

ACTIVIDAD 1.2 - CREACIÓN DE UNA VPC Y LANZAMIENTO DE UN SERVIDOR WEB

INTRODUCCIÓN

En este laboratorio, deberá utilizar Amazon Virtual Private Cloud (VPC) para crear su propia VPC y agregarle componentes adicionales con el fin de generar una red personalizada. Además, creará grupos de seguridad para su instancia EC2. Luego, tendrá que configurar y personalizar una instancia EC2 para ejecutar un servidor web y lanzarlo en la VPC.

Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar recursos de Amazon Web Services (AWS) en la red virtual que usted defina. Esta red virtual se asemeja en gran medida a una red tradicional que ejecutaría en su propio centro de datos, con los beneficios de utilizar la infraestructura escalable de AWS. Puede crear una VPC que abarque varias zonas de disponibilidad.

Situación

En este laboratorio, creará la siguiente infraestructura:

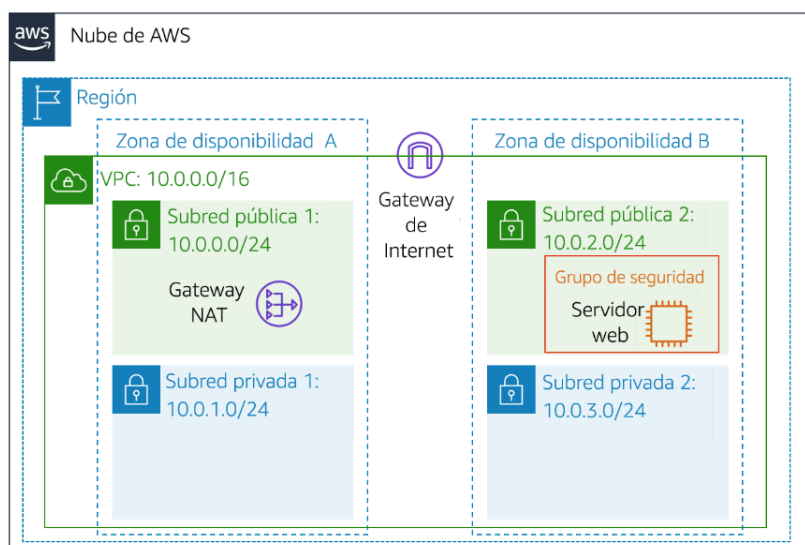


Tabla de enrutamiento pública

Destino	Objetivo
10.0.0.0/16	Local
0.0.0.0/0	Gateway de Internet

Tabla de enrutamiento privada

Destino	Objetivo
10.0.0.0/16	Local
0.0.0.0/0	Gateway NAT

Objetivos

Después de completar este laboratorio, podrá hacer lo siguiente:

- Crear una VPC
- Crear subredes
- Configurar un grupo de seguridad
- Lanzar una instancia EC2 en una VPC

ACCESO A LA CONSOLA DE ADMINISTRACIÓN DE AWS

1. En la parte superior de estas instrucciones, haga clic en Start Lab (Iniciar laboratorio) para lanzar su laboratorio.
Se abrirá el panel “Start Lab” (Iniciar laboratorio), donde se muestra el estado del laboratorio.
2. Espere hasta que aparezca el mensaje “**Lab status: ready**” (Estado del laboratorio: listo) y, luego, haga clic en la **X** para cerrar el panel “Start Lab (Iniciar laboratorio)”.
3. En la parte superior de estas instrucciones, haga clic en AWS.

La consola de administración de AWS se abrirá en una nueva pestaña del navegador. El sistema iniciará su sesión automáticamente.

Sugerencia: Si no se abre una pestaña nueva del navegador, debería aparecer un banner o un icono en la parte superior de este, el cual indique que el navegador no permite que se abran ventanas emergentes en el sitio. Haga clic en el banner o en el icono, y elija “Allow pop ups” (Permitir ventanas emergentes).

4. Ubique la pestaña de la consola de administración de AWS en un lugar donde aparezca al lado de estas instrucciones. Idealmente, debería poder ver ambas pestañas del navegador al mismo tiempo para que sea más sencillo seguir los pasos del laboratorio.

TAREA 1: CREAR UNA VPC

En esta tarea, utilizará el asistente de VPC para crear una VPC, una gateway de Internet y dos subredes en una única zona de disponibilidad. Una **gateway de Internet (IGW)** es un componente de la VPC que permite la comunicación entre instancias de la VPC e Internet.

Después de crear una VPC, puede agregar **subredes**. Cada subred está ubicada por completo dentro de una zona de disponibilidad y no puede abarcar otras zonas. Si el tráfico de una subred

se direcciona a una gateway de Internet, la subred recibe el nombre de *subred pública*. Si una subred no dispone de una ruta a la gateway de Internet, recibe el nombre de *subred privada*.

El asistente también creará una *Gateway NAT*, que se utiliza para proporcionar conectividad a Internet a instancias EC2 en las subredes privadas.

5. En la **consola de administración de AWS**, encontrará el menú **Servicios (Servicios)**, donde debe hacer clic en **VPC**.
6. Haga clic en **Crear VPC**.
7. Seleccione **VPC y más**.
8. Configure lo siguiente:
 - **Nombre de la VPC:** Lab VPC
 - **Bloque de CIDR IPv4:** 10.0.0.0/16
 - **Availability Zone (Zona de disponibilidad):** seleccione 1 zona de disponibilidad (asegúrese de que sea la *primera* zona). Personalizar → elige *us-east-1a*
 - **Seleccione 1 red pública**
 - **Seleccione 1 red privada**
 - **Personalice los bloques de CIDR de subredes**
 1. La subred pública tiene un CIDR de **10.0.0.0/24**, lo que significa que contiene todas las direcciones IP que comienzan con **10.0.0.x**.
 2. La subred privada tiene un CIDR de **10.0.1.0/24**, lo que significa que contiene todas las direcciones IP que comienzan con **10.0.1.x**.
 - Cree un **Gateway NAT** en 1 zona de disponibilidad
 - **Deshabilite los puntos de enlace de la VPC**

9. Haga clic en **Create VPC (Crear VPC)**

El asistente creará la VPC.

10. Una vez que la configuración esté completa, haga clic en **OK (Aceptar)**.

El asistente ha provisionado una VPC con una subred pública y una subred privada en la misma zona de disponibilidad, junto con tablas de enrutamiento para cada subred:

The screenshot shows the AWS VPC console configuration page for creating a new VPC. The configuration is as follows:

- Nombre de la VPC:** Lab VPC
- Bloque de CIDR IPv4:** 10.0.0.0/16 (65,536 IPs)
- Bloque de CIDR IPv6:** Sin bloque de CIDR IPv6
- Tenencia:** Predeterminado
- Número de zonas de disponibilidad (AZ):** 1 (us-east-1a)
- Cantidad de subredes públicas:** 1
- Cantidad de subredes privadas:** 1
- Bloque de CIDR de la subred pública en us-east-1a:** 10.0.0.0/24 (256 IPs)
- Bloque de CIDR de la subred privada en us-east-1a:** 10.0.1.0/24 (256 IPs)
- Gateways NAT (\$):** Ninguna
- Puntos de enlace de la VPC:** Ninguna
- Opciones de DNS:**
 - ☒ Habilitar nombres de host DNS
 - ☒ Habilitar la resolución de DNS

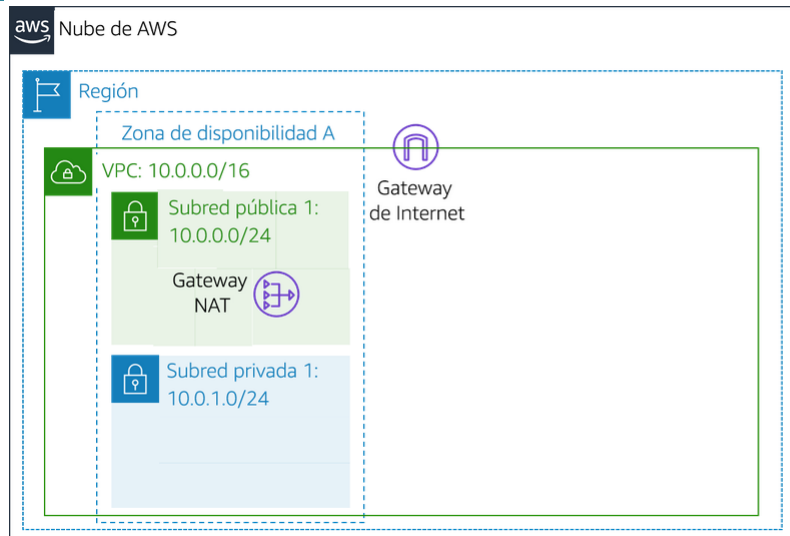


Tabla de enrutamiento pública

Destino	Objetivo
10.0.0.0/16	Local
0.0.0.0/0	Gateway de Internet

Tabla de enrutamiento privada

Destino	Objetivo
10.0.0.0/16	Local
0.0.0.0/0	Gateway NAT

TAREA 2: CREAR SUBREDES ADICIONALES

En esta tarea, creará dos subredes adicionales en una segunda zona de disponibilidad. Esto resulta útil a la hora de crear recursos en varias zonas de disponibilidad para ofrecer una *alta disponibilidad*.

- En el panel de navegación de la izquierda, haga clic en **Subnets** (Subredes).

Primero, creará una segunda subred pública.

- Haga clic en Create subnet (Crear subred) y, luego, configure lo siguiente:

- Name tag** (Etiqueta de nombre):
Public Subnet 2
(Subred pública 2)
- VPC:** *VPC de laboratorio*
- Availability Zone** (Zona de disponibilidad): seleccione la **segunda** zona de disponibilidad (**us-east-1b**)
- IPv4 CIDR block** (Bloque de CIDR IPv4):
10.0.2.0/24

La subred tendrá todas las direcciones IP que comiencen con **10.0.2.x**.

Crear subred [Información](#)

VPC

ID de la VPC
Cree subredes en esta VPC.

vpc-008081a3ac94778bd (LabVPC-vpc) ▼

CIDR de VPC asociados

CIDR IPv4
10.0.0.0/16

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 2

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.

EE.UU. Este (Norte de Virginia) / us-east-1b ▼

IPv4 VPC CIDR block [Información](#)
Choose the IPv4 VPC CIDR block to create a subnet in.

10.0.0.0/16 ▼

IPv4 subnet CIDR block

10.0.2.0/24 256 IPs

13. Haga clic en Create (Crear) y, posteriormente, en Close (Cerrar).

Ahora creará una segunda subred privada.

14. Haga clic en Create subnet (Crear subred) y, luego, configure lo siguiente:

- **Name tag** (Etiqueta de nombre): Private Subnet 2 (Subred privada 2)
- **VPC**: VPC de laboratorio
- **Availability Zone** (Zona de disponibilidad): seleccione la **(us-east-1b)** zona de disponibilidad: **(us-east-1b)**
- **CIDR block** (Bloque de CIDR): 10.0.3.0/24

La subred tendrá todas las direcciones IP que comiencen con **10.0.3.x**.

15. Haga clic en Create (Crear) y, posteriormente, en Close (Cerrar).

Ahora, configurará las subredes privadas para dirigir el tráfico orientado hacia Internet a la gateway NAT a fin de que los recursos de la subred privada puedan conectarse a Internet, a la vez que mantienen los recursos privados. Esto se realiza mediante la configuración de una *tabla de enrutamiento*.

Una *tabla de enrutamiento* contiene un conjunto de reglas llamadas *rutas* que se utilizan para determinar el destino del tráfico de red. Cada subred de una VPC debe estar asociada a una tabla de enrutamiento, que es la que controla el direccionamiento de la subred.

16. En el panel de navegación de la izquierda, haga clic en **Route Tables** (Tablas de enrutamiento).

Verás que tienes tres tablas de enrutamiento: una *public*, otra *private* y por último una sin nombre. La tabla sin nombre es la tabla principal de la VPC (Principal = Sí), que se asignará a las subredes nuevas. Haremos que esta tabla principal sea la tabla con las rutas de las redes privadas.

17. Seleccione la tabla de enrutamiento con **Main = Yes** (Principal = Sí) y **VPC = Lab VPC**. (Si fuera necesario, expanda la columna **_VPC ID [ID de VPC]** para ver el nombre de la VPC). Debería ser la que no tiene nombre

18. En el panel inferior, haga clic en la pestaña **Routes** (Rutas).

Tendrás la ruta 10.0.0.0/16 dirigida a local. Ahora añada una nueva ruta: pulsa Editar rutas, después Agregar ruta. Añade **Destination 0.0.0.0/0** (Destino 0.0.0.0/0) y el siguiente cajetín selecciona **Puerta de enlace NAT** y selecciona la ID sugerida. Guarda los cambios

Q 0.0.0.0/0 ×

Q nat- ×

nat-0ec84df7585145a67 (proyecto-nat-public1-us-east-1a)

Como resultado debería tener estas rutas:

Destino	Destino	Estado
0.0.0.0/0	nat-0ec84df7585145a67	✓ Activo
10.0.0.0/16	local	✓ Activo

LANZAMIENTO DE UN SERVIDOR WEB

Por lo tanto, esta tabla de enrutamiento se utiliza para direccionar el tráfico desde subredes privadas. Ahora, agregará un nombre a la tabla de enrutamiento para que sea más fácil de reconocer en el futuro.

19. En la columna **Name** (Nombre) de esta tabla de enrutamiento, haga clic en el lápiz y, a continuación, escriba `Private Route Table` (Tabla de enrutamiento privada) y haga clic en

20. En el panel inferior, haga clic en la pestaña **Subnet Associations** (Asociaciones de subredes).

Ahora, asociará esta tabla de enrutamiento a las subredes privadas.

21. Haga clic en `Edit subnet associations` (Editar asociaciones de subredes).

22. Seleccione ambas subredes privadas: **Private Subnet 1** (Subred privada 1) y **Private Subnet 2** (Subred privada 2).

Puede ampliar la columna *Subnet ID* (ID de subred) para visualizar los nombres de las subredes.

23. Haga clic en `Save` (Guardar).

Ahora, configurará la tabla de enrutamiento que utilizan las subredes públicas.

24. Seleccione la tabla de enrutamiento con **public en el nombre** y **VPC = Lab VPC**, y anule la selección de cualquier otra subred.

25. En la columna **Name** (Nombre) de esta tabla de enrutamiento, haga clic en el lápiz y, a continuación, escriba `Public Route Table` (Tabla de enrutamiento pública) y haga clic en

26. En el panel inferior, haga clic en la pestaña **Routes** (Rutas). Comprueba que tiene estas rutas

Destino	▼	Destino	▼	Estado
0.0.0.0/0		igw-0261a7aa9024ace05		🟢 Activo
10.0.0.0/16		local		🟢 Activo

Tenga en cuenta que **Destination 0.0.0.0/0** (Destino 0.0.0.0/0) está establecido en **Target igw-xxxxxxx** (Objetivo igw-xxxxxxx), que es la gateway de Internet. Esto significa que el tráfico orientado hacia Internet se enviará directamente a Internet mediante la gateway de Internet.

Ahora, asociará esta tabla de enrutamiento a las subredes públicas.

27. Haga clic en la pestaña **Subnet Associations** (Asociaciones de subredes).

28. Haga clic en `Edit subnet associations` (Editar asociaciones de subredes).

29. Seleccione ambas subredes: **Public Subnet 1** (Subred pública 1) y **Public Subnet 2** (Subred pública 2).

30. Haga clic en `Save` (Guardar).

Ahora tendrás un esquema de tablas de enrutamiento similar a este:

<input type="checkbox"/>	Name	ID de tabla de enrutam...	Asociaciones de subrede...	Asociaciones de b...	Princ...
<input type="checkbox"/>	public route table	rtb-0d351620516eb468b	2 subredes	–	No
<input type="checkbox"/>	proyecto-rtb-private1-us-east-1a	rtb-0e30a81323ee8a8fb	–	–	No
<input type="checkbox"/>	private route table	rtb-0248c6edf47daca67	2 subredes	–	Sí

Dos redes asociadas a la tabla pública y dos redes asociadas a la tabla privada que es principal, la tercera sobra. Selecciona la que no tiene redes asociadas (la central en la imagen), pulsa Acciones y Eliminar tabla de enrutamiento

La VPC ahora tiene subredes públicas y privadas configuradas en dos zonas de disponibilidad:

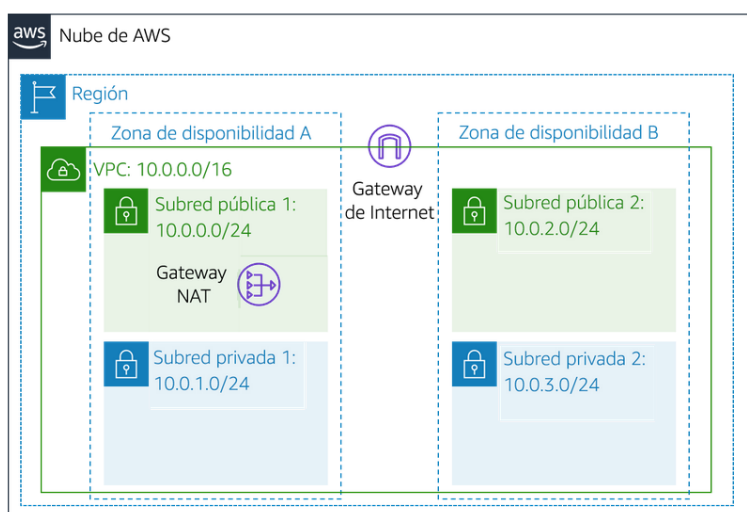


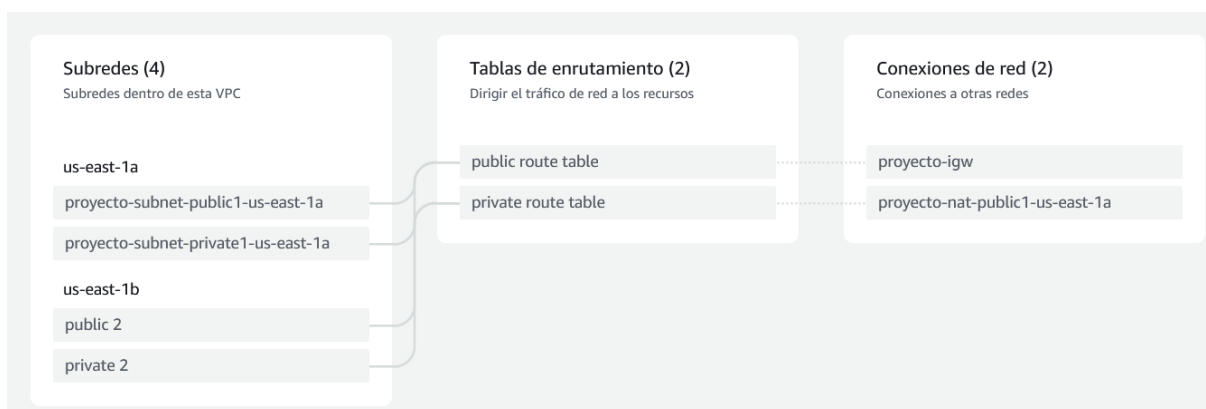
Tabla de enrutamiento pública

Destino	Objetivo
10.0.0.0/16	Local
0.0.0.0/0	Gateway de Internet

Tabla de enrutamiento privada

Destino	Objetivo
10.0.0.0/16	Local
0.0.0.0/0	Gateway NAT

El Mapa de recursos de tu VP debería ser este:



TAREA 3: CREAR UN GRUPO DE SEGURIDAD DE VPC

En esta tarea, creará un grupo de seguridad de VPC, que actúa como un firewall virtual. Cuando se lanza una instancia, se asocia uno o varios grupos de seguridad a ella. Puede agregar reglas a cada grupo de seguridad que permitan el tráfico hacia las instancias asociadas o desde ellas.


31. En el panel de navegación izquierdo, haga clic en **Security Groups** (Grupos de seguridad).
 32. Haga clic en **Create security group** (Crear grupo de seguridad) y, a continuación, configure lo siguiente:
 - **Security group name** (Nombre del grupo de seguridad): *Web Security Group* (Grupo de seguridad web)
 - **Description** (Descripción): *Enable HTTP access* (Habilitar acceso HTTP)
 - **VPC**: *VPC de laboratorio*
 33. En el panel **Inbound rules** (Reglas de entrada), seleccione **Add rule** (Agregar regla)
 34. Configure los siguientes ajustes:
 - **Type** (Tipo): *HTTP*
 - **Source** (Origen): *Anywhere* (Cualquiera)
 - **Description** (Descripción): *Permit web requests* (Permitir solicitudes web)
 35. Desplácese hasta la parte inferior de la página y seleccione **Create security group** (Crear grupo de seguridad)
- Utilizará este grupo de seguridad en la siguiente tarea a la hora de lanzar una instancia de Amazon EC2.

TAREA 4: LANZAR UNA INSTANCIA DE SERVIDOR WEB

En esta tarea, lanzará una instancia de Amazon EC2 en la nueva VPC. Configuraré la instancia para que actúe como un servidor web.

39. En el menú Services (Servicios), haga clic en **EC2**.
40. Haga clic en Launch Instance (Lanzar instancia) y, a continuación, seleccione Launch Instance (Lanzar instancia)
Primero, seleccionará una *Imagen de Amazon Machine (AMI)*, la cual contiene el sistema operativo deseado.
41. Dale nombre a la instancia: *WebServer*
42. Selecciona la imagen **Amazon Linux 2** (en la parte superior), haga clic en Select (Seleccionar)

Inicio rápido

Amazon Linux aws	macOS Mac	Ubuntu ubuntu	Windows Microsoft	Red Hat Red Hat	SUSE Li SUSE	 Buscar más AMI Inclusión de AMI de AWS, Marketplace y la comunidad
---------------------	--------------	------------------	----------------------	--------------------	-----------------	---

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) Kernel 5.10, SSD Volume Type ami-0bb4c991fa89d4b9b (64 bits (x86)) / ami-0a445ece583184891 (64 bits (Arm)) Virtualización: hvm Habilitado para ENA: true Tipo de dispositivo raíz: ebs	Apto para la capa gratuita ▼
--	------------------------------

El *tipo de instancia* define los recursos de hardware asignados a la instancia.

43. Seleccione **t2.micro**, que se muestra en la columna *Type (Tipo)*.
44. Selecciona el par de claves *vokey*
Ahora, configurará la instancia para lanzarla en una subred pública de la nueva VPC. Pulsa en Editar Configuraciones de red
45. Configure los siguientes ajustes:
 - **VPC:** *Lab VPC*
 - **Subnet** (Subred): *Public Subnet 2 (Subred pública 2) (no privada)*
 - **Auto-assign Public IP** (Asignar automáticamente IP pública): *Enable (Habilitar)*Configurará la instancia para que utilice el *Grupo de seguridad web* que creó anteriormente.
46. Seleccione **Select an existing security group** (Seleccionar un grupo de seguridad existente)
47. Seleccione **Web Security Group** (Grupo de seguridad web).

LANZAMIENTO DE UN SERVIDOR WEB

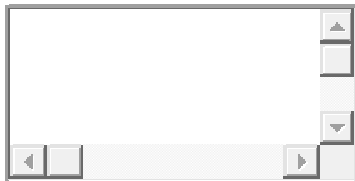
Este es el grupo de seguridad que creó en la tarea anterior. Le dará acceso HTTP a la instancia.

48. En la Configuración de almacenamiento utilizará los ajustes de almacenamiento predeterminados (8 GiB – gp3)

LANZAMIENTO DE UN SERVIDOR WEB

49. Expanda la sección **Advanced Details** (Detalles avanzados), en la parte inferior de la página.

50. Copie y pegue este código en el cuadro **User data** (Datos de usuario):



```
#!/bin/bash#
# Install Apache Web Server and PHP
yum install -y httpd mysql php
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-ACCLFO-2/2-lab2-vpc/s3/lab-app.zip
unzip lab-app.zip -d /var/www/html/
# Turn on web server
chkconfig httpd on
service httpd start
```

Este script se ejecutará automáticamente al lanzar la instancia por primera vez. El script carga y configura una aplicación web PHP.

51. Revise la información de la instancia y haga clic en Launch (Lanzar).

52. Haga clic en View all Instances (Visualizar todas las instancias).

53. Espere a que **Web Server 1** (Servidor web 1) muestre el mensaje *2/2 checks passed* (2/2 comprobaciones aprobadas) en la columna **Status Checks** (Comprobaciones de estado).

Es posible que esto tarde unos minutos. Haga clic en “Refresh” (Actualizar) en la parte superior derecha cada 30 segundos para obtener actualizaciones.


Ahora se conectará al servidor web que se ejecuta en la instancia EC2.

54. Copie el valor **Public DNS (IPv4)** (DNS público [IPv4]) que aparece en la pestaña **Description** (Descripción), en la parte inferior de la página.

LANZAMIENTO DE UN SERVIDOR WEB

55. Abra una nueva pestaña en el navegador web, pegue el valor **Public DNS** (DNS público) y presione “Enter (Intro)”.

Verá una página web que muestra el logotipo de AWS y los valores de metadatos de instancias.

 Load Test RDS

Meta-Data	Value
InstanceId	i-07a830ad3939571b1
Availability Zone	us-east-1b

Current CPU Load: **100%**

La arquitectura completa que ha implementado es la siguiente:

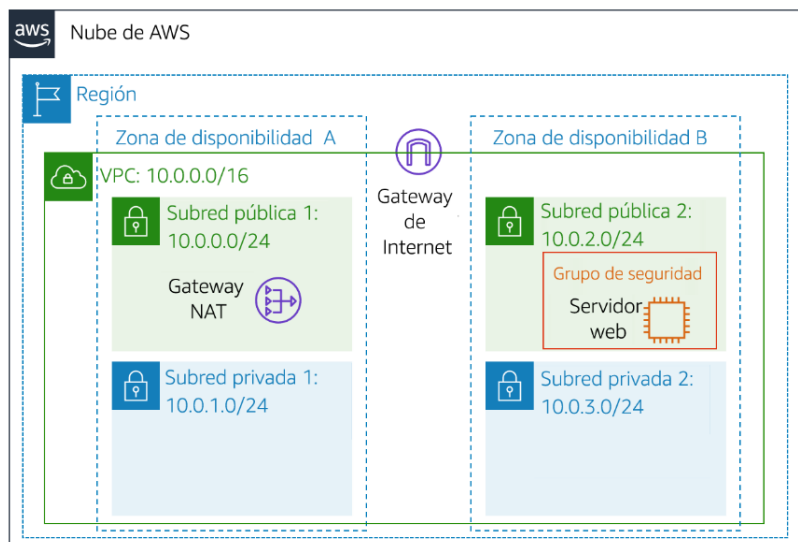


Tabla de enrutamiento pública

Destino	Objetivo
10.0.0.0/16	Local
0.0.0.0/0	Gateway de Internet

Tabla de enrutamiento privada

Destino	Objetivo
10.0.0.0/16	Local
0.0.0.0/0	Gateway NAT

FIN DEL LABORATORIO

¡Felicitaciones! Ha completado el laboratorio.

61. Haga clic en End Lab (Finalizar laboratorio) en la parte superior de esta página y, a continuación, en Yes (Sí) para confirmar que desea finalizar el laboratorio.

Aparecerá un panel en el que se indica: “DELETE has been initiated... You may close this message box now”. (Se ha iniciado la ELIMINACIÓN... Ya puede cerrar este cuadro de mensajes).

62. Haga clic en la **X** de la esquina superior derecha para cerrar el panel.