



training and  
certification

AWS Academy Cloud Foundations (ES)  
Module 05 Student Guide  
Versión 2.0.1

100-ACCLFO-20-ES-SG

© 2020 Amazon Web Services, Inc. o sus empresas afiliadas.  
Todos los derechos reservados.

Este contenido no puede reproducirse ni redistribuirse, total ni parcialmente,  
sin el permiso previo por escrito de Amazon Web Services, Inc. Queda prohibida  
la copia, el préstamo o la venta de carácter comercial.

Envíenos sus correcciones o comentarios relacionados con el curso a:  
[aws-course-feedback@amazon.com](mailto:aws-course-feedback@amazon.com).

Si tiene cualquier otra duda, contácte con nosotros en:  
<https://aws.amazon.com/contact-us/aws-training/>.

Todas las marcas comerciales pertenecen a sus propietarios.

# Contenido

Módulo 5: Redes y entrega de contenido

4

AWS Academy Cloud Foundations

# Módulo 5: Redes y entrega de contenido



© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

## Bienvenido al Módulo 5: Redes y entrega de contenido

Este módulo abarca tres aspectos fundamentales de Amazon Web Services (AWS) para la entrega de contenido y las redes: Amazon Virtual Private Cloud (Amazon VPC), Amazon Route 53 y Amazon CloudFront.

# Información general sobre el módulo



## Temas

- Conceptos básicos de las redes
- Amazon VPC
- Redes de VPC
- Seguridad de VPC
- Amazon Route 53
- Amazon CloudFront

## Actividades

- Etiquetar un diagrama de red
- Diseñar una arquitectura básica de VPC

## Demostración

- Demostración de VPC

## Laboratorio

- Creación de una VPC y lanzamiento de un servidor web



## Revisión de conocimientos

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

2

En este módulo, se abordarán los siguientes temas:

- Conceptos básicos de las redes
- Amazon Virtual Private Cloud (Amazon VPC)
- Redes de VPC
- Seguridad de VPC
- Amazon Route 53
- Amazon CloudFront

Este módulo incluye algunas actividades que lo desafían con el etiquetado de un diagrama de red y el diseño de una arquitectura básica de VPC.

Verá una demostración grabada para aprender a utilizar el asistente de VPC a la hora de crear una VPC con subredes públicas y privadas.

Luego, tendrá la oportunidad de aplicar lo que ha aprendido en un laboratorio práctico donde utilizará el asistente de VPC para crear una VPC y lanzar un servidor web.

Por último, se le pedirá que complete una revisión de conocimientos que demuestre su comprensión de los conceptos clave que se analizaron en este

módulo.

## Objetivos del módulo



Después de completar este módulo, debería ser capaz de lo siguiente:

- Reconocer los conceptos básicos de las redes
- Describir las redes virtuales en la nube con Amazon VPC
- Etiquetar un diagrama de red
- Diseñar una arquitectura básica de VPC
- Indicar los pasos para crear una VPC
- Identificar los grupos de seguridad
- Crear su propia VPC y agregarle componentes adicionales para generar una red personalizada
- Identificar los aspectos fundamentales de Amazon Route 53
- Reconocer los beneficios de Amazon CloudFront

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

5

Después de completar este módulo, debería ser capaz de lo siguiente:

- Reconocer los conceptos básicos de las redes
- Describir las redes virtuales en la nube con Amazon VPC
- Etiquetar un diagrama de red
- Diseñar una arquitectura básica de VPC
- Indicar los pasos para crear una VPC
- Identificar los grupos de seguridad
- Crear su propia VPC y agregarle componentes adicionales para generar una red personalizada
- Identificar los aspectos fundamentales de Amazon Route 53
- Reconocer los beneficios de Amazon CloudFront

## Módulo 5: Redes y entrega de contenido

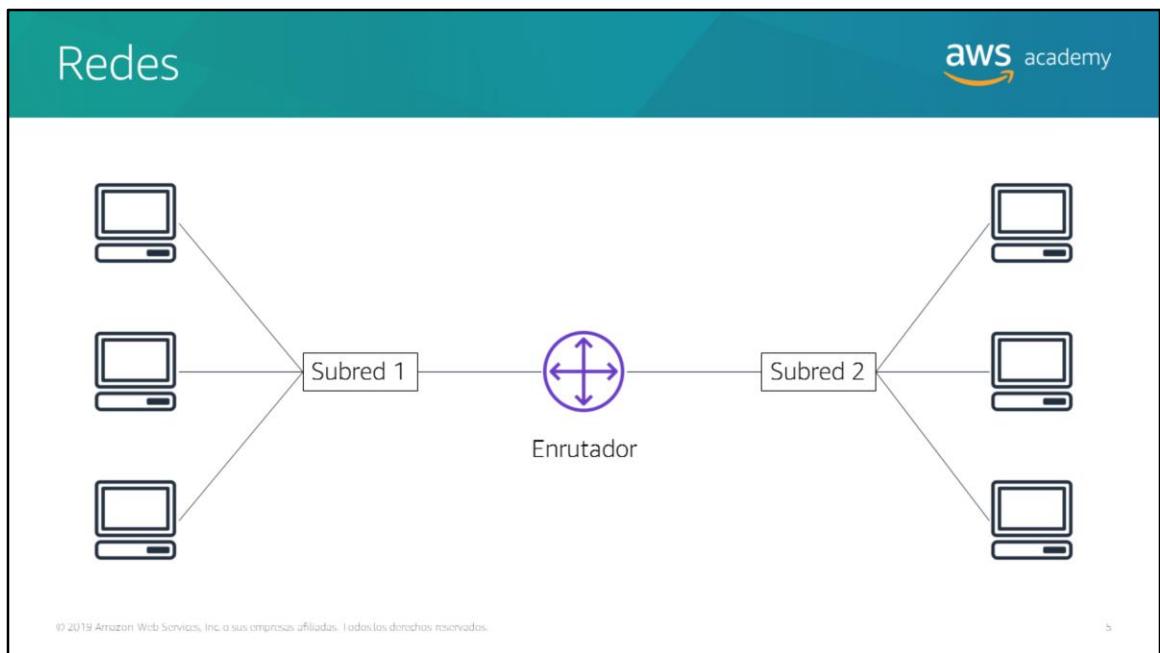
### Sección 1: Conceptos básicos de las redes

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.



### Sección 1: Conceptos básicos de las redes

En esta sección, revisará algunos conceptos básicos sobre redes que sientan las bases necesarias para comprender el servicio de redes de AWS, Amazon Virtual Private Cloud (Amazon VPC).



Una *red* informática implica la conexión de dos o más equipos cliente con el objetivo de compartir recursos. Una red se puede dividir lógicamente en *subredes*. Las redes requieren un dispositivo de red (como un enrutador o un conmutador) para conectar a todos los clientes y permitir la comunicación entre ellos.

## Direcciones IP

aws academy

192 . 0 . 2 . 0

↓      ↓      ↓      ↓

11000000 00000000 00000010 00000000

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Cada equipo cliente de una red tiene una dirección de protocolo de Internet (IP) única que lo identifica. Una dirección IP es una etiqueta numérica en formato decimal. Los equipos convierten ese número decimal a un formato binario.

En este ejemplo, la dirección IP es 192.0.2.0. Cada uno de los cuatro números separados por puntos (.) de la dirección IP representa 8 bits en formato numérico octal. Esto significa que cada uno de los cuatro números puede tener un valor comprendido entre 0 y 255. El total combinado de los cuatro números de una dirección IP es de 32 bits en formato binario.

## Direcciones IPv4 e IPv6



Dirección IPv4 (32 bits): 192.0.2.0

Dirección IPv6 (128 bits): 2600:1f18:22ba:8c00:ba86:a05e:a5ba:00FF

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

/

Una dirección IP de 32 bits se denomina dirección IPv4.

Las direcciones IPv6, que tienen 128 bits, también están disponibles. Las direcciones IPv6 pueden atender a más dispositivos de usuario.

Una dirección IPv6 está compuesta por ocho grupos de cuatro letras y números separados por dos puntos (:). En este ejemplo, la dirección IPv6 es 2600:1f18:22ba:8c00:ba86:a05e:a5ba:00FF. Cada uno de los ocho grupos separados por dos puntos de la dirección IPv6 representa 16 bits en formato numérico hexadecimal. Esto significa que cada uno de los ocho grupos puede ser cualquier valor desde 0 hasta FFFF. El total combinado de los ocho grupos para una dirección IPv6 es de 128 bits en formato binario.

## Direccionamiento entre dominios sin clases (CIDR)

aws academy

Identificador de red (prefijo de direccionamiento)	Identificador de host
192 . 0 . 2 .	. 0 / 24
<b>11000000</b>	<b>00000000</b>
<b>Estático</b>	<b>Indica cuántos bits son estáticos</b>
00000010	00000000
	hasta 11111111
	<b>Flexible</b>

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Un método común para describir redes es el direccionamiento entre dominios sin clases (CIDR). La dirección CIDR se expresa de la siguiente manera:

- Una dirección IP (que es la primera dirección de la red)
- A continuación, un carácter de barra inclinada (/)
- Por último, un número que le indica cuántos bits del prefijo de direccionamiento deben ser estáticos o cuántos deben asignarse para el identificador de red

Los bits que no son estáticos pueden cambiar. El CIDR es una forma de expresar un grupo de direcciones IP consecutivas entre sí.

En este ejemplo, la dirección CIDR es 192.0.2.0/24. El último número (24) le indica que los primeros 24 bits deben ser estáticos. Los últimos 8 bits son flexibles, lo que significa que hay  $2^8$  (o 256) direcciones IP disponibles para la red, que van desde 192.0.2.0 hasta 192.0.2.255. El cuarto dígito decimal puede cambiar de 0 a 255.

Si el CIDR era 192.0.2.0/16, el último número (16) le indica que los primeros 16 bits deben ser estáticos. Los últimos 16 bits son flexibles, lo que significa que hay  $2^{16}$  (o 65 536) direcciones IP disponibles para la red, que van desde 192.0.0.0 hasta 192.0.255.255. Ambos dígitos decimales en tercera y en cuarta posición pueden cambiar de 0 a 255.

Existen dos casos especiales:

- Las direcciones IP estáticas, en las que cada bit es estático, representan una única dirección IP (por ejemplo, 192.0.2.0/32). Este tipo de dirección es útil cuando desea configurar una regla de firewall y conceder acceso a un host específico.
- En el caso de Internet, en el que cada bit es flexible, se representa como 0.0.0.0/0.

Modelo de interconexión de sistemas abiertos (OSI)			
Capa	Número	Función	Protocolo/dirección
Aplicación	7	Es el medio por el que una aplicación obtiene acceso a una red informática	HTTP(S), FTP, DHCP, LDAP
Presentación	6	<ul style="list-style-type: none"> <li>Garantiza que la capa de aplicación pueda leer los datos</li> <li>Cifrado</li> </ul>	ASCI, ICA
Sesión	5	Permite un intercambio ordenado de datos	NetBIOS, RPC
Transporte	4	Proporciona protocolos para admitir la comunicación de host a host	TCP, UDP
Red	3	Direccionamiento y reenvío de paquetes (enrutadores)	IP
Enlace de datos	2	Transferir datos en la misma red LAN (concentradores y conmutadores)	MAC
Capa física	1	Transmisión y recepción de transmisiones de bits sin procesar a través de un medio físico	Señales (unos y ceros)

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

9

El modelo de interconexión de sistemas abiertos (OSI) es un modelo conceptual que se utiliza para explicar cómo viajan los datos a través de una red. Consta de siete capas y muestra los protocolos y las direcciones comunes que se utilizan para enviar datos en cada capa. Por ejemplo, los concentradores y los conmutadores funcionan en la capa 2 (la capa de enlace de datos). Los enrutadores funcionan en la capa 3 (la capa de red). El modelo OSI también se puede utilizar para comprender cómo se produce la comunicación en una nube virtual privada (VPC), lo que representa el tema de la siguiente sección.

## Módulo 5: Redes y entrega de contenido

### Sección 2: Amazon VPC

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.



### Sección 2: Amazon VPC

Muchos de los conceptos de una red en las instalaciones son válidos también para una red basada en la nube, pero gran parte de la complejidad de configurar una red se ha eliminado sin sacrificar el control, la seguridad ni la facilidad de uso. En esta sección, aprenderá sobre Amazon VPC y los componentes fundamentales de una VPC.

## Amazon VPC



Amazon  
VPC

- Le permite aprovisionar una sección de la nube de AWS **aislada lógicamente** en la que puede lanzar recursos de AWS en una red virtual que usted defina.
- Le permite **controlar sus recursos de red virtual** entre los que se cuentan los siguientes:
  - Selección del intervalo de direcciones IP
  - Creación de subredes
  - Configuración de tablas de enrutamiento y gateways de red
- Le permite **personalizar la configuración de red** de su VPC.
- Le permite utilizar **varias capas de seguridad**.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

11

Amazon Virtual Private Cloud (Amazon VPC) es un servicio que le permite aprovisionar una sección de la nube de AWS aislada lógicamente (denominada nube virtual privada o VPC) donde puede lanzar sus recursos de AWS.

Amazon VPC le permite controlar los recursos de red virtual, lo que incluye la selección de su propio intervalo de direcciones IP, la creación de subredes y la configuración de tablas de enrutamiento y gateways de red. Puede usar IPv4 e IPv6 en su VPC para acceder de forma segura a los recursos y a las aplicaciones.

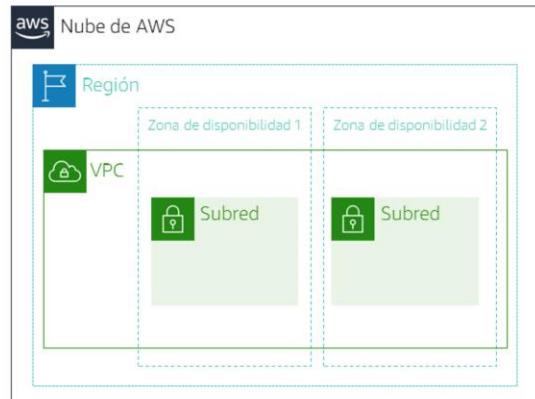
También puede personalizar la configuración de red de la VPC. Por ejemplo, puede crear una subred pública para los servidores web que tengan acceso a Internet público. También puede colocar sus sistemas de backend (como los servidores de aplicaciones o de bases de datos) en una subred privada sin acceso a Internet público.

Por último, puede utilizar varias capas de seguridad, como grupos de seguridad y listas de control de acceso a la red (ACL de red), para ayudar a controlar el acceso a las instancias de Amazon Elastic Compute Cloud (Amazon EC2) en cada subred.

# VPC y subredes



- VPC:
  - Están aisladas lógicamente de otras VPC.
  - Están dedicadas a su cuenta de AWS.
  - Pertenecen a una única **región de AWS** y pueden abarcar varias zonas de disponibilidad.
- Subredes:
  - Son el intervalo de direcciones IP que dividen una VPC.
  - Pertenecen a una única **zona de disponibilidad**.
  - Se clasifican como **públicas o privadas**.



© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

12

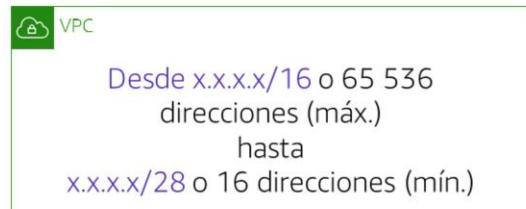
Amazon VPC le permite aprovisionar nubes virtuales privadas (VPC). Una VPC es una red virtual que está aislada lógicamente de las demás redes virtuales en la nube de AWS. Es exclusiva de su cuenta. Las VPC pertenecen a una única región de AWS y pueden abarcar varias zonas de disponibilidad.

Después de crear una VPC, puede dividirla en una o más subredes. Una *subred* es un intervalo de direcciones IP en una VPC. Las subredes pertenecen a una única zona de disponibilidad. Puede crear subredes en diferentes zonas de disponibilidad para conseguir un nivel elevado de disponibilidad. En general, las subredes se clasifican como públicas o privadas. *Las subredes públicas tienen acceso directo a Internet, pero las subredes privadas, no.*

## Direccionamiento IP



- Cuando crea una VPC, le asigna un **bloque de CIDR IPv4** (un intervalo de direcciones IPv4 **privadas**).
- No puede cambiar el intervalo de direcciones **después de crear la VPC**.
- El tamaño de bloque de CIDR IPv4 **más grande** es **/16**.
- El tamaño de bloque de CIDR IPv4 **más pequeño** es **/28**.
- También se admite IPv6 (con un límite de tamaño de bloque diferente).
- Los bloques de CIDR de subredes **no se pueden superponer**.



© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

15

Las direcciones IP permiten que los recursos de su VPC se comuniquen entre sí y con otros recursos a través de Internet. Cuando se crea una VPC, se le asigna un bloque de CIDR IPv4 (un intervalo de direcciones IPv4 *privadas*). Después de crear una VPC, no puede cambiar el intervalo de direcciones, por lo que es importante que lo elija cuidadosamente. El bloque de CIDR IPv4 puede ser tan grande como **/16** (que sería  $2^{16}$  o 65 536 direcciones) o tan pequeño como **/28** (que sería  $2^4$  o 16 direcciones).

De manera opcional, puede asociar un bloque de CIDR IPv6 a su VPC y sus subredes, y asignar direcciones IPv6 de ese bloque a los recursos de la VPC. Los bloques de CIDR IPv6 tienen un límite de tamaño diferente.

El bloque de CIDR de una subred puede ser del mismo tamaño que el bloque de CIDR de una VPC. En este caso, la VPC y la subred tienen el mismo tamaño (una sola subred en la VPC). Por otro lado, el bloque de CIDR de una subred puede ser un subconjunto del bloque de CIDR de la VPC. Esta estructura permite la definición de varias subredes. Si crea más de una subred en una VPC, los bloques de CIDR de las subredes no se pueden superponer. No puede tener direcciones IP duplicadas en la misma VPC.

Para obtener más información sobre las direcciones IP en una VPC, consulte la [documentación de AWS](#).

## Direcciones IP reservadas



Ejemplo: una VPC con un bloque de CIDR IPv4 de 10.0.0.0/16 tiene un total de 65 536 direcciones IP. La VPC tiene cuatro subredes del mismo tamaño. Por cada subred hay solo 251 direcciones IP disponibles para su uso.



Direcciones IP para el bloque de CIDR 10.0.0.0/24	Reservadas para
10.0.0.0	Dirección de red
10.0.0.1	Comunicación interna
10.0.0.2	Resolución del sistema de nombres de dominio (DNS)
10.0.0.3	Uso futuro
10.0.0.255	Dirección de transmisión de la red

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

14

Cuando crea una subred, esta requiere su propio bloque de CIDR. Por cada bloque de CIDR que especifique, AWS reserva cinco direcciones IP dentro de dicho bloque, y estas direcciones no están disponibles para su uso. AWS reserva estas direcciones IP para lo siguiente:

- Dirección de red
- Enrutador local de la VPC (comunicaciones internas)
- Resolución del sistema de nombres de dominio (DNS)
- Uso futuro
- Dirección de transmisión de la red

Por ejemplo, supongamos que crea una subred con un bloque de CIDR IPv4 de 10.0.0.0/24 (que tiene 256 direcciones IP en total). La subred tiene 256 direcciones IP, pero solo hay 251 disponibles porque cinco están reservadas.

## Tipos de direcciones IP públicas



### Dirección IPv4 pública

- Se asigna manualmente a través de una dirección IP elástica.
- Se asigna de manera automática a través de la configuración de asignación automática de direcciones IP públicas en el nivel de subred.

### Dirección IP elástica

- Está asociada a una cuenta de AWS.
- Se puede asignar y reasignar en cualquier momento.
- Podría implicar costos adicionales.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

15

Cuando crea una VPC, todas las instancias de esa VPC obtienen una dirección IP privada de manera automática. También puede solicitar que se asigne una dirección IP pública al crear la instancia mediante la modificación de las propiedades de asignación automática de la dirección IP pública de la subred.

Las *direcciones IP elásticas* son direcciones IPv4 estáticas y públicas, que se diseñaron para la informática en la nube dinámica. Puede asociar una dirección IP elástica a cualquier instancia o interfaz de red de cualquier VPC de su cuenta. Con una dirección IP elástica, puede enmascarar los errores de las instancias reasignando rápidamente la dirección a otra instancia de su VPC. Asociar la dirección IP elástica a la interfaz de red tiene una ventaja sobre asociarla de manera directa a la instancia. Puede trasladar todos los atributos de la interfaz de red de una instancia a otra en un solo paso.

Es posible que se apliquen costos adicionales si utiliza direcciones IP elásticas, por lo que es importante liberarlas cuando ya no las necesite.

Para obtener más información sobre las direcciones IP elásticas, consulte [Direcciones IP elásticas](#) en la documentación de AWS.

## Interfaz de red elástica



- Una interfaz de red elástica es una [interfaz de red virtual](#) que se puede:
  - Asociar a una instancia
  - Desconectar de la instancia y asociar a otra para redirigir el tráfico de red
- Cuando se vuelve a asociar a una nueva instancia, [sus atributos también se asocian](#).
- Cada instancia de su VPC tiene una [interfaz de red predeterminada](#) a la que se asigna una dirección IPv4 privada del intervalo de direcciones IPv4 de su VPC.



© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

1b

Una *interfaz de red elástica* es una interfaz de red virtual que puede asociarse a una instancia en una VPC o desconectarse de una. Los atributos de una interfaz de red también se asocian cuando se vuelve a asociar a otra instancia. Cuando mueve una interfaz de red de una instancia a otra, el tráfico de la red se redirige a la nueva instancia.

Cada instancia de su VPC tiene una interfaz de red predeterminada (la interfaz de red principal) que tiene asignada una dirección IPv4 privada del intervalo de direcciones IPv4 de su VPC. No se puede desconectar una interfaz de red principal de una instancia. Puede crear y asociar una interfaz de red adicional a cualquier instancia de su VPC. La cantidad de interfaces de red que puede asociar varía en función del tipo de instancia.

Para obtener más información acerca de [las interfaces de red elásticas](#), consulte la documentación de AWS.

## Tablas de enrutamiento y rutas



- Una **tabla de enrutamiento** contiene un conjunto de reglas (o rutas) que **puede configurar** para dirigir el tráfico de red de su subred.
- Cada **ruta** especifica un destino y un objetivo.
- De forma predeterminada, cada tabla de enrutamiento contiene una **ruta local** para la comunicación dentro de la VPC.
- Cada **subred debe estar asociada a una tabla de enrutamiento** (solamente a una).

**Tabla de enrutamiento principal (predeterminada)**

Destino	Objetivo
10.0.0/16	local

Bloque de CIDR de la VPC

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

1/

Una *tabla de enrutamiento* contiene un conjunto de reglas (denominadas *rutas*) que dirigen el tráfico de red de su subred. Cada ruta especifica un *destino* y un *objetivo*. El *destino* es el bloque de CIDR de destino al que desea que se dirija el tráfico de su subred. El *objetivo* es el recurso a través del cual se envía el tráfico de destino. De forma predeterminada, cada tabla de enrutamiento que crea contiene una *ruta local* para la comunicación en la VPC. Puede personalizar las tablas de enrutamiento agregando rutas. No puede eliminar la entrada de ruta local que se utiliza para las comunicaciones internas.

Cada subred de su VPC debe estar asociada a una tabla de enrutamiento. La *tabla de enrutamiento principal* es la tabla que se asigna automáticamente a su VPC. Controla el direccionamiento de todas las subredes que no estén asociadas de forma explícita a ninguna otra tabla de enrutamiento. Una subred puede asociarse a una sola tabla de enrutamiento por vez, pero pueden asociarse varias subredes a la misma tabla de enrutamiento.

Para obtener más información sobre las tablas de enrutamiento, consulte la [documentación de AWS](#).

## Aprendizajes clave de la sección 2



18

**aws academy**

- Una VPC es una sección de la nube de AWS aislada lógicamente.
- Pertenece a una región y requiere un bloque de CIDR.
- Se subdivide en subredes.
- Una subred pertenece a una zona de disponibilidad y requiere un bloque de CIDR.
- Las tablas de enrutamiento controlan el tráfico de una subred.
- Tienen una ruta local integrada.
- Las rutas adicionales se agregan a la tabla.
- La ruta local no se puede eliminar.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Estos son algunos de los aprendizajes clave de esta sección del módulo:

- Una VPC es una sección de la nube de AWS aislada lógicamente.
- Pertenece a una región y requiere un bloque de CIDR.
- Se subdivide en subredes.
- Una subred pertenece a una zona de disponibilidad y requiere un bloque de CIDR.
- Las tablas de enrutamiento controlan el tráfico de una subred.
- Tienen una ruta local integrada.
- Las rutas adicionales se agregan a la tabla.
- La ruta local no se puede eliminar.

## Módulo 5: Redes y entrega de contenido

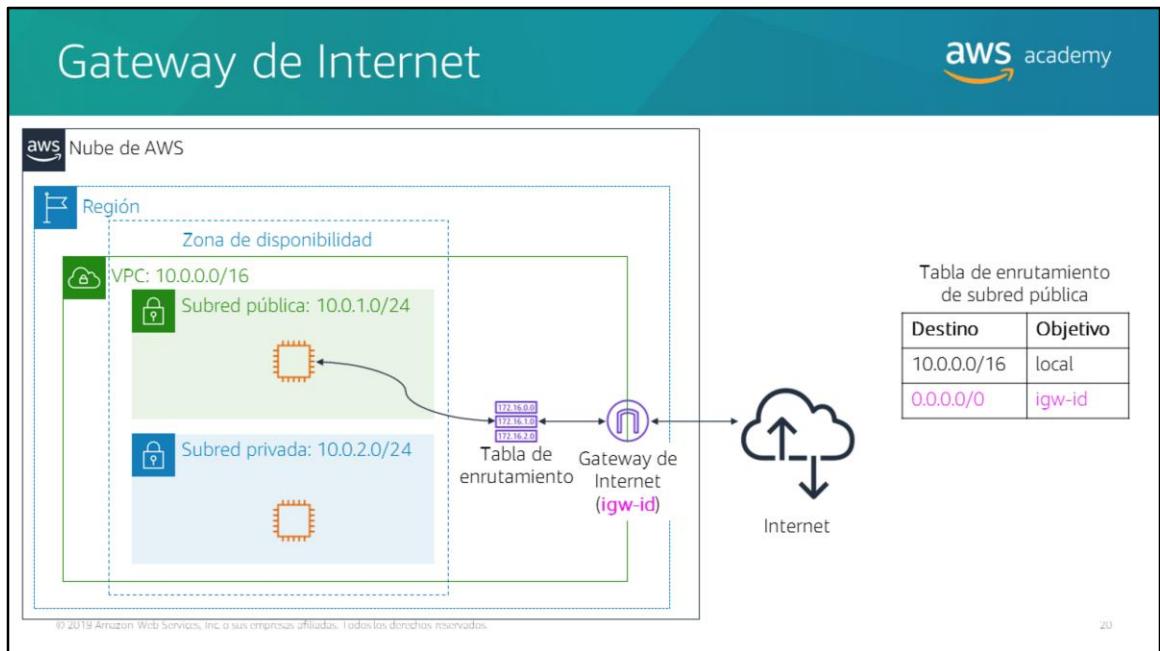
### Sección 3: Redes de VPC

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.



### Sección 3: Redes de VPC

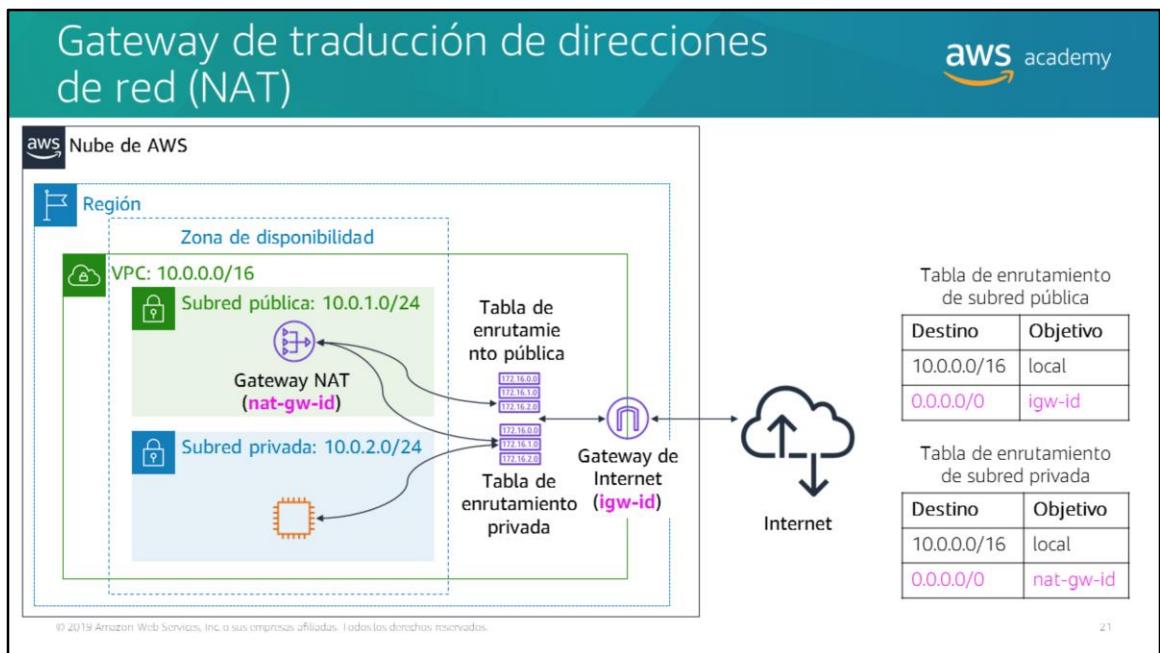
Ahora que ha aprendido sobre los componentes básicos de una VPC, puede comenzar a dirigir el tráfico de formas interesantes. En esta sección, aprenderá sobre las diferentes opciones de red.



Una *gateway de Internet* es un componente de VPC escalable, redundante y altamente disponible que posibilita la comunicación entre instancias de su VPC e Internet. Una gateway de Internet sirve para dos fines: proporcionar un objetivo en sus tablas de enruteamiento de VPC para el tráfico direccional a través de Internet y realizar la traducción de las direcciones de red para las instancias que tengan asignadas direcciones IPv4 públicas.

Para hacer *pública una subred*, *asocie una gateway de Internet a su VPC* y agregue una ruta a la tabla de enruteamiento para enviar el tráfico que no es local a Internet (0.0.0.0/0) a través de la gateway de Internet.

Para obtener más información acerca de las gateways de Internet, consulte [Gateways de Internet](#) en la documentación de AWS.



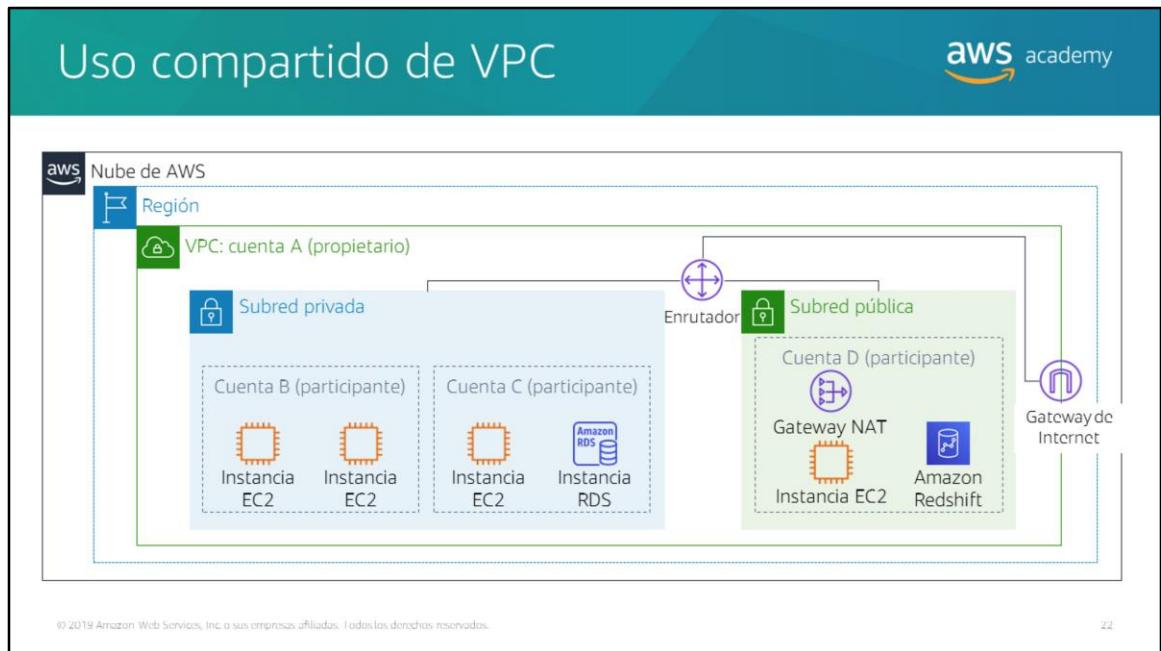
Una *gateway de traducción de las direcciones de red (NAT)* permite a las instancias de la subred privada conectarse a Internet o a otros servicios de AWS, a la vez que impide a Internet iniciar una conexión con esas mismas instancias.

Para crear una gateway NAT, debe especificar la subred pública en la que se debe ubicar la gateway NAT. También debe especificar una dirección IP elástica para asociar a la gateway NAT cuando la cree. Una vez creada una gateway NAT, debe actualizar la tabla de enruteamiento que esté asociada a una o más de sus subredes privadas para que dirija el tráfico orientado hacia Internet a la gateway NAT. De esta manera, las instancias de sus subredes privadas podrán comunicarse con Internet.

También puede utilizar una instancia NAT en una subred pública de su VPC en lugar de una gateway NAT. Sin embargo, una gateway NAT es un servicio NAT administrado que ofrece una mejor disponibilidad y un mayor ancho de banda, pero con menos esfuerzo administrativo. Para casos de uso comunes, AWS recomienda utilizar una gateway NAT en lugar de una instancia NAT.

Consulte la documentación de AWS para obtener más información sobre los siguientes temas:

- [Gateways NAT](#)
- [Instancias NAT](#)
- [Diferencias entre las gateways NAT y las instancias NAT](#)



El uso compartido de VPC permite a los clientes utilizar subredes de manera compartida con otras cuentas de AWS de la misma organización en AWS Organizations. También permite que varias cuentas de AWS creen sus recursos de aplicaciones, como instancias de Amazon EC2, bases de datos de Amazon Relational Database Service (Amazon RDS), clústeres de Amazon Redshift y funciones de AWS Lambda, en VPC compartidas y administradas de manera centralizada. En este modelo, la cuenta dueña de la VPC (propietaria) comparte una o más subredes con otras cuentas (participantes) que pertenecen a la misma organización en 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 los recursos que pertenezcan a otros participantes o al propietario de la VPC.

El uso compartido de VPC ofrece varios beneficios:

- **División de deberes:** la estructura de VPC, el direccionamiento y la asignación de direcciones IP se controlan de manera centralizada.
- **Titularidad:** los propietarios de la aplicación mantienen su derecho de propiedad sobre los recursos, las cuentas y los grupos de seguridad.
- **Grupos de seguridad:** los participantes que comparten la VPC pueden hacer referencia a los ID de los grupos de seguridad de los demás.
- **Eficiencias:** se consigue mayor densidad en las subredes, uso eficiente de las VPN y AWS Direct Connect.

- Falta de límites invariables: se pueden evitar los límites invariables (por ejemplo, un límite de 50 interfaces virtuales por conexión de AWS Direct Connect) a través de una arquitectura de red simplificada.
- Costos optimizados: los costos se pueden optimizar mediante la reutilización de gateways NAT, los puntos de enlace de interfaz de VPC y el tráfico dentro de la zona de disponibilidad.

El uso compartido de VPC le permite desacoplar cuentas y redes. Esto hace que tenga menos VPC, pero de mayor tamaño y con administración centralizada. Las aplicaciones altamente interconectadas se benefician de este enfoque de manera automática.

# Interconexión de VPC

Nube de AWS

VPC A: 10.0.0.0/16

VPC B: 10.3.0.0/16

Interconexión (pcx-id)

Tabla de enrutamiento para VPC A

Destino	Objetivo
10.0.0.0/16	local
10.3.0.0/16	pcx-id

Tabla de enrutamiento para VPC B

Destino	Objetivo
10.3.0.0/16	local
10.0.0.0/16	pcx-id

Puede conectar las VPC en su propia cuenta de AWS, entre cuentas de AWS o entre regiones de AWS.

Restricciones:

- Los espacios IP no se pueden superponer.
- No se admite la interconexión transitiva.
- Solo puede tener un recurso de interconexión entre las mismas dos VPC.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

2.5

Una *interconexión de VPC* es una conexión de red entre dos VPC que permite dirigir el tráfico entre ellas de forma privada. Las instancias de cualquier VPC pueden comunicarse entre ellas como si pertenecieran a la misma red. Puede crear una interconexión de VPC entre sus propias VPC, con una VPC de otra cuenta de AWS o con una VPC de otra región de AWS.

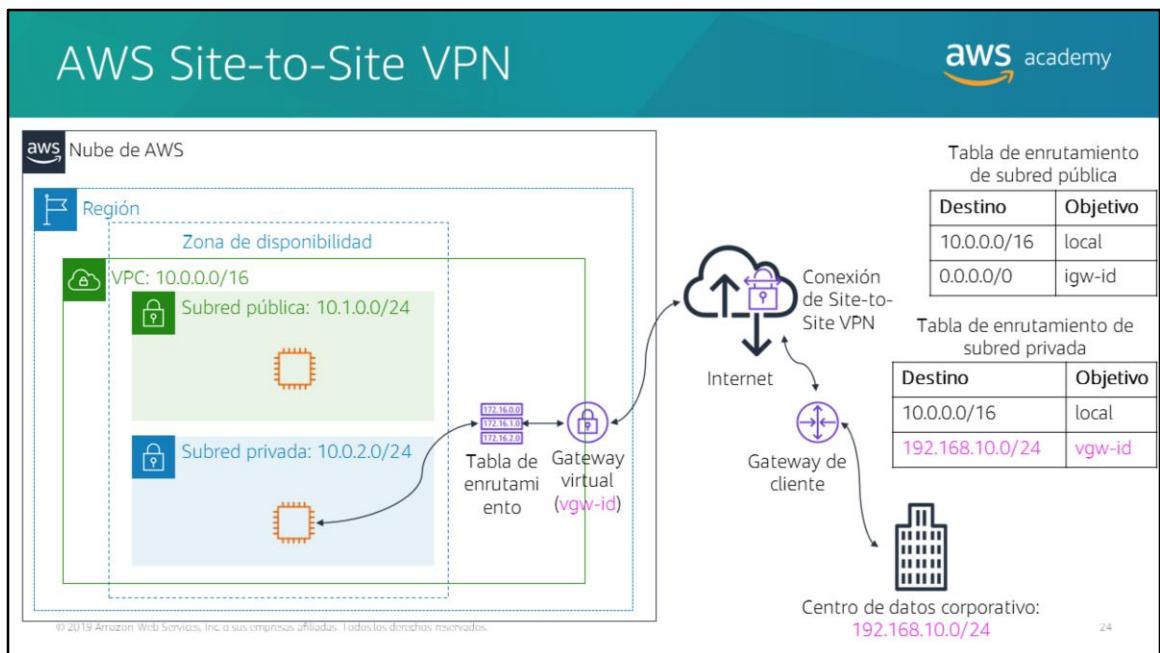
Cuando configura la interconexión, crea reglas en la tabla de enrutamiento para permitir que las VPC se comuniquen entre sí a través del recurso de interconexión. Por ejemplo, supongamos que tiene dos VPC. En la tabla de enrutamiento de la VPC A, establece que el destino sea la dirección IP de la VPC B y que el objetivo sea el ID del recurso de interconexión. En la tabla de enrutamiento de la VPC B, establece que el destino sea la dirección IP de la VPC A; y el objetivo, el ID del recurso de interconexión.

La interconexión de VPC tiene las siguientes restricciones:

- Los intervalos de direcciones IP no se pueden superponer.
- No se admite la interconexión transitiva. Por ejemplo, supongamos que tiene tres VPC: A, B y C. La VPC A está conectada a la VPC B, y la VPC A está conectada

- a la VPC C. Sin embargo, la VPC B *no* está conectada implícitamente a la VPC C. Para conectar la VPC B a la VPC C, debe establecer explícitamente dicha conectividad.
- Solo puede tener un recurso de interconexión entre las mismas dos VPC.

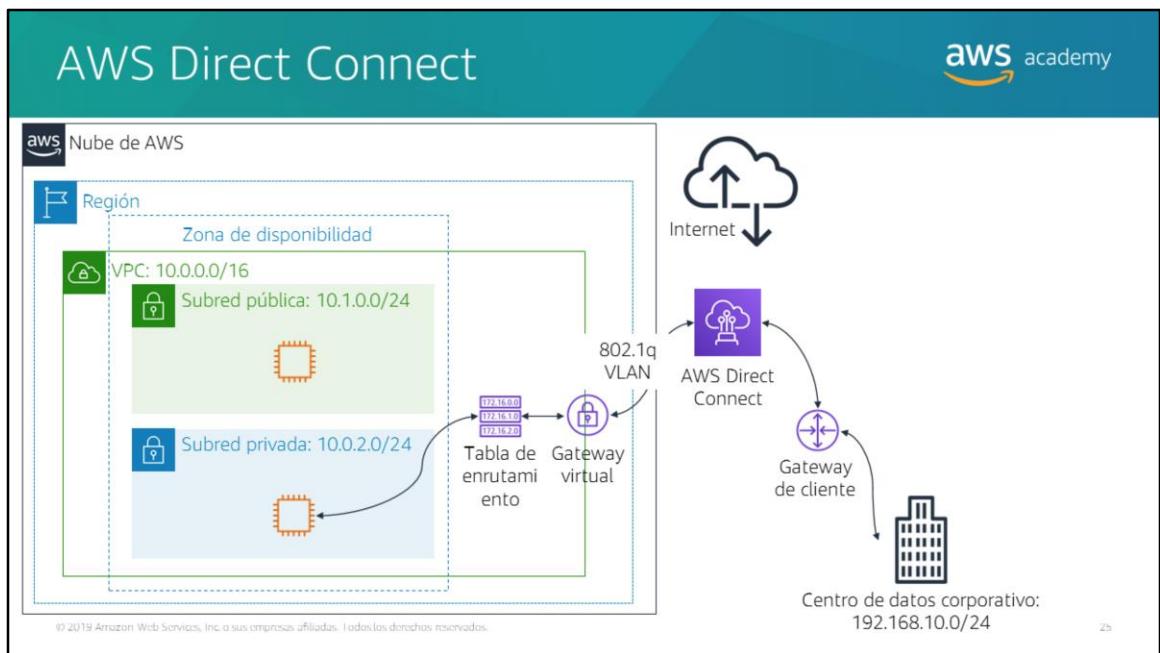
Para obtener más información acerca de la interconexión de VPC, consulte [Interconexión de VPC](#) en la documentación de AWS.



De forma predeterminada, las instancias que se lanzan en una VPC no pueden comunicarse con una red remota. Para conectar la VPC a su red remota (es decir, crear una red virtual privada o una conexión de VPN), debe hacer lo siguiente:

1. Cree un nuevo dispositivo de gateway virtual (denominado *gateway de red virtual privada [VPN]*) y asócielo a su VPC.
2. Defina la configuración del dispositivo de VPN o de la *gateway de cliente*. La gateway de cliente no es un dispositivo, sino un recurso de AWS que proporciona información a AWS sobre su dispositivo de VPN.
3. Cree una tabla de enruteamiento personalizada para dirigir el tráfico orientado hacia el centro de datos corporativo a la gateway de VPN. También debe actualizar las reglas del grupo de seguridad. (Aprenderá acerca de los grupos de seguridad en la siguiente sección).
4. Establezca una *conexión AWS Site-to-Site VPN (VPN de sitio a sitio)* para vincular los dos sistemas.
5. Configure el direccionamiento para transmitir el tráfico a través de la conexión.

Para obtener más información acerca de AWS Site-to-Site VPN y otras opciones de conectividad de VPN, consulte [Conexiones de VPN](#) en la documentación de AWS.



Uno de los desafíos de la comunicación de red es el rendimiento de la red. El rendimiento puede verse perjudicado si su centro de datos se encuentra lejos de la región de AWS. Para estas situaciones, AWS ofrece AWS Direct Connect, también llamado DX. AWS Direct Connect le permite establecer una conexión de red privada y dedicada entre su red y una de las ubicaciones de DX. Esta conexión privada puede reducir los costos de red, mejorar el rendimiento del ancho de banda y proporcionar una experiencia de red más consistente que las conexiones basadas en Internet. DX utiliza redes de área local virtual (VLAN) 802.1q de estándar abierto.

Para obtener más información sobre DX, consulte la [página del producto AWS Direct Connect](#).

# Puntos de enlace de la VPC

Nube de AWS

Región

Zona de disponibilidad

VPC: 10.0.0.0/16

Subred pública: 10.0.1.0/24

Subred privada: 10.0.2.0/24

Punto de enlace de la VPC (vpcep-id)

Amazon Simple Storage Service (Amazon S3)

Tabla de enruteamiento de subred pública

Destino	Objetivo
10.0.0.0/16	local
ID de Amazon S3	vpcep-id

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Dos tipos de puntos de enlace:

- **Puntos de enlace de interfaz** (con tecnología de AWS PrivateLink)
- **Puntos de enlace de gateway** (Amazon S3 y Amazon DynamoDB)

Un *punto de enlace de la VPC* es un dispositivo virtual que le permite conectar de forma privada su VPC a los servicios de AWS compatibles y a los servicios de punto de enlace de la VPC que funcionan con tecnología de AWS PrivateLink. La conexión con estos servicios no requiere una gateway de Internet, un dispositivo NAT, una conexión de VPN ni una conexión de AWS Direct Connect. Las instancias de la VPC no requieren direcciones IP públicas para comunicarse con los recursos en el servicio. El tráfico entre la VPC y el otro servicio no sale de la red de Amazon.

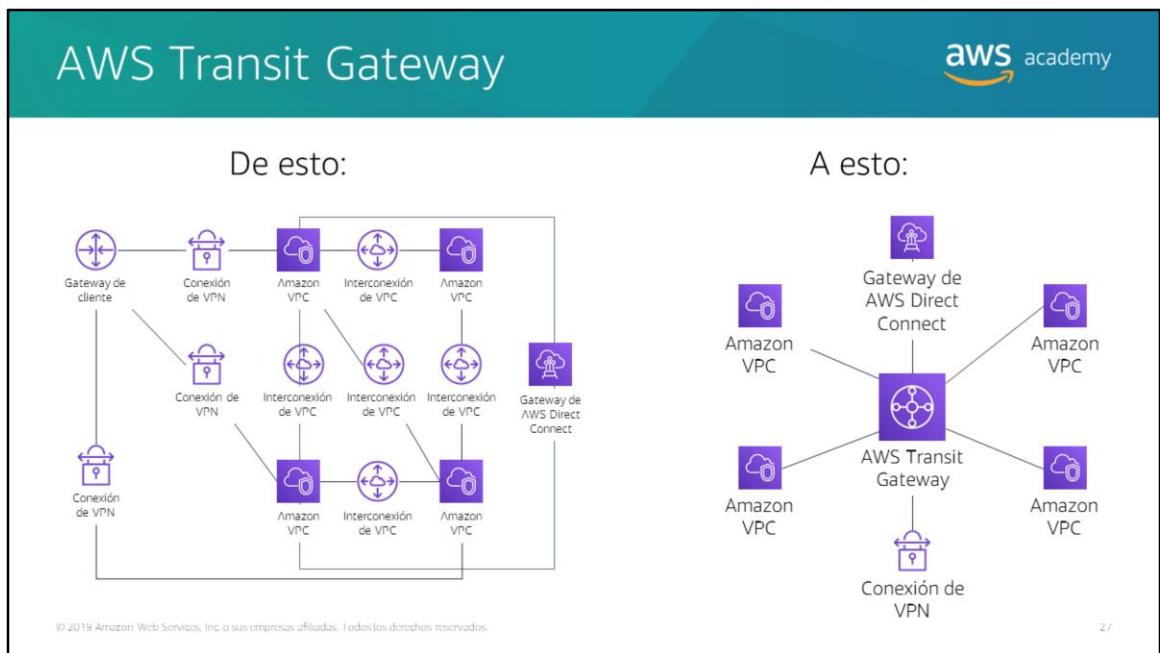
Existen dos tipos de puntos de enlace de la VPC:

- Un *punto de enlace de la VPC* (punto de enlace de interfaz) le permite conectarse a servicios con tecnología de AWS PrivateLink. Entre estos servicios, podemos encontrar algunos de AWS, algunos alojados por otros clientes de AWS o por socios de la red de socios de AWS (APN) en sus propias VPC (denominados *servicios de punto de enlace*), y los servicios de socios de APN compatibles en AWS Marketplace. El propietario del servicio es el *prestashop del servicio*, y usted, como entidad principal que crea el punto de enlace de interfaz, es el *consumidor del servicio*. Se le cobrará por crear y utilizar un punto de enlace de interfaz a un servicio. Se aplicarán tarifas de procesamiento de datos y de uso por horas. Consulte la documentación de AWS para ver una lista de los [puntos de enlace de](#)

interfaz compatibles.

- Puntos de enlace de gateway: el uso de puntos de enlace de gateway no conlleva ningún cargo adicional. Se aplicará la tarifa estándar por la transferencia de datos y por el uso de recursos.

Para obtener más información acerca de los puntos de enlace de la VPC, consulte [Puntos de enlace de la VPC](#) en la documentación de AWS.



Puede configurar sus VPC de varias maneras y aprovechar numerosas opciones de conectividad y gateways. Estas opciones y gateways incluyen AWS Direct Connect (a través de gateways DX), gateways NAT, gateways de Internet, interconexiones de VPC, entre otras. No es extraño encontrar clientes de AWS con cientos de VPC distribuidas entre cuentas y regiones de AWS que deben atender varias líneas de negocio, además de varios equipos, proyectos, etc. Todo se complica más cuando los clientes comienzan a configurar la conectividad entre sus VPC. Todas las opciones de conectividad son estrictamente de punto a punto, por lo que el número de conexiones de VPC a VPC puede crecer con rapidez. A medida que aumente el número de cargas de trabajo que se ejecutan en AWS, deberá ser capaz de ajustar la escala de sus redes en varias cuentas y VPC para seguir el ritmo de crecimiento.

Aunque puede utilizar la interconexión de VPC para conectar pares de VPC, administrar la conectividad de punto a punto en muchas VPC sin la capacidad de administrar de forma centralizada las políticas de conectividad puede resultar una tarea costosa y difícil desde un punto de vista operativo. Para la conectividad en las instalaciones, debe asociar su VPN a cada VPC. Esta solución puede requerir mucho tiempo de creación y ser difícil de administrar cuando el número de VPC alcanza los tres dígitos.

Si desea solucionar este problema, puede utilizar AWS Transit Gateway para simplificar su modelo de red. Con AWS Transit Gateway, solo tiene que crear y administrar una única conexión desde la gateway central a cada VPC, centro de datos en las instalaciones u oficina remota de su red. Las gateways de tránsito actúan como un concentrador que controla la manera en la que el tráfico se dirige a todas las redes conectadas que funcionan como radios. Este sistema radial simplifica de manera significativa la administración y reduce los costos operativos porque cada red solo tiene conectarse a la gateway de tránsito y no a todas las demás redes. Cualquier VPC nueva se conecta a la gateway de tránsito y luego queda disponible automáticamente para cualquier otra red que esté conectada a la gateway de tránsito. Esta facilidad para la conectividad simplifica el escalado de su red para acompañar el crecimiento.

## Actividad: Etiquetado del diagrama de red

aws academy

Este diagrama ilustra una arquitectura de red de VPC de AWS. Se muestra un VPC dividido en tres subnets:

- Subnet 1 (azul): IP: 10.0.1.0/24. Contiene un router (Q6) y una instancia de EC2 con Dirección IP: ?.
- Subnet 2 (verde): IP: 10.0.2.0/24. Contiene una instancia de EC2 con Dirección IP: ?.
- Subnet 3 (gris): IP: 10.0.0.0/16. Contiene un router (Q1) y una instancia de EC2 con Dirección IP: ?.

Las instancias de EC2 están conectadas a sus respectivos routers. Los routers están interconectados entre las subnets. Una conexión de salida sale de la Subnet 3 hacia la Internet, representada por una nube con flechas de subida y bajada.

Una tabla de rutas (Route Table) es mostrada en la parte inferior derecha:

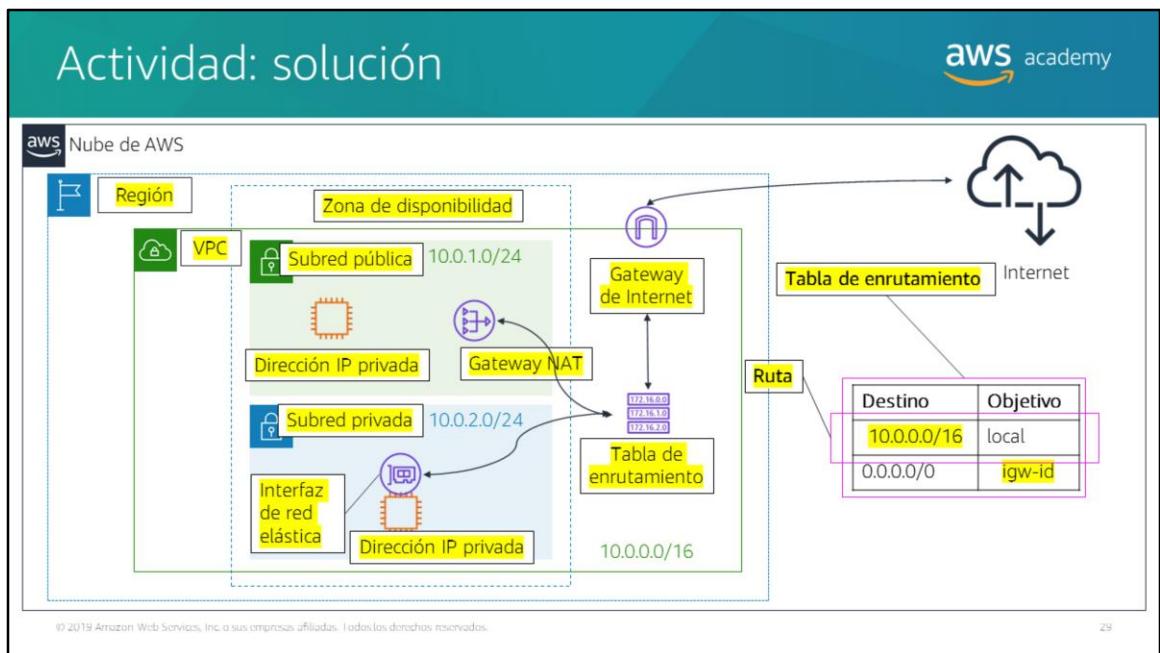
Destino	Objetivo
?	local
0.0.0.0/0	?

En el lado izquierdo, se muestra la interface de AWS CloudFormation con un diseño de nube.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

28

Compruebe que puede reconocer los distintos componentes de red de VPC sobre los que ha aprendido al etiquetar este diagrama de red.



Veamos cómo le fue.

The screenshot shows a dark-themed user interface for a recorded demonstration. On the left, a large dark blue panel displays the title "Demostración grabada de Amazon VPC" in white text. Below the title is a stylized graphic of green circuit board lines forming a perspective view. On the right, a white panel features the "aws academy" logo at the top. Below it, another "aws academy" logo is followed by the title "Configurar la demostración" in bold white text. Underneath the title, the subtitle "Amazon Virtual Private Cloud (VPC)" is displayed in a smaller white font. The bottom right corner of the white panel contains the number "50".

Ahora que sabe cómo diseñar una VPC, vea [esta demostración](#) y aprenda a utilizar el asistente de VPC para configurar una VPC con subredes públicas y privadas.



Aprendizajes clave de la sección 3

Takeaway

- Existen varias opciones de red de VPC, entre las que se incluyen:
  - Gateway de Internet
  - Gateway NAT
  - Punto de enlace de la VPC
  - Interconexión de VPC
  - Uso compartido de VPC
  - AWS Site-to-Site VPN
  - AWS Direct Connect
  - AWS Transit Gateway
- Puede utilizar el asistente de VPC para implementar su diseño.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Estos son algunos de los aprendizajes clave de esta sección del módulo:

- Existen varias opciones de red de VPC, entre las que se incluyen:
  - Gateway de Internet: conecta su VPC a Internet.
  - Gateway NAT: permite que las instancias de una subred privada se conecten a Internet.
  - Punto de enlace de la VPC: conecta la VPC a los servicios de AWS compatibles.
  - Interconexión de VPC: conecta su VPC a otras VPC.
  - Uso compartido de VPC: permite que varias cuentas de AWS creen sus recursos de aplicaciones en VPC de Amazon compartidas y administradas de forma centralizada.
  - AWS Site-to-Site VPN: conecta su VPC a redes remotas.
  - AWS Direct Connect: conecta su VPC a una red remota mediante una conexión de red dedicada.
  - AWS Transit Gateway: es una alternativa de conexión radial a la interconexión de VPC.
- Puede utilizar el asistente de VPC para implementar su diseño.

## Módulo 5: Redes y entrega de contenido

### Sección 4: Seguridad de VPC

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.



### Sección 4: Seguridad de VPC

Puede integrar la seguridad en su arquitectura de VPC de varias maneras para tener control total sobre el tráfico de entrada y de salida. En esta sección, aprenderá sobre dos opciones de firewall de Amazon VPC que puede utilizar para proteger su VPC: los grupos de seguridad y las listas de control de acceso a la red (ACL de red).

# Grupos de seguridad

Nube de AWS

aws academy

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Los grupos de seguridad funcionan en el **nivel de la instancia**.

Un *grupo de seguridad* funciona como un firewall virtual de la instancia para controlar el tráfico de entrada y de salida. Los grupos de seguridad actúan al nivel de la instancia, pero no en el de la subred. Por lo tanto, cada instancia de la subred de su VPC puede asignarse a un conjunto de grupos de seguridad diferente.

En el nivel más básico, un grupo de seguridad representa una forma de filtrar el tráfico hacia las instancias.

## Grupos de seguridad



Entrada				
Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
Todo el tráfico	Todo	Todo	sg-xxxxxxxx	
Salida				
Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
Todo el tráfico	Todo	Todo	sg-xxxxxxxx	

- Los grupos de seguridad tienen **reglas** que controlan el tráfico de entrada y de salida de las instancias.
- Los grupos de seguridad predeterminados **deniegan todo** el tráfico de **entrada** y permiten todo el tráfico de salida.
- Los grupos de seguridad **tienen estado**.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

54

Los grupos de seguridad tienen *reglas* que controlan el tráfico de entrada y de salida. Cuando se crea un grupo de seguridad, este carece de reglas de entrada. Por lo tanto, *no se permitirá el tráfico entrante que proceda de otro host hacia su instancia* hasta que agregue reglas de entrada al grupo de seguridad. De forma predeterminada, los grupos de seguridad incluyen una regla de salida que *permite todo el tráfico saliente*. Es posible quitar esta regla y agregar reglas de salida que permitan solo tráfico saliente específico. Si el grupo de seguridad no tiene reglas de salida, no se permitirá el tráfico saliente que proceda de su instancia.

Los grupos de seguridad tienen *estado*, lo que significa que la información de estado se conserva incluso después de que se procese una solicitud. Por ese motivo, si envía una solicitud desde su instancia, se permite el flujo entrante de tráfico de respuesta para dicha solicitud, independientemente de las reglas de entrada del grupo de seguridad. El flujo saliente de las respuestas al tráfico entrante está permitido independientemente de las reglas de salida.

## Grupos de seguridad personalizados



Entrada				
Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
HTTP	TCP	80	0.0.0.0/0	Todo el tráfico web
HTTPS	TCP	443	0.0.0.0/0	Todo el tráfico web
SSH	TCP	22	54.24.12.19/32	Dirección de la oficina

Salida				
Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
Todo el tráfico	Todo	Todo	0.0.0.0/0	
Todo el tráfico	Todo	Todo	::/0	

- Puede **especificar reglas de permiso**, pero no reglas de denegación.
- **Todas las reglas se evalúan** antes de decidir si se permite el tráfico o no.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

55

Cuando crea un grupo de seguridad personalizado, puede especificar reglas de permiso, pero no reglas de denegación. Todas las reglas se evalúan antes de decidir si se permite el tráfico o no.

## Listas de control de acceso a la red (ACL de red)

The diagram illustrates a VPC network structure. It shows a 'Región' (Region) containing a 'Zona de disponibilidad' (Availability Zone). Inside the AZ, there is a 'VPC: 10.0.0.0/16'. This VPC contains two subnets: a 'Subred pública: 10.0.0.0/24' (Public subnet) and a 'Subred privada: 10.0.4.0/22' (Private subnet). Each subnet has its own ACL icon (represented by a square with a lock and arrows) located to its right. A callout arrow points from the text 'Las ACL de red funcionan en el nivel de la subred.' to the ACL icons on the subnets.

Nube de AWS

Región

Zona de disponibilidad

VPC: 10.0.0.0/16

Subred pública: 10.0.0.0/24

Subred privada: 10.0.4.0/22

aws academy

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Las ACL de red funcionan en el nivel de la subred.

Una *lista de control de acceso a la red (ACL de red)* es una capa de seguridad opcional para su Amazon VPC. Actúa como firewall para controlar el tráfico que entra y sale de una o más subredes. Para agregar una capa de seguridad adicional a su VPC, puede configurar ACL de red con reglas similares a sus grupos de seguridad.

Cada subred de su VPC debe estar asociada a una ACL de red. Si no asocia una subred de forma explícita a una ACL de red, la subred se asociará automáticamente a la ACL de red predeterminada. Puede asociar una ACL de red a varias subredes; sin embargo, una subred solo se puede asociar a una ACL de red a la vez. Cuando se asocia una ACL de red a una subred, se elimina la asociación anterior.

## ACL de red



Entrada					
N.º de regla	Tipo	Protocolo	Intervalo de puertos	Origen	Permitir/Denegar
100	Todo el tráfico IPv4	Todo	Todo	0.0.0.0/0	PERMITIR
*	Todo el tráfico IPv4	Todo	Todo	0.0.0.0/0	DENEGAR
Salida					
N.º de regla	Tipo	Protocolo	Intervalo de puertos	Origen	Permitir/Denegar
100	Todo el tráfico IPv4	Todo	Todo	0.0.0.0/0	PERMITIR
*	Todo el tráfico IPv4	Todo	Todo	0.0.0.0/0	DENEGAR

- Una ACL de red tiene **reglas de entrada y de salida independientes**, y cada regla puede **permitir o denegar tráfico**.
- Las ACL de red** predeterminadas permiten **todo el tráfico IPv4 de entrada y de salida**.
- Las ACL de red **no tienen estado**.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

5 /

Una ACL de red tiene reglas de entrada y de salida independientes, y cada regla puede permitir o denegar tráfico. Su VPC incluye automáticamente una ACL de red predeterminada y modificable. De forma predeterminada, permite todo el tráfico IPv4 de entrada y de salida, además, si corresponde, del tráfico IPv6. La tabla muestra una ACL de red predeterminada.

Las *ACL de red* no tienen estado, lo que significa que no se mantiene información sobre una solicitud después de procesarla.

## ACL de red personalizadas



Entrada					
N.º de regla	Tipo	Protocolo	Intervalo de puertos	Origen	Permitir/Denegar
103	SSH	TCP	22	0.0.0.0/0	PERMITIR
100	HTTPS	TCP	443	0.0.0.0/0	PERMITIR
*	Todo el tráfico IPv4	Todo	Todo	0.0.0.0/0	DENEGAR

Salida					
N.º de regla	Tipo	Protocolo	Intervalo de puertos	Origen	Permitir/Denegar
103	SSH	TCP	22	0.0.0.0/0	PERMITIR
100	HTTPS	TCP	443	0.0.0.0/0	PERMITIR
*	Todo el tráfico IPv4	Todo	Todo	0.0.0.0/0	DENEGAR

- Las [ACL de red](#) personalizadas deniegan todo el tráfico de entrada y de salida hasta que se agregan reglas.
- Puede especificar reglas [de permiso y de denegación](#).
- Las reglas se evalúan según el orden numérico, comenzando por el [número más bajo](#).

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

58

Puede crear una ACL de red personalizada y asociarla a una subred. De forma predeterminada, todas las ACL de red personalizadas denegarán todo el tráfico de entrada y de salida hasta que agregue reglas.

Una ACL de red contiene una lista numerada de reglas que se evalúan en orden, empezando por la regla con el número más bajo. El objetivo es determinar si el tráfico tiene permitido entrar o salir de toda subred asociada a la ACL de red. El número más alto que puede utilizar para una regla es 32 766. AWS recomienda crear reglas en incrementos (por ejemplo, incrementos de 10 o 100) para que pueda insertar nuevas reglas cuando las necesite más adelante.

Para obtener más información acerca de las ACL de red, consulte [ACL de red](#) en la documentación de AWS.

Comparación entre grupos de seguridad y ACL de red		
Atributo	Grupos de seguridad	ACL de red
Alcance	Nivel de la instancia	Nivel de la subred
Reglas admitidas	Solo reglas de permiso	Reglas de permiso y de denegación
Estado	Con estado (el tráfico de retorno se permite automáticamente, sin importar las reglas)	Sin estado (las reglas deben permitir de forma explícita el tráfico de retorno)
Orden de las reglas	Todas las reglas se evalúan antes de decidir si se permite el tráfico	Las reglas se evalúan según el orden numérico antes de decidir si se permite el tráfico

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

59

A continuación, se muestra un resumen de las diferencias entre los grupos de seguridad y las ACL de red:

- Los grupos de seguridad actúan en el nivel de la instancia, pero las ACL de red lo hacen en el nivel de la subred.
- Los grupos de seguridad solo admiten reglas de permiso, pero las ACL de red admiten tanto reglas de permiso como de denegación.
- Los grupos de seguridad tienen estado, pero las ACL de red no tienen estado.
- Para los grupos de seguridad, todas las reglas se evalúan antes de que se tome la decisión de permitir el tráfico. Para las ACL de red, las reglas se evalúan en orden numérico antes de que se tome la decisión de permitir el tráfico.

## Actividad: Diseño de una VPC



**Situación:** tiene una pequeña empresa con un sitio web alojado en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Tiene datos de clientes almacenados en una base de datos de backend que quiere mantener en privado. Desea utilizar Amazon VPC para configurar una VPC que cumpla los siguientes requisitos:

- El servidor web y el servidor de base de datos deben estar en subredes independientes.
- La primera dirección de la red debe ser 10.0.0.0. Cada subred debe tener un total de 256 direcciones IPv4.
- Sus clientes deben tener acceso a su servidor web en todo momento.
- El servidor de base de datos debe tener acceso a Internet para realizar actualizaciones con parches.
- La arquitectura debe tener una alta disponibilidad y utilizar al menos una capa de firewall personalizada.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

40

¡Ahora es su turno! En este caso, es propietario de una pequeña empresa con un sitio web alojado en una instancia de Amazon Elastic Compute Cloud (Amazon EC2). Tiene datos de clientes almacenados en una base de datos de backend que quiere mantener en privado.

Compruebe si puede diseñar una VPC que cumpla los siguientes requisitos:

- El servidor web y el servidor de base de datos deben estar en subredes independientes.
- La primera dirección de la red debe ser 10.0.0.0. Cada subred debe tener 256 direcciones IPv4.
- Sus clientes deben tener acceso a su servidor web en todo momento.
- El servidor de base de datos debe tener acceso a Internet para realizar actualizaciones con parches.
- La arquitectura debe tener una alta disponibilidad y utilizar al menos una capa de firewall personalizada.

## Aprendizajes clave de la sección 4



41



- Incorpore seguridad en su arquitectura de VPC:
  - Aíslle las subredes si es posible.
  - Elija el dispositivo de gateway o la conexión de VPN adecuados para sus necesidades.
  - Utilice firewalls.
- Los grupos de seguridad y las ACL de red son opciones de firewall que puede utilizar para proteger su VPC.

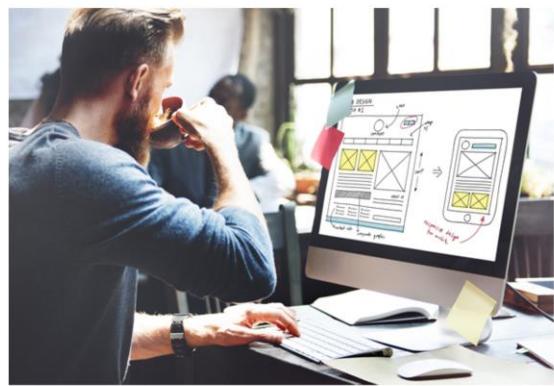
© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Los aprendizajes clave de esta sección del módulo son los siguientes:

- Incorpore seguridad en su arquitectura de VPC.
- Los grupos de seguridad y las ACL de red son opciones de firewall que puede utilizar para proteger su VPC.

## Laboratorio 2: Creación de una VPC y lanzamiento de un servidor web

42

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Ahora trabajará en el Laboratorio 2: Creación de una VPC y lanzamiento de un servidor web.

## Laboratorio 2: situación



En este laboratorio, utilizará Amazon VPC a fin de [crear su propia VPC](#) y agregarle algunos componentes para generar una red personalizada. Debe [crear un grupo de seguridad](#) para su VPC. También debe [crear una instancia EC2 y configurarla](#) para que ejecute un servidor web y utilice el grupo de seguridad. Después de esto, debe lanzar la instancia EC2 en la VPC.



Amazon  
VPC



Amazon  
EC2

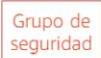
© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

4.5

En este laboratorio, utilizará Amazon VPC a fin de crear su propia VPC y agregarle algunos componentes para generar una red personalizada. También debe crear un grupo de seguridad para su VPC y, a continuación, crear una instancia EC2 y configurarla para que ejecute un servidor web y utilice el grupo de seguridad. Después de esto, debe lanzar la instancia EC2 en la VPC.

## Laboratorio 2: tareas



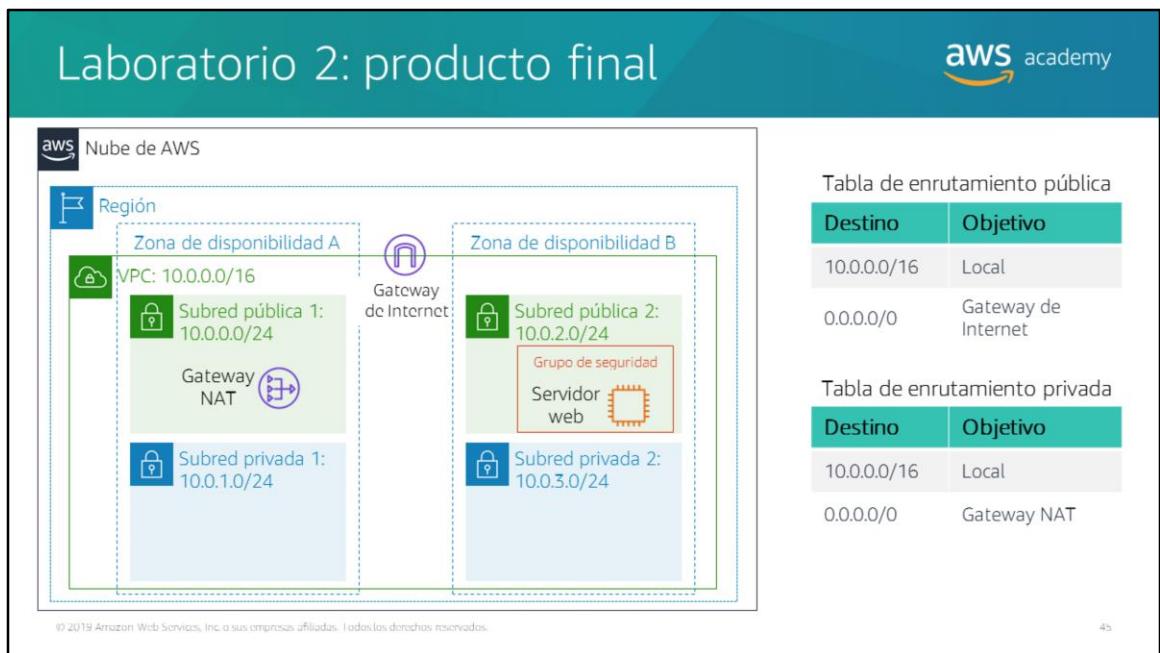
-  • Crear una VPC.
-  • Cree subredes adicionales.
-  **Grupo de seguridad** • Cree un grupo de seguridad de VPC.
-  • Lance una instancia de servidor web.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

44

En este laboratorio, completará las siguientes tareas:

- Crear una VPC.
- Crear subredes adicionales.
- Crear un grupo de seguridad de VPC.
- Lanzar una instancia de servidor web.



Este diagrama de arquitectura muestra lo que creará en el laboratorio.

A screenshot of a learning module from AWS Academy. The top left features a timer icon and the text "Aprox. 30 minutos". The top right has the AWS Academy logo. The main title on the right is "Comience el Laboratorio 2: Creación de una VPC y lanzamiento de un servidor web". The background image shows a blue cup of coffee next to a wooden scoop filled with coffee beans.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

4b

Ha llegado el momento de iniciar el laboratorio. Debería tardar aproximadamente 30 minutos en completarlo.



## Análisis posterior del laboratorio: aprendizajes clave



© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

4 /

En este laboratorio, hizo lo siguiente:

- Crear una Amazon VPC
- Crear subredes adicionales.
- Crear un grupo de seguridad de Amazon VPC
- Lanzar una instancia de servidor web en Amazon EC2

## Módulo 5: Redes y entrega de contenido

### Sección 5: Amazon Route 53

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.



### Sección 5: Amazon Route 53

## Amazon Route 53



Amazon  
Route 53

- Es un servicio web de DNS (Sistema de nombres de dominio) de gran disponibilidad y escalabilidad.
- Se utiliza para redirigir a los usuarios finales a las aplicaciones en Internet mediante la traducción de nombres (como [www.ejemplo.com](http://www.ejemplo.com)) en direcciones IP numéricas (como 192.0.2.1) que los equipos utilizan con el objetivo de conectarse entre ellos.
- Es totalmente compatible con IPv4 e IPv6.
- Conecta las solicitudes de los usuarios a la infraestructura que se ejecuta en AWS y también fuera de AWS.
- Se utiliza para comprobar el estado de los recursos.
- Cuenta con una característica para el flujo de tráfico.
- Permite registrar nombres de dominio.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

49

Amazon Route 53 es un servicio web del [sistema de nombres de dominio \(DNS\)](#) con gran escalabilidad y disponibilidad en la nube. Está diseñado para ofrecer a los desarrolladores y a las empresas una forma confiable y rentable de dirigir a los usuarios a las aplicaciones de Internet mediante la traducción de nombres (como [www.example.com](http://www.example.com)) en direcciones IP numéricas (como 192.0.2.1) que los equipos utilizan para conectarse entre ellos. Además, Amazon Route 53 es totalmente compatible con IPv6.

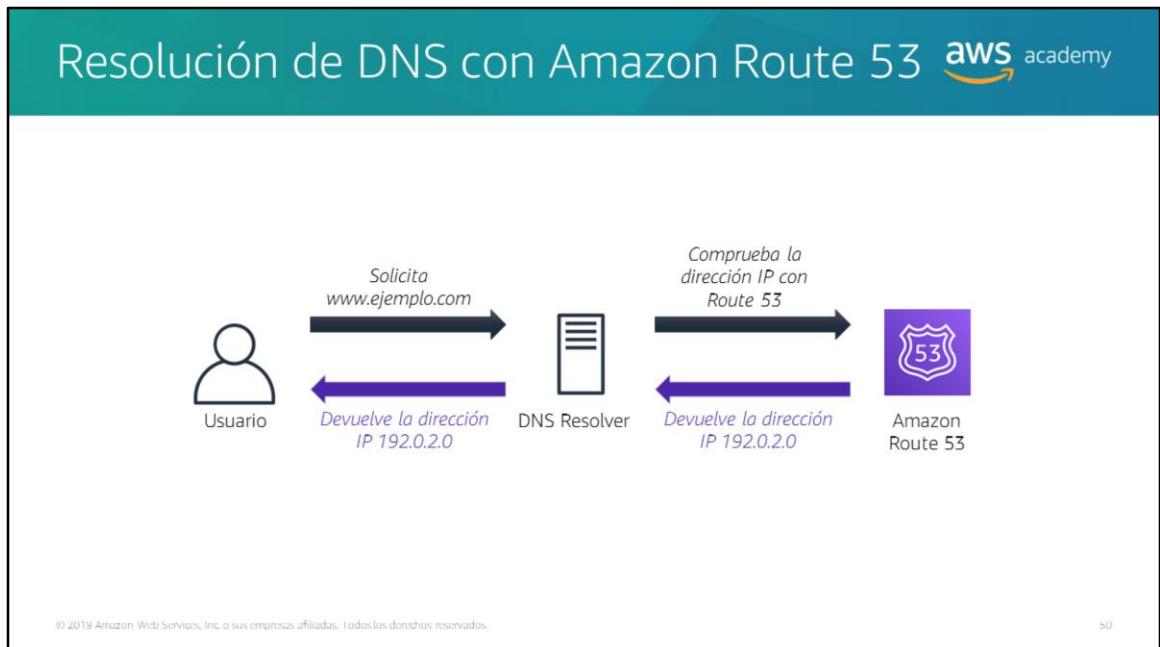
Amazon Route 53 conecta de forma efectiva las solicitudes del usuario con la infraestructura que se ejecuta en AWS, como las instancias de Amazon EC2, los balanceadores de carga de Elastic Load Balancing o los buckets de Amazon S3. También puede utilizarse para dirigir a los usuarios a las infraestructuras fuera de AWS.

Puede utilizar Amazon Route 53 para configurar comprobaciones de estado de DNS a fin de redirigir el tráfico a los puntos de enlace en buen estado o monitorear de manera independiente el estado de la aplicación y sus puntos de enlace.

La característica de flujo de tráfico de Amazon Route 53 le permite administrar el tráfico globalmente a través de varios tipos de direccionamiento, los cuales se

pueden combinar con la conmutación por error a nivel de DNS para habilitar varias arquitecturas de baja latencia y tolerantes a errores. Puede utilizar el sencillo editor visual del flujo de tráfico de Amazon Route 53 para administrar el modo en que se redirige a los usuarios hacia los puntos de enlace de su aplicación, ya sea en una sola región de AWS o en todo el mundo.

Amazon Route 53 también ofrece el registro de nombre de dominio. Puede adquirir y administrar nombres de dominio (como *ejemplo.com*), y Amazon Route 53 configurará automáticamente los ajustes de DNS para sus dominios.



Aquí observamos el patrón básico que sigue Amazon Route 53 cuando un usuario inicia una solicitud DNS. Para la resolución de DNS, se comprueba el dominio en Route 53, se obtiene la dirección IP y se la devuelve al usuario.

## Direccionamiento admitido por Amazon Route 53



- **Direccionamiento sencillo:** utilícelo en entornos de un solo servidor.
- **Direccionamiento de turno rotativo ponderado:** asigne ponderaciones a los conjuntos de registros de recursos para especificar la frecuencia.
- **Direccionamiento basado en la latencia:** utilícelo para mejorar las aplicaciones con nivel mundial.
- **Direccionamiento por geolocalización:** dirija el tráfico en función de la ubicación de los usuarios.
- **Direccionamiento por geoproximidad:** dirija el tráfico en función de la ubicación de los recursos.
- **Direccionamiento tras commutación por error:** realice la commutación por error a un sitio de copia de seguridad si ya no se puede acceder al sitio principal.
- **Direccionamiento de respuesta con varios valores:** responda a consultas DNS con hasta ocho registros en buen estado que se seleccionan al azar.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

51

Amazon Route 53 admite varios tipos de políticas de direccionamiento, las cuales determinan cómo Amazon Route 53 responde a las consultas:

- *Direccionamiento simple (turno rotativo):* se utiliza para un único recurso que realiza una función determinada para su dominio (por ejemplo, un servidor web que ofrece contenido para el sitio web ejemplo.com).
- *Direccionamiento de turno rotativo ponderado:* se utiliza para dirigir el tráfico a varios recursos en las proporciones que especifique. Le permite asignar ponderaciones a conjuntos de registros de recursos para especificar la frecuencia con la que se ofrecen diferentes respuestas. Es posible que quiera utilizar esta capacidad para realizar pruebas A/B, en las que envía una pequeña porción del tráfico a un servidor en el que realizó un cambio de software. Por ejemplo, supongamos que cuenta con dos conjuntos de registros asociados a un mismo nombre de DNS: uno con ponderación 3 y el otro con ponderación 1. En este caso, el 75 % del tiempo, Amazon Route 53 devolverá el conjunto de registros que tenga la ponderación 3, y el 25 % de las veces, lo hará con el conjunto de registros que tenga la ponderación 1. El número de ponderaciones puede oscilar entre 0 y 255.
- *Direccionamiento basado en la latencia (LBR):* se utiliza si tiene recursos en varias regiones de AWS y desea dirigir el tráfico a la región que proporciona la mejor latencia. El direccionamiento basado en la latencia se encarga de dirigir a los

clientes al punto de enlace de AWS (por ejemplo, instancias de Amazon EC2, direcciones IP elásticas o balanceadores de carga) que ofrece la experiencia más rápida en función de las mediciones de rendimiento real de las distintas regiones de AWS donde se ejecuta la aplicación.

- *Direccionamiento por geolocalización*: se utiliza cuando desea dirigir el tráfico en función de la ubicación de los usuarios. Al usar este tipo de direccionamiento, puede ubicar el contenido de su sitio web y presentarlo de forma parcial o total en el idioma de sus usuarios. También puede usar el direccionamiento basado en geolocalización para limitar la distribución de contenido a solo las ubicaciones para las que tenga derechos de distribución. Otro uso que se le puede dar es el balanceo de carga entre puntos de enlace de una forma predecible y fácil de administrar, para que la ubicación de cada usuario se dirija uniformemente al mismo punto de enlace.
- *Direccionamiento por geoproximidad*: se utiliza si desea dirigir el tráfico en función de la ubicación de los recursos y, opcionalmente, desviar el tráfico desde los recursos de una ubicación a los de otra.
- *Direccionamiento tras conmutación por error (a nivel de DNS)*: se utiliza si desea configurar la conmutación por error activa-pasiva. Amazon Route 53 lo ayuda a detectar interrupciones en su sitio web y a redirigir a los usuarios hacia ubicaciones alternativas donde la aplicación funcione de manera adecuada. Cuando habilite esta característica, los agentes de comprobación de estado de Amazon Route 53 monitorearán cada ubicación o punto de enlace de la aplicación para determinar su disponibilidad. Puede aprovechar esta característica para incrementar la disponibilidad de la aplicación orientada a los clientes.
- *Direccionamiento de respuesta con varios valores*: se utiliza si desea que Route 53 responda a consultas DNS con hasta ocho registros en buen estado que se seleccionan al azar. Puede configurar Amazon Route 53 para que devuelva varios valores, como direcciones IP para sus servidores web, en respuesta a las consultas DNS. Puede especificar varios valores para casi cualquier registro, pero el direccionamiento de respuesta con varios valores también le permite revisar el estado de cada recurso, para que Route 53 devuelva solo los valores correspondientes a los recursos en buen estado. Si bien no sustituye a un balanceador de carga, la capacidad de devolver varias direcciones IP cuyo estado sea comprobable constituye una forma de utilizar el DNS para mejorar la disponibilidad y el balanceo de carga.

## Caso de uso: implementación en varias regiones

aws academy

La implementación en varias regiones es un caso de uso de Amazon Route 53 que sirve como ejemplo. Con Amazon Route 53, se dirige al usuario automáticamente al balanceador de carga de Elastic Load Balancing que se encuentre más cerca del usuario.

Entre los beneficios de la implementación en varias regiones de Route 53, se incluyen los siguientes:

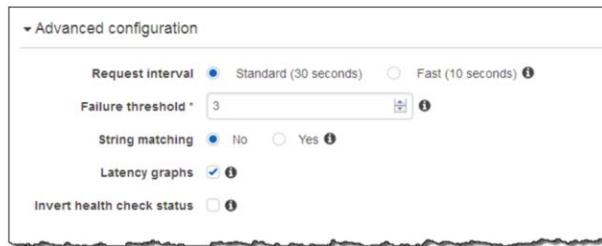
- Direccionamiento basado en la latencia hacia la región
- Direccionamiento del balanceo de carga hacia la zona de disponibilidad

## Conmutación por error a nivel de DNS de Amazon Route 53



Mejore la disponibilidad de las aplicaciones que se ejecutan en AWS de las siguientes formas:

- Configuración de las situaciones de copia de seguridad y de conmutación por error para sus propias aplicaciones
- Habilitación de las arquitecturas en varias regiones de alta disponibilidad en AWS
- Creación de comprobaciones de estado

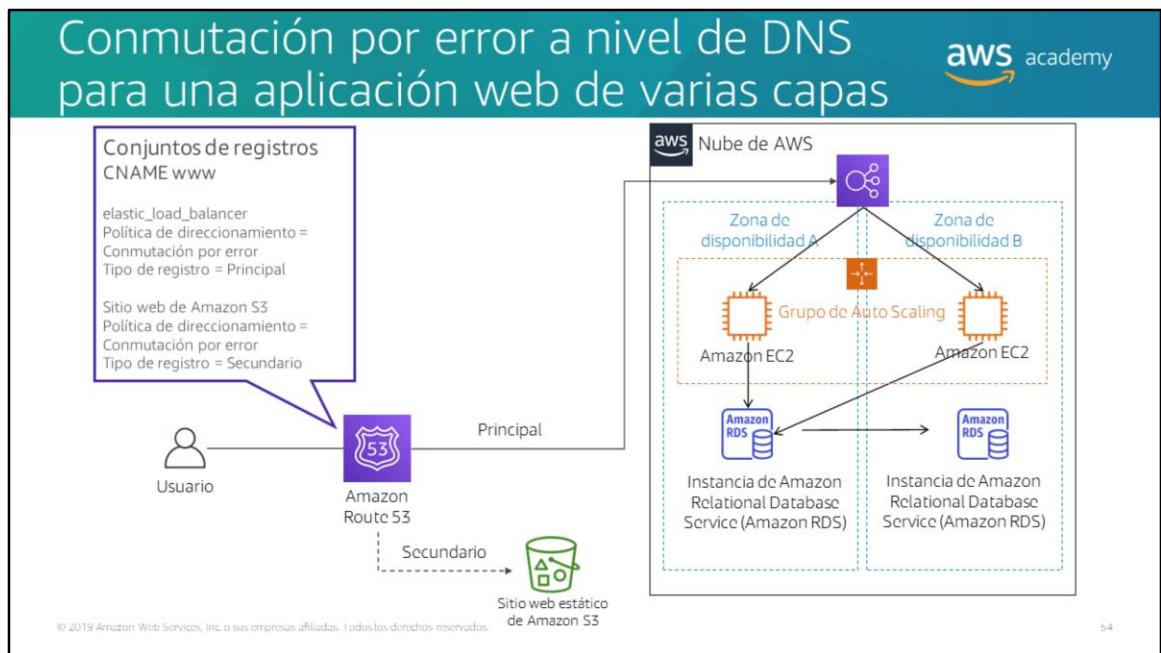


© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

5.5

Amazon Route 53 le permite mejorar la disponibilidad de las aplicaciones que se ejecutan en AWS a través de las siguientes acciones:

- Configuración de las situaciones de copia de seguridad y conmutación por error de sus propias aplicaciones
- Habilitación de las arquitecturas en varias regiones con alta disponibilidad en AWS
- Creación de comprobaciones de estado para monitorear el estado y el rendimiento de sus aplicaciones web, servidores web y otros recursos. Cada comprobación de estado que cree puede monitorear el estado de una de las siguientes opciones: el de un recurso específico, como un servidor web; el de otras comprobaciones de estado; y el de una alarma de Amazon CloudWatch.



Aquí, se muestra cómo funciona la comutación por error a nivel de DNS en la arquitectura habitual de una aplicación web con varios niveles. Route 53 transfiere el tráfico a un平衡器 de carga, el cual luego lo distribuye en una flota de instancias EC2.

Para garantizar la alta disponibilidad, puede realizar las siguientes tareas con Route 53:

1. Cree dos registros de DNS para el Registro de nombre canónico (CNAME) www con una política de *direcciónamiento tras comutación por error*. El primer registro es la política de direcciónamiento principal, la cual lleva al balanceador de carga de su aplicación web. El segundo registro es la política de direcciónamiento secundaria que lleva al sitio web estático de Amazon S3.
2. Utilice las comprobaciones de estado de Route 53 para asegurarse de que la política principal se esté ejecutando. Si es así, se dirigirá todo el tráfico a la pila de aplicaciones web de forma predeterminada. La comutación por error al sitio de copia de seguridad estático se activaría si el servidor web dejara de funcionar (o se bloqueara) o si fuera la instancia de base de datos la que no funciona más.

## Aprendizajes clave de la sección 5



55

aws academy

- Amazon Route 53 es un servicio web de DNS en la nube con gran escalabilidad y disponibilidad que convierte los nombres de dominio en direcciones IP numéricas.
- Amazon Route 53 admite varios tipos de políticas de direccionamiento.
- La implementación en varias regiones mejora el rendimiento de la aplicación para un público internacional.
- Puede utilizar la conmutación por error de Amazon Route 53 para mejorar la disponibilidad de sus aplicaciones.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Estos son algunos de los aprendizajes clave de esta sección del módulo:

- Amazon Route 53 es un servicio web de DNS en la nube con gran escalabilidad y disponibilidad que convierte los nombres de dominio en direcciones IP numéricas.
- Amazon Route 53 admite varios tipos de políticas de direccionamiento.
- La implementación en varias regiones mejora el rendimiento de la aplicación para un público internacional.
- Puede utilizar la conmutación por error de Amazon Route 53 para mejorar la disponibilidad de sus aplicaciones.

## Módulo 5: Redes y entrega de contenido

### Sección 6: Amazon CloudFront

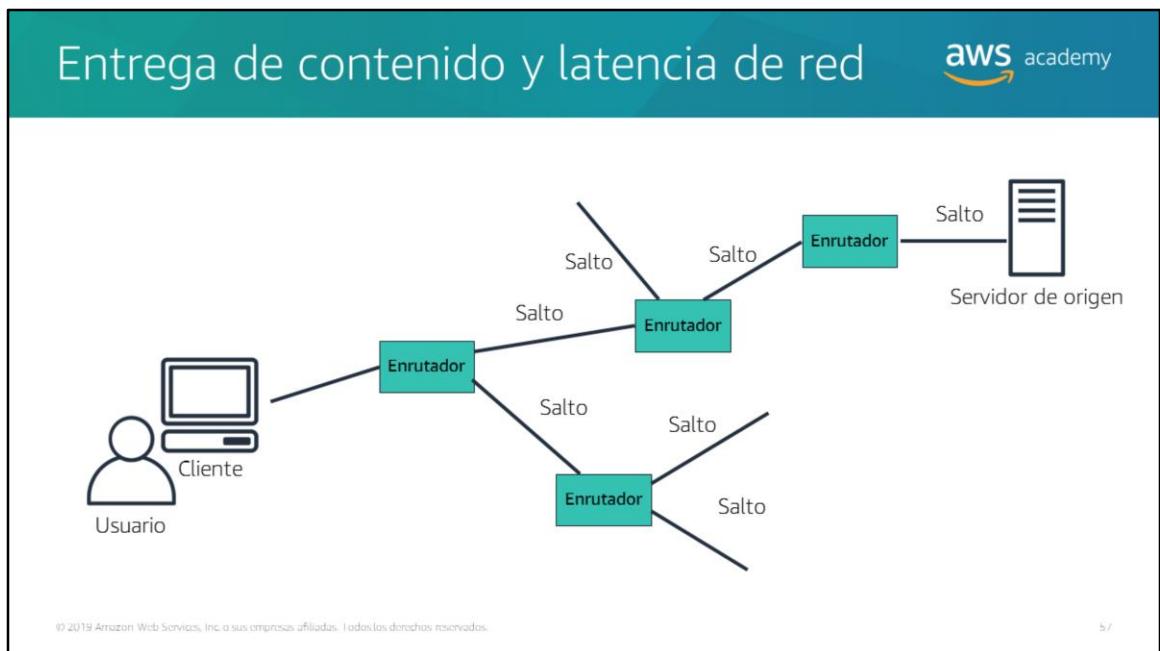
© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.



### Sección 6: Amazon CloudFront

El objetivo de las redes es compartir información entre los recursos conectados. Hasta ahora, en este módulo ha aprendido acerca de las redes de VPC con Amazon VPC. Aprendió también sobre las diferentes opciones para conectar su VPC a Internet, a redes remotas, a otras VPC y a los servicios de AWS.

La entrega de contenido también se produce a través de redes, por ejemplo, cuando transmite una película desde su servicio de streaming favorito. En esta última sección, aprenderá sobre Amazon CloudFront, que es un servicio de la red de entrega de contenido (CDN).



Como se explicó anteriormente en este módulo cuando analizábamos el tema de AWS Direct Connect, uno de los desafíos de la comunicación de red es el rendimiento de la red. Cuando navega por un sitio web o transmite un video, su solicitud se dirige a través de muchas redes diferentes hasta llegar a un servidor de origen. El servidor de origen (u origen) almacena las versiones originales y definitivas de los objetos (páginas web, imágenes y archivos multimedia). El número de saltos de red y la distancia que debe recorrer la solicitud afectan significativamente al rendimiento y a la capacidad de respuesta del sitio web. Además, la latencia de red es diferente en las distintas ubicaciones geográficas. Por estas razones, una red de entrega de contenido podría ser la solución.

## Red de entrega de contenido (CDN)



- Es un sistema distribuido a nivel mundial de servidores de almacenamiento en caché.
- Almacena en caché copias de archivos solicitados habitualmente (contenido estático).
- Entrega una copia local del contenido solicitado desde un borde de caché cercano o punto de presencia.
- Acelera la entrega de contenido dinámico.
- Mejora el rendimiento y el escalado de las aplicaciones.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

58

Una red de entrega de contenido (CDN) es un sistema de servidores de almacenamiento en caché distribuido a nivel mundial. Una CDN almacena en caché copias de archivos solicitados habitualmente (contenido estático, como Hypertext Markup Language o HTML; hojas de estilo en cascada o CSS; JavaScript; y archivos de imagen) que se alojan en el servidor de origen de la aplicación. La CDN entrega una copia local del contenido solicitado desde una ubicación de borde o un punto de presencia de caché que proporciona la entrega más rápida al solicitante.

Las CDN también entregan contenido dinámico que es exclusivo del solicitante y que no se puede almacenar en caché. Disponer de una CDN de entrega de contenido dinámico mejora el rendimiento y el escalado de la aplicación. La CDN establece y mantiene conexiones seguras más cerca del solicitante. Si la CDN está en la misma red que el origen, se acelera el direccionamiento de regreso al origen para recuperar contenido dinámico. Además, ciertos contenidos, como los datos de formularios, las imágenes y los textos, se pueden incorporar y enviar de regreso al origen, por lo que se aprovechan así las conexiones de baja latencia y el comportamiento de proxy del punto de presencia.

## Amazon CloudFront



Amazon  
CloudFront

- Servicio de CDN rápido, mundial y seguro
- Red global de ubicaciones de borde y cachés de borde regionales
- Modelo de autoservicio
- Precios de pago por uso

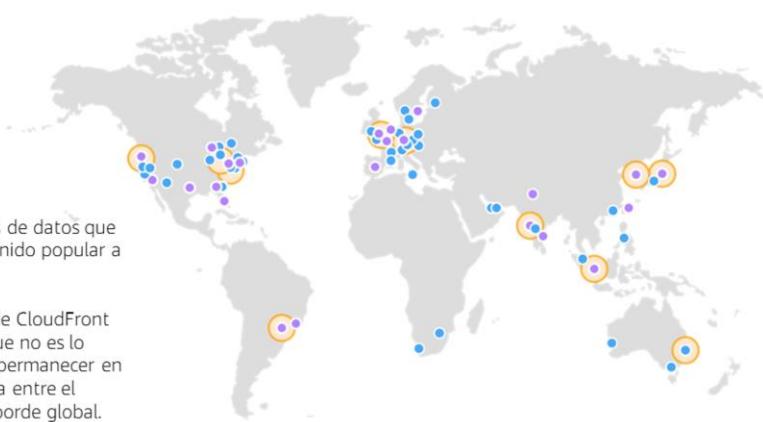
© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

59

Amazon CloudFront es un servicio rápido de CDN que entrega datos, videos, aplicaciones e interfaces de programación de aplicaciones (API) de manera segura a clientes de todo el mundo con baja latencia y altas velocidades de transferencia.

También proporciona un entorno idóneo para desarrolladores. Amazon CloudFront entrega archivos a los usuarios a través de una red mundial de ubicaciones de borde y cachés de borde regionales. Es diferente de las soluciones tradicionales de entrega de contenido, ya que le permite obtener rápidamente los beneficios de una entrega de contenido de alto rendimiento sin contratos, precios elevados ni tarifas mínimas. Al igual que otros servicios de AWS, Amazon CloudFront es una oferta de autoservicio con precios de pago por uso.

## Infraestructura de Amazon CloudFront



The map illustrates the global distribution of CloudFront infrastructure. It shows several clusters of points across continents, representing different types of edge locations:

- Ubicaciones de borde (blue dots): Global edge locations.
- Varias ubicaciones de borde (purple dots): Multi-origin edge locations.
- Cachés de borde regionales (orange circles): Regional edge caches.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Amazon CloudFront entrega el contenido a través de una red mundial de centros de datos que reciben el nombre de *ubicaciones de borde*. Cuando un usuario solicita contenido que se distribuye con CloudFront, se lo dirige a la ubicación de borde que presente la menor latencia (o retardo) para entregar el contenido con el mayor rendimiento posible. Las ubicaciones de borde de CloudFront están diseñadas para ofrecer contenido popular a sus espectadores con rapidez.

A medida que los objetos se hacen menos populares, las ubicaciones de borde individuales podrán eliminarlos a fin de liberar espacio para el contenido más solicitado. Para el contenido menos popular, CloudFront dispone de *cachés de borde regionales*. Las cachés de borde regionales son ubicaciones de CloudFront que se implementan a nivel mundial y están cerca de sus espectadores. Están ubicadas entre el servidor de origen y las ubicaciones de borde globales que distribuyen contenido directamente a los espectadores. Una caché de borde regional tiene una memoria caché más grande que una ubicación de borde individual, por lo que los objetos permanecen en la caché de borde regional durante más tiempo. Mayor cantidad de su contenido permanece más cerca de los espectadores, lo que reduce la necesidad de que CloudFront vuelva al servidor de origen y mejora el rendimiento general para los espectadores.

Para obtener más información sobre cómo funciona Amazon CloudFront, consulte [Cómo CloudFront entrega contenido](#) en la documentación de AWS.

## Beneficios de Amazon CloudFront



- Rapidez y alcance mundial
- Seguridad en el borde
- Alta capacidad de programación
- Integración total con AWS
- Rentabilidad

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

b1

Amazon CloudFront proporciona los siguientes beneficios:

- *Rapidez y alcance mundial*: Amazon CloudFront se escala de forma masiva y se distribuye globalmente. Para entregar contenido a los usuarios finales con baja latencia, Amazon CloudFront utiliza una red mundial que está compuesta por ubicaciones de borde y cachés regionales.
- *Seguridad en el borde* : Amazon CloudFront brinda protección tanto a nivel de red como a nivel de aplicación. Las aplicaciones y el tráfico se ven beneficiados por distintas protecciones integradas, como AWS Shield Standard, sin costo adicional. También puede utilizar características configurables, como AWS Certificate Manager (ACM), para crear y administrar certificados de capa de conexión segura (SSL) personalizados sin costo adicional.
- *Alta capacidad de programación*: las características de Amazon CloudFront se pueden personalizar en función de los requisitos específicos de sus aplicaciones. Se integra con Lambda@Edge para que pueda ejecutar código personalizado en ubicaciones de AWS de todo el mundo, lo que le permite acercar la lógica de aplicación compleja a los usuarios para mejorar la capacidad de respuesta. La CDN también admite integraciones con otras herramientas e interfaces de automatización para DevOps. Ofrece entornos de integración y entrega continuas (CI/CD).

- *Integración completa con AWS:* Amazon CloudFront se integra con AWS, tanto con ubicaciones físicas conectadas directamente a la infraestructura global de AWS como con otros servicios de AWS. Puede utilizar las API o la consola de administración de AWS para configurar mediante programación todas las características de la CDN.
- *Rentabilidad:* Amazon CloudFront es rentable porque no tiene compromisos mínimos y solo le cobra por lo que usa. En comparación con el autoalojamiento, Amazon CloudFront evita los gastos y la complejidad de operar una red de servidores de caché en varios sitios de Internet. Elimina la necesidad de aprovisionar en exceso la capacidad para atender posibles picos de tráfico. Amazon CloudFront también usa técnicas, como agrupar solicitudes simultáneas del espectador en una ubicación de borde para el mismo archivo en una sola solicitud al servidor de origen. El resultado es una reducción de la carga en los servidores de origen y una menor necesidad de escalar la infraestructura de origen, lo que puede traducirse en un mayor ahorro de costos. Si utiliza servicios de origen de AWS, como Amazon Simple Storage Service (Amazon S3) o Elastic Load Balancing, paga solo por los costos de almacenamiento y no por los datos transferidos entre estos servicios y CloudFront.

# Precios de Amazon CloudFront



## Transferencia saliente de datos

- Se cobra por el volumen de datos transferidos desde la ubicación de borde de Amazon CloudFront a Internet o a su origen.

## Solicitudes HTTP(S)

- Se cobra por la cantidad de solicitudes HTTP(S).

## Solicitudes de anulación

- Las primeras 1000 rutas para solicitudes de anulación al mes no incurren en ningún tipo de costo adicional. A partir de entonces, se cobra 0,005 USD por ruta solicitada para anulación.

## Capa de conexión segura (SSL) personalizada con IP dedicada

- Deberá pagar 600 USD al mes por cada certificado SSL personalizado que esté asociado a una o más distribuciones de CloudFront con uso de la versión de IP dedicada del soporte para certificados SSL personalizados.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

b2

Los cargos de Amazon CloudFront se basan en el uso real del servicio en las siguientes cuatro áreas:

- *Transferencia saliente de datos*: se le cobrará por el volumen de datos que se transfiera desde las ubicaciones de borde de Amazon CloudFront, medido en GB, hacia Internet o hacia su origen (tanto orígenes de AWS como otros servidores de origen). El uso de la transferencia de datos se suma por separado para cada región geográfica en particular y, a continuación, el costo se calcula en función de las capas de precios de cada área. Si utiliza otros servicios de AWS como orígenes de sus archivos, se le cobrará de manera independiente el uso de dichos servicios, que incluyen las horas de cómputo y el almacenamiento.
- *Solicitudes HTTP(S)*: se le cobrará por la cantidad de solicitudes HTTP(S) que se realicen a Amazon CloudFront para su contenido.
- *Solicitudes de anulación*: se le cobrará por ruta en la solicitud de anulación. Las rutas incluidas en la solicitud de anulación representan la dirección URL (o las direcciones URL si la ruta contiene un carácter comodín) del objeto que desea anular de la memoria caché de CloudFront. Puede solicitar hasta 1000 rutas al mes desde Amazon CloudFront sin costo adicional. A partir de las primeras 1000 rutas, se le cobrará por ruta que aparezca en las solicitudes de anulación.

- *Capa de conexión segura (SSL) personalizada con IP dedicada:* deberá pagar 600 USD al mes por cada certificado SSL personalizado que esté asociado a una o más distribuciones de CloudFront con la utilización de la versión de IP dedicada del soporte para certificados SSL personalizados. Esta tarifa mensual se prorrata por hora. Por ejemplo, si su certificado SSL personalizado se asoció a por lo menos una distribución de CloudFront durante solo 24 horas (es decir, 1 día) en el mes de junio, el cargo total por utilizar la característica de certificado SSL personalizado en junio es de  $(1 \text{ día}/30 \text{ días}) * 600 \text{ USD} = 20 \text{ USD}$ .

Para obtener la información más reciente sobre los precios, consulte la [página de precios de Amazon CloudFront](#).

## Aprendizajes clave de la sección 6



6.5

aws academy

- Una CDN es un sistema de servidores de almacenamiento en caché distribuido a nivel mundial que acelera la entrega de contenido.
- Amazon CloudFront es un servicio rápido de CDN que entrega datos, videos, aplicaciones y API de manera segura a través de una infraestructura mundial con latencia baja y velocidades de transferencia altas.
- Amazon CloudFront ofrece muchos beneficios.

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

Estos son algunos de los aprendizajes clave de esta sección del módulo:

- Una CDN es un sistema de servidores de almacenamiento en caché distribuido a nivel mundial que acelera la entrega de contenido.
- Amazon CloudFront es un servicio rápido de CDN que entrega datos, videos, aplicaciones y API de manera segura a través de una infraestructura mundial con latencia baja y velocidades de transferencia altas.
- Amazon CloudFront ofrece muchos beneficios, entre los que se incluyen:
  - Rapidez y alcance mundial
  - Seguridad en el borde
  - Alta capacidad de programación
  - Integración total con AWS
  - Rentabilidad

## Módulo 5: Redes y entrega de contenido

### Conclusión del módulo

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.



Ha llegado el momento de hacer un repaso del módulo y concluir con una revisión de conocimientos y un debate sobre una pregunta del examen de certificación como práctica.

## Resumen del módulo



En resumen, en este módulo, aprendió a hacer lo siguiente:

- Reconocer los conceptos básicos de las redes
- Describir las redes virtuales en la nube con Amazon VPC
- Etiquetar un diagrama de red
- Diseñar una arquitectura básica de VPC
- Indicar los pasos para crear una VPC
- Identificar los grupos de seguridad
- Crear su propia VPC y agregarle componentes adicionales para generar una red personalizada
- Identificar los aspectos fundamentales de Amazon Route 53
- Reconocer los beneficios de Amazon CloudFront

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

65

En resumen, en este módulo, aprendió a hacer lo siguiente:

- Reconocer los conceptos básicos de las redes
- Describir las redes virtuales en la nube con Amazon VPC
- Etiquetar un diagrama de red
- Diseñar una arquitectura básica de VPC
- Indicar los pasos para crear una VPC
- Identificar los grupos de seguridad
- Crear su propia VPC y agregarle componentes adicionales para generar una red personalizada
- Identificar los aspectos fundamentales de Amazon Route 53
- Reconocer los beneficios de Amazon CloudFront

## Complete la revisión de conocimientos



© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

bb

Ahora, complete la revisión de conocimientos.

## Pregunta del examen de muestra



¿Qué servicio de redes de AWS permite a una empresa crear una red virtual dentro de AWS?

- A. AWS Config
- B. Amazon Route 53
- C. AWS Direct Connect
- D. Amazon VPC

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

b/

Observe las opciones de respuesta y descarte algunas en función de las palabras clave que se destacaron previamente.

## Recursos adicionales



- [Página de información general sobre Amazon VPC](#)
- [Documento técnico](#) "Opciones de conectividad a la red con Amazon Virtual Private Cloud"
- [Publicación del blog de arquitectura de AWS](#) "One to Many: Evolving VPC Design" (De una a muchas: evolución del diseño de la VPC)
- [Guía del usuario de Amazon VPC](#)
- [Página de información general sobre Amazon CloudFront](#)

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados.

b8

Si desea obtener más información acerca de los temas que se trataron en este módulo, tal vez le resulten útiles los siguientes recursos adicionales:

- [Página de información general sobre Amazon VPC](#)
- [Documento técnico](#) "Opciones de conectividad a la red con Amazon Virtual Private Cloud"
- [Publicación del blog de arquitectura de AWS](#) "One to Many: Evolving VPC Design" (De una a muchas: evolución del diseño de la VPC)
- [Guía del usuario de Amazon VPC](#)
- [Página de información general sobre Amazon CloudFront](#)



Gracias

© 2019 Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados. Este contenido no puede reproducirse ni redistribuirse, total ni parcialmente, sin el permiso previo por escrito de Amazon Web Services, Inc. Queda prohibida la copia, el préstamo o la venta de carácter comercial. Envíenos sus correcciones o comentarios relacionados con el curso a: [aws.course.feedback@amazon.com](mailto:aws.course.feedback@amazon.com). Si tiene cualquier otra duda, contáctese con nosotros en: [https://aws.amazon.com/contact-us/aws\\_training/](https://aws.amazon.com/contact-us/aws_training/). Todas las marcas comerciales pertenecen a sus propietarios.



¡Gracias por participar!