

## S4: Laboratorio: Recursos de redes para una VPC

### Objetivos

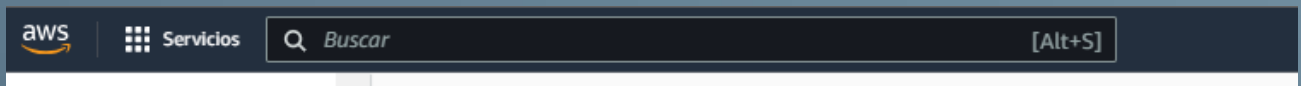
En este laboratorio usted:

1. Resumir la situación del cliente
2. Crear una VPC, una puerta de enlace de Internet, una tabla de enrutamiento, un grupo de seguridad, una lista de acceso de redes y una instancia de EC2 para generar un red enrutable dentro de la VPC.
3. Familiarizarse con la consola
4. Desarrollar una solución para el problema del cliente presentado en esta sesión de laboratorio

La sesión de laboratorio se completará una vez que pueda utilizar con éxito el comando ping por fuera de la VPC.

### Tarea 1: investigar el entorno del cliente

1. Una vez que se encuentre en la consola de AWS, haga clic en VPC, en Recently visited services (Servicios visitados recientemente). Si no está allí, navegue hasta la esquina superior izquierda y seleccione VPC (VPC) en Networking and Content Delivery (Redes y entrega de contenido), en el panel de navegación Services (Servicios).



1. Ahora se encuentra en el panel de Amazon VPC. Utilice el servicio Amazon Virtual Private Cloud (Amazon VPC) para crear la VPC.
2. Comience por la parte superior del panel de navegación izquierdo, en Your VPCs (Sus VPC), y avance hacia abajo. Seleccione Your VPCs (Sus VPC), navegue hasta la esquina superior derecha, y seleccione Create VPC (Crear VPC).

**Crear VPC**

**Lanzar instancias EC2**

Nota: Sus instancias se lanzarán en la región EE.UU. Oeste.

## Configuración de la VPC

### Recursos que se van a crear [Información](#)

Cree únicamente el recurso de VPC o la VPC y otros recursos de red.

☒ Solo la VPC

☐ VPC y más

### Etiqueta de nombre - *opcional*

Crea una etiqueta con una clave de "Nombre" y el valor que usted especifique.

Test VPC

### Bloque de CIDR IPv4 [Información](#)

☒ Entrada manual de CIDR IPv4

☐ Bloque de CIDR IPv4 asignado por IPAM

### CIDR IPv4

192.168.0.0/18

El tamaño del bloque CIDR debe estar entre /16 y /28.

### Bloque de CIDR IPv6 [Información](#)

☒ Sin bloque de CIDR IPv6

☐ Bloque de CIDR IPv6 asignado por IPAM

☐ Bloque de CIDR IPv6 proporcionado por Amazon

☐ CIDR IPv6 de mi propiedad

### Tenencia [Información](#)

Predeterminado

## Etiquetas

Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizar las etiquetas para buscar y filtrar sus recursos o hacer un seguimiento de los costos de AWS.

### Clave

Q Name

X

### Valor - *opcional*

Q Test VPC

X

Eliminar etiqueta

Agregar etiqueta

Puede agregar 49 etiquetas más

3. Asigne un nombre a la VPC: Test VPC. Bloque de CIDR IPv4: 192.168.0.0/18
4. Deje el resto de los parámetros con los valores predeterminados y seleccione Create VPC (Crear VPC)
5. Ahora que la VPC está completa, mire el panel de navegación izquierdo y seleccione Subnets (Subredes). En la esquina superior derecha, seleccione Create subnet (Crear subred).

Nota: aunque se puede crear casi todo en cualquier orden, es más fácil abordar un enfoque. Seguir un flujo o un enfoque le servirá para solucionar problemas y garantizar que no se olvide un recurso.

6. Establezca la configuración según la siguiente imagen:

## Crear subred [Información](#)

### VPC

ID de la VPC

Cree subredes en esta VPC.

vpc-024377366905b4d95 (Test VPC) ▼

### CIDR de VPC asociados

CIDR IPv4

192.168.0.0/18

### Configuración de la subred

Especifique los bloques de CIDR y la zona de disponibilidad de la subred.

#### Subred 1 de 1

Nombre de la subred

Cree una etiqueta con una clave de "Nombre" y el valor que especifique.

Public Subnet

El nombre puede tener un máximo de 256 caracteres.

Zona de disponibilidad [Información](#)

Elija la zona en la que residirá la subred o deje que Amazon elija una por usted.

Sin preferencia ▼

IPv4 VPC CIDR block [Información](#)

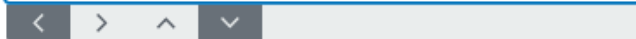
Choose the IPv4 VPC CIDR block to create a subnet in.

192.168.0.0/18 ▼

IPv4 subnet CIDR block

192.168.0.0/28

16 IPs



7. Navegue hasta el panel de navegación izquierdo y seleccione Route Tables (Tablas de enrutamiento). En la esquina superior derecha, seleccione Create route table (Crear tabla de enrutamiento).

8. Establezca la configuración según la siguiente imagen:

## Crear tabla de enrutamiento [Información](#)

Una tabla de enrutamiento especifica cómo se envían los paquetes entre las subredes de la VPC, Internet y la conexión de la VPN.

### Configuración de la tabla de enrutamiento

#### Nombre - *opcional*

Cree una etiqueta con una clave de "Nombre" y el valor que especifique.

#### VPC

La VPC que se debe usar para esta tabla de enrutamiento.

### Etiquetas

Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizar las etiquetas para buscar y filtrar sus recursos o hacer un seguimiento de los costos de AWS.

#### Clave



#### Valor - *opcional*



Puede agregar 49 más etiquetas.

9. Elija Create route table (Crear tabla de enrutamiento).
10. En el panel de navegación izquierdo, seleccione Internet Gateways (Puertas de enlace de Internet). Seleccione Create internet gateway (Crear puerta de enlace de Internet) en la esquina superior derecha para crear una puerta de enlace de Internet (IGW).
11. Establezca la configuración según la siguiente imagen:

## Crear gateway de Internet [Información](#)

Una gateway de Internet es un router virtual que conecta una VPC a Internet. Para crear una nueva gateway de Internet, especifique el nombre de la gateway a continuación.

### Configuración de gateway de Internet

#### Etiqueta de nombre

Crea una etiqueta con una clave de "Nombre" y el valor que usted especifique.

#### Etiquetas: *opcional*

Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizar las etiquetas para buscar y filtrar sus recursos o hacer un seguimiento de los costos de AWS.

#### Clave



#### Valor - *opcional*



Puede agregar 49 más etiquetas.

12. Elija Create internet gateway (Crear puerta de enlace de internet).
13. Una vez creada, adjunte la puerta de enlace de Internet a la VPC seleccionando Attach to VPC (Adjuntar a VPC).
14. Seleccione Test VPC (VPC de prueba).
15. Elija Attach Internet gateway (Adjuntar puerta de enlace de Internet).

### Conectar a la VPC (igw-0e38f579aeb9e898d) [Información](#)

#### VPC

Conecte una gateway de Internet a la VPC para habilitar la comunicación con Internet. Especifique la VPC que desea asociar a continuación.

VPC disponibles

Conecte la gateway de Internet a esta VPC.

► Comando de la interfaz de línea de comandos de AWS

[Cancelar](#) [Conectar gateway de Internet](#)

16. Navegue hasta la sección Route Table (Tabla de enrutamiento), ubicada en el panel de navegación izquierdo. Seleccione Public Route Tables(Tablas de enrutamiento públicas), desplácese hasta la parte inferior y seleccione la pestaña Routes (Rutas). Seleccione el botón “Edit routes” (Editar rutas), ubicado en la casilla de rutas.

En la página “Edit routes” (Editar rutas), la primera dirección IP es la ruta local, que no se puede modificar.

Seleccione Add route (Agregar ruta).

- En la sección Destination (Destino), escriba 0.0.0.0/0 en la casilla de búsqueda. Esta es la ruta a la IGW. Se le indica a la tabla de enrutamiento que cualquier tráfico que necesite conectarse a Internet usará 0.0.0.0/0 para llegar a la IGW y a Internet.
- Haga clic en la sección Target (Objetivo) y seleccione Internet Gateway (Puerta de enlace de Internet), ya que está dirigiendo todo el tráfico que necesita ir a Internet a la IGW. Una vez que seleccione la IGW, aparecerá su TEST VPC IGW (IGW DE LA VPC DE PRUEBA). Seleccione esa IGW, navegue hasta la parte inferior derecha y seleccione Save changes (Guardar cambios).

## Editar rutas

Destino	Destino	Estado
192.168.0.0/18	local	✓ Activo
<input type="text" value="Q 0.0.0.0/0"/>	<input type="text" value="local"/>	
	<input type="text" value="Puerta de enlace de Internet"/>	-
	<input type="text" value="igw-0e38f579aeb9e898d"/>	

Ahora el tráfico tiene una ruta a Internet a través de la IGW.

- En el panel de la tabla de enrutamiento pública, seleccione la pestaña Subnet associations (Asociaciones de subred). Seleccione el botón Edit subnet associations (Editar asociaciones de subred).
- Seleccione Save associations (Guardar asociaciones).

Nota: Todas las tablas de enrutamiento deben estar asociadas a una subred. Ahora, asocie esta tabla de enrutamiento a esta subred. Como habrá notado, la convención de nomenclatura se mantiene igual (tabla de enrutamiento pública, subred pública, etc.) para asociar los mismos recursos en conjunto. Tenga en cuenta esto cuando aumenten la red y los recursos. Puede haber varios recursos iguales y, por ende, generarse confusión sobre adónde pertenece cada uno.

## Editar asociaciones de subredes

Cambiar las subredes que están asociadas a esta tabla de enrutamiento.

Subredes disponibles (1/1)			
<input type="text" value="Filtrar asociaciones de subredes"/>			
<input checked="" type="checkbox"/>	Nombre	ID de subred	CIDR IPv4
<input checked="" type="checkbox"/>	Public Subnet	<a href="#">subnet-024205d83e3ba5df0</a>	192.168.0.0/28

**Subredes seleccionadas**

- En el panel de navegación izquierdo, seleccione Network ACLs (ACL de red). Navegue hasta la esquina superior derecha y seleccione Create network ACL (Crear ACL de red) para crear una lista de control de acceso a la red (NACL).
- Nómbrela Public Subnet NACL. En VPC seleccione Test VPC (VPC de prueba).
- Seleccione Create network ACL (Crear ACL de red).

## Crear ACL de red

[Información](#)

Una ACL de red es una capa de seguridad opcional que funciona como un firewall para controlar el tráfico entrante y saliente de una subred.

### Configuración de ACL de red

#### Nombre - *opcional*

Crea una etiqueta con una clave de "Nombre" y el valor que usted especifique.

Public Subnet NACL

#### VPC

La VPC que se debe usar para esta ACL de red.

vpc-024377366905b4d95 (Test VPC)

### Etiquetas

Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizar las etiquetas para buscar y filtrar sus recursos o hacer un seguimiento de los costos de AWS.

#### Clave

Q Name X

#### Valor - *opcional*

Q Public Subnet NACL X

Eliminar etiqueta

Agregar etiqueta

Puede agregar 49 etiquetas más

Cancelar

Crear ACL de red

22. Seleccione Public Subnet NACL (NACL de subred pública). Seleccione la pestaña Inbound rules (Reglas de entrada) y elija Edit inbound rules (Editar reglas de entrada).
23. Elija Add new rule (Agregar nueva regla). En Rule number (Número de regla), use 100. En Type (Tipo), seleccione All Traffic (Todo el tráfico).
24. Deje los valores predeterminados en Source (Origen) y Allow/Deny (Permitir/denegar) por defecto y elija Save changes (Guardar cambios).

## Editar reglas de entrada

[Información](#)

Las reglas de entrada controlan el tráfico entrante que tiene permiso para llegar a la VPC.

Número de regla <a href="#">Información</a>	Tipo <a href="#">Información</a>	Protocolo <a href="#">Información</a>	Rango de puertos <a href="#">Información</a>
100	Todo el tráfico	Todo	Todo
*	Todo el tráfico	Todo	Todo
Agregar nueva regla Ordenar por número de regla			

25. Haga lo mismo con Outbound rules (Reglas de salida).

## Editar reglas de salida [Información](#)

Las reglas de salida controlan el tráfico saliente que tiene permiso para dejar la VPC.

Número de  
regla [Información](#)

100

\*

Tipo [Información](#)

Todo el tráfico

Todo el tráfico

Protocolo [Información](#)

Todo

Todo

Agregar nueva regla

Ordenar por número de regla

Entrada Después de crear la NACL, debería tener el siguiente aspecto. Esto indica que hay un solo número de regla, que es 100 y que establece que todo el tráfico, todos los protocolos y todos los rangos de puerto desde cualquier origen (0.0.0.0/0) pueden ingresar (entrar) a la subred. El asterisco \* indica que se rechaza todo lo que no coincida con esta regla.

ACL de red (1/3) [Información](#)

Find resources by attribute or tag

Name	ID de ACL de red	Asociada a	Predeter...	ID de la VPC	Recuento de reglas de e...	Recuento de reglas de s...	Propietario
-	<a href="#">acl-08ab78b0f64a729c8</a>	<a href="#">4 Subredes</a>	Sí	<a href="#">vpc-0b9fb43b88b62ed4d</a>	2 Reglas de entrada	2 Reglas de salida	122642828031
-	<a href="#">acl-0053c2dca48fc453</a>	<a href="#">subnet-024205d83e3ba5df0 / Public Subnet</a>	Sí	<a href="#">vpc-024377366905b4d95 / Test VPC</a>	2 Reglas de entrada	2 Reglas de salida	122642828031
<input checked="" type="checkbox"/> Public Subnet NACL	<a href="#">acl-0353eaf3b9ecfc70</a>	-	No	<a href="#">vpc-024377366905b4d95 / Test VPC</a>	2 Reglas de entrada	2 Reglas de salida	122642828031

acl-0353eaf3b9ecfc70 / Public Subnet NACL

Detalles **Reglas de entrada** Reglas de salida Asociaciones de subredes Etiquetas

Reglas de entrada (2) [Editar reglas de entrada](#)

Filter inbound rules

Número de regla	Tipo	Protocolo	Rango de puertos	Origen	Permitir/denegar
100	Todo el tráfico	Todo	Todo	0.0.0.0/0	Allow
*	Todo el tráfico	Todo	Todo	0.0.0.0/0	Deny

26. En el panel de navegación izquierdo, seleccione Security Groups (Grupos de seguridad). Navegue hasta la esquina superior derecha y seleccione Create security group (Crear grupo de seguridad) para crear uno.

Establezca la configuración según la siguiente imagen :

Nota: en la parte de la VPC, elimine la VPC actual y seleccione Test VPC (VPC de prueba).



## Crear grupo de seguridad [Información](#)

Un grupo de seguridad actúa como un firewall virtual para que la instancia controle el tráfico de entrada y salida. Para crear un nuevo grupo de seguridad, complete los campos siguientes.

### Detalles básicos

Nombre del grupo de seguridad [Información](#)

Public security group

El nombre no se puede editar después de su creación.

Descripción [Información](#)

allows public acces

VPC [Información](#)

vpc-024377366905b4d95 (Test VPC)

### Reglas de entrada [Información](#)

Tipo <a href="#">Información</a>	Protocolo <a href="#">Información</a>	Intervalo de puertos <a href="#">Información</a>	Origen <a href="#">Información</a>
SSH	TCP	22	Anywhere-IPv4
HTTPS	TCP	443	Anywhere-IPv4
HTTP	TCP	80	Anywhere-IPv4

## 27. Elija Create security group (Crear grupo de seguridad).

Ahora tiene una VPC funcional. La siguiente tarea es lanzar una instancia de EC2 para verificar que todo funcione.

## Tarea 2: lanzar la instancia de EC2 y establecer una conexión SSH con la instancia

- Navegue hasta Services (Servicios) en la parte superior izquierda y seleccione EC2. En el panel de EC2, seleccione Instances (Instancias).
- Selecione Launch instances (Iniciar instancias) en la esquina superior derecha. A continuación, utilice las siguientes configuraciones:
- Asigne a la instancia el nombre: Test EC2
- En Application and OS Images (Amazon Machine Image) (Imágenes de aplicaciones y sistemas operativos [Imagen de máquina de Amazon]) deje seleccionada la Amazon Linux 2023 AMI predeterminada.
- En Instance Type (Tipo de instancia), deje seleccionado el valor predeterminado t2.micro.
- En Key pair (login) (Par de claves [inicio de sesión]) seleccione AWS Labs KeyPair-\*
- En Network settings (Configuración de red) seleccione Edit (Editar) y asegúrese de seleccionar Test VPC (VPC de prueba).
- En Subnet (Subred) asegúrese de que está seleccionada Public Subnet (Subred pública).
- En Auto-assign Public IP (Asignar automáticamente IP pública) seleccione Enable (Habilitar).
- En Firewall (security groups) (Firewall [grupos de seguridad]): elija Select existing security group (Seleccionar grupo de seguridad existente).
- Selecione un grupo de seguridad público.

▼ Configuraciones de red [Información](#)

VPC - required [Información](#)

vpc-024377366905b4d95 (Test VPC)  
192.168.0.0/18

↻

Subred [Información](#)

subnet-024205d83e3ba5df0  
Public Subnet  
VPC: vpc-024377366905b4d95 Propietario: 122642828031  
Zona de disponibilidad: us-west-2c Direcciones IP disponibles: 11  
CIDR: 192.168.0.0/28

↻ [Crear nueva subred](#)

Asignar automáticamente la IP pública [Información](#)

Habilitar

▼

Firewall (grupos de seguridad) [Información](#)

Un grupo de seguridad es un conjunto de reglas de firewall que controlan el tráfico de la instancia. Agregue reglas para permitir que un tráfico específico llegue a la instancia.

☐ Crear grupo de seguridad

☒ Seleccionar un grupo de seguridad existente

Grupos de seguridad comunes [Información](#)

Seleccionar grupos de seguridad

↻ [Compare reglas de grupo de seguridad](#)

Public security group sg-003cc02b5fd0deaf7 ✕  
VPC: vpc-024377366905b4d95

Los grupos de seguridad que agrega o elimine aquí se agregarán a todas las interfaces de red o se eliminarán de ellas.

► Configuración de red avanzada

39. En Configure storage (Configurar almacenamiento) deje seleccionado el gp3 predeterminado.
40. Seleccione Launch Instance (Iniciar instancia).
41. En la parte inferior, seleccione View all instances (Ver todas las instancias).
42. Seleccione la instancia de EC2 de prueba y, en la pestaña Details (Detalles), copie la dirección IPv4 pública.

### Tarea 3: usar el ping para probar la conectividad a Internet

Ejecute el siguiente comando para probar la conectividad a Internet:

ping google.com

```
ec2-user@ip-192-168-0-8:~  
login as: ec2-user  
Authenticating with public key "imported-openssh-key"  
  
#  
_#####_ Amazon Linux 2023  
~~\#####\  
~~\_#####\  
~~\_###|  
~~\_#/ https://aws.amazon.com/linux/amazon-linux-2023  
~~V~' '~>  
~~~~  
~~.-.  
_____  
/_m/' ~
```

[ec2-user@ip-192-168-0-8 ~]\$ ping google.com  
PING google.com (172.217.14.238) 56(84) bytes of data:  
64 bytes from sea30s02-in-fl4.1el100.net (172.217.14.238): icmp\_seq=1 ttl=55 time =6.53 ms  
64 bytes from sea30s02-in-fl4.1el100.net (172.217.14.238): icmp\_seq=2 ttl=55 time =6.53 ms  
64 bytes from sea30s02-in-fl4.1el100.net (172.217.14.238): icmp\_seq=3 ttl=55 time =6.53 ms  
64 bytes from sea30s02-in-fl4.1el100.net (172.217.14.238): icmp\_seq=4 ttl=55 time =6.61 ms  
64 bytes from sea30s02-in-fl4.1el100.net (172.217.14.238): icmp\_seq=5 ttl=55 time =6.58 ms

Ejecute el ping para probar la conectividad. Los resultados anteriores indican que tiene respuestas de google.com y que tiene una pérdida de paquetes del 0 %.

Si recibe respuestas, significa que tiene conectividad.