AWS)
- Planificación de la topología de red (Marco de AWS Well-Architected)
- Opciones de conectividad de Amazon Virtual Private Cloud (Documentos técnicos de AWS)

Ejemplo: VPC para un entorno de prueba

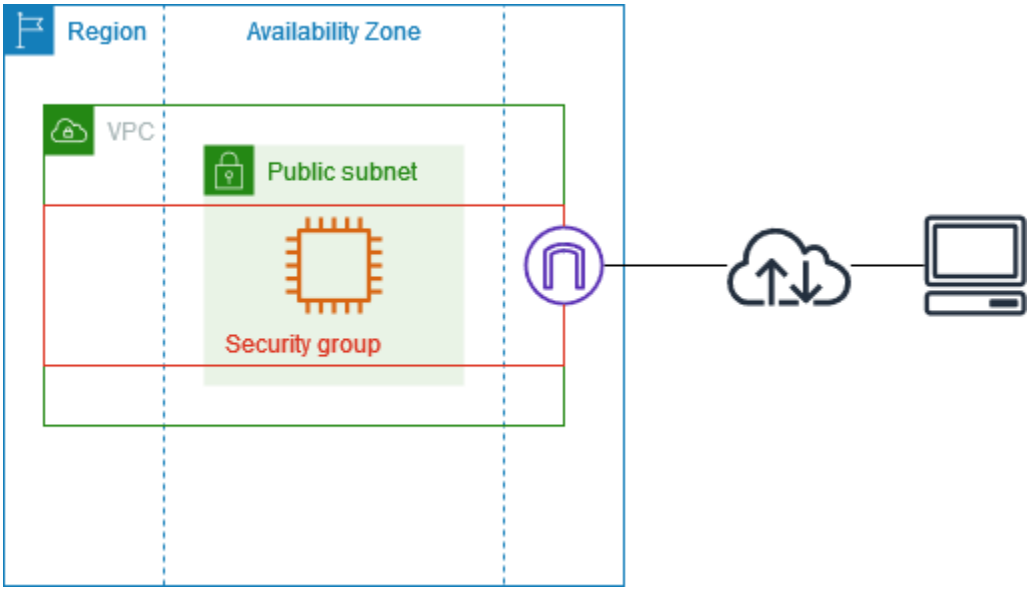
En este ejemplo se muestra cómo crear una VPC que se puede utilizar como entorno de desarrollo o de prueba. Dado que esta VPC no está pensada para ser utilizada en producción, no es necesario desplegar sus servidores en múltiples zonas de disponibilidad. Para mantener bajos los costes y la complejidad, puede desplegar sus servidores en una única zona de disponibilidad.

Contenido

- Descripción general
- 1. Creación de la VPC
- 2. Implementar la aplicación
- 3. Pruebe la configuración
- 4. Limpieza

Descripción general

En el diagrama siguiente, se proporciona información general sobre los recursos que se incluyen en este ejemplo. La VPC tiene una subred pública en una única zona de disponibilidad y una puerta de enlace de Internet. El servidor es una instancia de EC2 que se ejecuta en la subred pública. El grupo de seguridad de la instancia permite el tráfico SSH desde su propio equipo, además de cualquier otro tráfico que se requiera de forma específica para sus actividades de desarrollo o de prueba.



Enrutamiento

Cuando crea esta VPC con la consola de Amazon VPC, creamos una tabla de enrutamiento para la subred pública con rutas locales y rutas a la puerta de enlace de Internet. A continuación, se muestra un ejemplo de una tabla de enrutamiento con rutas para IPv4 e IPv6. Si crea una subred solo para IPv4 en lugar de una subred de doble pila, la tabla de enrutamiento solo contiene las rutas IPv4.

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

Para esta configuración de ejemplo, debe crear un grupo de seguridad para su instancia que permita el tráfico que necesita su aplicación. Por ejemplo, puede que necesite añadir una regla que permita el tráfico SSH desde su ordenador o el tráfico HTTP desde su red.

Los siguientes son ejemplos de reglas de entrada para un grupo de seguridad, con reglas para IPv4 e IPv6. Si crea subredes solo de IPv4 en lugar de subredes de doble pila, solo necesitará las reglas para IPv4.

Origen	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	Permite el acceso HTTP entrante desde todas las direcciones IPv6
0.0.0.0/0	TCP	443	Permite el acceso HTTPS de entrada desde todas las direcciones IPv4
::/0	TCP	443	Permite el acceso HTTPS entrante desde todas las direcciones IPv6
Rango de direcciones IPv4 públicas de su red	TCP	22	(Opcional) Permite el acceso SSH de entrada desde las direcciones IP IPv4 de su red
Rango de direcciones IPv6 de su red	TCP	22	(Opcional) Permite el acceso SSH de entrada desde las direcciones IP IPv6 de su red
Rango de direcciones IPv4 públicas de su red	TCP	3389	(Opcional) Permite el acceso RDP de entrada desde las direcciones IP IPv4 de su red
Rango de direcciones IPv6 de su red	TCP	3389	(Opcional) Permite el acceso RDP de entrada desde las direcciones IP IPv6 de su red

1. Creación de la VPC

Utilice el siguiente procedimiento para crear una VPC con una subred pública en una zona de disponibilidad. Esta configuración es adecuada para un entorno de desarrollo o de prueba.

Para crear la VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel, elija Crear VPC.
3. En Recursos para crear, elija VPC y más.
4. Configurar la VPC
    a. En Generación automática de etiquetas de nombre, ingrese un nombre para la VPC.
    b. En Bloque de CIDR IPv4, puede conservar la sugerencia predeterminada o, como alternativa, ingresar el bloque de CIDR necesario para su aplicación o red. Para obtener más información, consulte the section called “Bloques de CIDR de VPC”.
    c. (Opcional) Si su aplicación se comunica mediante direcciones IPv6, elija Bloque de CIDR IPv6, Bloque de CIDR IPv6 proporcionado por Amazon.
5. Configurar las subredes
    a. Para Cantidad de zonas de disponibilidad, elija 1. Puede conservar la zona de disponibilidad predeterminada o, si lo prefiere, puede desplegar el menú Personalizar las zonas de disponibilidad y seleccionar una zona.
    b. Para Number of public subnets (Número de subredes públicas), elija 1.
    c. Para Number of private subnets (Número de subredes privadas), elija 0.
    d. Puede conservar el bloque de CIDR predeterminado para la subred pública o, si lo prefiere, puede ampliar Personalizar los bloques de CIDR de la subred e introducir un bloque de CIDR. Para obtener más información, consulte the section called “Bloques de CIDR de subred”.
6. En Puertas de enlace NAT, mantenga el valor predeterminado: Ninguno.
7. Para VPC endpoints (Puntos de conexión de la VPC), elija None (Ninguno). Un punto de conexión de VPC de puerta de enlace para S3 solo se usa para acceder a Amazon S3 desde subredes privadas.
8. Mantenga ambas opciones seleccionadas en Opciones de DNS. Como resultado, la instancia recibirá un nombre de host de DNS público que corresponde a su dirección IP pública.

9. Seleccione Creación de VPC.

2. Implementar la aplicación

Hay diversas formas para implementar instancias de EC2. Por ejemplo:

- Asistente de lanzamiento de instancias de Amazon EC2
- Amazon EC2 Auto Scaling
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Tras implementar una instancia de EC2, puede conectarse a la instancia, instalar el software que necesita para la aplicación y, a continuación, crear una imagen para usarla en el futuro. Para obtener más información, consulte Creación de una AMI en la Guía del usuario de Amazon EC2. También puede utilizar EC2 Image Builder para crear y administrar su Imagen de máquina de Amazon (AMI).

3. Pruebe la configuración

Una vez que haya terminado de implementar la aplicación, puede probarla. Si no puede conectarse a su instancia de EC2 o si su aplicación no puede enviar ni recibir el tráfico esperado, puede utilizar el Analizador de accesibilidad como ayuda para solucionar problemas. Por ejemplo, el Analizador de accesibilidad puede identificar problemas de configuración en sus tablas de enrutamiento o grupos de seguridad. Para obtener más información, consulte la Guía del Analizador de accesibilidad.

4. Limpieza

Cuando complete esta configuración, puede eliminarla. Antes de eliminar la VPC, debe terminar la instancia. Para obtener más información, consulte the section called “Eliminar su VPC”.

Ejemplo: una VPC para servidores web y de bases de datos

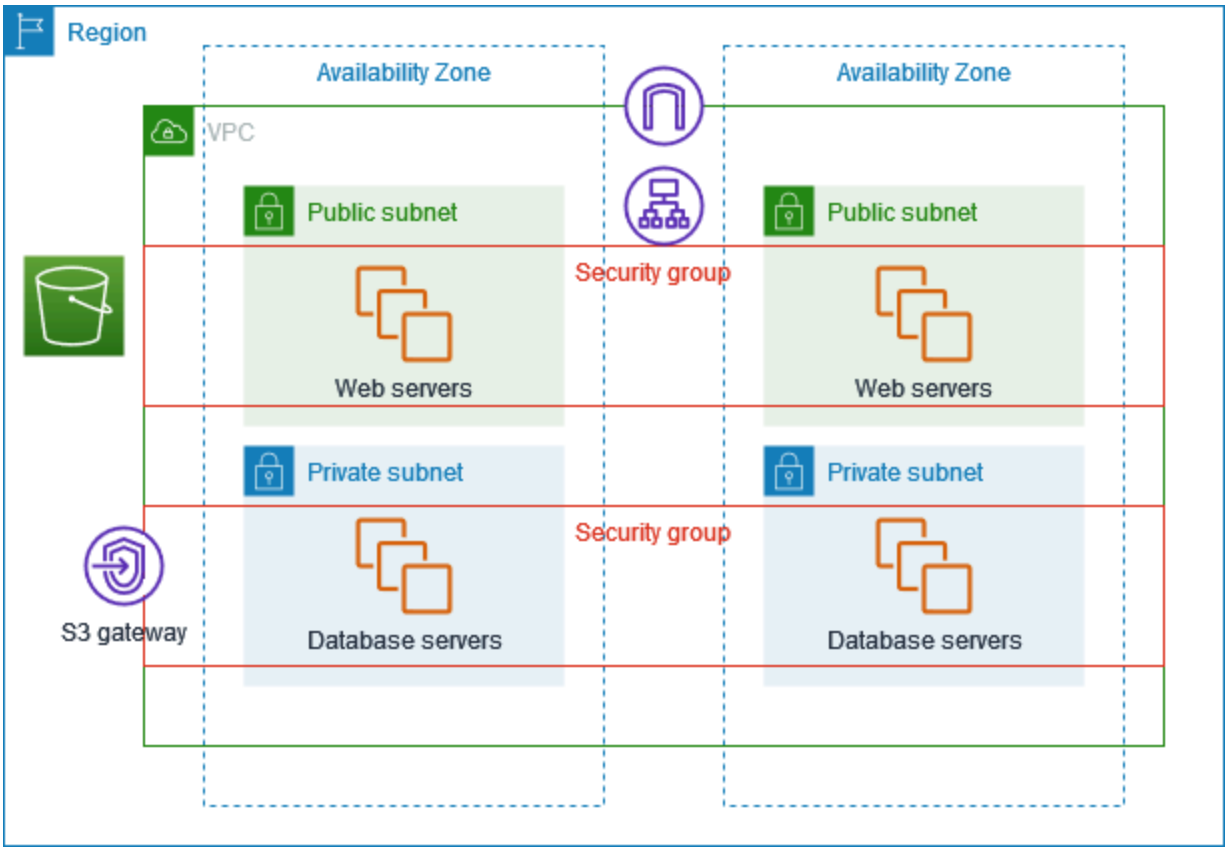
En este ejemplo se muestra cómo crear una VPC que se puede utilizar para una arquitectura de dos niveles en un entorno de producción. Para mejorar la resiliencia, los servidores se implementan en dos zonas de disponibilidad.

Contenido

- Descripción general
- 1. Creación de la VPC
- 2. Implementar la aplicación
- 3. Pruebe la configuración
- 4. Limpieza

Descripción general

En el diagrama siguiente, se proporciona información general sobre los recursos que se incluyen en este ejemplo. La VPC tiene subredes privadas y públicas en dos zonas de disponibilidad. Los servidores web se ejecutan en las subredes públicas y reciben tráfico desde los clientes a través de un equilibrador de carga. El grupo de seguridad de los servidores web permite el tráfico del equilibrador de carga. Los servidores de bases de datos se ejecutan en las subredes privadas y reciben tráfico desde los servidores web. El grupo de seguridad de los servidores de bases de datos permite el tráfico desde los servidores web. Los servidores de bases de datos pueden conectarse a Amazon S3 mediante un punto de conexión de VPC de puerta de enlace.



Enrutamiento

Cuando crea esta VPC con la consola de Amazon VPC, creamos una tabla de enrutamiento para las subredes públicas con rutas locales y rutas a la puerta de enlace de Internet y una tabla de enrutamiento para cada subred privada con rutas locales y una ruta al punto de conexión de VPC de la puerta de enlace.

El siguiente es un ejemplo de una tabla de enrutamiento para las subredes públicas, con rutas tanto para IPv4 como para IPv6. Si crea subredes solo para IPv4 en lugar de subredes de doble pila, la tabla de enrutamiento solo contiene las rutas IPv4.

Destino	Objetivo
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	*igw-id*
::/0	*igw-id*

El siguiente es un ejemplo de una tabla de enrutamiento para las subredes privadas, con rutas locales para IPv4 e IPv6. Si creó subredes solo para IPv4, la tabla de enrutamiento solo contiene la ruta IPv4. La última ruta envía el tráfico destinado a Amazon S3 al punto de conexión de VPC de la puerta de enlace.

Destino	Objetivo
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
s3-prefix-list-id	*s3-gateway-id*

Seguridad

Para esta configuración de ejemplo, se crea un grupo de seguridad para el equilibrador de carga, un grupo de seguridad para los servidores web y un grupo de seguridad para los servidores de bases de datos.

Balanceador de carga

El grupo de seguridad del equilibrador de carga de aplicación o del equilibrador de carga de red debe permitir el tráfico entrante de los clientes en el puerto de agente de escucha del equilibrador de carga. Para aceptar tráfico desde cualquier lugar de Internet, especifique 0.0.0.0/0 como origen. El grupo de seguridad del equilibrador de carga también debe permitir el tráfico saliente del equilibrador de carga a las instancias de destino en el puerto de agente de escucha de la instancia y en el puerto de comprobación de estado.

Servidores web

Las siguientes reglas del grupo de seguridad permiten que los servidores web reciban tráfico HTTP y HTTPS del equilibrador de carga. Si lo desea, puede permitir que los servidores web reciban tráfico SSH o RDP desde su red. Los servidores web pueden enviar tráfico SQL o MySQL a los servidores de bases de datos.

Origen	Protocolo	Rango de puerto	Descripción
ID del grupo de seguridad del equilibrador de carga	TCP	80	Permite el acceso HTTP de entrada desde el equilibrador de carga
ID del grupo de seguridad del equilibrador de carga	TCP	443	Permite el acceso HTTPS de entrada desde el equilibrador de carga
Rango de direcciones IPv4 públicas de su red	TCP	22	(Opcional) Permite el acceso SSH de entrada desde las direcciones IP IPv4 de su red

Origen	Protocolo	Rango de puerto	Descripción
Rango de direcciones IPv6 de su red	TCP	22	(Opcional) Permite el acceso SSH de entrada desde las direcciones IP IPv6 de su red
Rango de direcciones IPv4 públicas de su red	TCP	3389	(Opcional) Permite el acceso RDP de entrada desde las direcciones IP IPv4 de su red
Rango de direcciones IPv6 de su red	TCP	3389	(Opcional) Permite el acceso RDP de entrada desde las direcciones IP IPv6 de su red

Destino	Protocolo	Rango de puerto	Descripción
ID del grupo de seguridad para instancias que ejecuten Microsoft SQL Server	TCP	1433	Permite el acceso saliente de Microsoft SQL Server a los servidores de bases de datos
ID del grupo de seguridad para instancias que ejecuten MySQL	TCP	3306	Permite el acceso saliente de MySQL a los servidores de bases de datos

Servidores de bases de datos

Las siguientes reglas para el grupo de seguridad permiten a los servidores de bases de datos recibir solicitudes de lectura y escritura desde los servidores web.

Origen	Protocolo	Rango de puerto	Comentarios
ID del grupo de seguridad del servidor web	TCP	1433	Permite el acceso entrante de Microsoft SQL Server desde los servidores web
ID del grupo de seguridad del servidor web	TCP	3306	Permite el acceso entrante de MySQL Server desde los servidores web

Destino	Protocolo	Rango de puerto	Comentarios
0.0.0.0/0	TCP	80	Permite el acceso HTTP saliente a internet a través de IPv4
0.0.0.0/0	TCP	443	Permite el acceso HTTPS saliente a internet a través de IPv4

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.

1. Creación de la VPC

Utilice el siguiente procedimiento para crear una VPC con una subred pública y una subred privada en dos zonas de disponibilidad.

Para crear la VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel, elija Crear VPC.
3. En Recursos para crear, elija VPC y más.
4. Configurar la VPC:

a. Mantenga seleccionada la opción Generación automática de etiquetas de nombre para crear etiquetas de nombre para los recursos de la VPC, o desactívela para proporcionar sus propias etiquetas de nombre para los recursos de la VPC.

b. En Bloque de CIDR IPv4, puede conservar la sugerencia predeterminada o, como alternativa, ingresar el bloque de CIDR necesario para su aplicación o red. Para obtener más información, consulte the section called “Bloques de CIDR de VPC”.

c. (Opcional) Si su aplicación se comunica mediante direcciones IPv6, elija Bloque de CIDR IPv6, Bloque de CIDR IPv6 proporcionado por Amazon.

d. Elija una opción de tenencia. Esta opción define si las instancias de EC2 que lance en la VPC se ejecutarán en hardware compartido con otras Cuentas de AWS o en hardware dedicado para su uso exclusivo. Si elige que la tenencia de la VPC sea `Default`, las instancias de EC2 lanzadas en esta VPC utilizarán el atributo de tenencia especificado al lanzar la instancia. Para obtener más información, consulte Lanzar una instancia mediante parámetros definidos en la Guía del usuario de Linux de Amazon EC2. Si elige que la tenencia de la VPC sea `Dedicated`, las instancias siempre se ejecutarán como Instancias dedicadas en hardware dedicado para su uso.

5. Configurar las subredes:

a. En Número de zonas de disponibilidad, elija 2 para poder lanzar instancias en dos zonas de disponibilidad y mejorar la resiliencia.

b. Para Número de subredes públicas, elija 2.

c. Para Número de subredes privadas, elija 2.

d. Puede conservar los bloques de CIDR predeterminados para las subredes o, si lo prefiere, puede expandir Personalizar los bloques de CIDR de subredes e introducir un bloque de CIDR. Para obtener más información, consulte the section called “Bloques de CIDR de subred”.

6. En Puertas de enlace NAT, mantenga el valor predeterminado: Ninguno.

7. En Puntos de conexión de VPC, mantenga el valor predeterminado, Puerta de enlace de S3. Si bien no tiene ningún efecto, a menos que acceda a un bucket de S3, habilitar este punto de conexión de VPC no tiene ningún costo.

8. Mantenga ambas opciones seleccionadas en Opciones de DNS. Como resultado, los servidores web recibirán nombres de host DNS públicos que corresponden a sus direcciones IP públicas.

9. Seleccione Creación de VPC.

2. Implementar la aplicación

Lo ideal es que ya haya probado sus servidores web y servidores de bases de datos en un entorno de desarrollo o de prueba y haya creado los scripts o las imágenes que utilizará para implementar la aplicación en producción.

Puede utilizar instancias de EC2 para sus servidores web. Hay diversas formas para implementar instancias de EC2. Por ejemplo:

- Asistente de lanzamiento de instancias de Amazon EC
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Para mejorar la disponibilidad, puede utilizar Amazon EC2 Auto Scaling para implementar servidores en varias zonas de disponibilidad y mantener la capacidad mínima de servidor que requiere su aplicación.

Puede utilizar Elastic Load Balancing para distribuir el tráfico de manera uniforme entre los servidores. Puede asociar un equilibrador de carga a un grupo de escalado automático.

Puede usar instancias de EC2 para sus servidores de bases de datos o uno de nuestros tipos de bases de datos personalizadas. Para obtener más información, consulte Bases de datos en AWS: Cómo elegir.

3. Pruebe la configuración

Una vez que haya terminado de implementar la aplicación, puede probarla. Si la aplicación no puede enviar ni recibir el tráfico esperado, puede utilizar el Analizador de accesibilidad para solucionar problemas. Por ejemplo, el Analizador de accesibilidad puede identificar problemas de configuración en sus tablas de enrutamiento o grupos de seguridad. Para obtener más información, consulte la Guía del Analizador de accesibilidad.

4. Limpieza

Cuando complete esta configuración, puede eliminarla. Antes de poder eliminar la VPC, debe terminar las instancias y eliminar el equilibrador de carga. Para obtener más información, consulte the section called “Eliminar su VPC”.

Ejemplo: una VPC con servidores en subredes privadas y NAT

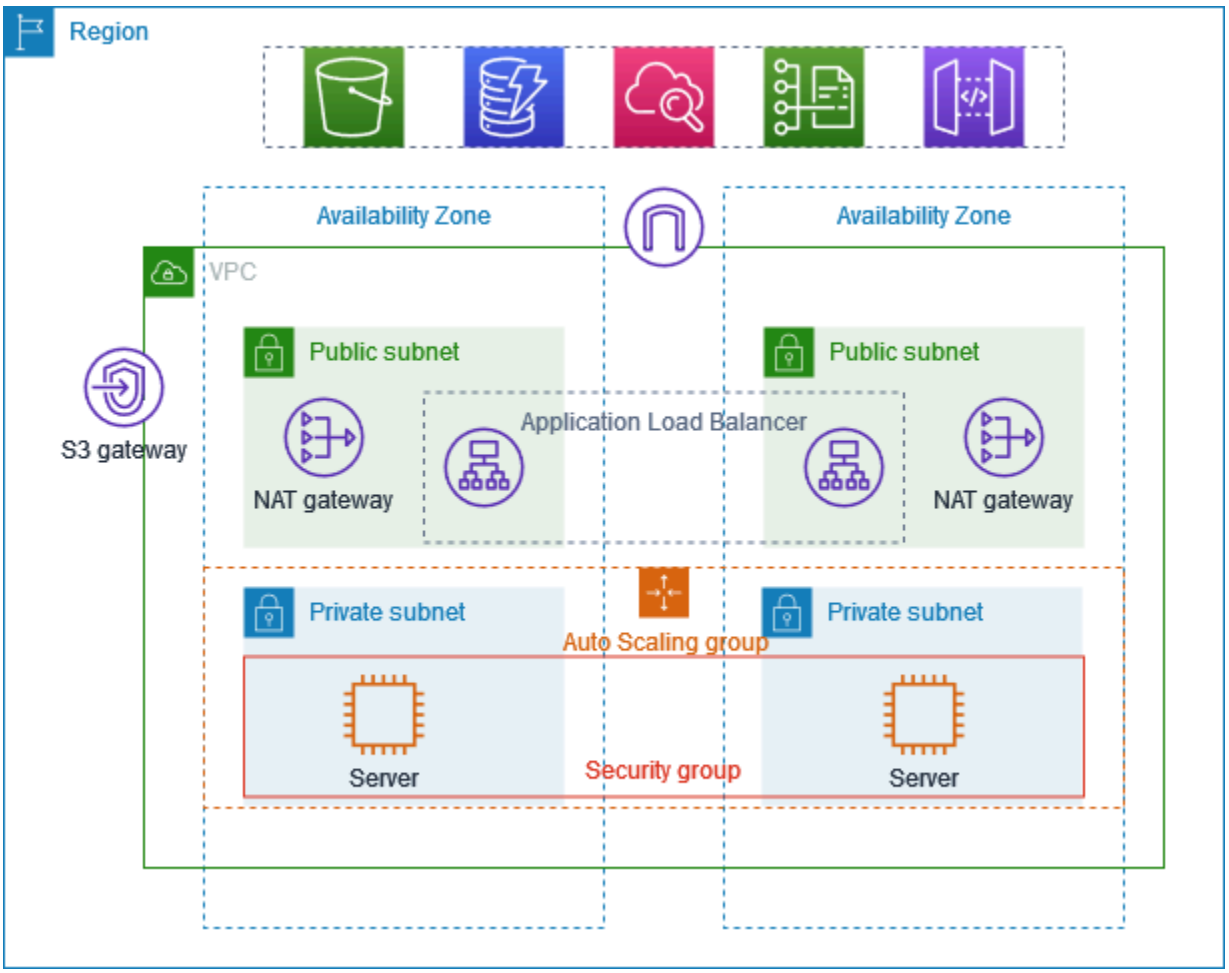
En este ejemplo se muestra cómo crear una VPC que se puede utilizar para los servidores de un entorno de producción. Para mejorar la resiliencia, los servidores se implementan dos zonas de disponibilidad, mediante un grupo de escalado automático y un equilibrador de carga de aplicación. Para obtener mayor seguridad, los servidores se implementan en subredes privadas. Los servidores reciben las solicitudes a través del equilibrador de carga. Los servidores pueden conectarse a Internet mediante una puerta de enlace NAT. Para mejorar la resiliencia, la puerta de enlace NAT se implementa en ambas zonas de disponibilidad.

Contenido

- Descripción general
- 1. Creación de la VPC
- 2. Implementar la aplicación
- 3. Pruebe la configuración
- 4. Limpieza

Descripción general

En el diagrama siguiente, se proporciona información general sobre los recursos que se incluyen en este ejemplo. La VPC tiene subredes privadas y públicas en dos zonas de disponibilidad. Cada subred pública contiene una puerta de enlace NAT y un nodo equilibrador de carga. Los servidores se ejecutan en las subredes privadas, se lanzan y terminan mediante un grupo de escalado automático y reciben tráfico desde el equilibrador de carga. Los servidores pueden conectarse a Internet mediante la puerta de enlace NAT. Los servidores pueden conectarse a Amazon S3 mediante un punto de conexión de VPC de puerta de enlace.



Enrutamiento

Cuando crea esta VPC con la consola de Amazon VPC, creamos una tabla de enrutamiento para las subredes públicas con rutas locales y rutas a la puerta de enlace de Internet. También creamos una tabla de enrutamiento para las subredes privadas con rutas locales y rutas a la puerta de enlace NAT, la puerta de enlace de Internet solo de salida y el punto de conexión de VPC de la puerta de enlace.

A continuación, se muestra un ejemplo de la tabla de enrutamiento para las subredes públicas, con rutas para IPv4 e IPv6. Si crea subredes solo para IPv4 en lugar de subredes de doble pila, la tabla de enrutamiento solo incluye las rutas IPv4.

Destino	Objetivo
10.0.0.0/16	local

Destino	Objetivo
2001:db8:1234:1a00::/56	local
0.0.0.0/0	*igw-id*
::/0	*igw-id*

El siguiente es un ejemplo de una tabla de enrutamiento para una de las subredes privadas, con rutas tanto para IPv4 como para IPv6. Si creó subredes solo para IPv4, la tabla de enrutamiento incluye solo las rutas IPv4. La última ruta envía el tráfico destinado a Amazon S3 al punto de conexión de VPC de la puerta de enlace.

Destino	Objetivo
10.0.0.0/16	local
2001:db8:1234:1a00::/56	local
0.0.0.0/0	*nat-gateway-id*
::/0	*eigw-id*
s3-prefix-list-id	*s3-gateway-id*

Seguridad

A continuación, se muestra un ejemplo de las reglas que puede crear para el grupo de seguridad que asocia a sus servidores. El grupo de seguridad debe permitir el tráfico procedente del equilibrador de carga a través del oyente y el protocolo. También debe permitir la comprobación de estado del tráfico.

Origen	Protocolo	Rango de puerto	Comentarios
ID del grupo de seguridad del equilibrador de carga	*protocolo del oyente*	*puerto del oyente*	Permite el tráfico entrante desde el equilibrador de carga en el puerto del oyente
ID del grupo de seguridad del equilibrador de carga	*protocolo de comprobación de estado*	*puerto de comprobación de estado*	Permite el tráfico de comprobación de estado entrante desde el equilibrador de carga

1. Creación de la VPC

Utilice el siguiente procedimiento para crear una VPC con una subred pública y una subred privada en dos zonas de disponibilidad y una puerta de enlace NAT en cada zona de disponibilidad.

Para crear la VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel, elija Crear VPC.
3. En Recursos para crear, elija VPC y más.
4. Configurar la VPC
    a. En Generación automática de etiquetas de nombre, ingrese un nombre para la VPC.
    b. En Bloque de CIDR IPv4, puede conservar la sugerencia predeterminada o, como alternativa, ingresar el bloque de CIDR necesario para su aplicación o red.
    c. Si la aplicación se comunica mediante direcciones IPv6, elija Bloque de CIDR IPv6, Bloque de CIDR IPv6 proporcionado por Amazon.
5. Configurar las subredes
    a. En Cantidad de zonas de disponibilidad, elija 2 para poder lanzar instancias en varias zonas de disponibilidad y mejorar la resiliencia.
    b. Para Número de subredes públicas, elija 2.

c. Para Número de subredes privadas, elija 2.

d. Puede conservar el bloque de CIDR predeterminado para la subred pública o, si lo prefiere, puede ampliar Personalizar los bloques de CIDR de la subred e introducir un bloque de CIDR. Para obtener más información, consulte the section called “Bloques de CIDR de subred”.

6. En Puertas de enlace NAT, elija 1 por AZ para mejorar la resiliencia.
7. Si la aplicación se comunica mediante direcciones IPv6, seleccione Sí en Puerta de enlace de Internet solo de salida.
8. En Puntos de conexión de VPC, si las instancias deben acceder a un bucket de S3, conserve la Puerta de enlace de S3 predeterminada. De lo contrario, las instancias de su subred privada no podrán acceder a Amazon S3. Esta opción no tiene ningún costo, por lo que puede conservar la opción predeterminada si quiere utilizar un bucket de S3 en el futuro. Si selecciona Ninguno, siempre podrá agregar un punto de conexión de VPC de puerta de enlace más adelante.
9. Para ver las Opciones de DNS, desactive Habilitar nombres de host de DNS.
10. Seleccione Creación de VPC.

2. Implementar la aplicación

Lo ideal es que termine de probar los servidores en un entorno de desarrollo o prueba y cree los scripts o las imágenes que utilizará para implementar la aplicación en producción.

Puede utilizar Amazon EC2 Auto Scaling para implementar servidores en varias zonas de disponibilidad y mantener la capacidad mínima de servidor requerida por su aplicación.

Para lanzar instancias mediante un grupo de escalado automático

1. Cree una plantilla de lanzamiento para especificar la información de configuración necesaria para lanzar sus instancias de EC2 mediante Amazon EC2 Auto Scaling. Para obtener un tutorial detallado, consulte Creación de una plantilla de lanzamiento para un grupo de escalado automático en la Guía del usuario de Amazon EC2 Auto Scaling.
2. Cree un grupo de escalado automático, que es una colección de instancias de EC2 con un tamaño mínimo, máximo y deseado. Para obtener un tutorial detallado, consulte Crear un grupo de escalado automático mediante una plantilla de lanzamiento en la Guía del usuario de Amazon EC2 Auto Scaling.
3. Cree un equilibrador de carga que distribuya el tráfico de manera uniforme entre las instancias del grupo de escalado automático y asocie el equilibrador de carga al grupo de escalado

automático. Para obtener más información, consulte la Guía del usuario de Elastic Load Balancing y Uso de Elastic Load Balancing en la Guía del usuario de Amazon EC2 Auto Scaling.

3. Pruebe la configuración

Una vez que haya terminado de implementar la aplicación, puede probarla. Si la aplicación no puede enviar ni recibir el tráfico esperado, puede utilizar el Analizador de accesibilidad para solucionar problemas. Por ejemplo, el Analizador de accesibilidad puede identificar problemas de configuración en sus tablas de enrutamiento o grupos de seguridad. Para obtener más información, consulte la Guía del Analizador de accesibilidad.

4. Limpieza

Cuando complete esta configuración, puede eliminarla. Antes de poder eliminar la VPC, debe eliminar el grupo de escalado automático, terminar las instancias, eliminar las puertas de enlace NAT y eliminar el equilibrador de carga. Para obtener más información, consulte the section called “Eliminar su VPC”.

Tutoriales de VPC

La nube privada virtual (VPC) de Amazon es la base de su infraestructura de red en AWS. Si bien la consola de administración de AWS proporciona una interfaz fácil de usar, la interfaz de la línea de comandos (CLI) de AWS ofrece mayor flexibilidad y capacidades de automatización para crear y administrar los recursos de su VPC.

Esta guía presenta dos escenarios de implementación de la VPC esenciales:

- Una configuración de la VPC básica con una subred pública, ideal para aplicaciones web sencillas.
- Una configuración de la VPC avanzada con subredes públicas y privadas mediante puertas de enlace NAT, adecuada para aplicaciones de varios niveles.

Al seguir estos tutoriales, aprenderá lo siguiente:

- Crear VPC con diferentes configuraciones de subred.
- Configurar puertas de enlace de Internet y NAT.
- Configurar tablas de enrutamiento y grupos de seguridad.
- Usar comandos de la AWS CLI para administrar la infraestructura de su red.
- Implementar prácticas recomendadas para las redes de AWS.

Comencemos a crear la infraestructura de su red de AWS utilizando la línea de comandos.

Tutoriales

- Introducción a Amazon VPC mediante la CLI de AWS
- Creación de una VPC con subredes privadas y puertas de enlace NAT mediante la AWS CLI

Introducción a Amazon VPC mediante la CLI de AWS

En este tutorial, se explica cómo crear una nube privada virtual (VPC) mediante la interfaz de la línea de comandos (AWS CLI) de AWS. Aprenderá a configurar una VPC con subredes públicas y privadas, configurar la conectividad a Internet e implementar instancias de EC2 para demostrar una arquitectura de aplicaciones web común.

Requisitos previos

Antes de comenzar este tutorial, asegúrese de tener lo siguiente:

1. la , AWS CLI. Si necesita instalarla, siga la guía de instalación de la AWS CLI.
2. La AWS CLI debe estar configurada con las credenciales apropiadas. Si aún no ha configurado sus credenciales, ejecute `aws configure`.
3. Comprensión básica de los conceptos sobre redes.
4. Identity and Access Management para Amazon VPC para crear y administrar los recursos de VPC en su cuenta de AWS.

Consideraciones sobre costos

En este tutorial, se crean recursos de AWS que pueden suponer costos en su cuenta. El costo principal proviene de la puerta de enlace de NAT (0,045 USD por hora más gastos de procesamiento de datos) y de las instancias de EC2 (t2.micro, aproximadamente 0,0116 USD por hora cada una). Si completa este tutorial en una hora y, a continuación, limpia todos los recursos, el costo total será de aproximadamente 0,07 USD. Para optimizar los costos en los entornos de desarrollo, considere la posibilidad de utilizar una instancia de NAT en lugar de una puerta de enlace de NAT, lo que puede reducir los costos de forma significativa.

Comprobemos que su AWS CLI está correctamente configurada antes de continuar.

```
aws configure list
```

Debería ver su clave de acceso, su clave secreta y la región predeterminada de AWS. Además, compruebe que tiene los permisos necesarios para crear recursos de VPC.

```
aws sts get-caller-identity
```

Este comando muestra su ID de cuenta, su ID de usuario y su ARN de AWS, lo que confirma que sus credenciales son válidas.

Creación de una VPC

Una nube privada virtual (VPC) es una red virtual dedicada para su cuenta de AWS. En esta sección, creará una VPC con un bloque CIDR de 10.0.0.0/16, que proporciona hasta 65 536 direcciones IP.

Creación de la VPC

El siguiente comando crea una nueva VPC y le asigna una etiqueta de nombre.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications
 'ResourceType=vpc,Tags=[{Key=Name,Value=MyVPC}]'
```

En la salida, tome nota del ID de la VPC. Lo necesitará para comandos posteriores. Para el propósito de este tutorial, utilizaremos “vpc-0123456789abcdef0” como un ejemplo de ID de la VPC. Reemplácelo con su ID de la VPC real en todos los comandos.

Habilitación de la compatibilidad y los nombres de host de DNS

De forma predeterminada, la resolución de DNS y los nombres de host de DNS están deshabilitados en una VPC nueva. Active estas características para permitir que las instancias de su VPC resuelvan los nombres de dominio.

```
aws ec2 modify-vpc-attribute --vpc-id vpc-0123456789abcdef0 --enable-dns-support
aws ec2 modify-vpc-attribute --vpc-id vpc-0123456789abcdef0 --enable-dns-hostnames
```

Estos comandos no producen ninguna salida si se ejecutan correctamente. Su VPC ahora tiene habilitada la resolución de compatibilidad y nombres de host de DNS.

Creación de subredes

Las subredes son segmentos del rango de direcciones IP de una VPC en los que puede colocar grupos de recursos aislados. En esta sección, creará subredes públicas y privadas en dos zonas de disponibilidad para obtener alta disponibilidad.

Obtención de las zonas de disponibilidad disponibles

En primer lugar, recupere las zonas de disponibilidad disponibles en su región.

```
aws ec2 describe-availability-zones
```

Para este tutorial, utilizaremos las dos primeras zonas de disponibilidad. Cuando vea la salida, anote sus nombres (por ejemplo, “us-east-1a” y “us-east-1b”).

Creación de dos subredes públicas

Las subredes públicas se utilizan para los recursos que deben ser accesibles desde Internet, como los servidores web.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.0.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Public-Subnet-AZ1}]'
```

Cuando vea la salida, anote el ID de la subred. En este tutorial, usaremos “subnet-0123456789abcdef0” como ejemplo de la primera subred pública.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.1.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Public-Subnet-AZ2}]'
```

Cuando vea la salida, anote el ID de la subred. En este tutorial, usaremos “subnet-0123456789abcdef1” como ejemplo de la segunda subred pública.

Crear subredes privadas

Las subredes privadas se utilizan para recursos que no deben ser accesibles directamente desde Internet, como las bases de datos.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.2.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Private-Subnet-AZ1}]'
```

Cuando vea la salida, anote el ID de la subred. En este tutorial, usaremos “subnet-0123456789abcdef2” como ejemplo de la primera subred privada.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.3.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Private-Subnet-AZ2}]'
```

Cuando vea la salida, anote el ID de la subred. En este tutorial, usaremos “subnet-0123456789abcdef3” como ejemplo de la segunda subred privada.

Ahora tiene cuatro subredes: dos públicas y dos privadas, distribuidas en dos zonas de disponibilidad.

Consejo: Cuando planifique sus bloques de CIDR, asegúrese de que no se superpongan con las redes existentes. Para los entornos de producción, asigne suficientes direcciones IP para el crecimiento futuro y, al mismo tiempo, mantenga las subredes de un tamaño razonable para la seguridad y la administración.

Configuración de la conectividad a Internet

Para permitir que los recursos de su VPC se comuniquen con Internet, debe crear y conectar una puerta de enlace de Internet. En esta sección, configurará la conectividad a Internet para su VPC.

Crear una gateway de Internet

Una puerta de enlace de Internet permite la comunicación entre su VPC e Internet.

```
aws ec2 create-internet-gateway \
  --tag-specifications 'ResourceType=internet-gateway,Tags=[{Key=Name,Value=MyIGW}]'
```

Cuando vea la salida, anote el ID de la puerta de enlace de Internet. Para este tutorial, usaremos “igw-0123456789abcdef0” como ejemplo.

Conexión de una puerta de enlace de Internet a su VPC

Después de crear la puerta de enlace de Internet, adjúntela a su VPC.

```
aws ec2 attach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0
```

Creación y configuración de tablas de enrutamiento

Las tablas de enrutamiento contienen reglas (rutas) que determinan la dirección del tráfico de la red. En primer lugar, cree una tabla de enrutamiento para las subredes públicas.

```
aws ec2 create-route-table \
  --vpc-id vpc-0123456789abcdef0 \
```

```
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Public-RT}]'
```

Cuando vea la salida, anote el ID de la tabla de enrutamiento. En este tutorial, usaremos "rtb-0123456789abcdef0" como ejemplo de la tabla de enrutamiento pública.

Añada una ruta a la puerta de enlace de Internet en la tabla de enrutamiento pública.

```
aws ec2 create-route --route-table-id rtb-0123456789abcdef0 --destination-cidr-block
 0.0.0.0/0 --gateway-id igw-0123456789abcdef0
```

Asocie las subredes públicas con la tabla de enrutamiento pública.

```
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef0 --subnet-id
 subnet-0123456789abcdef0
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef0 --subnet-id
 subnet-0123456789abcdef1
```

Ahora, cree una tabla de enrutamiento para sus subredes privadas.

```
aws ec2 create-route-table \
  --vpc-id vpc-0123456789abcdef0 \
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Private-RT}]'
```

Cuando vea la salida, anote el ID de la tabla de enrutamiento. En este tutorial, usaremos "rtb-0123456789abcdef1" como ejemplo de la tabla de enrutamiento privada.

Asocie las subredes privadas con la tabla de enrutamiento privada.

```
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef1 --subnet-id
 subnet-0123456789abcdef2
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef1 --subnet-id
 subnet-0123456789abcdef3
```

Creación de una puerta de enlace NAT

Una puerta de enlace de NAT permite que las instancias en subredes privadas inicien el tráfico saliente a Internet a la vez que evita el tráfico entrante desde Internet. Esto es esencial para las instancias que necesitan descargar actualizaciones o acceder a servicios externos.

Asignación de una IP elástica

En primer lugar, asigne una dirección IP elástica a su puerta de enlace NAT.

```
aws ec2 allocate-address --domain vpc
```

Cuando vea la salida, anote el ID de la asignación. Para este tutorial, usaremos “eipalloc-0123456789abcdef0” como ejemplo.

Creación de la puerta de enlace NAT

Cree una puerta de enlace de NAT en una de sus subredes públicas utilizando la IP elástica asignada.

```
aws ec2 create-nat-gateway \
  --subnet-id subnet-0123456789abcdef0 \
  --allocation-id eipalloc-0123456789abcdef0 \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=MyNATGateway}]'
```

Cuando vea la salida, anote el ID de la puerta de enlace NAT. Para este tutorial, usaremos “nat-0123456789abcdef0” como ejemplo.

Espere a que la puerta de enlace de NAT esté disponible antes de continuar.

```
aws ec2 wait nat-gateway-available --nat-gateway-ids nat-0123456789abcdef0
```

Adición de una ruta a la puerta de enlace de NAT

Agregue una ruta a la puerta de enlace de NAT en la tabla de enrutamiento privada para permitir que las instancias de las subredes privadas accedan a Internet.

```
aws ec2 create-route --route-table-id rtb-0123456789abcdef1 --destination-cidr-block
 0.0.0.0/0 --nat-gateway-id nat-0123456789abcdef0
```

Nota: Para los entornos de producción, considere la posibilidad de crear una puerta de enlace de NAT en cada zona de disponibilidad en la que tenga subredes privadas para eliminar los puntos únicos de error.

Configuración de los ajustes de la subred

Configure las subredes públicas para asignar de forma automática direcciones IP públicas a instancias iniciadas en ellas.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-0123456789abcdef0 --map-public-ip-
on-launch
aws ec2 modify-subnet-attribute --subnet-id subnet-0123456789abcdef1 --map-public-ip-
on-launch
```

Esto garantiza que las instancias lanzadas en las subredes públicas reciban una dirección IP pública de forma predeterminada, lo que permite acceder a ellas desde Internet.

Creación de grupos de seguridad

Los grupos de seguridad funcionan como firewalls virtuales para que las instancias controlen el tráfico entrante y saliente. En esta sección, creará grupos de seguridad para servidores web y servidores de bases de datos.

Creación de un grupo de seguridad para los servidores web

```
aws ec2 create-security-group \
  --group-name WebServerSG \
  --description "Security group for web servers" \
  --vpc-id vpc-0123456789abcdef0
```

Cuando vea la salida, anote el ID del grupo de seguridad. En este tutorial, usaremos “sg-0123456789abcdef0” como ejemplo del grupo de seguridad del servidor web.

Permita que el tráfico HTTP y HTTPS llegue a sus servidores web.

```
aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef0 --protocol tcp
 --port 80 --cidr 0.0.0.0/0
aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef0 --protocol tcp
 --port 443 --cidr 0.0.0.0/0
```

Nota: Para los entornos de producción, restrinja el tráfico entrante a rangos de IP específicos en lugar de permitir el tráfico desde 0.0.0.0/0 (cualquier dirección IP).

Creación de un grupo de seguridad para los servidores de base de datos

```
aws ec2 create-security-group \
  --group-name DBServerSG \
  --description "Security group for database servers" \
```

```
  --vpc-id vpc-0123456789abcdef0
```

Cuando vea la salida, anote el ID del grupo de seguridad. En este tutorial, usaremos “sg-0123456789abcdef1” como ejemplo del grupo de seguridad del servidor de la base de datos.

Permita el tráfico de MySQL/Aurora únicamente desde servidores web.

```
aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef1 --protocol tcp
 --port 3306 --source-group sg-0123456789abcdef0
```

Esta configuración garantiza que solo las instancias del grupo de seguridad del servidor web puedan conectarse a los servidores de bases de datos en el puerto 3306, siguiendo el principio de privilegio mínimo.

Verificación de la configuración VPC

Tras crear todos los componentes necesarios, compruebe la configuración de la VPC para asegurarse de que todo está correcto.

Compruebe su VPC

```
aws ec2 describe-vpcs --vpc-id vpc-0123456789abcdef0
```

Compruebe sus subredes

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Compruebe sus tablas de enrutamiento

```
aws ec2 describe-route-tables --filters "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Compruebe su puerta de enlace de Internet

```
aws ec2 describe-internet-gateways --filters "Name=attachment.vpc-
id,Values=vpc-0123456789abcdef0"
```

Compruebe su puerta de enlace de NAT

```
aws ec2 describe-nat-gateways --filter "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Compruebe sus grupos de seguridad

```
aws ec2 describe-security-groups --filters "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Estos comandos proporcionan información detallada sobre cada componente de su VPC, lo que le permite verificar que todo está configurado correctamente.

Implementación de las instancias de EC2

Ahora que ha creado la infraestructura de su VPC, puede implementar instancias de EC2 para demostrar cómo funciona. Lanzará un servidor web en una subred pública y un servidor de bases de datos en una subred privada.

Creación de un par de claves para el acceso SSH

En primer lugar, cree un par de claves para conectarse de forma segura a las instancias:

```
aws ec2 create-key-pair --key-name vpc-tutorial-key --query 'KeyMaterial' --output text
 > vpc-tutorial-key.pem
chmod 400 vpc-tutorial-key.pem
```

Este comando crea un nuevo par de claves y guarda la clave privada en un archivo con permisos restringidos.

Hallazgo de la AMI de Amazon Linux 2 más reciente

Busque la AMI de Amazon Linux 2 más reciente para utilizarla en las instancias:

```
aws ec2 describe-images --owners amazon \
  --filters "Name=name,Values=amzn2-ami-hvm-*-x86_64-gp2" "Name=state,Values=available"
 \
  --query "sort_by(Images, &CreationDate)[-1].ImageId" --output text
```

Cuando vea la salida, anote el ID de la AMI. Para este tutorial, usaremos “ami-0123456789abcdef0” como ejemplo.

Lanzamiento de un servidor web en la subred pública

Ahora, inicie una instancia de EC2 en la subred pública para que sirva como servidor web.

```
aws ec2 run-instances \
  --image-id ami-0123456789abcdef0 \
  --count 1 \
  --instance-type t2.micro \
  --key-name vpc-tutorial-key \
  --security-group-ids sg-0123456789abcdef0 \
  --subnet-id subnet-0123456789abcdef0 \
  --associate-public-ip-address \
  --user-data '#!/bin/bash
               yum update -y
               yum install -y httpd
               systemctl start httpd
               systemctl enable httpd
               echo "<h1>Hello from $(hostname -f)</h1>" > /var/www/html/index.html' \
  --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=WebServer}]'
```

Cuando vea la salida, anote el ID de la instancia. En este tutorial, usaremos “i-0123456789abcdef0” como ejemplo de la instancia del servidor web.

Lanzamiento de un servidor de base de datos en la subred privada

A continuación, inicie una instancia de EC2 en la subred privada para que sirva como servidor de base de datos:

```
aws ec2 run-instances \
  --image-id ami-0123456789abcdef0 \
  --count 1 \
  --instance-type t2.micro \
  --key-name vpc-tutorial-key \
  --security-group-ids sg-0123456789abcdef1 \
  --subnet-id subnet-0123456789abcdef2 \
  --user-data '#!/bin/bash
               yum update -y
               yum install -y mariadb-server
               systemctl start mariadb
               systemctl enable mariadb' \
  --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=DBServer}]'
```

Cuando vea la salida, anote el ID de la instancia. En este tutorial, usaremos “i-0123456789abcdef1” como ejemplo de la instancia de la base de datos.

Acceso a su servidor web

Una vez que la instancia de su servidor web esté en ejecución, podrá acceder a ella mediante su dirección IP pública:

```
aws ec2 describe-instances \
  --instance-ids i-0123456789abcdef0 \
  --query 'Reservations[0].Instances[0].PublicIpAddress' \
  --output text
```

Este comando generará la dirección IP pública de su servidor web. Para este tutorial, usaremos “203.0.113.10” como ejemplo.

Ahora puede abrir esta URL en su navegador web: http://203.0.113.10

Conéctese a las instancias mediante SSH.

Para conectarse a su servidor web:

```
ssh -i vpc-tutorial-key.pem ec2-user@203.0.113.10
```

Para conectarse a su servidor de base de datos, primero debe usar SSH con su servidor web y, después, con su servidor de base de datos:

```
# Get the private IP of the database server
aws ec2 describe-instances \
  --instance-ids i-0123456789abcdef1 \
  --query 'Reservations[0].Instances[0].PrivateIpAddress' \
  --output text
```

Este comando generará la dirección IP privada de su servidor de bases de datos. Para este tutorial, usaremos “10.0.2.10” como ejemplo.

```
# First SSH to web server, then to database server
ssh -i vpc-tutorial-key.pem -A ec2-user@203.0.113.10
ssh ec2-user@10.0.2.10
```

Esto demuestra la arquitectura de red que ha creado: el servidor web es de acceso público, mientras que el servidor de base de datos solo es accesible desde la VPC.

Solución de problemas

A continuación, se indican algunos problemas comunes que puede encontrar al crear una VPC y se explica cómo resolverlos:

Superposiciones de bloques de CIDR

Si recibe un error sobre superposiciones de bloques de CIDR, asegúrese de que los bloques de CIDR de su VPC y sus subredes no se superpongan con las VPC o subredes existentes en su cuenta.

Errores de permisos

Si encuentra errores de permisos, verifique que su usuario o rol de IAM tenga los permisos necesarios para crear y administrar recursos de la VPC. Es posible que necesite adjuntar la política `AmazonVPCFullAccess` o crear una política personalizada con los permisos necesarios.

Límites de recursos

Las cuentas de AWS tienen límites predeterminados en cuanto al número de VPC, subredes y otros recursos que se pueden crear. Si alcanza estos límites, puede solicitar un aumento a través del Centro de soporte de AWS.

Fallos de dependencia durante la limpieza

Al limpiar los recursos, es posible que encuentre errores de dependencia si intenta eliminar los recursos en un orden incorrecto. Elimine siempre los recursos en el orden inverso al de su creación, comenzando por los recursos más dependientes.

Eliminar recursos

Cuando haya terminado con su VPC, puede limpiar los recursos para evitar incurrir en costos adicionales. Elimine los recursos en el orden inverso de su creación para gestionar las dependencias correctamente.

Termine las instancias de EC2

```
aws ec2 terminate-instances --instance-ids i-0123456789abcdef0 i-0123456789abcdef1
aws ec2 wait instance-terminated --instance-ids i-0123456789abcdef0 i-0123456789abcdef1
```

Elimine el par de claves

```
aws ec2 delete-key-pair --key-name vpc-tutorial-key
rm vpc-tutorial-key.pem
```

Elimine la puerta de enlace NAT

```
aws ec2 delete-nat-gateway --nat-gateway-id nat-0123456789abcdef0
aws ec2 wait nat-gateway-deleted --nat-gateway-ids nat-0123456789abcdef0
```

Liberación de la IP elástica

```
aws ec2 release-address --allocation-id eipalloc-0123456789abcdef0
```

Elimine los grupos de seguridad

```
aws ec2 delete-security-group --group-id sg-0123456789abcdef1
aws ec2 delete-security-group --group-id sg-0123456789abcdef0
```

Elimine las tablas de enrutamiento

Primero, busque los ID de asociación de la tabla de enrutamiento:

```
aws ec2 describe-route-tables --route-table-id rtb-0123456789abcdef0
aws ec2 describe-route-tables --route-table-id rtb-0123456789abcdef1
```

A continuación, desasocie las tablas de enrutamiento de las subredes (sustituya los ID de asociación por los de su salida):

```
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef0
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef1
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef2
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef3
```

A continuación, elimine las tablas de enrutamiento:

```
aws ec2 delete-route-table --route-table-id rtb-0123456789abcdef1
aws ec2 delete-route-table --route-table-id rtb-0123456789abcdef0
```

Separe y elimine la puerta de enlace de Internet

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
 vpc-0123456789abcdef0
aws ec2 delete-internet-gateway --internet-gateway-id igw-0123456789abcdef0
```

Elimine las subredes

```
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef0
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef1
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef2
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef3
```

Elimine la VPC

```
aws ec2 delete-vpc --vpc-id vpc-0123456789abcdef0
```

Paso a la producción

Este tutorial se ha diseñado para ayudarlo a aprender a crear una VPC mediante la AWS CLI. Para los entornos de producción, tenga en cuenta las siguientes prácticas recomendadas de seguridad y arquitectura:

1. Reglas de grupo de seguridad: restrinja el tráfico entrante a rangos de IP específicos en lugar de permitir el tráfico desde 0.0.0.0/0.
2. Alta disponibilidad: implemente puertas de enlace de NAT en cada zona de disponibilidad donde tenga subredes privadas para eliminar los puntos únicos de error.
3. ACL de red: implemente las ACL de red como una capa adicional de seguridad más allá de los grupos de seguridad.
4. Registros de flujo de la VPC: habilite los registros de flujo de la VPC para monitorear y analizar los patrones de tráfico de la red.
5. Etiquetado de recursos: implemente una estrategia de etiquetado integral para una mejor gestión de los recursos.

Para obtener más información sobre cómo crear arquitecturas listas para producción, consulte Marco de AWS Well-Architected y AWS Security Best Practices.

Siguientes pasos

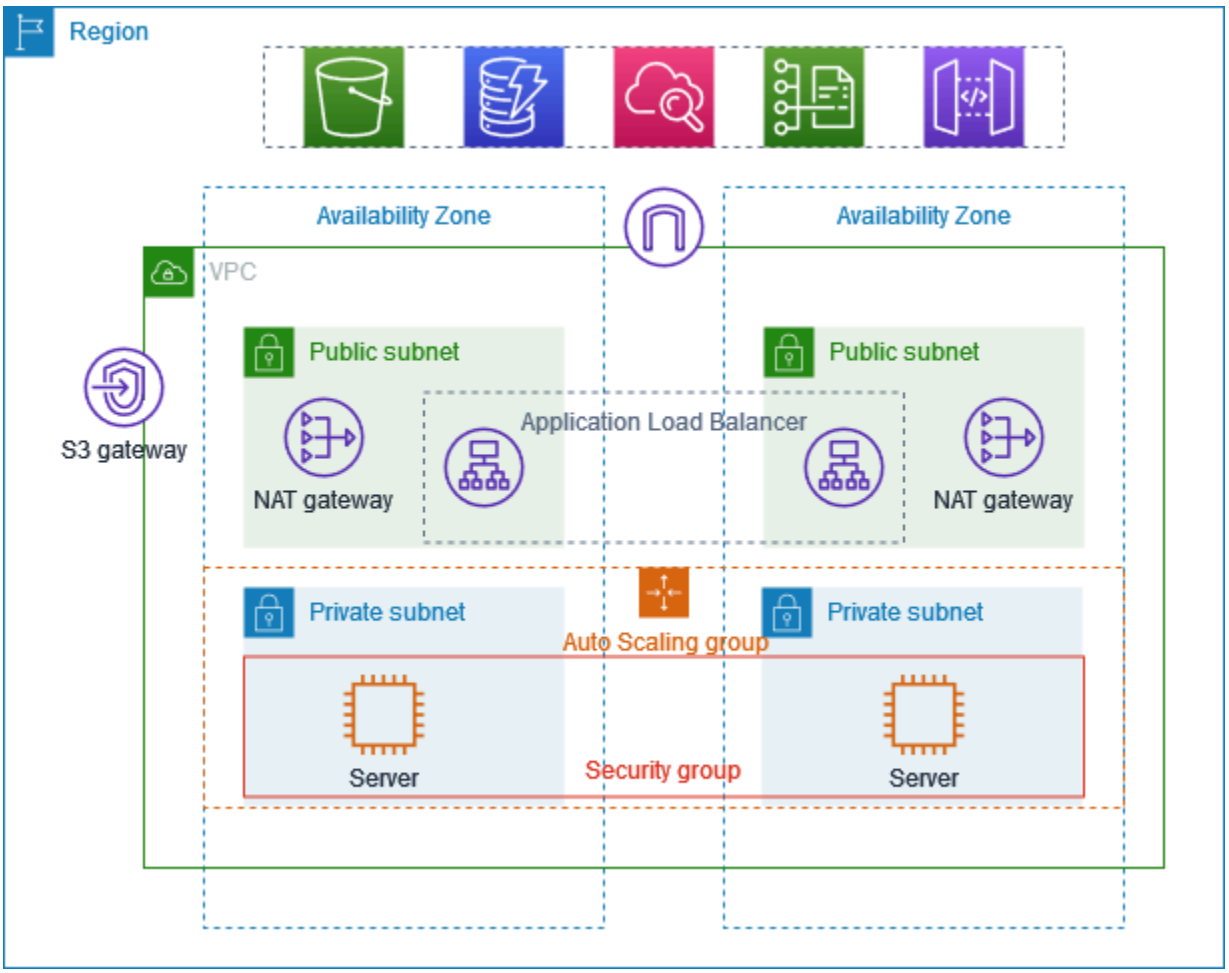
Ahora que ha creado una VPC con subredes públicas y privadas, puede hacer lo siguiente:

1. Lanzar instancias de EC2 en sus subredes públicas o privadas.
2. Implementar equilibradores de carga para distribuir el tráfico entre múltiples instancias.
3. Configurar grupos de escalado automático para obtener alta disponibilidad y escalabilidad.
4. Configurar las bases de datos de RDS en sus subredes privadas.
5. Implementar el emparejamiento de la VPC para conectarse con otras VPC.
6. Configurar las conexiones de VPN para conectar la VPC con la red en las instalaciones.

Creación de una VPC con subredes privadas y puertas de enlace NAT mediante la AWS CLI

En este tutorial, se muestra cómo crear una VPC que se puede utilizar para los servidores de un entorno de producción mediante la AWS CLI. Para mejorar la resiliencia, implementará servidores en dos zonas de disponibilidad, mediante un grupo de escalado automático y un equilibrador de carga de aplicación. Para obtener mayor seguridad, implementará los servidores en subredes privadas. Los servidores recibirán las solicitudes a través del equilibrador de carga y podrán conectarse a Internet mediante puertas de enlace NAT. Para mejorar la resiliencia, implementará una puerta de enlace NAT en cada zona de disponibilidad.

En el diagrama siguiente, se proporciona información general sobre los recursos que se incluyen en este tutorial. La VPC tiene subredes privadas y públicas en dos zonas de disponibilidad. Cada subred pública contiene una puerta de enlace NAT y un nodo equilibrador de carga. Los servidores se ejecutan en las subredes privadas, se lanzan y terminan mediante un grupo de escalado automático y reciben tráfico desde el equilibrador de carga. Los servidores pueden conectarse a Internet mediante la puerta de enlace NAT. Los servidores pueden conectarse a Amazon S3 mediante un punto de conexión de VPC de puerta de enlace.



Requisitos previos

Antes de comenzar este tutorial, necesita lo siguiente:

- La AWS CLI debe estar instalada y configurada con permisos para crear recursos de VPC, instancias de EC2, equilibradores de carga y grupos de escalado automático. Para obtener información sobre cómo instalar AWS CLI, consulte Instalar o actualizar la versión más reciente de AWS CLI.
- Conocimientos básicos de los conceptos sobre las VPC, incluidas subredes, tablas de enrutamiento y puertas de enlace de Internet.
- Debe estar instalado el procesador de línea de comandos JSON `jq`. Se utiliza para analizar el resultado de los comandos de la AWS CLI. Para obtener información sobre la instalación de jq, consulte Download jq (Descarga de jq).
- Contar con cuotas de servicio suficientes para los recursos que creará, que incluyen lo siguiente:
- Al menos 2 direcciones IP elásticas disponibles

- Al menos 2 puertas de enlace NAT
- Al menos 1 VPC
- Al menos 4 subredes
- Al menos 1 equilibrador de carga de aplicación

Costo estimado: los recursos creados en este tutorial incurrirán en cargos en su cuenta de AWS: Puertas de enlace NAT: ~0,045 USD por hora, más cargos por procesamiento de datos Direcciones IP elásticas: gratuitas cuando se asocian a instancias en ejecución, ~0,005 USD por hora cuando no están asociadas Instancias de EC2: varía según el tipo de instancia (en este tutorial, se utiliza t3.micro) Equilibrador de carga de aplicación: ~0,0225 USD por hora, más cargos por procesamiento de datos

Creación de las VPC y las subredes

En primer lugar, creará una VPC con un bloque CIDR de 10.0.0.0/16, que proporciona hasta 65 536 direcciones IP privadas.

```
# Create a VPC with CIDR block 10.0.0.0/16
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications
 'ResourceType=vpc,Tags=[{Key=Name,Value=ProductionVPC}]'
```

El comando devuelve un resultado similar al siguiente:

```
{
    "Vpc": {
        "CidrBlock": "10.0.0.0/16",
        "DhcpOptionsId": "dopt-abcd1234",
        "State": "pending",
        "VpcId": "vpc-abcd1234",
        "OwnerId": "123456789012",
        "InstanceTenancy": "default",
        "Ipv6CidrBlockAssociationSet": [],
        "CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-abcd1234",
                "CidrBlock": "10.0.0.0/16",
                "CidrBlockState": {
                    "State": "associated"
                }
```

```
            }
        ],
        "IsDefault": false,
        "Tags": [
            {
                "Key": "Name",
                "Value": "ProductionVPC"
            }
        ]
    }
}
```

Cuando vea la salida, anote el ID de la VPC (por ejemplo, `vpc-abcd1234`). Utilizará este ID en comandos posteriores.

A continuación, identificará dos zonas de disponibilidad en su región para crear una arquitectura resiliente.

```
# Get available Availability Zones
aws ec2 describe-availability-zones --query 'AvailabilityZones[0:2].ZoneName' --output
 text
```

El comando devuelve un resultado similar al siguiente:

```
us-east-1a us-east-1b
```

Ahora, cree cuatro subredes: dos públicas para el equilibrador de carga y las puertas de enlace NAT, y dos privadas para los servidores de su aplicación. Reemplace `vpc-abcd1234` con su ID de la VPC real, y `us-east-1a` y `us-east-1b` con sus zonas de disponibilidad reales.

```
# Create public subnet in first AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.0.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PublicSubnet1}]'

# Create private subnet in first AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.1.0/24 \
```

```
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PrivateSubnet1}]'

# Create public subnet in second AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.2.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PublicSubnet2}]'

# Create private subnet in second AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.3.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PrivateSubnet2}]'
```

Cada comando devuelve un resultado que contiene el ID de la subred. Anote estos ID para usarlos en comandos posteriores:

- Subred pública 1: `subnet-abcd1234`
- Subred privada 1: `subnet-abcd5678`
- Subred pública 2: `subnet-efgh1234`
- Subred privada 2: `subnet-efgh5678`

Creación y configuración de la conectividad a Internet

En esta sección, creará una puerta de enlace de Internet para permitir la comunicación entre la VPC e Internet, y la adjuntará a la VPC.

```
# Create an Internet Gateway
aws ec2 create-internet-gateway --tag-specifications 'ResourceType=internet-
gateway,Tags=[{Key=Name,Value=ProductionIGW}]'
```

El comando devuelve una salida que contiene el ID de la puerta de enlace de Internet. Anote este ID (por ejemplo, `igw-abcd1234`).

Adjunte la puerta de enlace de Internet a su VPC. Reemplace `igw-abcd1234` con su ID de la puerta de enlace de Internet real y `vpc-abcd1234` con su ID de la VPC real.

```
# Attach the Internet Gateway to the VPC
aws ec2 attach-internet-gateway --internet-gateway-id igw-abcd1234 --vpc-id vpc-
abcd1234
```

Luego, cree tablas de enrutamiento para sus subredes públicas y privadas. Reemplace `vpc-abcd1234` por su ID de la VPC real.

```
# Create a route table for public subnets
aws ec2 create-route-table --vpc-id vpc-abcd1234 --tag-specifications
 'ResourceType=route-table,Tags=[{Key=Name,Value=PublicRouteTable}]'

# Create route table for private subnet in first AZ
aws ec2 create-route-table --vpc-id vpc-abcd1234 --tag-specifications
 'ResourceType=route-table,Tags=[{Key=Name,Value=PrivateRouteTable1}]'

# Create route table for private subnet in second AZ
aws ec2 create-route-table --vpc-id vpc-abcd1234 --tag-specifications
 'ResourceType=route-table,Tags=[{Key=Name,Value=PrivateRouteTable2}]'
```

Cada comando devuelve una salida que contiene el ID de la tabla de enrutamiento. Anote estos ID:

- Tabla de enrutamiento pública: `rtb-abcd1234`
- Tabla de enrutamiento privada 1: `rtb-efgh1234`
- Tabla de enrutamiento privada 2: `rtb-ijkl1234`

Agregue una ruta a la puerta de enlace de Internet en la tabla de enrutamiento pública para habilitar el acceso a Internet. Reemplace `rtb-abcd1234` con su ID de la tabla de enrutamiento pública real y `igw-abcd1234` con su ID de la puerta de enlace de Internet real.

```
# Add a route to the Internet Gateway
aws ec2 create-route --route-table-id rtb-abcd1234 --destination-cidr-block 0.0.0.0/0
 --gateway-id igw-abcd1234
```

Asocie las subredes con sus tablas de enrutamiento respectivas. Reemplace los ID de la tabla de enrutamiento y los ID de la subred con sus ID reales.

```
# Associate public subnets with the public route table
aws ec2 associate-route-table --route-table-id rtb-abcd1234 --subnet-id subnet-abcd1234
aws ec2 associate-route-table --route-table-id rtb-abcd1234 --subnet-id subnet-efgh1234
```

```
# Associate private subnets with their respective route tables
aws ec2 associate-route-table --route-table-id rtb-efgh1234 --subnet-id subnet-abcd5678
aws ec2 associate-route-table --route-table-id rtb-ijkl1234 --subnet-id subnet-efgh5678
```

Creación de puertas de enlace NAT

La puerta de enlace NAT permite que las instancias de las subredes privadas se conecten a Internet o a otros servicios de AWS, pero impede que Internet inicie conexiones con dichas instancias. En primer lugar, asigne direcciones IP elásticas a las puertas de enlace NAT.

```
# Allocate Elastic IP for NAT Gateway in first AZ
aws ec2 allocate-address --domain vpc --tag-specifications 'ResourceType=elastic-
ip,Tags=[{Key=Name,Value=NAT1-EIP}]'

# Allocate Elastic IP for NAT Gateway in second AZ
aws ec2 allocate-address --domain vpc --tag-specifications 'ResourceType=elastic-
ip,Tags=[{Key=Name,Value=NAT2-EIP}]'
```

Cada comando devuelve una salida que contiene el ID de la asignación. Anote estos ID:

- ID de la asignación de EIP 1: `eipalloc-abcd1234`
- ID de la asignación de EIP 2: `eipalloc-efgh1234`

Cree puertas de enlace NAT en cada subred pública. Reemplace los ID de la subred y los ID de la asignación con sus ID reales.

```
# Create NAT Gateway in public subnet of first AZ
aws ec2 create-nat-gateway \
  --subnet-id subnet-abcd1234 \
  --allocation-id eipalloc-abcd1234 \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=NAT-Gateway1}]'

# Create NAT Gateway in public subnet of second AZ
aws ec2 create-nat-gateway \
  --subnet-id subnet-efgh1234 \
  --allocation-id eipalloc-efgh1234 \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=NAT-Gateway2}]'
```

Cada comando devuelve una salida que contiene el ID de la puerta de enlace NAT. Anote estos ID:

- Puerta de enlace NAT 1: `nat-abcd1234`
- Puerta de enlace NAT 2: `nat-efgh1234`

Las puertas de enlace NAT tardan unos minutos en aprovisionarse. Espere a que estén disponibles antes de continuar. Reemplace los ID de la puerta de enlace NAT con sus ID reales.

```
# Wait for NAT Gateways to be available
aws ec2 wait nat-gateway-available --nat-gateway-ids nat-abcd1234
aws ec2 wait nat-gateway-available --nat-gateway-ids nat-efgh1234
```

Agregue rutas a las puertas de enlace NAT en las tablas de enrutamiento privadas para permitir el acceso a Internet a las instancias en subredes privadas. Reemplace los ID de la tabla de enrutamiento y los ID de la puerta de enlace NAT con sus ID reales.

```
# Add route to NAT Gateway 1 in private route table 1
aws ec2 create-route \
  --route-table-id rtb-efgh1234 \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id nat-abcd1234

# Add route to NAT Gateway 2 in private route table 2
aws ec2 create-route \
  --route-table-id rtb-ijkl1234 \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id nat-efgh1234
```

Creación de un punto de conexión de VPC para Amazon S3

Un punto de conexión de VPC para Amazon S3 permite que las instancias en sus subredes privadas accedan a S3 sin pasar por la puerta de enlace NAT, lo que reduce los costos de transferencia de datos y proporciona un mejor rendimiento de la red. Reemplace `vpc-abcd1234` con su ID de la VPC real y los ID de la tabla de enrutamiento con sus ID reales.

```
# Get the prefix list ID for S3 in your region
S3_PREFIX_LIST_ID=$(aws ec2 describe-prefix-lists --filters "Name=prefix-
list-name,Values=com.amazonaws.$(aws configure get region).s3" --query
 'PrefixLists[0].PrefixListId' --output text)

# Create the VPC endpoint for S3
aws ec2 create-vpc-endpoint \
```

```
  --vpc-id vpc-abcd1234 \
  --service-name com.amazonaws.$(aws configure get region).s3 \
  --route-table-ids rtb-efgh1234 rtb-ijkl1234 \
  --tag-specifications 'ResourceType=vpc-endpoint,Tags=[{Key=Name,Value=S3-Endpoint}]'
```

El comando devuelve una salida que contiene el ID del punto de conexión de VPC. Anote este ID (por ejemplo, `vpce-abcd1234`).

Configuración de grupos de seguridad

Los grupos de seguridad funcionan como firewalls virtuales para que las instancias controlen el tráfico entrante y saliente. Cree un grupo de seguridad para el equilibrador de carga que permita el tráfico HTTP entrante desde cualquier lugar. Reemplace `vpc-abcd1234` por su ID de la VPC real.

```
# Create security group for the load balancer
aws ec2 create-security-group \
  --group-name LoadBalancerSG \
  --description "Security group for the load balancer" \
  --vpc-id vpc-abcd1234 \
  --tag-specifications 'ResourceType=security-
group,Tags=[{Key=Name,Value=LoadBalancerSG}]'
```

El comando devuelve una salida que contiene el ID del grupo de seguridad. Anote este ID (por ejemplo, `sg-abcd1234`).

Permita que el tráfico entrante HTTP llegue al equilibrador de carga. Reemplace `sg-abcd1234` con el ID real del grupo de seguridad del equilibrador de carga.

```
# Allow inbound HTTP traffic from anywhere
aws ec2 authorize-security-group-ingress \
  --group-id sg-abcd1234 \
  --protocol tcp \
  --port 80 \
  --cidr 0.0.0.0/0
```

Cree un grupo de seguridad para los servidores de la aplicación que permita que solo entre tráfico desde el equilibrador de carga. Reemplace `vpc-abcd1234` por su ID de la VPC real.

```
# Create security group for the application servers
aws ec2 create-security-group \
```

```
  --group-name AppServerSG \
  --description "Security group for the application servers" \
  --vpc-id vpc-abcd1234 \
  --tag-specifications 'ResourceType=security-
group,Tags=[{Key=Name,Value=AppServerSG}]'
```

El comando devuelve una salida que contiene el ID del grupo de seguridad. Anote este ID (por ejemplo, `sg-efgh1234`).

Permita que el tráfico HTTP entrante llegue del grupo de seguridad del equilibrador de carga a los servidores de la aplicación. Reemplace `sg-efgh1234` con el ID real del grupo de seguridad del servidor de la aplicación y `sg-abcd1234` con el ID real del grupo de seguridad del equilibrador de carga.

```
# Allow inbound HTTP traffic from the load balancer security group
aws ec2 authorize-security-group-ingress \
  --group-id sg-efgh1234 \
  --protocol tcp \
  --port 80 \
  --source-group sg-abcd1234
```

Creación de una plantilla de lanzamiento para instancias de EC2

Una plantilla de lanzamiento contiene la información de configuración para iniciar una instancia, como el ID de la AMI, el tipo de instancia y los grupos de seguridad. En primer lugar, cree un script de datos de usuario que se ejecutará cuando se lance la instancia.

```
cat > user-data.sh << 'EOF'
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
echo "<h1>Hello from $(hostname -f) in $(curl -s http://169.254.169.254/latest/meta-
data/placement/availability-zone)</h1>" > /var/www/html/index.html
EOF
```

Codifique el script de datos de usuario en base64.

```
USER_DATA=$(base64 -w 0 user-data.sh)
```

Obtenga el ID de la AMI de Amazon Linux 2 más reciente.

```
# Get the latest Amazon Linux 2 AMI ID
aws ec2 describe-images --owners amazon --filters "Name=name,Values=amzn2-ami-hvm-
*-x86_64-gp2" "Name=state,Values=available" --query 'sort_by(Images, &CreationDate)
[-1].ImageId' --output text
```

Cree una plantilla de lanzamiento con el ID de la AMI, el tipo de instancia, el grupo de seguridad y los datos de usuario. Reemplace `sg-efgh1234` con su ID real del grupo de seguridad del servidor de la aplicación, y `$AMI_ID` y `$USER_DATA` con los valores obtenidos de los comandos anteriores.

```
# Create a launch template
aws ec2 create-launch-template \
  --launch-template-name AppServerTemplate \
  --version-description "Initial version" \
  --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=Name,Value=AppServerTemplate}]' \
  --launch-template-data '{
    "NetworkInterfaces": [{
      "DeviceIndex": 0,
      "Groups": ["sg-efgh1234"],
      "DeleteOnTermination": true
    }],
    "ImageId": "ami-abcd1234",
    "InstanceType": "t3.micro",
    "UserData":
 "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAteQp5dW0gaW5zdGFsbCAteSBodHRwZApzeXN0ZW1jdGwgc3RhcnQgaHR0cGQKc
+SGVsbG8gZnJvbSAkKGhvc3RuYW1lIC1mKSBpbiAkKGN1cmwgLXMgaHR0cDovLzE2OS4yNTQuMTY5LjI1NC9sYXRlc3QvbW
    "TagSpecifications": [{
      "ResourceType": "instance",
      "Tags": [{
        "Key": "Name",
        "Value": "AppServer"
      }]
    }]
  }'
```

Creación de un equilibrador de carga y un grupo de destino

Un grupo de destino direcciona las solicitudes a destinos registrados, como instancias de EC2, mediante el protocolo y el puerto especificado. Cree un grupo de destino para los servidores de su aplicación. Reemplace `vpc-abcd1234` por su ID de la VPC real.

```
# Create a target group
aws elbv2 create-target-group \
  --name AppTargetGroup \
  --protocol HTTP \
  --port 80 \
  --vpc-id vpc-abcd1234 \
  --target-type instance \
  --health-check-protocol HTTP \
  --health-check-path / \
  --health-check-port traffic-port
```

El comando devuelve una salida que contiene el ARN del grupo de destino. Anote este ARN (por ejemplo, `arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/AppTargetGroup/abcd1234`).

Cree un equilibrador de carga de aplicación en las subredes públicas. Reemplace los ID de la subred y del grupo de seguridad por sus valores reales.

```
# Create a load balancer
aws elbv2 create-load-balancer \
  --name AppLoadBalancer \
  --subnets subnet-abcd1234 subnet-efgh1234 \
  --security-groups sg-abcd1234 \
  --tags Key=Name,Value=AppLoadBalancer
```

El comando devuelve una salida que contiene el ARN del equilibrador de carga. Anote este ARN (por ejemplo, `arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234`).

Espere a que el equilibrador de carga esté activo antes de continuar. Reemplace `arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234` por el ARN de su equilibrador de carga real.

```
# Wait for load balancer to be active
aws elbv2 wait load-balancer-available \
  --load-balancer-arns arn:aws:elasticloadbalancing:us-
east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234
```

Cree un oyente para el equilibrador de carga que reenvíe el tráfico HTTP al grupo de destino. Reemplace el ARN del equilibrador de carga y el ARN del grupo de destino por sus ARN reales.

```
# Create a listener
aws elbv2 create-listener \
  --load-balancer-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/
app/AppLoadBalancer/abcd1234 \
  --protocol HTTP \
  --port 80 \
  --default-actions Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:us-
east-1:123456789012:targetgroup/AppTargetGroup/abcd1234
```

Creación de un grupo de escalado automático

Un Auto Scaling group (grupo de escalado automático) contiene una colección de instancias de Amazon EC2 que se tratan como una agrupación lógica a efectos de escalado automático y administración. Cree un grupo de escalado automático que utilice la plantilla de lanzamiento y coloque las instancias en las subredes privadas. Reemplace los ID de la subred y el ARN del grupo de destino con sus ID y ARN reales.

```
# Create an Auto Scaling group
aws autoscaling create-auto-scaling-group \
  --auto-scaling-group-name AppAutoScalingGroup \
  --launch-template LaunchTemplateName=AppServerTemplate,Version='$Latest' \
  --min-size 2 \
  --max-size 4 \
  --desired-capacity 2 \
  --vpc-zone-identifier "subnet-abcd5678,subnet-efgh5678" \
  --target-group-arns arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/
AppTargetGroup/abcd1234 \
  --health-check-type ELB \
  --health-check-grace-period 300 \
  --tags Key=Name,Value=AppServer,PropagateAtLaunch=true
```

Pruebe la configuración

Una vez que el grupo de escalado automático lance las instancias y estas pasen las comprobaciones de estado, puede probar su equilibrador de carga. Obtenga el nombre del DNS del equilibrador de carga. Reemplace el ARN del equilibrador de carga por su ARN real.

```
# Get the DNS name of the load balancer
aws elbv2 describe-load-balancers \
  --load-balancer-arns arn:aws:elasticloadbalancing:us-
east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234 \
```

```
  --query "LoadBalancers[0].DNSName" \
  --output text
```

Use curl para probar la aplicación con el nombre del equilibrador de carga.

```
curl http://LoadBalancerName
```

Si actualiza la página varias veces, debería ver las respuestas de distintas instancias en diferentes zonas de disponibilidad.

Eliminar recursos

Cuando haya terminado con este tutorial, elimine todos los recursos para evitar de incurrir en costos adicionales. Reemplace todos los ID con los ID de sus recursos reales.

```
# Delete the Auto Scaling group
aws autoscaling delete-auto-scaling-group \
  --auto-scaling-group-name AppAutoScalingGroup \
  --force-delete

# Wait for the Auto Scaling group to be deleted
sleep 60

# Delete the load balancer
aws elbv2 delete-load-balancer \
  --load-balancer-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/
app/AppLoadBalancer/abcd1234

# Wait for the load balancer to be deleted
sleep 30

# Delete the target group
aws elbv2 delete-target-group \
  --target-group-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/
AppTargetGroup/abcd1234

# Delete the launch template
aws ec2 delete-launch-template \
  --launch-template-name AppServerTemplate

# Delete the NAT Gateways
aws ec2 delete-nat-gateway --nat-gateway-id nat-abcd1234
```

```
aws ec2 delete-nat-gateway --nat-gateway-id nat-efgh1234

# Wait for the NAT Gateways to be deleted
sleep 90

# Release the Elastic IPs
aws ec2 release-address --allocation-id eipalloc-abcd1234
aws ec2 release-address --allocation-id eipalloc-efgh1234

# Delete the VPC endpoint
aws ec2 delete-vpc-endpoints --vpc-endpoint-ids vpce-abcd1234

# Wait for security group dependencies to clear
sleep 30

# Delete the security groups
aws ec2 delete-security-group --group-id sg-efgh1234
aws ec2 delete-security-group --group-id sg-abcd1234

# Detach the Internet Gateway
aws ec2 detach-internet-gateway --internet-gateway-id igw-abcd1234 --vpc-id vpc-
abcd1234

# Delete the Internet Gateway
aws ec2 delete-internet-gateway --internet-gateway-id igw-abcd1234

# Delete the route tables
aws ec2 delete-route-table --route-table-id rtb-efgh1234
aws ec2 delete-route-table --route-table-id rtb-ijkl1234
aws ec2 delete-route-table --route-table-id rtb-abcd1234

# Delete the subnets
aws ec2 delete-subnet --subnet-id subnet-abcd1234
aws ec2 delete-subnet --subnet-id subnet-efgh1234
aws ec2 delete-subnet --subnet-id subnet-abcd5678
aws ec2 delete-subnet --subnet-id subnet-efgh5678

# Delete the VPC
aws ec2 delete-vpc --vpc-id vpc-abcd1234
```

Pasos a seguir a continuación

Ahora que ha creado una VPC con subredes privadas y puertas de enlace NAT, es posible que desee explorar estos temas relacionados:

- Prácticas recomendadas de seguridad de la VPC
- Registro del tráfico de IP con registros de flujo de la VPC
- Políticas de escalado por grupo de escalado automático
- Comprobaciones de estado para los grupos de destino del equilibrador de carga

Cuotas de Amazon VPC

En las tablas siguientes, se muestran las cuotas, antes llamadas límites, para los recursos de Amazon VPC para su cuenta de AWS. A menos que se indique lo contrario, estas cuotas son por región.

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	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	5	Sí (hasta 50)	La cantidad de CIDR que puede asignar a una única VPC.
Exclusiones de bloqueo de acceso público de la VPC por cuenta y por región	50	Sí. Para solicitar un aumento, consulte Solicitud	El número de exclusiones de BPA de la VPC que puede crear en una cuenta.

Nombre	Predeterminado	Ajustable	Comentarios
		de aumento de cuota en la Guía del usuario de AWS.	

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

Nombre	Predeterminado	Ajustable	Comentarios
Direcciones IP elásticas por región	5	Sí	Esta cuota aplica a las VPC de la Cuenta de AWS individuales y a las VPC compartidas.
Direcciones IP elásticas por puerta de enlace de NAT pública	2	Sí	Puede solicitar un aumento de cuota de hasta 8.

Puertas de enlace

Nombre	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, solo se tienen en cuenta las puertas de enlace de NAT en los estados `pending`, `active` y `deleting`.
Cuota de direcciones IP privadas por puerta de enlace NAT	8	Sí	
Gateways de operador por VPC	1	No	

Listas de prefijos administradas por el cliente

Si bien las cuotas predeterminadas para las listas de prefijos administradas por los clientes se pueden ajustar, no se puede solicitar un aumento mediante la consola de Service Quotas. Debe abrir un caso de soporte. Consulte Solicitud de aumento de cuota en la Guía del usuario de AWS.

Nombre	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	Puede cambiar el tamaño de una lista de prefijos administrada por el cliente hasta 1000. Para obtener más información, consulte Cambiar una 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.
Referencias a una lista de prefijos por tipo de recurso	10 000	Sí	Esta cuota se aplica por el tipo de recurso que puede hacer referencia a una lista de prefijos. Por ejemplo, puede tener 10 000 referencias a una lista de prefijos en todos los grupos de seguridad más 10 000 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,

Nombre	Predeterminado	Ajustable	Comentarios
			las referencias de las otras cuentas a su lista de prefijos cuentan para su cuota.

ACL de red

Nombre	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	Esta cuota determina tanto el número máximo de reglas entrantes como el número máximo de reglas salientes. Esta cuota se puede aumentar hasta un máximo de 40 reglas entrantes y 40 reglas salientes (para un total de 80 reglas), pero el rendimiento de la red podría verse afectado.

Interfaces de red

Nombre	Predeterminado	Ajustable	Comentarios
Interfaces de red por instancia	Varía según el tipo de instancias	No	Para obtener más información, consulte Interfaces de red por tipo de instancias.

Nombre	Predeterminado	Ajustable	Comentarios
Interfaces de red por región	5 000	Sí	Esta cuota aplica a las VPC de la Cuenta de AWS individuales y a las VPC compartidas. Este límite se aplica según la zona de disponibilidad (AZ). Si, por ejemplo, las interfaces de red están en tres zonas de disponibilidad, cada una de estas tendrá un límite de 5000 y la región tendrá un límite de 15 000.

Tablas de enrutamiento

Nombre	Predeterminado	Ajustable	Comentarios
Tablas de rutas por VPC	200	Sí	La tabla de ruteo principal cuenta para esta cuota. Tenga en cuenta que si solicita un aumento de cuota para las tablas de enrutamiento, es posible que también desee solicitar un aumento de cuota para las subredes. Puede asociar varias subredes a una misma tabla de enrutamiento, pero una subred únicamente puede asociarse a una tabla de enrutamiento a la vez.
Rutas por tabla de rutas (rutas no propagadas)	500	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

Nombre	Predeterminado	Ajustable	Comentarios
			recomendamos que pagine las llamadas para describir las tablas de ruteo.
Rutas propagadas por tabla de enrutamiento	100	No	Si necesita más prefijos, anuncie una ruta predeterminada.

Servidores de enrutamiento

Nombre	Predeterminado	Ajustable	Comentarios
Servidores de enrutamiento por VPC	5	Sí. Para solicitar un aumento, consulte Solicitud de aumento de cuota en la Guía del usuario de AWS.	
punto de conexión del servidor de enrutamiento por servidor de enrutamiento	10	Sí. Para solicitar un aumento, consulte Solicitud de aumento	

Nombre	Predeterminado	Ajustable	Comentarios
		de cuota en la Guía del usuario de AWS.	
Sesiones de emparejamiento por interfaz de red	20	Sí. Para solicitar un aumento, consulte Solicitud de aumento de cuota en la Guía del usuario de AWS.	
Punto de conexión del servidor de enrutamiento por servidor de enrutamiento y subred	2	No	Por motivos de redundancia, solo puede tener dos puntos de conexión en la misma subred para el mismo servidor de enrutamiento.
Rutas por servidor de enrutamiento por par	100	No	Es el número de rutas que se pueden anunciar dinámicamente en un servidor de enrutamiento del mismo nivel
Rutas por servidor de enrutamiento	100	No	Es el número de rutas que se pueden instalar en la Base de información de reenvío (FIB) de un servidor de rutas.

Grupos de seguridad

Nombre	Predeterminado	Ajustable	Comentarios
Grupos de seguridad de VPC por región	2.500	Sí	Esta cuota aplica a las VPC de la Cuenta 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 pagine las llamadas para describir los grupos de seguridad.
Reglas entrantes o salientes por grupo de seguridad	60	Sí	Esta cuota se aplica de forma independiente para las reglas de entrada y salida. En el caso de una cuenta con una cuota predeterminada de 60 reglas, un grupo de seguridad puede tener 60 reglas de entrada y 60 reglas de salida. Además, esta cuota se aplica de forma independiente para las reglas IPv4 e IPv6. En el caso de una cuenta con una cuota predeterminada de 60 reglas, un grupo de seguridad puede tener 60 reglas de entrada para el tráfico IPv4 y 60 reglas de entrada para el tráfico IPv6. Para obtener más información, consulte the section called “Tamaño del grupo de seguridad”. 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.

Nombre	Predeterminado	Ajustable	Comentarios
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. Para reducir la cuota de grupos de seguridad por interfaz de red por debajo del valor predeterminado de 5, consulte Solicitar un aumento de cuota en la Guía del usuario de AWS. Para solicitar una reducción, se utiliza el mismo proceso que para solicitar un aumento.

Uso compartido de subredes de VPC

Todas las cuotas de VPC estándar se aplican a subredes de VPC compartidas.

Nombre	Predeterminado	Ajustable	Comentarios
Cuentas de participante por VPC	100	Sí	El número máximo 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. Los propietarios de la VPC pueden ver las interfaces de red y los grupos de seguridad asociados a los recursos de los participantes.
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.

Uso de direcciones de red

El uso de direcciones de red (NAU) se compone de direcciones IP, interfaces de red y CIDR en listas de prefijos administradas. El NAU es una métrica que se aplica a los recursos de una VPC para ayudarlo a planificar y supervisar el tamaño de su VPC. Para obtener más información, consulte Uso de direcciones de red.

Los recursos que componen el recuento de NAU tienen sus propias Service Quotas individuales. Incluso si una VPC tiene capacidad de NAU disponible, no podrá lanzar recursos a la VPC si los recursos han superado sus Service Quotas.

Nombre	Predeterminado	Ajustable	Comentarios
Uso de direcciones de red	64 000	Sí (hasta 256 000)	El número máximo de unidades de NAU por VPC.
Uso de direcciones de red interconectadas	128 000	Sí (hasta 512 000)	El número máximo de unidades de NAU para una VPC y todas sus VPC interconectadas dentro de la región. Las VPC que se conectan en diferentes regiones no contribuyen a este número.

Limitación controlada de API de Amazon EC2

Para obtener más información sobre las limitaciones de Amazon EC2, consulte Limitación controlada de solicitudes en la Guía para desarrolladores de Amazon EC2.

Recursos de cuotas adicionales

Para obtener más información, consulte los siguientes temas:

- Cuotas de AWS Client VPN en la Guía del administrador de AWS Client VPN
- Cuotas de Direct Connect en la Guía del usuario de AWS Direct Connect
- Cuotas de interconexión en la Guía de interconexión de Amazon VPC
- Cuotas de PrivateLink en la Guía de AWS PrivateLink

- Cuotas de Site-to-Site VPN en laGuía del usuario de AWS Site-to-Site VPN
- Cuotas de creación de reflejo de tráfico en la Guía de creación de reflejo de tráfico de Amazon VPC
- Cuotas de las puertas de enlace de tránsito en la Guía de puertas de enlace de tránsito de Amazon VPC

Historial de revisión

En la siguiente tabla se describen los cambios importantes de cada versión de la Amazon VPC User Guide (Guía del usuario de Amazon RDS).

Cambio	Descripción	Fecha
Controles de cifrado de VPC	Ahora puede aplicar el cifrado en tránsito al tráfico de red dentro de la VPC mediante los controles de cifrado de VPC. Esta característica proporcio na capacidades centraliz adas para aplicar y supervisar políticas de cifrado.	21 de noviembre de 2025
Puertas de enlace NAT regionales para la expansión automática en varias zonas de disponibilidad	Ahora puede usar puertas de enlace NAT regionales que se amplían automáticamente entre zonas de disponibilidad en función de la preencia de la carga de trabajo. Las puertas de enlace NAT regionales proporcionan una configura ción simplificada, mayor seguridad y alta disponibilidad automática sin intervención manual.	19 de noviembre de 2025
Enrute el tráfico de VPC entrante a direcciones IP públicas	Ahora es posible configura r las reglas de enrutamie nto avanzadas para dirigir el tráfico entrante de Internet a direcciones IP públicas específicas dentro de la VPC. Esto permite un control del flujo de tráfico y de las	13 de agosto de 2025

	decisiones de enrutamie nto para los escenarios de ingreso.	
Enrutamiento dinámico en su VPC mediante VPC Route Server de Amazon	VPC Route Server de Amazon simplifica el enrutamiento del tráfico entre las cargas de trabajo que se implement an dentro de una VPC y sus puertas de enlace de Internet. Con esta característica, VPC Route Server actualiza dinámicamente las tablas de enrutamiento de VPC y puerta de enlace con sus rutas IPv4 o IPv6 preferida s para lograr la tolerancia a errores de enrutamiento para esas cargas de trabajo. Esto permite redirigir automátic amente el tráfico dentro de una VPC, lo que aumenta la capacidad de administración del enrutamiento de la VPC y la interoperabilidad con cargas de trabajo de terceros.	31 de marzo de 2025
AWS Actualización de política administrada por	Amazon VPC actualizó las políticas administradas de AmazonVPCFullAccess y AmazonVPCReadOnlyAccess.	9 de diciembre de 2024

Soporte de política declarativa para el BPA de la VPC	Si utiliza AWS Organizations para administrar las cuentas en su organización, puede usar una política declarativa para aplicar el BPA de la VPC en las cuentas de la organización.	1 de diciembre de 2024
Bloqueo de acceso público (BPA) en la VPC)	El bloqueo de acceso público (BPA) en la VPC le permite bloquear los recursos de las VPC y subredes de su propiedad en una región para que no lleguen o sean accesibles desde la Internet a través de puertas de enlace de Internet y puertas de enlace de Internet de solo salida.	19 de noviembre de 2024
Grupos de seguridad compartidos	Esta característica le permite compartir un grupo de seguridad con otras cuentas de AWS Organizations.	30 de octubre de 2024
Asociaciones de grupos de seguridad y VPC	Esta característica le permite asociar un grupo de seguridad a varias VPC de la misma región.	30 de octubre de 2024
Compatibilidad de MTU con la puerta de enlace NAT	Las puertas de enlace NAT admiten tráfico con una unidad de transmisión máxima (MTU) de 8500.	10 de septiembre de 2024

Dirección IPv6 privada	Se agregó información sobre el direccionamiento IPv6 privado. Las direcciones IPv6 privadas solo están disponibles en el Administrador de direcciones IP de Amazon VPC.	8 de agosto de 2024
Tiempo de arrendamiento preferido de IPv6	Ahora puede elegir la frecuencia con la que se renueva la concesión de DHCPv6 a una instancia en ejecución con un IPv6 asignado.	20 de febrero de 2024
Revisión y mejoras en la estructura de la guía	Se revisó la estructura de la guía y se introdujeron reformas para mejorar la experiencia del cliente en relación con la búsqueda de información en situaciones específicas.	20 de febrero de 2024
AWS Actualización de política administrada por	Amazon VPC actualizó las políticas administradas de AmazonVPCFullAccess y AmazonVPCReadOnlyAccess.	8 de febrero de 2024
AWS Actualización de política administrada por	Amazon VPC actualizó la política administrada de AmazonVPCCrossAccountNetworkInterfaceOperations.	25 de septiembre de 2023

EC2-Classic quedó obsoleto	Con EC2-Classic, las instancias de EC2 se ejecutan en una sola red plana que se comparte con otros clientes. Amazon VPC sustituye a EC2-Classic. Con Amazon VPC, las instancias se ejecutan en una nube privada virtual (VPC) que está aislada lógicamente para su Cuenta de AWS.	31 de julio de 2023
Agregación de direcciones IPv4 secundarias a las puertas de enlace de NAT	Puede agregar direcciones IPv4 privadas secundarias a puertas de enlace de NAT públicas y privadas. Las direcciones IPv4 secundarias aumentan la cantidad de puertos disponibles y, por lo tanto, aumentan el límite de conexiones simultáneas que las cargas de trabajo pueden establecer mediante una puerta de enlace NAT.	31 de enero de 2023
Implementación de las prácticas recomendadas de IAM	Guía actualizada para implementar las prácticas recomendadas de IAM. Para obtener más información, consulte Prácticas recomendadas de seguridad en IAM.	4 de enero de 2023

Seleccionar la dirección IP privada de la puerta de enlace NAT	Al crear una puerta de enlace NAT, ahora puede elegir la dirección IP privada que se asigna a la puerta de enlace NAT. Anteriormente, se asignaba de forma automátic a una dirección IP privada del intervalo de direcciones IP de la subred.	17 de noviembre de 2022
Configuración IPv6 del enrutador de puerta de enlace predeterminado	Ahora hay tres direcciones IPv6 reservadas para uso del enrutador de VPC predeterm inado.	11 de noviembre de 2022
Transferir direcciones IP elásticas	Ahora puede transferir direcciones IP elásticas de una cuenta de AWS a otra.	31 de octubre de 2022
Métricas de uso de direccion es de red	Puede habilitar las métricas de uso de direcciones de red para su VPC para ayudarlo a planificar y supervisar el tamaño de la VPC.	4 de octubre de 2022
Publicar registros de flujo a Amazon Data Firehose	Puede especificar un flujo de entrega de Amazon Data Firehose como el destino de los datos del registro de flujo.	8 de septiembre de 2022

Ancho de banda de puerta de enlace NAT	Las puertas de enlace NAT ahora admiten un ancho de banda de hasta 100 Gbps (un aumento de 45 Gbps) y pueden procesar hasta 10 millones de paquetes por segundo (en comparación con los cuatro millones de paquetes anteriores).	15 de junio de 2022
Múltiples bloques de CIDR IPv6	Puede asociar hasta cinco bloques de CIDR IPv6 a una VPC.	12 de mayo de 2022
Reorganización	Reorganización general de esta Guía del usuario de Amazon Virtual Private Cloud.	2 de enero de 2022
Gateway NAT de IPv6 a IPv4	La puerta de enlace 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	Puede especificar el formato de archivo de registro de Apache Parquet, las particion es 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	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 establece r 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	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
Puertas de enlace NAT privadas	Puede utilizar una puerta de enlace 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

Etiqueta al crear	Puede agregar etiquetas al crear una VPC, opciones DHCP, puerta de enlace de Internet, puerta de enlace 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 de 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 puerta de enlace NAT	Puede agregar una etiqueta al crear una puerta de enlace 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 consola de Amazon VPC.	22 de enero de 2020

Tablas de ruteo de puerta de enlace	Puede asociar una tabla de enrutamiento a una puerta de enlace 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
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
Crear subred predeterminada	Si una zona de disponibi lidad no tienen una subred predeterminada, puede crearla.	9 de noviembre de 2017
Compatibilidad de etiquetad o para las puerta de enlaces NAT	Puede etiquetar su puerta de enlace NAT.	7 de septiembre de 2017
Métricas de Amazon CloudWatch para puerta de enlaces NAT	Puede consultar métricas de CloudWatch para la puerta de enlace 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 IPv6	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 1918	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
Puertas de enlace NAT	Puede crear una puerta de enlace 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	Con ClassicLink, puede vincular una instancia de EC2-Classic a una VPC de su cuenta. Puede asociar los grupos de seguridad de VPC a la instancia de EC2-Classic, lo que hace posible la comunicación entre la instancia de EC2-Classic y las instancias de la VPC utilizando 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
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	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	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