

# Creating an Amazon Virtual Private Cloud (VPC) with AWS CloudFormation (Spanish) | Amazon Web Services

1 hora

1 crédito



**SPL-15: Versión 4.1.10**

© 2022 Amazon Web Services, Inc. y 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.

¿Errores, correcciones u otras preguntas? Contacte con nosotros en [AWS Training and Certification](#).

## Información general

En este laboratorio se muestra cómo crear una Amazon Virtual Private Cloud (VPC) mediante AWS CloudFormation.

El uso de AWS CloudFormation es una forma excelente de implementar VPC de forma fiable y repetible, ya que la plantilla utilizada por CloudFormation actúa como documentación para mostrar exactamente lo que se está implementando.

Se le explicarán las secciones de una plantilla de AWS CloudFormation y los recursos que se implementan. También aprenderá a realizar actualizaciones a través de CloudFormation.

## Temas tratados

En este laboratorio podrá hacer lo siguiente:

- implementar una plantilla de AWS CloudFormation que cree una Amazon VPC
- examinar los componentes de la plantilla
- actualizar de una pila de CloudFormation
- examinar una plantilla con AWS CloudFormation Designer
- eliminar una pila de CloudFormation

## Requisitos previos de conocimientos técnicos

Para completar correctamente este laboratorio, debe estar familiarizado con los conceptos de Amazon Virtual Private Cloud (VPC).

## Presentación de las tecnologías

### AWS CloudFormation

**AWS CloudFormation** ofrece a los desarrolladores y administradores de sistemas una forma sencilla de crear y administrar una colección de recursos de AWS relacionados, aprovisionarlos y actualizarlos de forma ordenada y predecible.

Puede utilizar las plantillas de muestra de AWS CloudFormation o crear sus propias **plantillas** para describir los recursos de AWS y las dependencias asociadas o los parámetros de tiempo de ejecución necesarios para ejecutar su aplicación. No necesita averiguar el orden de aprovisionamiento de los servicios de AWS ni las sutilezas de hacer que esas dependencias funcionen. CloudFormation se encarga de esto por usted. Una vez implementados los recursos de AWS, puede modificarlos y actualizarlos de forma controlada y predecible, para ello debe aplicar el control de versiones a su infraestructura de AWS de la misma manera que lo hace con el software.

Puede implementar y actualizar una plantilla y su colección de recursos asociada (denominada **“pila”**) mediante la consola de administración de AWS, la interfaz de línea de comandos de AWS o las API. CloudFormation está disponible sin cargo adicional y solo

paga por los recursos de AWS necesarios para ejecutar sus aplicaciones.

## Amazon Virtual Private Cloud (VPC)

**Amazon Virtual Private Cloud (Amazon VPC)** le permite aprovisionar una sección aislada de forma lógica de la nube de AWS en la que puede lanzar recursos dentro de una red virtual. Tiene control total sobre su entorno de red virtual, incluida la selección de su propio intervalo de direcciones IP, la creación de subredes y la configuración de tablas de enrutamiento y puertas de enlace de red.

Puede personalizar fácilmente la configuración de red de su nube virtual privada. Por ejemplo, puede crear una **subred de acceso público** para sus servidores web que tenga acceso a Internet y colocar sus sistemas de backend, como bases de datos o servidores de aplicaciones, en una **subred privada** sin acceso a Internet. Puede aprovechar varios niveles de seguridad, incluidos los grupos de seguridad y las listas de control de acceso a la red, para ayudar a controlar el acceso a las instancias de Amazon EC2 en cada subred.

## Iniciar laboratorio

1. Para lanzar el laboratorio, haga clic en Start Lab (Iniciar laboratorio) en la parte superior de la pantalla.

Esto iniciará el proceso de aprovisionamiento de los recursos de laboratorio. Se mostrará el tiempo estimado que llevará aprovisionar dichos recursos. Debe esperar a que se hayan aprovisionado los recursos para continuar.

Si se le pide un token, utilice el que se le ha otorgado (o los créditos que haya adquirido).

1. Para abrir el laboratorio, haga clic en Open Console (Abrir consola).

Con esto, iniciará sesión automáticamente en la consola de administración de AWS.

**No cambie la región a menos que se lo indiquen.**

## Errores comunes de inicio de sesión

### Error: Credenciales federadas de inicio de sesión

Your unique, federated login credentials are being created. Please try again in 30 seconds.

Si aparece este mensaje de error:

- Cierre la pestaña del navegador para regresar a la ventana inicial de laboratorio.
- Espere unos segundos.
- Haga clic nuevamente en Open Console (Abrir consola).

Ahora debería poder acceder a la consola de administración de AWS.

### Error: Primero debe cerrar sesión

#### Amazon Web Services Sign In

You must first log out before logging into a different AWS account.

To logout, [click here](#)

Si aparece el mensaje **You must first log out before logging into a different AWS account** (Para poder acceder a una cuenta de AWS diferente, primero debe cerrar sesión):

- Haga clic en **click here** (haga clic aquí).
- Cierre la pestaña del navegador para regresar a la ventana inicial de Qwiklabs.
- Haga clic nuevamente en Open Console (Abrir consola).

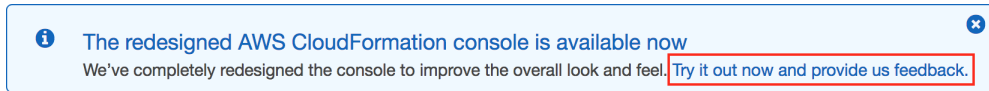
## Tarea 1: Implementar una pila con AWS CloudFormation

En esta tarea, implementará una plantilla predefinida para crear una VPC.

1. Haga clic con el botón secundario del mouse en este enlace y descargue la plantilla de CloudFormation en su equipo: [vpc-1.yaml](#)

Examinará el contenido de la plantilla en la siguiente tarea.

1. En la **Consola de Administración de AWS**, en el menú Service (Servicios), haga clic en **CloudFormation**.
2. Si ve este mensaje, haga clic en Try it out now and provide us feedback (Pruébelo ahora y envíenos sus comentarios):



1. Haga clic en Create stack (Crear pila) > **With new resources** (Con nuevos recursos) y, a continuación, configure lo siguiente:
  - Haga clic en Upload a template file (Subir un archivo de plantilla).
  - Haga clic en Choose file (Elegir archivo).
  - Busque y seleccione el archivo `vpc-1.yaml` que descargó.
  - Haga clic en Next (Siguiente).

1. En la página **Create stack** (Crear pila), configure lo siguiente:
  - **Stack name** (Nombre de la pila):
  - Haga clic en Next (Siguiente).

La página **Options** (Opciones) permite especificar etiquetas, permisos y opciones avanzadas.

1. En la página **Configure stack options** (Configurar opciones de pila), desplácese hasta la parte inferior de la pantalla y haga clic en Next (Siguiente).

Utilizará los valores predeterminados.

1. En la página **Review lab** (Revisar laboratorio):
  - Revisar la configuración
  - Haga clic en Create stack (Crear pila).

El estado de la pila será `CREATE_IN_PROGRESS` hasta que se hayan creado los recursos.

Mientras espera, consulte la pestaña **Events** (Eventos) para ver el trabajo que CloudFormation está realizando.

Si no ve la pestaña **Events** (Eventos), es porque la ventana de su navegador web es demasiado estrecha. Haga que la ventana sea más ancha hasta que aparezcan las pestañas o haga clic en la flecha desplegable de la pestaña **Overview** (información general).

1. Haga clic en la pestaña **Stack info** (Información de pila).
2. Espere hasta que el estado cambie a **CREATE\_COMPLETE**. Haga clic en el ícono actualizar cada 30 segundos para actualizar el estado.

Cuando el estado de la pila sea **CREATE\_COMPLETE** significa que los recursos se han creado.

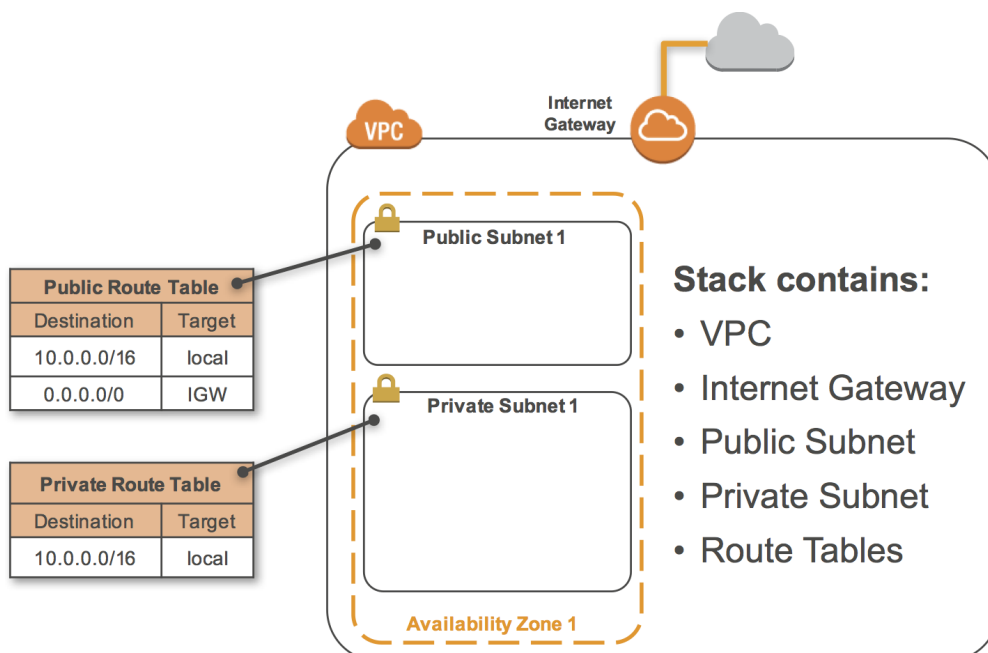
1. Haga clic en la pestaña **Resources** (Recursos).

Se muestra una lista de recursos. Estos recursos se explicarán en la siguiente tarea. Es posible que tenga que actualizar la pantalla para ver los recursos.

## Tarea 2: Examinar la VPC

En esta tarea, examinará los recursos de VPC que se crearon junto con el código de la plantilla de CloudFormation que creó los recursos.

Estos son los recursos que CloudFormation ha creado:



- Una Amazon VPC

- Una puerta de enlace de Internet
- Dos subredes
- Dos tablas de enrutamiento

Todos estos recursos residen en una **zona de disponibilidad**. Una zona de disponibilidad es una ubicación aislada dentro de una región y que consta de uno o más centros de datos.

1. En el menú Services (Servicios), haga clic en **VPC**.
2. En la esquina superior izquierda **Filter by VPC** (Filtrar por VPC), seleccione **Lab VPC** (VPC de laboratorio).

Esto configura la consola de VPC para que solo muestre los recursos que pertenecen a la VPC creada por CloudFormation.

1. En el panel de navegación izquierdo, haga clic en **Your VPCs** (Mis VPC).
2. Seleccione **Lab VPC** (VPC de laboratorio).

Una VPC es una sección aislada de AWS Cloud que permite que los recursos se comuniquen entre sí y, de forma selectiva, con Internet. Al implementar recursos como instancias de Amazon EC2, debe seleccionar la VPC en la que se lanzará la instancia.

En la pestaña **Details** (Detalles) se muestra **IPv4 CIDR**, que es un rango de direcciones IP asignadas a la VPC. Esta VPC tiene un CIDR de *10.0.0.0/16*, lo que significa que contiene todas las direcciones IP que empiezan por .

Este es el código de la plantilla de CloudFormation que creó esta VPC:

```
AWSTemplateFormatVersion: 2010-09-09
Description: Deploy a VPC
Resources:
  VPC:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.0.0.0/16
```

```
EnableDnsHostnames: true
Tags:
  - Key: Name
    Value: Lab VPC
```

Este código está en formato YAML. AWS CloudFormation también puede aceptar código en formato JSON. Si está más familiarizado con JSON, puede descargar la versión [JSON de esta plantilla](#).

El parámetro **Type** del código anterior establece el tipo de recursos que CloudFormation crea. A continuación, la sección **Properties** (Propiedades) especifica más información sobre el recurso que se va a crear. En este caso, se define lo siguiente:

- **CidrBlock**: intervalo de direcciones IP asociadas a la VPC.
- **EnableDnsHostnames**: configura la VPC para asociar nombres DNS con instancias de Amazon EC2.
- **Etiquetas**: agregue un nombre descriptivo al recurso.

Cada tipo de recurso tiene un conjunto diferente de propiedades que se pueden utilizar.

1. En el panel de navegación izquierdo, haga clic en **puerta de enlace de Internet**.

Una **puerta de enlace de Internet** es un componente de VPC de alta disponibilidad, redundante y de escala horizontal que permite la comunicación entre las instancias de la VPC e Internet. Por lo tanto, no impone riesgos de disponibilidad ni restricciones de banda ancha para el tráfico de red.

Una puerta de enlace de Internet tiene dos propósitos: proporcionar un destino en las tablas de enrutamiento de la VPC para el tráfico de enrutamiento de Internet y realizar la traducción de direcciones de red (NAT) para las instancias a las que se han asignado direcciones IPv4 públicas.

Este es el código de la plantilla de CloudFormation que creó esta puerta de enlace de Internet:



```
InternetGateway:
  Type: AWS::EC2::InternetGateway
  Properties:
    Tags:
      - Key: Name
        Value: Lab Internet Gateway
```

En la consola de administración, la puerta de enlace de Internet muestra que está *conectada* a la VPC. Esto se hizo con este código en la plantilla de CloudFormation:

```
AttachGateway:
  Type: AWS::EC2::VPCGatewayAttachment
  Properties:
    VpcId: !Ref VPC
    InternetGatewayId: !Ref InternetGateway
```

Un adjunto de puerta de enlace de VPC crea una relación entre una VPC y una puerta de enlace, como esta puerta de enlace de Internet.

Observe que la plantilla hace referencia a otros elementos de la plantilla con la palabra clave *!Ref*, seguida del nombre del otro recurso. Esto facilita la creación de recursos que se vinculan entre sí simplemente mediante una referencia a su nombre.

1. En el panel de navegación izquierdo, haga clic en **Subnets** (Subredes).

Aparecerán dos subredes:

- **La subred pública 1** está conectada a Internet a través de la puerta de enlace de Internet y puede ser utilizada por recursos de acceso público.
- **La subred privada 1** *no* está conectada a Internet. No se puede acceder a los recursos de esta subred desde Internet, lo que proporciona seguridad adicional en torno a estos recursos.

Este es el código de la plantilla de CloudFormation que creó las subredes:

```
PublicSubnet1:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref VPC
    CidrBlock: 10.0.0.0/24
    AvailabilityZone: !Select
      - '0'
      - !GetAZs ''
  Tags:
    - Key: Name
      Value: Public Subnet 1
PrivateSubnet1:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref VPC
    CidrBlock: 10.0.1.0/24
    AvailabilityZone: !Select
      - '0'
      - !GetAZs ''
  Tags:
    - Key: Name
      Value: Private Subnet 1
```

Las propiedades son las siguientes:

- **VpcId** hace referencia a la VPC que contiene la subred.
- **CidrBlock** es el intervalo de direcciones IP asignadas a la subred.
- **AvailabilityZone** define qué ubicación física dentro de la región debe contener la subred.

Tenga en cuenta que la zona de disponibilidad utiliza una función denominada **!Select** y una función llamada **!GetAZs**. El código recupera una lista de zonas de disponibilidad de la región y hace referencia al primer elemento de la lista. De este modo, la plantilla se puede utilizar en cualquier región porque recupera la lista de zonas de disponibilidad en tiempo de ejecución en lugar de tener las zonas de disponibilidad codificadas de forma rígida en la plantilla.

1. En el panel de navegación izquierdo, haga clic en **Route Tables** (Tabla de enrutamiento).
2. Seleccione la **tabla de enrutamiento pública**.
3. Haga clic en la pestaña **Routes** (Rutas) en la mitad inferior de la ventana.

Las tablas de enrutamiento se utilizan para dirigir (o *dirigir*) el tráfico dentro y fuera de las subredes. La configuración de esta tabla de enrutamiento es la siguiente:

- Para el tráfico dentro de la VPC (10.0.0.0/16), dirija el tráfico de forma local.
- Para el tráfico que va a Internet (0.0.0.0/0), dirija el tráfico a la puerta de enlace de Internet (indicada con *igw*-).

Este es el código de la plantilla de CloudFormation que creó la tabla de enrutamiento pública:

```
PublicRouteTable:
  Type: AWS::EC2::RouteTable
  Properties:
    VpcId: !Ref VPC
    Tags:
      - Key: Name
        Value: Public Route Table
```

También hay un código similar para la tabla de enrutamiento privada.

Este es el código que definió la ruta a Internet dentro de la tabla de enrutamiento pública:

```
PublicRoute:
  Type: AWS::EC2::Route
  Properties:
    RouteTableId: !Ref PublicRouteTable
    DestinationCidrBlock: 0.0.0.0/0
    GatewayId: !Ref InternetGateway
```

La configuración de la ruta es la siguiente:

- **RouteTableId** indica la tabla de enrutamiento que tiene la ruta.
- **DestinationCidrBlock** define el intervalo de direcciones IP para esta regla de enrutamiento (donde 0.0.0.0/0 se refiere al tráfico destinado a Internet).
- **GatewayId** define a dónde dirigir el tráfico, que en este caso es la puerta de enlace de Internet definida anteriormente en la plantilla.

Esta ruta solo está configurada para la tabla de enrutamiento pública, que es lo que la hace *pública*.

1. Haga clic en la pestaña **Subnet Associations** (Asociaciones de subred).

En la consola se muestra que la tabla de enrutamiento pública está *asociada* a la **subred pública 1**. Una tabla de enrutamiento se puede asociar a varias subredes, y cada asociación requiere una vinculación explícita.

Este es el código que definió esta vinculación:

```
PublicSubnetRouteTableAssociation1:
  Type: AWS::EC2::SubnetRouteTableAssociation
  Properties:
    SubnetId: !Ref PublicSubnet1
    RouteTableId: !Ref PublicRouteTable
```

Declare que la **subred pública 1** está asociada a la **tabla de enrutamiento pública**.

Además de crear recursos, CloudFormation puede proporcionar información sobre los recursos que se han creado.

1. En el menú Services (Servicios), haga clic en **CloudFormation**.
2. Haga clic en la pila **Lab** (Laboratorio).
3. Haga clic en la pestaña **Outputs** (Salidas).

La plantilla de CloudFormation se ha configurado para devolver información sobre los recursos que creó:

- **VPC** es el ID de la VPC que se creó.
- **AZ1** muestra la zona de disponibilidad en la que se crearon las subredes.

Este es el código que configuró las salidas:

```
Outputs:
  VPC:
    Description: VPC
    Value: !Ref VPC
  AZ1:
    Description: Availability Zone 1
    Value: !GetAtt
      - PublicSubnet1
      - AvailabilityZone
```

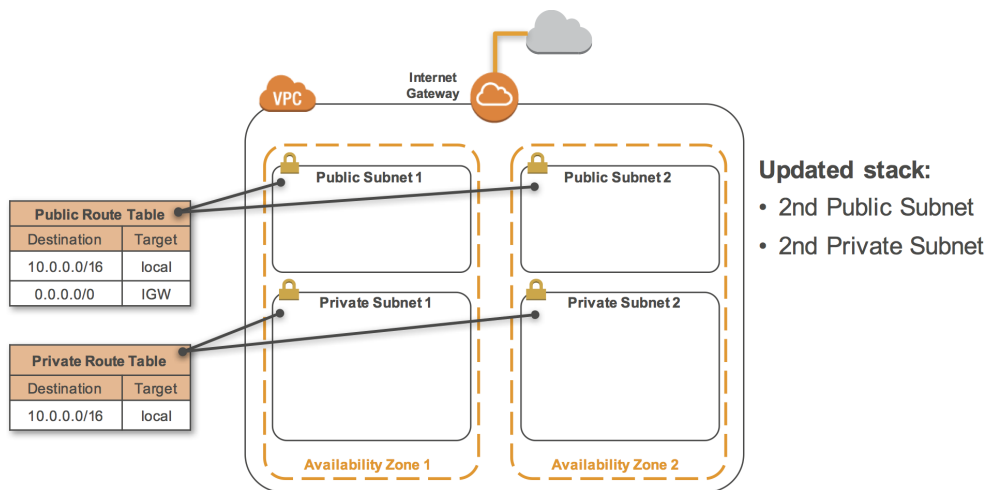
La salida de la VPC es simplemente una referencia a la VPC, lo que hace que se muestre el ID de la VPC.

La salida AZ1 utiliza la función **!GetAtt** para recuperar un *atributo* de los recursos. En este caso, recupere el atributo AvailabilityZone de la subred pública 1.

## Tarea 3: Actualizar una pila

Una vez implementada una pila de CloudFormation, se recomienda que cualquier cambio en los recursos se realice a través de CloudFormation en lugar de modificarlos directamente.

En esta tarea, actualizará la pila con una nueva plantilla de CloudFormation que define los siguientes recursos:



Se han agregado subredes públicas y privadas adicionales en otra zona de disponibilidad. Esta es una práctica recomendada para garantizar que los recursos se puedan ejecutar en varios centros de datos (zonas de disponibilidad) para garantizar la *alta disponibilidad* en caso de que se produzcan fallos del sistema.

1. Haga clic con el botón secundario en este enlace para descargar una plantilla de CloudFormation actualizada a su equipo: [vpc-2.yaml](#)

1. Haga clic en Update (Actualizar) y luego configure lo siguiente:

- Seleccione Replace current template (Reemplazar plantilla actual).
- Haga clic en Upload a template file (Subir un archivo de plantilla).
- Haga clic en Choose file (Elegir archivo).
- Seleccione la plantilla **vpc-2.yaml** que acaba de descargar.

1. Haga clic en Next (Siguiente).

2. Haga clic en Next (Siguiente).

Aceptará las opciones predeterminadas.

1. Desplácese hasta la parte inferior de la pantalla y haga clic en Next (Siguiente).

Examine la sección **Change set preview** (Cambiar configuración de vista previa) en la parte inferior de la página. Muestra lo que sucederá cuando se actualice la pila:

Indica que se crearán dos nuevas subredes. Además, se agregarán dos *asociaciones de tablas de enrutamiento* para asociar estas

subredes con las tablas de enrutamiento adecuadas.

1. Desplácese hasta la parte inferior de la pantalla y haga clic en Update stack (Actualizar pila).

Examine la pestaña **Events** (Eventos) mientras se actualiza la pila.

1. Haga clic en la pestaña **Stack info** (Información de pila).

Haga clic en Refresh (Actualizar) hasta que el estado sea **UPDATE\_COMPLETE**.

1. Haga clic en la pestaña **Outputs** (Salidas).

Se muestra una zona de disponibilidad adicional, con un valor diferente al de la zona de disponibilidad original.

1. En el menú Services (Servicios), haga clic en **VPC**.
2. En la esquina superior izquierda **Filter by VPC** (Filtrar por VPC), seleccione **Lab VPC** (VPC de laboratorio).
3. En el panel de navegación izquierdo, haga clic en **Subnets** (Subredes).

Ahora se muestran cuatro subredes. Haga clic en cada una de ellas y examine su configuración en la pestaña **Route Table** (Tabla de enrutamiento).

La VPC se ha actualizado para admitir aplicaciones de alta disponibilidad.

## Tarea 4: Visualizar una pila en AWS CloudFormation Designer

En esta tarea, verá la plantilla mediante AWS CloudFormation Designer.

AWS CloudFormation Designer (Designer) es una herramienta gráfica para crear, ver y modificar plantillas de AWS CloudFormation. Con Designer, puede crear diagramas de los recursos de su plantilla

mediante una interfaz de arrastrar y soltar y, a continuación, editar sus detalles con el editor JSON y YAML integrado. Tanto si es un usuario nuevo como si es un usuario experimentado de AWS CloudFormation, AWS CloudFormation Designer puede ayudarlo a ver rápidamente la interrelación entre los recursos de una plantilla y a modificarla con facilidad.

1. En el menú Services (Servicios), haga clic en **CloudFormation**.
2. Haga clic en la pila **Lab** (Laboratorio).
3. Haga clic en la pestaña **Template** (Plantilla).
4. Haga clic en View in Designer (Ver en Designer)

La parte superior de la ventana proporciona información general gráfica de la VPC definida por la plantilla.

1. Utilice los controles de Zoom para examinar el diagrama. Arrastre la imagen para mover el diagrama.
2. En la parte inferior de la página, haga clic en la pestaña **Components** (Componentes).
3. Haga clic en algunos elementos del diagrama.

En la parte inferior de la ventana se muestra el código de la plantilla que define el recurso.

Las flechas muestran la relación entre los recursos, como las tablas de enrutamiento asociadas a las subredes.

1. En **Choose template language** (Elegir idioma de plantilla), haga clic en **JSON**.

Designer también puede convertir código entre formatos JSON y YAML.

## Tarea 5: Eliminar la pila

En esta tarea, eliminará la pila, lo que eliminará automáticamente la VPC y sus componentes.



1. En la parte superior izquierda de la pantalla, haga clic en el enlace **Close** (Cerrar).

Esto cerrará Designer. Haga clic en **Leave Page** (Abandonar página), si le aparece esta opción, para salir.

1. Seleccione la pila de **Lab** (Laboratorio).
2. Haga clic en Delete (Eliminar) y, a continuación, en Delete stack (Eliminar pila).
3. Haga clic en la pestaña **Events** (Eventos) para ver los detalles de la eliminación.

Haga clic en Refresh (Actualizar) hasta que se elimine la pila.

Cuando se haya eliminado la pila, desaparecerá de la lista.

La VPC también se ha eliminado.

1. En el menú Services (Servicios), haga clic en **VPC**.
2. En el panel de navegación izquierdo, haga clic en **Your VPCs** (Mis VPC).

La **VPC de laboratorio** ya no aparece en la lista. Además, se han eliminado la puerta de enlace de Internet, las subredes y las tablas de enrutamiento asociadas.

## Conclusión

Felicitaciones. Ahora ha aprendido correctamente cómo hacer lo siguiente:

- implementar una plantilla de AWS CloudFormation que cree una Amazon VPC
- examinar los componentes de la plantilla
- actualizar de una pila de CloudFormation
- examinar una plantilla con AWS CloudFormation Designer
- eliminar una pila de CloudFormation

# Finalizar laboratorio

Siga los pasos que se indican a continuación para cerrar la consola, finalizar el laboratorio y evaluar la experiencia.

1. Regrese a la consola de administración de AWS.
2. En la barra de navegación, haga clic en **awsstudent@<AccountNumber>** y luego en **Sign Out** (Cerrar sesión).
3. Haga clic en End Lab (Finalizar laboratorio).
4. Haga clic en OK (Aceptar).
5. (Opcional):
  - Seleccione la cantidad de estrellas que correspondan.
  - Escriba un comentario.
    - 1 estrella = Muy insatisfecho
    - 2 estrellas = Insatisfecho
    - 3 estrellas = Neutral
    - 4 estrellas = Satisfecho
    - 5 estrellas = Muy satisfecho

Puede cerrar el cuadro de diálogo si no quiere enviar comentarios.

Para obtener más información acerca de AWS Training and Certification, consulte <http://aws.amazon.com/training/>.

*Se agradecen sus comentarios.*

Si desea compartir comentarios, sugerencias o correcciones, proporcione los detalles en nuestro [Formulario de contacto de AWS Training and Certification](#).