

---

# Amazon Virtual Private Cloud

Guía de introducción

API Version 2012-12-01



# Amazon Web Services

## Amazon Virtual Private Cloud: Guía de introducción

Amazon Web Services

Copyright © 2013 Amazon Web Services, Inc. or its affiliates. All rights reserved.

The following are trademarks or registered trademarks of Amazon: Amazon, Amazon.com, Amazon.com Design, Amazon DevPay, Amazon EC2, Amazon Web Services Design, AWS, CloudFront, EC2, Elastic Compute Cloud, Kindle, and Mechanical Turk. In addition, Amazon.com graphics, logos, page headers, button icons, scripts, and service names are trademarks, or trade dress of Amazon in the U.S. and/or other countries. Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon.

All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

---

Información general sobre el ejercicio .....	1
Introducción .....	4
Paso 1: inscripción en Amazon VPC .....	4
Paso 2: configuración de la VPC y la puerta de enlace de Internet .....	5
Paso 3: configuración de un grupo de seguridad para la VPC .....	8
Paso 4: lanzamiento de una instancia en su VPC .....	13
Paso 5: asignación de una dirección IP elástica a su instancia .....	14
¿Qué hacer a partir de aquí? .....	16
Remítanos sus comentarios .....	20

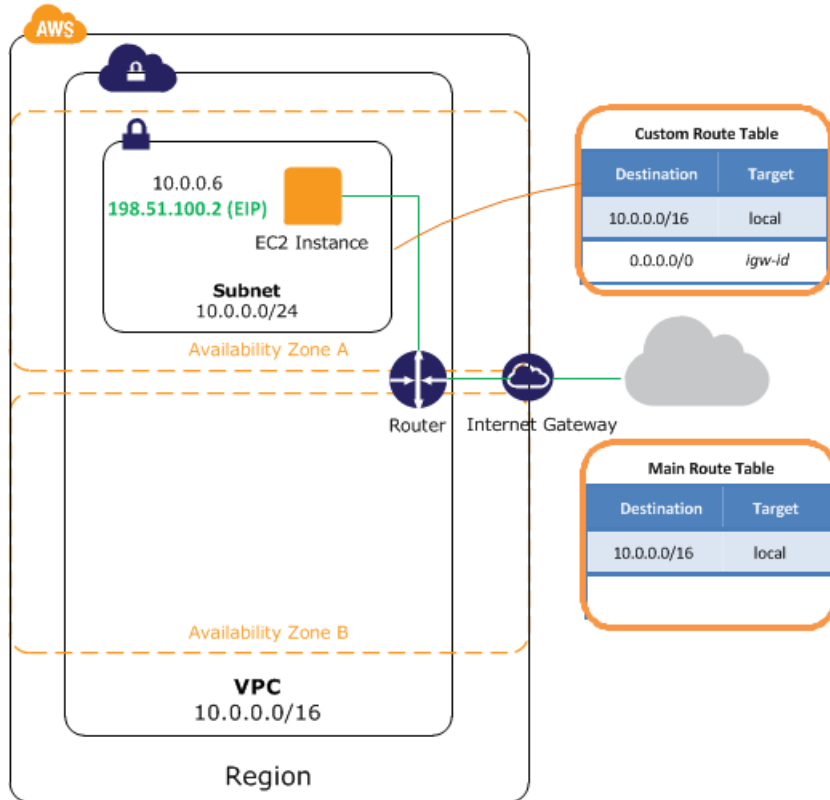
# Información general sobre el ejercicio

---

Una nube privada virtual (VPC) es una red virtual muy parecida a la red tradicional que podría utilizar en su propio centro de datos, con las ventajas de emplear la infraestructura escalable de Amazon Web Services (AWS). Una vez finalizadas las tareas de este ejercicio, dispondrá de una instancia de Amazon EC2 ejecutándose en una nondefault VPC a la que podrá acceder desde Internet utilizando SSH (para instancias de Linux) o Escritorio remoto (para instancias de Windows).

Para ver información general acerca de Amazon VPC, consulte [What is Amazon VPC?](#) en *Amazon Virtual Private Cloud User Guide*.

En el diagrama siguiente se muestra la arquitectura que creará a medida que complete el ejercicio en esta guía. El grupo de seguridad que configura y asocia con la instancia permite el tráfico únicamente a través de puertos concretos y bloquea la comunicación con la instancia en función de las reglas especificadas. El uso de una dirección IP elástica (EIP) permite acceder a una instancia en una VPC, que por lo demás es privada, desde Internet a través de una puerta de enlace de Internet (por ejemplo, podría actuar como un servidor web).



En la tabla siguiente se resumen las tareas que realizará a medida que complete el ejercicio en esta guía.

<p>Paso 1: inscripción en Amazon VPC(4)</p>	<p>Inscríbase en Amazon VPC, si aún no lo ha hecho.</p>
<p>Paso 2: configuración de la VPC y la puerta de enlace de Internet(5)</p>	<p>Utilice el asistente de VPC para realizar las acciones siguientes:</p> <ol style="list-style-type: none"> <li>1. Crear una VPC, que consiste en una parte aislada de la nube de AWS.</li> <li>2. Crear y adjuntar una puerta de enlace de Internet, que conecta la VPC directamente a Internet y proporciona acceso a otros productos de AWS como, por ejemplo, Amazon Simple Storage Service (Amazon S3).</li> <li>3. Crear una subred de Amazon VPC, que consiste en un segmento del rango de direcciones IP de la VPC en el que puede lanzar instancias de Amazon EC2. Las subredes le permiten agrupar instancias en función de sus necesidades operativas y de seguridad.</li> <li>4. Configurar el enrutamiento de la VPC para permitir que el tráfico fluya entre la subred e Internet. Su VPC dispone de un enrutador implícito, tal como se muestra en el diagrama.</li> </ol>

<p>Paso 3:                  creación                  de                  un                  grupo                  de                  seguridad                  para                  la                  VPC</p>	<p>Utilice la consola de Amazon VPC para configurar un grupo de seguridad que controle el tráfico entrante y saliente de la instancia.</p>
<p>Paso 4:                  lanzamiento                  de                  una                  instancia                  en                  su                  VPC</p>	<p>Utilice la consola de Amazon EC2 para lanzar una instancia en una subred. La instancia obtiene una dirección IP privada del rango de direcciones de la subred.</p>
<p>Paso 5:                  asignación                  de                  una                  dirección                  IP                  elástica                  a su                  instancia</p>	<p>Utilice la consola de Amazon VPC para indicar una dirección IP elástica y asignarla a la instancia. Una dirección IP elástica proporciona a la instancia una dirección IP pública además de su dirección privada, para que se pueda acceder a la instancia desde Internet.</p>
<p>Paso 6:                  parada                  de                  la                  VPC</p>	<p>Utilice la consola de Amazon EC2 para finalizar la instancia y la consola de Amazon VPC para eliminar la VPC.</p>

# Introducción a Amazon VPC

---

Esta guía proporciona una introducción práctica sobre cómo se utiliza Amazon VPC mediante AWS Management Console. El ejercicio de esta guía le plantea una situación sencilla en la que se configura una VPC con una sola subred pública que contiene una instancia de EC2 en ejecución con una dirección IP elástica.

## Topics

- [Paso 1: inscripción en Amazon VPC \(p. 4\)](#)
- [Paso 2: configuración de la VPC y la puerta de enlace de Internet \(p. 5\)](#)
- [Paso 3: configuración de un grupo de seguridad para la VPC \(p. 8\)](#)
- [Paso 4: lanzamiento de una instancia en su VPC \(p. 13\)](#)
- [Paso 5: asignación de una dirección IP elástica a su instancia \(p. 14\)](#)

Para ver la información general del ejercicio, consulte [Información general sobre el ejercicio \(p. 1\)](#). Para ver información general básica acerca de Amazon VPC, consulte [What is Amazon VPC?](#) en *Amazon Virtual Private Cloud User Guide*.

## Paso 1: inscripción en Amazon VPC

Al crear una cuenta de AWS, inscribimos automáticamente la cuenta en todos los servicios de AWS, como EC2 y Amazon VPC. Solo pagará por los servicios que utilice. Para este ejemplo, los cargos serán mínimos.

Si ya dispone de una cuenta de AWS, pase al siguiente paso. Si no dispone de una cuenta de AWS, utilice el siguiente procedimiento para crear una.

### Para crear una cuenta de AWS

1. Visite <http://aws.amazon.com> y haga clic en Inscribirse.
2. Siga las instrucciones en pantalla.  
Parte del procedimiento de inscripción consiste en recibir una llamada telefónica e introducir un número PIN con el teclado del teléfono.

Cuando su cuenta esté activada y lista para usar, se lo notificaremos por correo electrónico.



## Paso 2: configuración de la VPC y la puerta de enlace de Internet

En este paso, vamos a utilizar el asistente de VPC para crear una VPC. El asistente ejecuta los siguientes pasos por usted:



### Tip

Si lo prefiere, puede ejecutar estos pasos manualmente con AWS Management Console.


- Crear una VPC de tamaño /16 (una red con 65 536 direcciones IP privadas).
- Vincular una puerta de enlace de Internet a la VPC.
- Añadir una subred de tamaño /24 (un rango de 256 direcciones IP privadas).
- Configurar el enrutamiento en la VPC de forma que el tráfico pueda fluir entre la subred y la puerta de enlace de Internet.

Para crear una VPC utilizando el asistente de VPC en AWS Management Console

1. Inicie sesión en AWS Management Console y abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de VPC, haga clic en Get started creating a VPC.

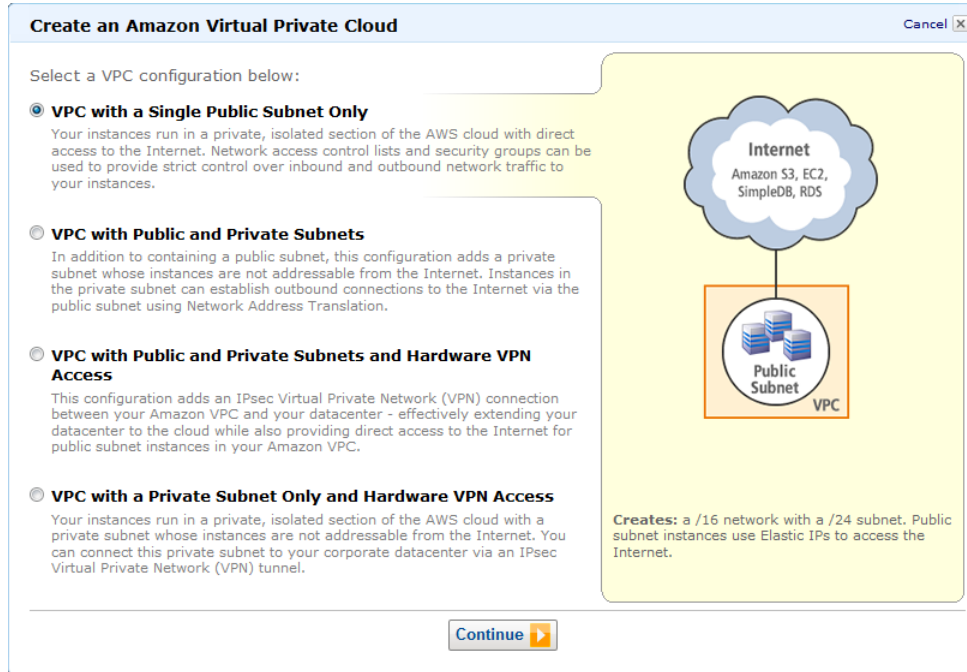
Amazon VPC enables you to create a virtual network topology - including subnets and route tables - for your EC2 resources.

Click the button below to create a Virtual Private Cloud.

[Get started creating a VPC](#) 

3. Seleccione la primera opción VPC with a Single Public Subnet Only y, a continuación, haga clic en Continue.

Amazon Virtual Private Cloud Guía de introducción  
Paso 2: configuración de la VPC y la puerta de enlace de Internet

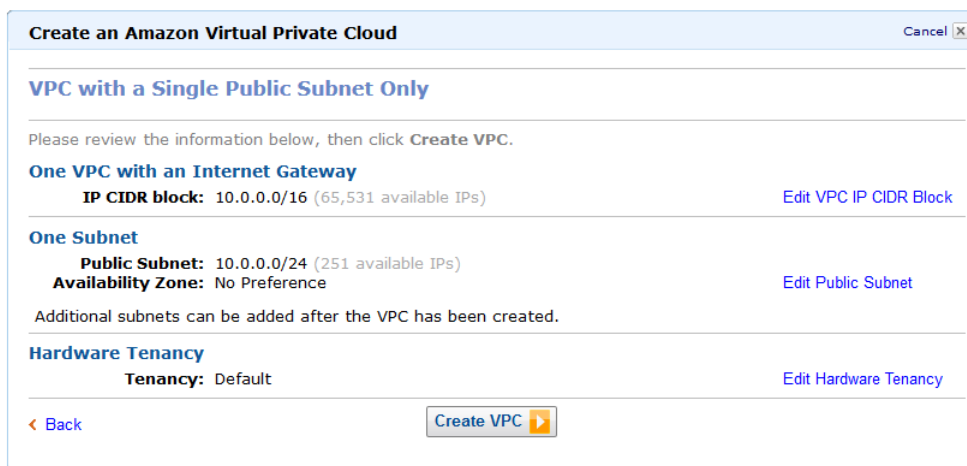


4. La página de confirmación muestra los rangos de CIDR que se utilizarán para la VPC y la subred (10.0.0.0/16 y 10.0.0.0/24, respectivamente), y la configuración de la tenencia de hardware. Realice los cambios necesarios en la configuración y, a continuación, haga clic en Create VPC para crear la VPC, la puerta de enlace de Internet, la subred y la tabla de enrutamiento.



Note

Si desea obtener información acerca de la notación CIDR, consulte el [artículo de Wikipedia acerca del enrutamiento entre dominios sin clases](#). Para obtener más información sobre la tenencia de hardware, consulte [Using EC2 Dedicated Instances](#) en *Amazon Virtual Private Cloud User Guide*.



5. En una ventana de estado se muestra el trabajo en curso. Cuando finaliza el trabajo, una ventana de estado confirma que la VPC se ha creado correctamente. Haga clic en Close para cerrar la ventana de estado y volver al panel de VPC.

## Verificación de los componentes de su VPC

Puede utilizar la configuración predeterminada para los componentes que el asistente de VPC ha creado por usted durante la realización del ejercicio de esta guía. En esta sección se describe cómo ver estos componentes y su configuración utilizando la consola de VPC.

En el panel de navegación, haga clic en **Your VPCs** y, a continuación, seleccione la VPC que acaba de crear .



### Tip

Puede que necesite actualizar la página para que aparezca la VPC.

La consola muestra la VPC que acaba de crear. Cada VPC incluye un conjunto de opciones de DHCP, una tabla de enrutamiento principal y una ACL de red predeterminada. Para obtener más información, consulte [DHCP Options Sets](#), [Route Tables](#) y [Network ACLs](#) en *Amazon Virtual Private Cloud User Guide*.

	VPC ID	State	CIDR	DHCP Options	Main Route Table	Default Network ACL
<input type="checkbox"/>	vpc-09ab8662	available	172.31.0.0/16	dopt-00ab866b	rtb-02ab8669	acl-03ab8668
<input checked="" type="checkbox"/>	vpc-071db56d	available	10.0.0.0/16	dopt-00ab866b	rtb-1a1db570	acl-051db56f

Para visualizar información sobre sus puertas de enlace de Internet, haga clic en **Internet Gateways** en el panel de navegación.

	ID	State	VPC
<input type="checkbox"/>	igw-0eab8665	available	vpc-09ab8662 (172.31.0.0/16)
<input checked="" type="checkbox"/>	igw-041db56e	available	vpc-071db56d (10.0.0.0/16)

La VPC que acaba de crear tiene dos tablas de enrutamiento. La VPC incluía una tabla de enrutamiento principal de forma predeterminada y, además, el asistente de VPC ha creado una tabla de enrutamiento personalizada. La subred está asociada a la tabla de enrutamiento personalizada, lo que significa que usamos las rutas de esa tabla para determinar la forma en que fluye el tráfico de la subred. Si añade una nueva subred a su VPC, utiliza la tabla de enrutamiento principal de forma predeterminada.

Para ver las tablas de enrutamiento


1. Haga clic en **Route Tables** en el panel de navegación.
2. Seleccione la tabla de enrutamiento personalizada (en la columna **Main** aparece la opción **No**) para visualizar la información de enrutamiento en el panel de detalles.

Viewing: All Route Tables

	Route Table ID	Associated With	Main	VPC
<input type="checkbox"/>	rtb-02ab8669	0 Subnets	Yes	vpc-09ab8662 (172.31.0.0/16)
<input checked="" type="checkbox"/>	rtb-ed1db587	1 Subnet	No	vpc-071db56d (10.0.0.0/16)
<input type="checkbox"/>	rtb-1a1db570	0 Subnets	Yes	vpc-071db56d (10.0.0.0/16)

- La primera fila de la tabla se corresponde con la ruta local, que permite que las instancias en la VPC se comuniquen. Esta ruta está presente de forma predeterminada en todas las tablas de enrutamiento y no se puede eliminar.


En la segunda fila se muestra la ruta que añadió el asistente de VPC para permitir el tráfico destinado a una dirección IP fuera de la VPC (0.0.0.0/0) para que fluya de la subred a la puerta de enlace de Internet. A esta subred la denominamos *pública* porque todo el tráfico de la subred se dirige a la puerta de enlace de Internet.

 **Route Table: rtb-ed1db587**

Routes Associations Route Propagation

Destination	Target	Status	Propagated	Actions
10.0.0.0/16	local	<span style="color: green;">●</span> active	No	<input type="button" value="Remove"/>
0.0.0.0/0	igw-041db56e	<span style="color: green;">●</span> active	No	<input type="button" value="Remove"/>
<input type="text"/>	select a target			<input type="button" value="Add"/>

- Seleccione la tabla de enrutamiento principal. Esta tabla de enrutamiento principal solamente tiene una ruta local. Por lo tanto, cualquier subred que cree en principio no está expuesta a Internet; esto quiere decir que será una *subred privada*. Para exponer una subred nueva como una subred pública, puede cambiar el enrutamiento en la tabla de enrutamiento principal o asociar la subred con una tabla de enrutamiento personalizada.

 **Route Table: rtb-1a1db570**

Routes Associations Route Propagation

Destination	Target	Status	Propagated	Actions
10.0.0.0/16	local	<span style="color: green;">●</span> active	No	<input type="button" value="Remove"/>
<input type="text"/>	select a target			<input type="button" value="Add"/>

## Paso 3: configuración de un grupo de seguridad para la VPC

Un *grupo de seguridad* funciona como un firewall virtual para controlar el tráfico permitido en sus instancias asociadas. Para utilizar grupos de seguridad, debe crear un grupo, añadir las reglas de entrada y salida

que desea utilizar y, a continuación, asociar sus instancias con el grupo de seguridad cuando las lanza. Si añade y elimina reglas desde el grupo de seguridad, aplicamos automáticamente esos cambios a las instancias asociadas con el grupo de seguridad.

La VPC incluye un *grupo de seguridad predeterminado*. Cualquier instancia no asociada con otro grupo de seguridad se asocia con el grupo de seguridad predeterminado. Aunque podríamos utilizar el grupo de seguridad predeterminado para este ejercicio, en vez de eso hemos elegido crear el grupo `WebServerSG`. Especificará este grupo de seguridad al lanzar una instancia en su VPC.

#### Topics

- [Reglas para el grupo de seguridad WebServerSG \(p. 9\)](#)
- [Creación del grupo de seguridad WebServerSG \(p. 10\)](#)
- [Añadir reglas al grupo de seguridad WebServerSG \(p. 10\)](#)

## Reglas para el grupo de seguridad WebServerSG

Las reglas de entrada regulan el tráfico admitido en las instancias asociadas con el grupo de seguridad (el origen del tráfico y el puerto de escucha de la instancia). Todo el tráfico de retorno se admite automáticamente en las instancias. Por ejemplo, si un cliente de Internet envía una solicitud a un servidor web de la VPC asociada con `WebServerSG`, la instancia puede responder, independientemente de las reglas de salida del grupo. De esta forma, los grupos de seguridad tienen información de estado.

Las reglas de salida controlan a qué destinos pueden enviar tráfico las instancias asociadas con el grupo de seguridad (el destino del tráfico y el puerto de destino). De forma automática se permite que todo el tráfico de retorno (como una respuesta del host que recibió el tráfico) llegue a las instancias, independientemente de las reglas de entrada que se establezcan para el grupo de seguridad.

En la siguiente tabla se muestran las reglas de entrada y salida del grupo de seguridad `WebServerSG` y cuál es su función.



#### Note

Si la empresa utiliza solo Linux o solo Windows, no tiene que añadir acceso para SSH y RDP.

Entrada			
IP de origen	Protocolo	Rango de puerto	Comentarios
0.0.0.0/0	TCP	80	Permite el acceso de HTTP entrante desde cualquier lugar
0.0.0.0/0	TCP	443	Permite el acceso de HTTPS entrante desde cualquier lugar
Rango de direcciones IP públicas de su red doméstica	TCP	22	Permite el acceso de SSH entrante desde la red doméstica (solo Linux/UNIX)
Rango de direcciones IP públicas de su red doméstica	TCP	3389	Permite el acceso de RDP entrante desde su red doméstica (solo Windows)
Salida			

IP destino	Protocolo	Rango de puerto	Comentarios
0.0.0.0/0	TCP	80	Permite el acceso de HTTP saliente a servidores de Internet (por ejemplo, para actualizaciones de software)
0.0.0.0/0	TCP	443	Permite el acceso de HTTPS saliente a servidores de Internet (por ejemplo, para actualizaciones de software)

En este ejercicio, no añadirá una regla para permitir que las instancias asociadas con el grupo de seguridad se comuniquen entre sí. Para permitir este tipo de comunicación, debe añadir una regla al grupo de seguridad con este fin. Para obtener más información, consulte [Security Groups](#) en *Amazon Virtual Private Cloud User Guide*.

## Creación del grupo de seguridad WebServerSG

Para crear el grupo de seguridad WebServerSG

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. Haga clic en Security Groups en el panel de navegación.
3. Haga clic en el botón Create Security Group.
4. Especifique `WebServerSG` como el nombre del grupo de seguridad y proporcione una descripción. En el menú VPC seleccione el ID de la VPC y, a continuación, haga clic en Yes, Create.

De forma predeterminada, los grupos de seguridad nuevos empiezan con una única regla de salida que permite que todo el tráfico salga de las instancias. Debe añadir reglas para permitir el tráfico entrante o restringir el tráfico saliente.

## Añadir reglas al grupo de seguridad WebServerSG

Para añadir reglas al grupo de seguridad WebServerSG

1. Haga clic en Security Groups en el panel de navegación para visualizar sus grupos de seguridad.
2. Seleccione el grupo de seguridad `WebServerSG` que acaba de crear. En el panel de detalles se incluye una pestaña para proporcionar información acerca del grupo de seguridad, además de pestañas para trabajar con sus reglas de entrada y salida.
3. Añada reglas para el acceso de HTTP y HTTPS entrante desde cualquier lugar:
  - a. En la pestaña Inbound, seleccione `HTTP` en la lista desplegable Create a new rule y asegúrese de que Source sea `0.0.0.0/0`.
  - b. Haga clic en Add Rule. Esta operación añade una regla para permitir el acceso de HTTP desde cualquier lugar. Tenga en cuenta que el botón Apply Rule Changes está activado y que el texto "Your changes have not been applied yet" se muestra sobre el botón. El sistema hará clic en este botón para aplicar los cambios de reglas una vez añadidas todas las reglas de entrada.

Security Group: WebServerSG

Details Inbound\* Outbound

Create a new rule: Custom TCP rule

Port range: 80 (HTTP)  
(e.g., 80 or 49152-65535)

Source: 0.0.0.0/0  
(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

+ Add Rule

Your changes have not been applied yet.

Apply Rule Changes

TCP	Port (Service)	Source	Action
	80 (HTTP)	0.0.0.0/0	Delete

- c. Seleccione HTTPS en la lista desplegable Create a new rule y asegúrese de que Source sea 0.0.0.0/0.
  - d. Haga clic en Add Rule. Esta operación añade una regla para permitir el acceso de HTTPS desde cualquier lugar.
4. Añada reglas para el acceso de SSH y de escritorio remoto (RDP) entrante al grupo desde el rango de direcciones IP públicas de su red:



#### Caution

Si utiliza 0.0.0.0/0, permite que todas las direcciones IP tengan acceso a su instancia mediante SSH o RDP. Esto es aceptable para este pequeño ejercicio, pero constituye una práctica peligrosa en entornos de producción. En producción, se autorizaría el acceso a la instancia únicamente a una dirección IP o a un rango de direcciones IP específico.



#### Tip

También puede obtener la dirección IP pública de su equipo local utilizando un servicio. Para localizar un servicio que proporcione su dirección IP, utilice la frase de búsqueda "what is my IP address". Si realiza la conexión a través de un ISP o desde la protección de un firewall sin una dirección IP estática, debe buscar el rango de direcciones IP utilizado por los equipos cliente.

- a. En la pestaña Inbound, seleccione SSH en la lista desplegable Create a new rule.
  - b. En el campo Source, introduzca el rango de direcciones IP públicas de su red (por ejemplo, 192.0.2.0/24). Si no conoce este rango de direcciones, puede utilizar 0.0.0.0/0 para este ejercicio (consulte las secciones de precaución y consejo para este paso).
  - c. Haga clic en Add Rule.
  - d. Seleccione RDP en la lista desplegable Create a new rule.
  - e. En el campo Source, introduzca el rango de direcciones IP públicas de su red doméstica. Si no conoce este rango de direcciones, puede utilizar 0.0.0.0/0 para este ejercicio (consulte las secciones de precaución y consejo para este paso).
  - f. Haga clic en Add Rule.
5. Haga clic en Apply Rule Changes para aplicar estas reglas de entrada.

Security Group: WebServerSG

Details Inbound Outbound

Create a new rule: Custom TCP rule

Port range: 0.0.0.0/0  
(e.g., 80 or 49152-65535)

Source: 0.0.0.0/0  
(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

+ Add Rule

Apply Rule Changes

TCP Port (Service)	Source	Action
80 (HTTP)	0.0.0.0/0	Delete
443 (HTTPS)	0.0.0.0/0	Delete
22 (SSH)	0.0.0.0/0	Delete
3389 (RDP)	0.0.0.0/0	Delete

6. Limite el acceso de salida a solo HTTP y HTTPS desde el grupo a cualquier lugar:
  - a. En la pestaña Outbound, localice la regla predeterminada que permite todo el tráfico saliente y haga clic en Delete. La regla se marca para eliminarla. Sin embargo, este cambio no se aplicará hasta que haga clic en Apply Rule Changes, operación que realizará una vez añadidas las reglas de salida para HTTP y HTTPS.

Security Group: WebServerSG

Details Inbound Outbound\*

Create a new rule: Custom TCP rule

Port range: 0.0.0.0/0  
(e.g., 80 or 49152-65535)

Destination: 0.0.0.0/0  
(e.g., 192.168.2.0/24, sg-47ad482e, or 1234567890/default)

+ Add Rule

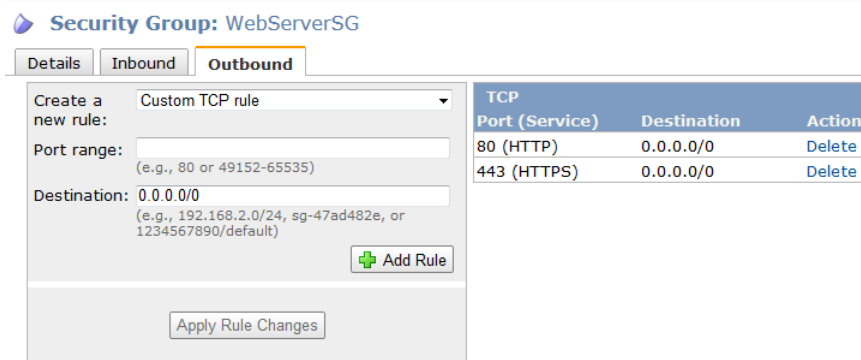
Your changes have not been applied yet.

Apply Rule Changes

ALL Port (Service)	Destination	Action
ALL	0.0.0.0/0	Undelete

- b. Seleccione HTTP en la lista desplegable Create a new rule y, a continuación, haga clic en Add Rule. Con esta operación se añade una regla que permite el acceso de HTTP saliente a cualquier lugar.
    - c. Seleccione HTTPS en la lista desplegable Create a new rule y, a continuación, haga clic en Add Rule. Con esta operación se añade una regla que permite el acceso de HTTPS saliente a cualquier lugar.
7. Haga clic en Apply Rule Changes para aplicar estas reglas de salida.



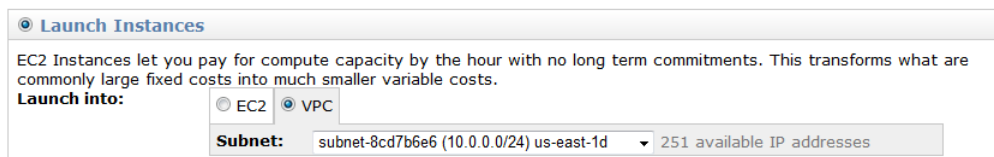


## Paso 4: lanzamiento de una instancia en su VPC

Al lanzar una instancia de EC2 en una VPC, debe especificar el ID de una subred en la VPC.

Para lanzar una instancia de EC2 en una VPC

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Desde la barra de navegación, seleccione la región para la instancia. Para este ejercicio, puede utilizar la región predeterminada. Para obtener más información acerca de las regiones y las zonas de disponibilidad, consulte [Regions and Availability Zones](#) en *Amazon Elastic Compute Cloud User Guide*.
3. En el panel, haga clic en el botón Launch Instance.
4. En la página Create a New Instance, seleccione Classic Wizard y, a continuación, haga clic en Continue.
5. En la página CHOOSE AN AMI se encuentra una pestaña denominada Quick Start en la que se muestra una lista de configuraciones básicas denominadas imágenes de máquina de Amazon (AMI). Seleccione la AMI que desea utilizar y, a continuación, haga clic en el botón Select.
6. En el menú Instance Type de la página INSTANCE DETAILS, deje el valor predeterminado Micro (t1.micro) para lanzar una única microinstancia.
7. En Launch Instances, confirme que su subred está seleccionada en la lista desplegable Subnet y, a continuación, haga clic en Continue.



8. En Advanced Instance Options, puede especificar la dirección IP que desea utilizar para la instancia. No obstante, para este ejercicio dejaremos el campo IP Address vacío y haremos clic en Continue para aceptar la configuración predeterminada.
9. Haga clic en Continue para utilizar el dispositivo de almacenamiento predeterminado.
10. Especifique las etiquetas que desee para la instancia y, a continuación, haga clic en Continue.
11. En la página Create Key Pair puede seleccionar un par de claves existente o crear uno nuevo. Para este ejercicio, vamos a crear un par de claves.
  - a. Haga clic en Create a new Key Pair.

- b. Especifique un nombre para el par de claves (por ejemplo, `VPC_Keypair`) y, a continuación, haga clic en **Create & Download your Key Pair**. Necesitará el contenido de la clave privada para conectarse a la instancia después de lanzarla. Amazon Web Services no almacena la parte privada de los pares de claves.
  - c. Cuando se le pida, guarde la clave privada en un lugar seguro del sistema y, a continuación, haga clic en **Continue**.
12. En la página **CONFIGURE FIREWALL**, seleccione **Choose one or more of your existing Security Groups**. Seleccione el grupo `WebServerSG` que ha creado anteriormente y, a continuación, haga clic en **Continue**.
  13. En la página **REVIEW**, revise la configuración. Cuando esté conforme con las selecciones realizadas, haga clic en **Launch** para lanzar la instancia.

## Paso 5: asignación de una dirección IP elástica a su instancia

De forma predeterminada, una instancia en una VPC es privada. Para hacer pública una instancia en una VPC, se debe adjuntar una puerta de enlace de Internet a la VPC y asignar una dirección IP pública a la instancia. En este ejercicio, ha utilizado el asistente de VPC para crear una puerta de enlace de Internet para su VPC. A continuación, creará una dirección IP elástica, que es una dirección IP pública que pertenece a su cuenta de AWS, y la asociará con su instancia para que sea accesible desde Internet.

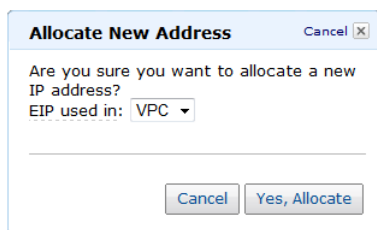
Para obtener información sobre direcciones IP elásticas, consulte [Elastic IP Addresses](#) en *Amazon Virtual Private Cloud User Guide*.

Para indicar y asignar una dirección IP elástica

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. Haga clic en **Elastic IPs** en el panel de navegación.
3. Haga clic en el botón **Allocate New Address**.



4. En la lista **EIP used in:**, **VPC** haga clic en **Yes, Allocate**.



5. Seleccione la dirección IP elástica en la lista y haga clic en el botón **Associate Address**.
6. En el cuadro de diálogo **Associate Address**, seleccione la instancia con la que desea asociar la dirección y, a continuación, haga clic en **Yes, Associate**.

Amazon Virtual Private Cloud Guía de introducción  
Paso 5: asignación de una dirección IP elástica a su instancia

---

**Associate Address** Cancel

Select the instance or network interface to which you wish to associate this IP address.

Instance: Select an instance

Private IP address: i-ac921fd2  
\* denotes the primary private IP address

or

Network Interface: Select a network interface

Private IP address:   
\* denotes the primary private IP address

Allow Reassociation

Cancel Yes, Associate

Tras completar este procedimiento, ya será posible acceder a su instancia desde Internet. También puede acceder a la instancia con SSH o Escritorio remoto desde la red doméstica, para lo que debe especificar la dirección IP elástica de la instancia como la dirección a la que desea conectarse. Para obtener instrucciones sobre cómo conectarse a una instancia de Linux, consulte [Connect to Your Linux Instance](#) en *Amazon Elastic Compute Cloud User Guide*. Para obtener instrucciones sobre cómo conectarse a una instancia de Windows, consulte [Connect to Your Windows Instance](#) en *Amazon Elastic Compute Cloud Microsoft Windows Guide*.

Con esto finaliza el ejercicio; su VPC está configurada, se está ejecutando una instancia en su VPC y tiene la capacidad de conectarse a su instancia desde Internet. Puede continuar utilizando su instancia y su VPC o puede finalizar la instancia y eliminar la VPC. Para obtener información acerca de la limpieza o para acceder a documentación adicional sobre la VPC, consulte [¿Qué hacer a partir de aquí? \(p. 16\)](#).

## ¿Qué hacer a partir de aquí?

---

### Topics

- [Paso opcional: eliminación de la VPC \(p. 16\)](#)
- [Cuenta de AWS y credenciales de seguridad \(p. 17\)](#)
- [Seguridad adicional para la VPC \(p. 17\)](#)
- [Situaciones adicionales para Amazon VPC \(p. 17\)](#)
- [Formas de acceder a Amazon VPC \(p. 17\)](#)
- [Documentación de apoyo \(p. 18\)](#)
- [Dónde obtener ayuda adicional \(p. 18\)](#)

Si ha seguido los pasos del ejemplo en esta guía, habrá configurado una VPC y habrá lanzado una instancia en esta. Si lo desea, puede continuar utilizando su VPC. De lo contrario, puede eliminar la VPC. Independientemente de si elimina su VPC, también puede crear otras VPC.

## Paso opcional: eliminación de la VPC

Antes de poder eliminar una VPC, debe finalizar las instancias que se estén ejecutando en esta. La eliminación de una VPC también elimina recursos que están asociados con la VPC, como subredes, grupos de seguridad, ACL de red, conjuntos de opciones de DHCP, tablas de enrutamiento y puertas de enlace de Internet.

### Para eliminar la VPC

1. Abra la consola de Amazon EC2 en <https://console.aws.amazon.com/ec2/>.
2. Haga clic en Instancias en el panel de navegación.
3. Haga clic con el botón derecho en la instancia que se está ejecutando en la VPC y seleccione Terminate.
4. Cuando se le solicite confirmación, haga clic en Yes, Terminate.
5. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
6. Haga clic en Your VPCs en el panel de navegación.
7. Seleccione la VPC y haga clic en el botón Delete.
8. Cuando se le solicite confirmación, haga clic en Yes, Delete.

## Cuenta de AWS y credenciales de seguridad

En esta guía se le explica cómo inscribirse en el servicio y cómo crear una cuenta de AWS para después completar un breve ejercicio. Ahora que ha completado el ejercicio, le recomendamos que compruebe con un administrador o con un compañero de trabajo si ellos ya tienen una cuenta y credenciales de seguridad de AWS para que pueda utilizarlas en futuras interacciones con AWS.

Si usted es propietario o administrador de cuentas y desea saber más sobre AWS Identity and Access Management, visite <http://aws.amazon.com/es/iam> y la [Using AWS Identity and Access Management](#).

## Seguridad adicional para la VPC

Si desea incluir otra capa de seguridad además de su grupo de seguridad, puede utilizar una lista de control de acceso (ACL) de red. Las ACL de red controlan el tráfico al nivel de la subred. En este ejercicio solo se utilizan grupos de seguridad, que controlan el tráfico a nivel de instancia. Si desea obtener más información acerca de las ACL de red, consulte [Network ACLs](#) en *Amazon Virtual Private Cloud User Guide*.

## Situaciones adicionales para Amazon VPC

En esta guía se presenta una situación sencilla para Amazon VPC. El asistente de VPC proporciona situaciones adicionales. Para ver información detallada de estas situaciones, consulte [Escenarios for Amazon VPC](#) en *Amazon Virtual Private Cloud User Guide*.

## Formas de acceder a Amazon VPC

En esta guía se le ha explicado cómo utilizar Amazon VPC mediante AWS Management Console. Puede seguir utilizando el servicio a través de la consola, o bien probar alguna de las otras interfaces.

### Continuar utilizando la consola

Para obtener información adicional acerca de cómo utilizar Amazon VPC mediante la consola, consulte [Amazon Virtual Private Cloud User Guide](#).

### Utilización de la interfaz de línea de comandos

Amazon EC2 y Amazon VPC comparten una interfaz de línea de comandos basada en Java. Estas herramientas de línea de comandos son un método rápido de utilizar Amazon EC2 y Amazon VPC sin realizar codificaciones en la API ni utilizar una biblioteca. Si desea obtener información acerca de cómo empezar a utilizar las herramientas de línea de comandos, consulte [Getting Started with the Command Line Tools](#) en *Amazon Elastic Compute Cloud User Guide*. Para obtener una descripción completa de los comandos, consulte [Amazon Elastic Compute Cloud Command Line Reference](#).

### Utilización de la biblioteca existente

Amazon EC2 y Amazon VPC comparten la misma interfaz de programación. Si prefiere utilizar Amazon VPC mediante una API, existen bibliotecas y recursos disponibles para los siguientes lenguajes:

- [Java](#)

- [PHP](#)
- [Python](#)
- [Ruby](#)
- [Windows y .NET](#)

Si desea conocer bibliotecas y código de muestra en todos los lenguajes, vaya a [Código de muestra & bibliotecas](#).

## Codificación directa en la API del servicio web

Si desea escribir código directamente en la API para Amazon EC2 y Amazon VPC, consulte [Making API Requests](#) en *Amazon Elastic Compute Cloud User Guide*. En esta guía se describe cómo crear y autenticar solicitudes de API, además de cómo utilizar Amazon EC2 y Amazon VPC a través de las API. Para obtener una descripción completa de las acciones de la API, consulte [Amazon Elastic Compute Cloud API Reference](#).

## Documentación de apoyo

En esta Guía de introducción para Amazon VPC se describen los aspectos básicos del uso de Amazon VPC. En la tabla siguiente se enumera el resto de documentación para Amazon VPC.

Descripción	Documentación
Información sobre cómo utilizar Amazon VPC	<a href="#">Amazon Virtual Private Cloud User Guide</a>
Información acerca de cómo configurar la puerta de enlace del cliente (si decide utilizar una conexión de VPN con la VPC)	<a href="#">Amazon Virtual Private Cloud Network Administrator Guide</a>
Una introducción práctica a Amazon EC2	<a href="#">Getting Started with Amazon EC2</a>
Información sobre cómo utilizar Amazon EC2	<a href="#">Amazon Elastic Compute Cloud User Guide</a>
Descripciones de los comandos para Amazon EC2 y Amazon VPC	<a href="#">Amazon Elastic Compute Cloud Command Line Reference</a>
Descripciones de las acciones, tipos de datos y errores de la API para Amazon EC2 y Amazon VPC	<a href="#">Amazon Elastic Compute Cloud API Reference</a>
Descripciones de referencia rápida de los comandos de Amazon VPC utilizados habitualmente	<a href="#">Amazon Virtual Private Cloud Quick Reference Card</a>

## Dónde obtener ayuda adicional

Le recomendamos que consulte los foros de debate de AWS. Estos son foros de comunidades dirigidos a usuarios que desean debatir cuestiones técnicas relacionadas con los servicios de AWS. Para acceder al foro de Amazon VPC, visite <https://forums.aws.amazon.com/forum.jspa?forumID=58>.

También puede obtener ayuda si se suscribe a AWS Premium Support, un canal de asistencia personalizada de respuesta rápida (si desea obtener más información, visite <http://aws.amazon.com/premiumsupport>).

## Remítanos sus comentarios

---

Sus comentarios son importantes para ayudarnos a conseguir que nuestra documentación resulte útil y fácil de usar. Rellene nuestra [encuesta de introducción](#) para informarnos acerca de su primera experiencia con Amazon VPC.

Gracias.