Ivan Castillo

S7: Laboratorio: Creación de una VPC y lanzamiento

de un servidor web

En este laboratorio usted:

* Crear una Virtual Private Cloud (VPC)
* Crear subredes
* Configurar un grupo de seguridad
* Lanzar una instancia de Amazon Elastic Compute Cloud (Amazon EC2) en la VPC

**Tarea 1: crear una VPC**

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

Después de crear una VPC, puede agregar subredes. Cada subred reside por completo en una zona de disponibilidad y no puede abarcar otras zonas. Si el tráfico de una subred se dirige a una puerta de enlace de Internet, la subred recibe el nombre de subred pública. Si una subred no dispone de una ruta a la puerta de enlace de Internet, la subred recibe el nombre de subred privada.

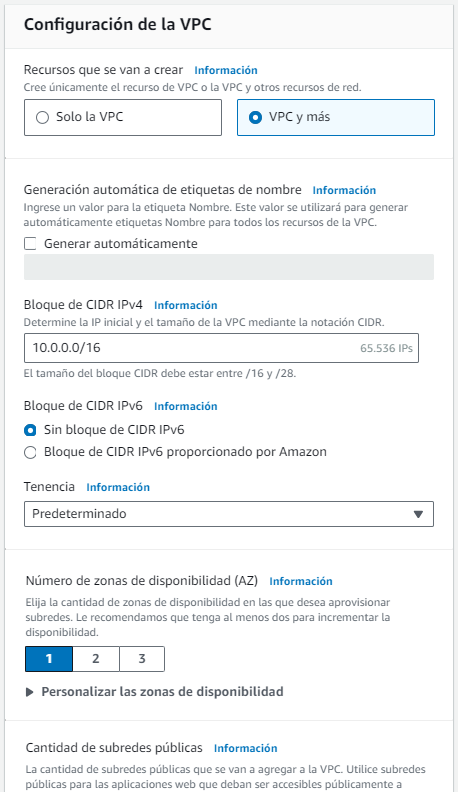
El asistente también creará una puerta de enlace de NAT, que se utiliza para brindar conectividad a Internet a instancias EC2 en las subredes privadas.

1. En la Consola de administración de AWS, en la barra de búsqueda, ingrese y seleccione la VPC

para ir al VPC Dashboard (Panel de la VPC).

1. Elija Create VPC (Crear VPC) y configure las siguientes opciones:

* Resources to create (Recursos a crear): elija VPC and more (VPC y más)
* En Name tag auto-generation (Generación automática de etiqueta de nombre): desmarque Auto-generate (Auto generar)
* IPv4 CIDR: ingrese 10.0.0.0/16
* IPv6 CIDR block (Bloque de CIDR IPv6) seleccione No IPv6 CIDR block (sin bloque de CIDR IPv6).
* Tenancy (Tenencia): seleccione Default (Predeterminado).
* Number of availability Zones (AZs) (Número de zonas de disponibilidad): 1
* Number of public subnets (Número de subredes públicas): 1
* Number of private subnets (Número de subredes privadas): 1
* Expanda Customize subnets CIDR blocks (Personalizar bloques de CIDR de las subredes)
* Public subnet CIDR block in region (Bloque de CIDR de la subred pública): 10.0.0.0/24
* Private subnet CIDR block in region (Bloque de CIDR de la subred privada): 10.0.1.0/24
* NAT gateways (Puertas de enlace NAT): seleccione In 1 AZ (En 1 zona de disponibilidad)
* VPC endpoints (Puntos de enlace de la VPC): elija None (Ninguno).

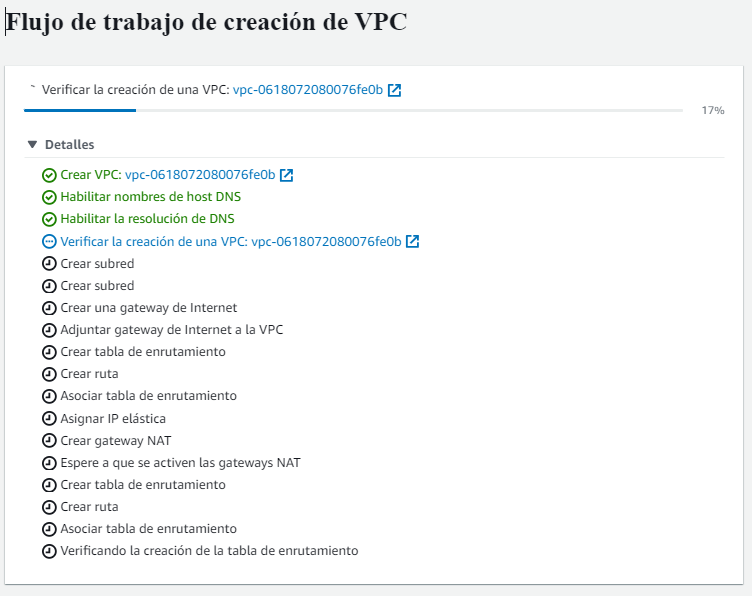
****

1. En el panel de vista previa, asigne los siguientes nombres a los recursos: VPC: Lab VPC

* Subredes (2)
* Primera casilla, subred pública uno sin etiqueta de nombre: Public Subnet 1
* Segunda casilla, subred privada uno sin etiqueta de nombre: Private Subnet 1
* Tablas de enrutamiento (2)
* Primera casilla, tabla de enrutamiento pública sin etiqueta de nombre: Public Route Table
* Segunda casilla, tabla de enrutamiento privada sin etiqueta de nombre: Private Route Table

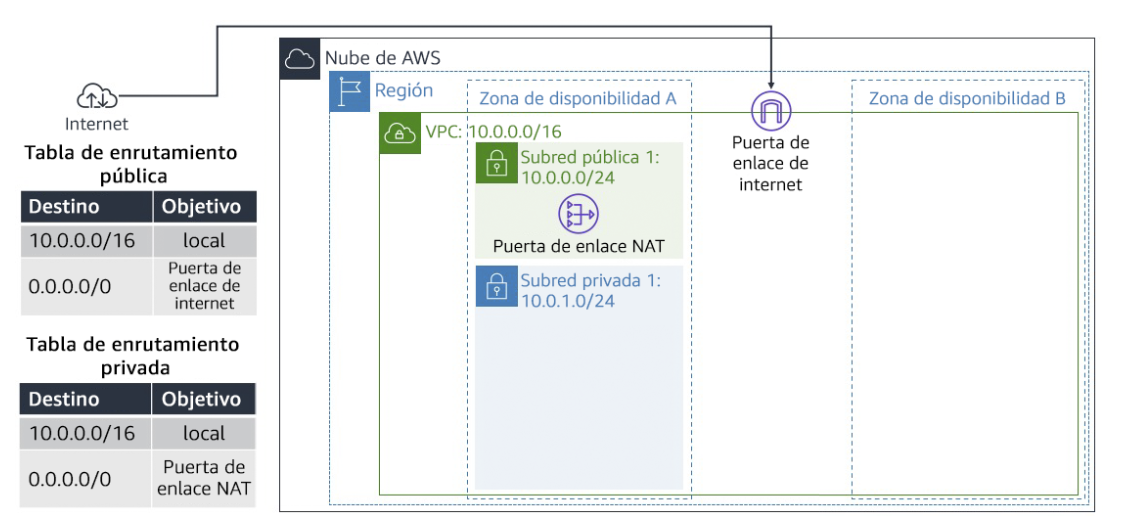


1. ****Elija Create VPC (Crear VPC).



1. Seleccione View VPC (Ver VPC).

Los detalles de Lab-vpc se muestran según la configuración.



****La subred pública tiene un enrutamiento entre dominios sin clase (CIDR) de 10.0.0.0/24, lo que significa que contiene todas las direcciones IP que comienzan con 10.0.0.x.

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.

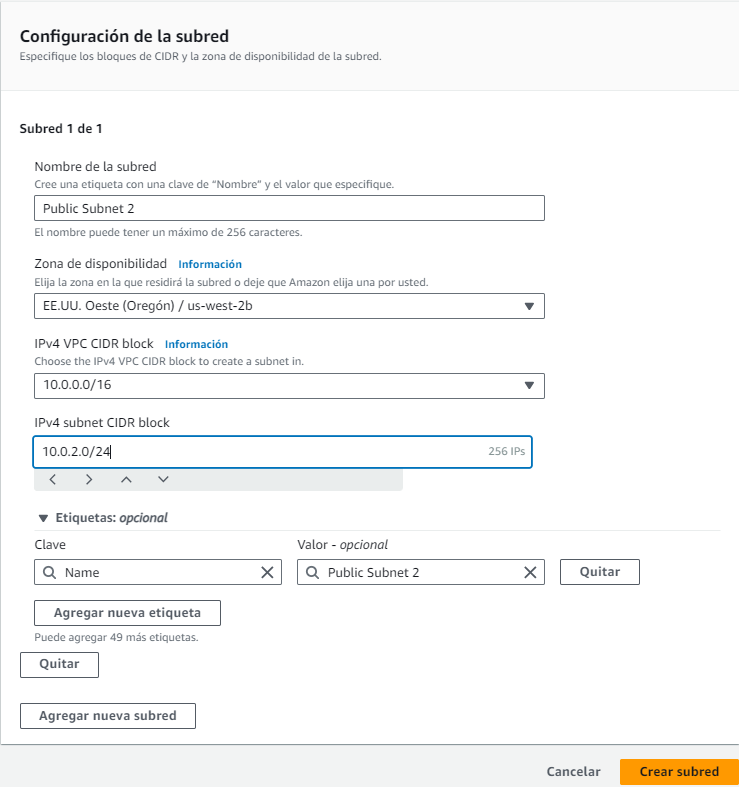
**Tarea 2: Crear subredes adicionales**

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

1. En el panel de navegación izquierdo, haga clic en **Subnets** (Subredes).
2. Para configurar la segunda subred pública, elija **Create subnet** (Crear subred) y configure las siguientes opciones:

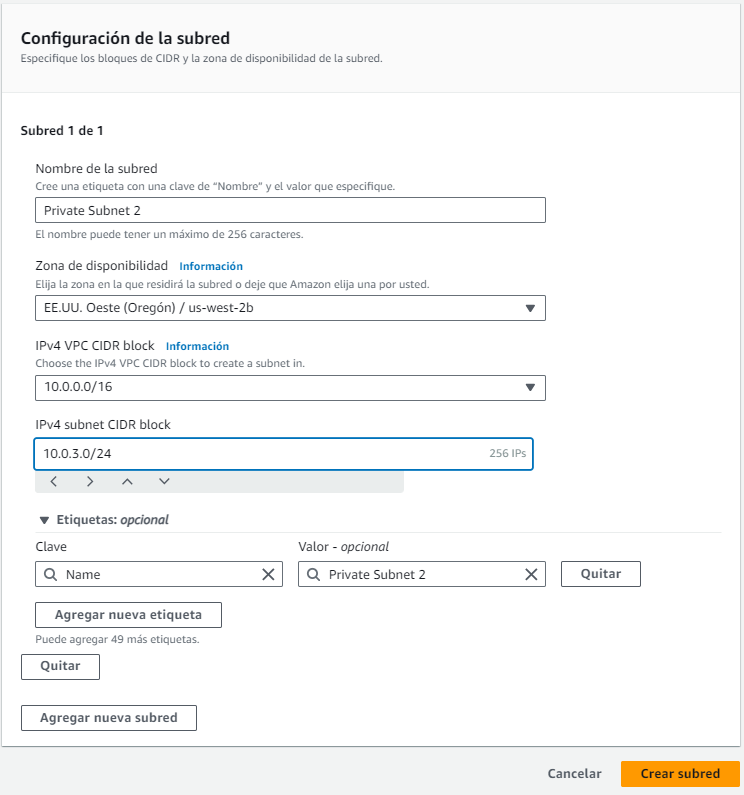
* **VPC ID** (ID de la VPC): en la lista desplegable, elija **Lab VPC** (VPC de laboratorio).
* **Subnet name** (Nombre de subred): ingrese Public Subnet 2
* **Availability Zone** (Zona de disponibilidad): en la lista desplegable, elija la segunda zona de disponibilidad.
* **IPv4 CIDR block** (Bloque de CIDR IPv4): ingrese 10.0.2.0/24

1. Elija **Create subnet** (Crear subred).



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

1. Para configurar la segunda subred privada, seleccione **Create subnet** (Crear subred) y configure las siguientes opciones:

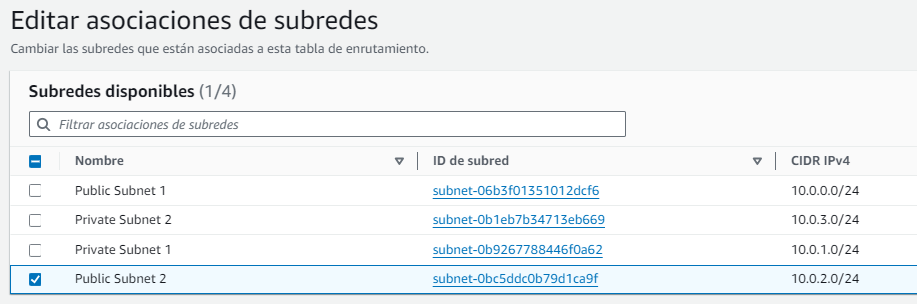
* **VPC ID** (ID de la VPC): en la lista desplegable, elija **Lab VPC** (VPC de laboratorio).
* **Subnet name** (Nombre de subred): ingrese Private Subnet 2
* **Availability Zone** (Zona de disponibilidad): en la lista desplegable, elija la segunda zona de disponibilidad.
* **IPv4 CIDR block** (Bloque de CIDR IPv4): ingrese 10.0.3.0/24

1. Elija **Create subnet** (Crear subred).

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

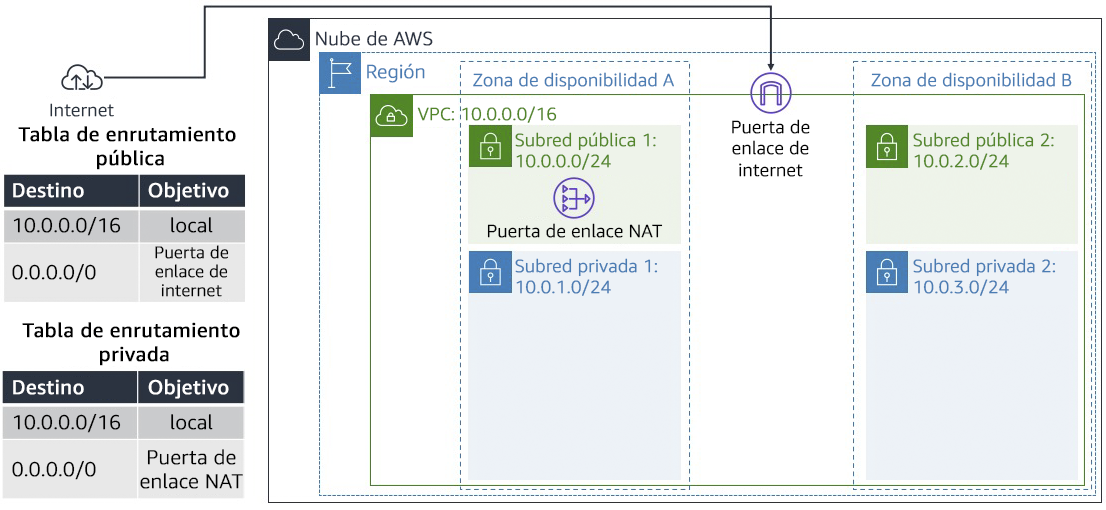
## Tarea 3: asociar las subredes y agregar rutas

1. En el panel de navegación izquierdo, elija **Route Tables** (Tablas de enrutamiento).
2. Seleccione **Public Route Table** (Tabla de enrutamiento pública)
3. En el panel inferior, haga clic en la pestaña **Subnet associations** (Asociaciones de subredes).
4. En **Subnets without explicit associations** (Subredes sin asociaciones explícitas), elija **Edit subnet associations** (Editar asociaciones de subredes).
5. Marque la casilla de **Public Subnet 2** (Subred pública 2).
6. Elija **Save associations** (Guardar asociaciones).



Ahora configurará la tabla de enrutamiento que utilizan las subredes privadas.

1. Seleccione **Private route table** (Tabla de enrutamiento privada).
2. En el panel inferior, haga clic en la pestaña **Subnet associations** (Asociaciones de subredes).
3. En **Subnets without explicit associations** (Subredes sin asociaciones explícitas), elija **Edit subnet associations** (Editar asociaciones de subredes).
4. Marque la casilla de **Private Subnet 2** (Subred privada 2).
5. Elija **Save associations** (Guardar asociaciones).

Ahora la VPC tiene subredes públicas y privadas configuradas en dos zonas de disponibilidad:

****

**Tarea 4: crear un grupo de seguridad de VPC**

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

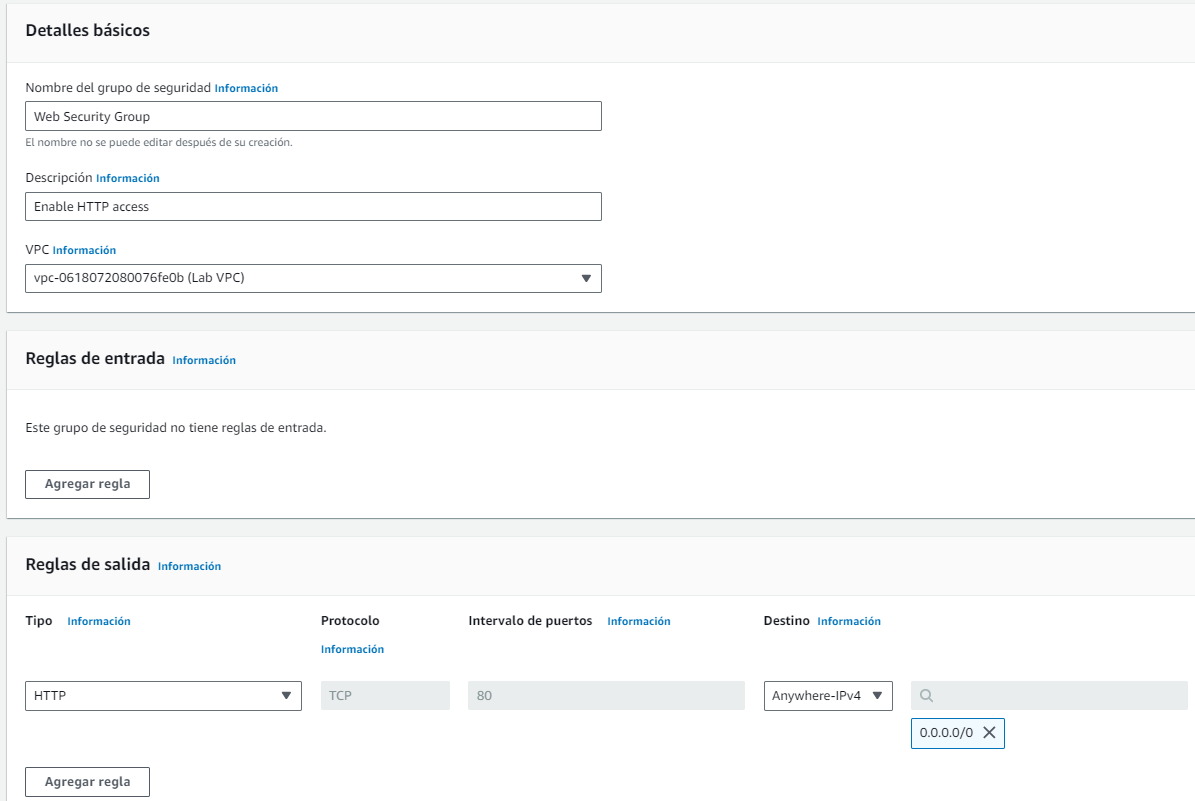
1. En el panel de navegación izquierdo, elija **Security Groups** (Grupos de seguridad).
2. Elija **Create security group** (Crear grupo de seguridad).
3. Configure el grupo de seguridad con las siguientes opciones:

* **Security group name** (Nombre del grupo de seguridad) ingrese Web Security Group
* **Description** (Descripción): ingrese Enable HTTP access
* **VPC:** elija **Lab VPC** (VPC de laboratorio).

1. En **Inbound rules** (Reglas de entrada), seleccione **Add rule** (Agregar regla).
2. Configure las siguientes opciones:

* **Type** (Tipo): elija **HTTP**.
* **Source** (Fuente): seleccione **Anywhere IPv4** (IPv4 en cualquier lugar).
* **Description** (Descripción): ingrese Permit web requests

1. Elija **Create security group** (Crear grupo de seguridad).

En la siguiente tarea, utilizará este grupo de seguridad cuando lance una instancia de EC2.

**Tarea 5: lanzar una instancia de servidor web**

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

1. En la Consola de administración de AWS, en la barra de **búsqueda**, ingrese y seleccione la EC2 para ir a la **Consola de administración de EC2**.
2. En el panel de navegación izquierdo, seleccione **Instances** (Instancias).
3. Elija **Launch Instances** (Iniciar instancias) y configure las siguientes opciones:

* En la sección **Name and tags** (Nombre y etiquetas), **Name** (Nombre): Web Server 1
* En la sección **Application and OS Images (Amazon machine Image)** (Imágenes de la aplicación y el sistema operativo [Imagen de máquina de Amazon]), configure las siguientes opciones:
* **Quick Start:** seleccione **Amazon Linux**.
* **Imagen de máquina de Amazon (AMI):** en el menú desplegable, seleccione **Amazon Linux 2023 AMI**.
* En la sección **Instance type** (Tipo de instancia), elija **t3.micro**.
* En la sección **Key pair (login)** (Par de claves [inicio de sesión]), seleccione **AWSLabsKeyPair-<random string - stack Id>**.

1. En la sección **Network Settings** (Configuración de red), seleccione **Edit** (Editar) y configure las siguientes opciones:

* **VPC - *required*** (VPC: obligatoria): elija **Lab VPC** (VPC de laboratorio).
* **Subnet** (Subred): elija **Public Subnet 2** (Subred pública 2).
* **Auto-assign public IP** (Asignar automáticamente IP pública): elija **Enable** (Habilitar).
* En **Firewall (security groups)** (Firewall [grupos de seguridad]): elija **Select existing security group** (Seleccionar grupo de seguridad existente).
  + Seleccione **Web Security Group** (Grupo de seguridad web).

1. Expanda **Advanced details** (Detalles avanzados).
2. En **User data** (Datos de usuario), copie y pegue el siguiente código.

#!/bin/bash

#Install Apache Web Server and PHP

dnf install -y httpd mariadb105-server php

#Download Lab files

wget https://us-east-1-tcprod.s3.amazonaws.com/courses/CUR-TF-100-RSNETK/v3.0.0.prod-ea58589a/267-lab-NF-build-vpc-web-server/scripts/lab-app.zip

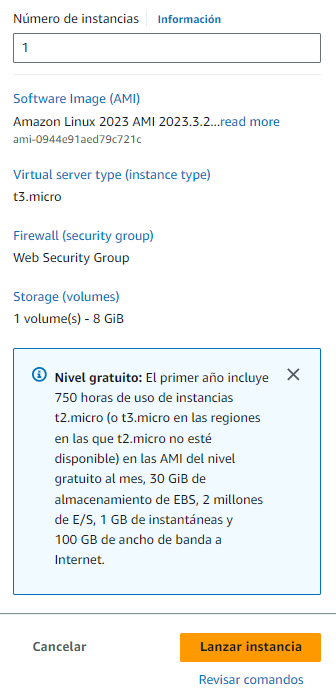
unzip lab-app.zip -d /var/www/html/

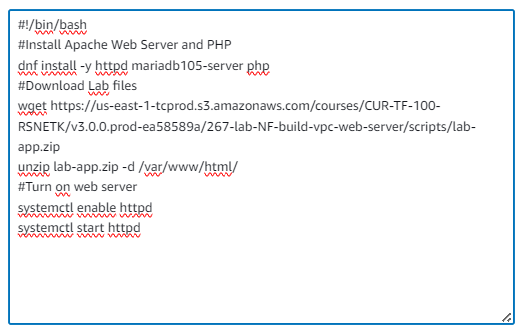
#Turn on web server

systemctl enable httpd

systemctl start httpd

1. ****Seleccione **Launch Instance** (Iniciar instancia).
2. Para ver las instancias lanzadas, elija **View all instances** (Ver todas las instancias).
3. 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).
4. Esto puede tardar unos minutos. Para actualizar la página, elija actualizar  en la parte superior de la página.

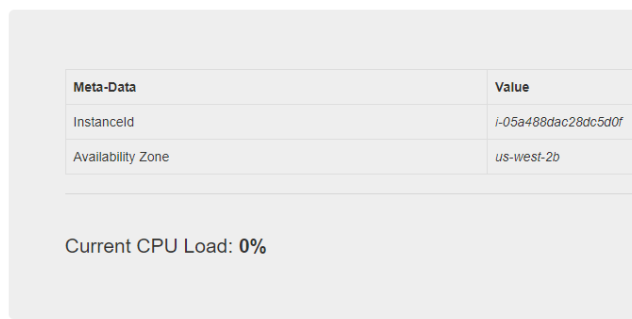




****Ahora se conectará al servidor web que se ejecuta en la instancia de EC2.

1. Seleccione la casilla de verificación de la instancia y elija la pestaña **Details** (Detalles).
2. Copie el valor de **Public IPv4 DNS** (DNS público de IPv4).
3. Abra una pestaña nueva del navegador web, pegue el valor de **Public DNS** (DNS público) y presione Enter.

La página debería verse de la siguiente manera:



La siguiente es la arquitectura completa que implementó:

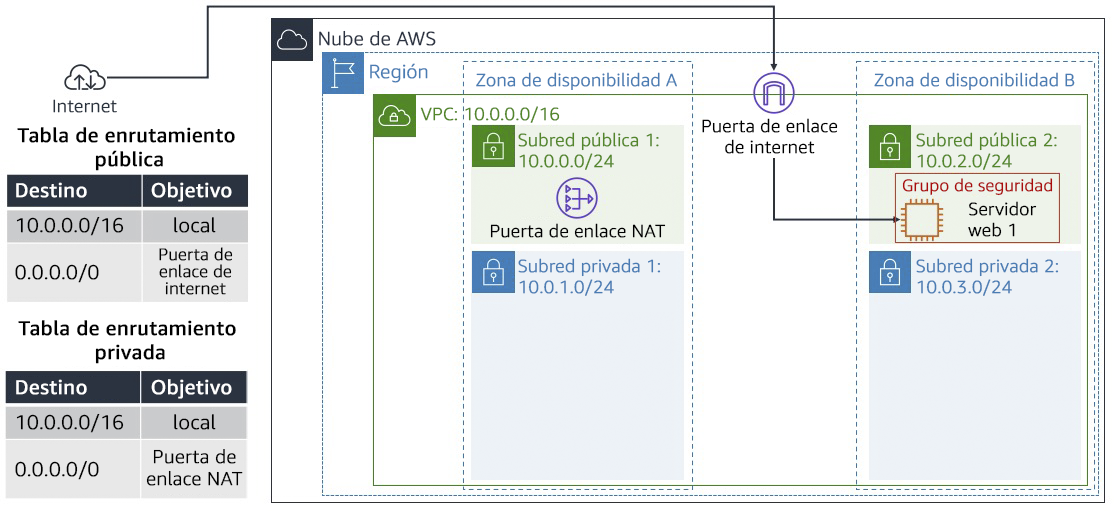


Figura: una imagen del producto final, que es la entrega de la solicitud exacta del cliente: una VPC completamente funcional con sus recursos (red y seguridad) y un servidor web.