



TRABAJO DE GRADO
Opción Seminario-Diplomado.

Implementación de arquitectura en la nube con los servicios de AWS para
FoodTecno

Corporación Universitaria Remington.
Facultad de Ingenierías
Ingeniería de Sistemas

Jean Carlos Chaverra Caicedo
Jhonier Jose Garzón Romaña
Santiago Borja Charris
Tutor del trabajo de grado
Juan Pablo Berrio López
Trabajo de grado - Seminario
2025

Dedicatoria

A Dios porque sin el nada de esto fuera posible, a mis compañeros de grupo y a nuestras familias, por el apoyo constante durante este proceso de formación profesional.

Tabla de contenido

Resumen.....	5
Palabras clave.....	5
Marco conceptual y contextual.....	6
Desarrollo e implementación del aprendizaje.....	9
Entrega 1.....	9
Diagrama de Arquitectura.....	9
Descripción de la Arquitectura.....	10
Configuración del Servidor Web.....	12
Creación de VPC y Subredes.....	14
Creación de instancia con Windows Server 2016.....	15
Creación de instancia con Amazon Linux 2023.....	24
Acceso vía RDP a la instancia Windows.....	30
Instalación del rol IIS.....	36
Acceso vía SSH a la instancia Linux.....	44
Instalación del servidor Apache en Linux.....	48
Prueba de conectividad de Windows a Linux.....	52
Validación de acceso web desde Linux.....	56
Entrega 2.....	57
Creación de Instancias EC2.....	58
Creación de Balanceador de Carga.....	66
Creación del Auto Scaling.....	77
Implementación del servicio de Docker.....	91

	4
Proxy Reverso con instancias	103
Prueba de proxy reverso desde cada una de las IP.....	108
Verificación del funcionamiento del proxy reverso con la IP pública.....	110
Diagrama de los servicios usados	112
Indice de figuras.....	113
Conclusiones	118
Referencias.....	119

Resumen

Este trabajo detalla el diseño e implementación de una arquitectura escalable y altamente disponible en la nube, a través de los servicios de Amazon Web Services (AWS), para FoodTecno, un startup que busca posicionarse como pionera en la industria alimentaria mediante la integración de soluciones tecnológicas; conectando a restaurantes con clientes mediante entregas en menor tiempo. Haciendo uso de los principales servicios de AWS como VPC, Amazon EC2, Load Balancer, Auto Scaling y Contenedores Docker.

Inicialmente se realizó la configuración de una red por medio de una VPC las cuales asigna subredes públicas y privadas, que permiten alojar las instancias EC2, en las que se implementaron servidores web con Apache Linux 2023 y Windows Server 2016 Base. Estas máquinas quedaron accesibles desde internet por medio de las direcciones IP públicas. Se implementó ALB para la distribución del tráfico web (HTTP/HTTPS); se habilitó el auto escalado garantizando que la arquitectura se adapte a la demanda de manera automática. Por último, se implementó el servicio de Elastic Container Service (ECS) para administrar contenedores Docker facilitando su despliegue y escalabilidad.

Palabras clave

Computación en la nube

Amazon Web Services (AWS)

VPC

Contenedores

Auto Scaling

Marco conceptual y contextual

AWS: Es la plataforma de servicios en la Nube de Amazon donde puedes tener una cuenta con diversos productos, soluciones o aplicaciones. Se basa en la infraestructura de su nube y proporciona una amplia gama de servicios, desde almacenamiento y bases de datos hasta inteligencia artificial y análisis de datos. (Mendieta, 2017).

Computación en la nube: El cloud computing es el acceso bajo demanda a recursos informáticos (servidores físicos o virtuales, almacenamiento de datos, capacidades de red, herramientas de desarrollo de aplicaciones, software, plataformas analíticas con IA y más) a través de Internet con precios de pago por uso. (Susnjara & Smalley, 2025)

VPC: Amazon Virtual Private Cloud (Amazon VPC) es un servicio de AWS que brinda control total sobre el entorno de redes virtuales en la nube. Con Amazon VPC, puedes definir y controlar una sección aislada de la nube de AWS donde puedes desplegar tus recursos y servicios de manera segura. (C, 2022).

Amazon EC2: La herramienta de Amazon EC2, también conocida como Amazon Elastic Compute Cloud, se refiere a un tipo de servicio web que se encarga de ofrecer capacidad informática en la nube, con propiedades como seguridad, un tamaño ajustable y computación escalable en la plataforma de Amazon Web Service (AWS).

Amazon EC2 también permite la creación y ejecución de casi cualquier aplicación del usuario, gracias a sus múltiples opciones y recursos, lo que la hace ideal para su implementación. (Mallón, 2024).

Contenedores: Los contenedores de software, o contenedores en la nube, son herramientas que simplifican la distribución de código. Como lo dijimos anteriormente, la principal misión de un contenedor es el transporte confiable de software de un entorno a otro. (Morales, 2022).

Instantáneas: Amazon Elastic Block Store (Amazon EBS) es un servicio que proporciona almacenamiento persistente a nivel de bloque para instancias de Amazon Elastic Compute Cloud (Amazon EC2). En pocas palabras, este servicio de AWS asigna discos duros fiables (es decir, volúmenes) a servidores basados en la nube. Una de las funciones más útiles de Amazon EBS son las instantáneas de volumen. (NAKIVO, 2024).

Volumen: Un volumen de Amazon EBS es un dispositivo de almacenamiento de nivel de bloque duradero que se puede adjuntar a sus instancias. Después de asociar un volumen a una instancia, puede usarlo como cualquier otro disco duro físico. Los volúmenes de EBS son flexibles. En el caso de los volúmenes de la generación actual adjuntados a los tipos de instancias de la generación actual, puede aumentar el tamaño de forma dinámica, modificar la capacidad de IOPS provisionadas y cambiar el tipo de volumen de los volúmenes de producción activos. (AWS).

Balanceador: Elastic Load Balancing distribuye automáticamente el tráfico entrante entre varios destinos, como EC2 instancias, contenedores y direcciones IP, en una o más zonas de disponibilidad. Monitorea el estado de los destinos registrados y enrutar el tráfico solamente a destinos en buen estado. Elastic Load Balancing escala de forma automática su capacidad de equilibrador de carga en respuesta a los cambios en el tráfico entrante.

AMI: Una imagen de máquina de Amazon, también conocida como AMI, se refiere a un tipo de imagen gestionada y compatible con la plataforma de Amazon Web Service. Su función es la de ofrecer la información que se necesita para lanzar una instancia en específico. Así pues, una misma imagen de máquina de Amazon tiene la capacidad de lanzar múltiples instancias que tengan una misma configuración, de la misma manera que varias AMI pueden lanzar instancias con configuraciones diferentes. (Mallón, 2024).

Escalabilidad: La escalabilidad es un concepto fundamental en el desarrollo de software que se refiere a la capacidad de un sistema para adaptarse a un aumento en la carga de trabajo sin comprometer su rendimiento. En un mundo donde las aplicaciones y plataformas digitales crecen rápidamente, entender y aplicar la escalabilidad se ha vuelto crucial para el éxito a largo plazo de cualquier proyecto tecnológico. (Takami, 2024).

Desarrollo e implementación del aprendizaje

Entrega 1

Diagrama de Arquitectura

- Representación gráfica de la red que muestra:

EC2 Instancia (Linux/Windows)

VPC

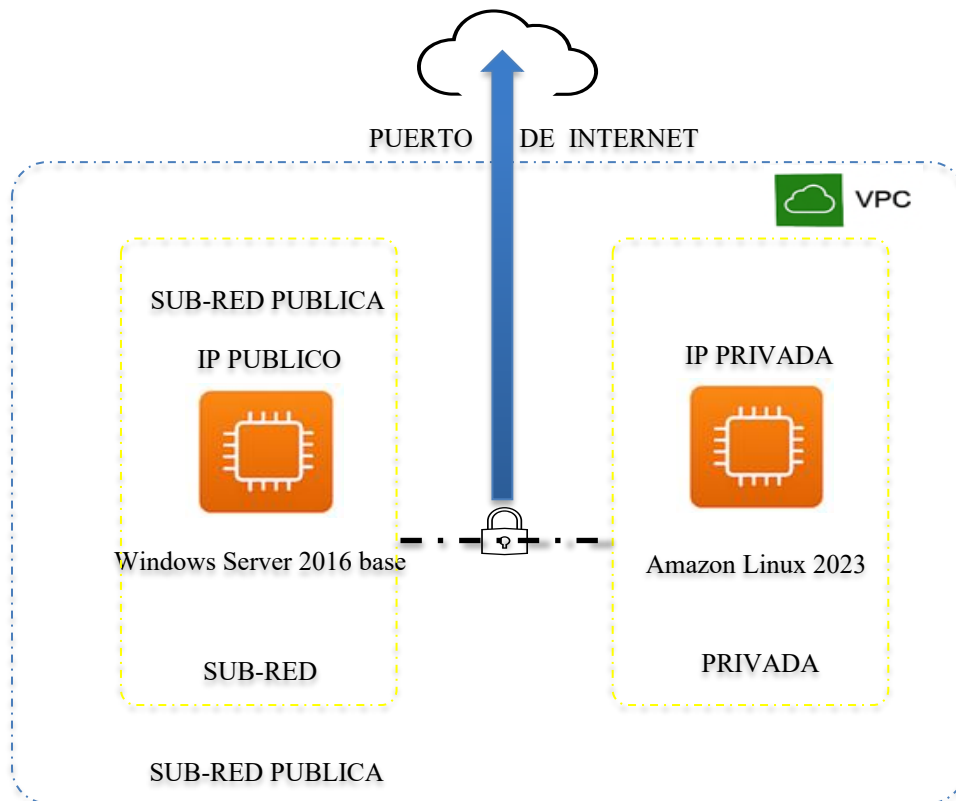
Subredes públicas y privadas

Internet Gateway

Grupos de Seguridad

IPS públicas y privadas

Figura 1 Diseño general de la red en AWS



Descripción de la Arquitectura

Se creó una arquitectura básica en AWS utilizando una VPC personalizada, dividida en subredes públicas y privadas. A cada subred se le asignaron instancias EC2 para distintos propósitos (servidor web Windows y Linux).

Instancias usadas:

- Windows Server 2019 Base (para servidor web con IIS)
- Ubuntu Server 22.04 LTS (para servidor web con Apache)

Justificación:

- VPC personalizada para mayor control del tráfico.
- Subred pública para instancias accesibles desde Internet.
- Internet Gateway para conexión externa.
- Grupos de seguridad para permitir el tráfico necesario(RDP, SSH,HTTP).

Configuraciones Realizadas

- Creación de una VPC con subredes públicas
 - Asociar una tabla de rutas con acceso a IGW.
 - Crear y asociar Internet Gateway a la VPC.
- Creación de Instancias EC2 con Amazon Linux y Windows Server

- Tipo t2.micro (capa gratuita).
- Asignar IPS públicas durante el lanzamiento.
- Crear par de claves (.pem) para acceso RDP y SSH.
- Grupos de Seguridad
 - Windows Server: RDP puerto(3389), puerto HTTP (80): se creó un grupo de seguridad nombrado sgWindowsServer.
 - Amazon Linux: SSH puerto (22), HTTP puerto(80): se creó un grupo de seguridad nombrado launch-wizard-2.
- Asignación de IPS
 - Cada instancia tiene asignada una IP pública, configurada de forma automática.
 - IPS privadas asignadas automáticamente por la subred.

Procedimiento de Acceso

- Windows Server (RDP)
 - Usar cliente RDP (Remote Desktop).
 - Descargar archivo .rdp desde AWS.
 - Obtener la contraseña usando la clave privada del archivo .pem, cargado desde la instancia en AWS para descifrarla.
- Amazon Linux (SSH)
 - Usar consola o cliente SSH.
 - Ingresar las credenciales y acceder.
 - Comando: `ssh -i "/ruta/ServerLinux2.pem" ec2-user@`

- Consideraciones de seguridad
 - Usar archivos .pem protegidos.
 - No compartir contraseñas ni clave PEM.
 - Limitar rangos de IP en el grupo de seguridad.
 - Asegurarse de que el acceso solo sea desde nuestra IP.

Configuración del Servidor Web

Windows Server (IIS)

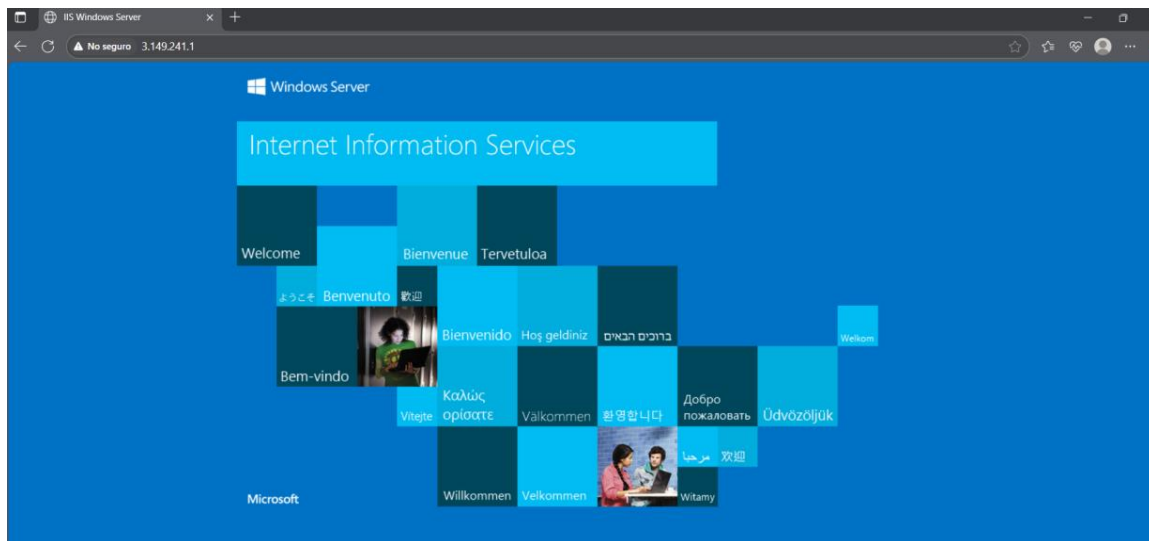
- Acceder por RDP.
- Ir a server Manager – Manage – Add Roles Feactures.
- Seleccionar Web Server (IIS).
- Completar la instalación.
- Verificar accediendo a la IP pública.

Linux Apache

- Acceder vía SSH.
- Ejecutar comandos:
 - Para entrar en modo administrador - sudo su
 - Para instalar Apache - dnf install httpd
 - Para iniciar servicio – systemctl start httpd
 - Para verificar el estado del servicio – systemctl status httpd
- Probar en el navegador con la IP pública.

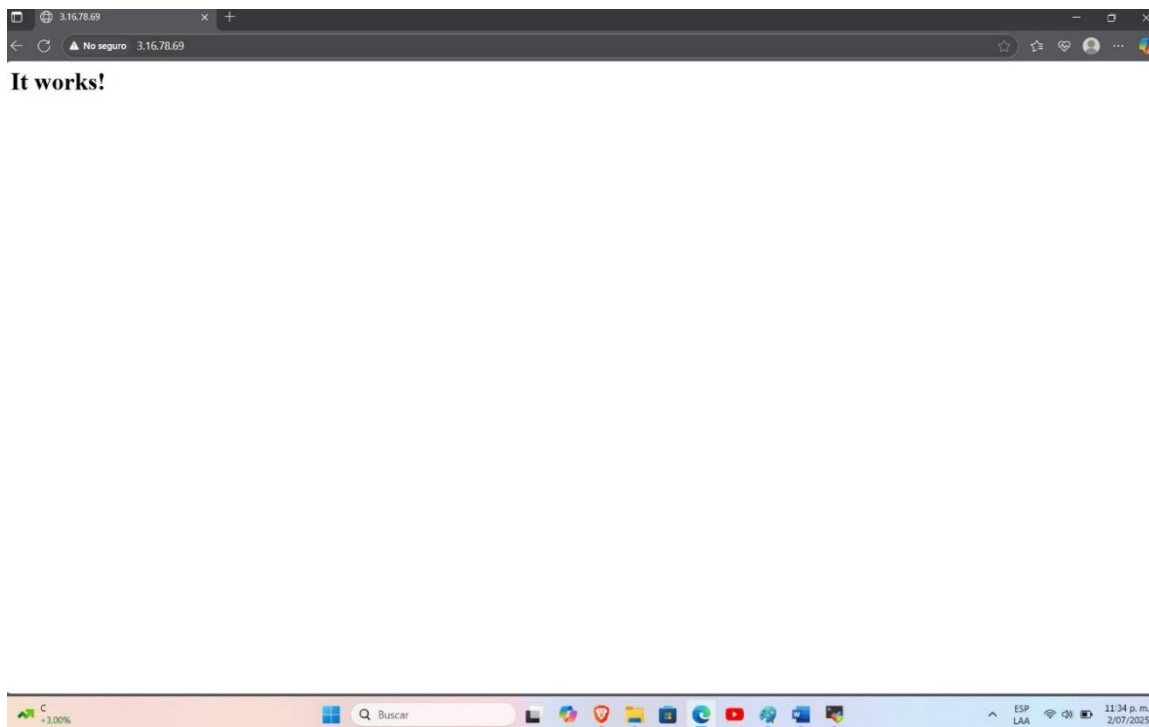
Prueba de acceso al servidor Windows desde el navegador.

Figura 2 Servidor IIS operativo.



Prueba de acceso al servidor de Linux desde el navegador.

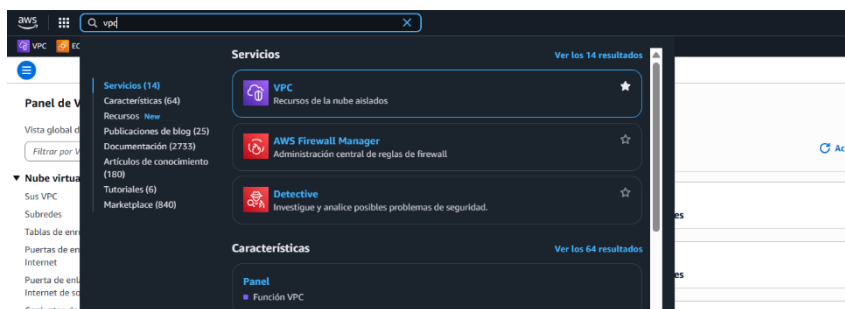
Figura 3 Servidor Apache activo



Creación de VPC y Subredes

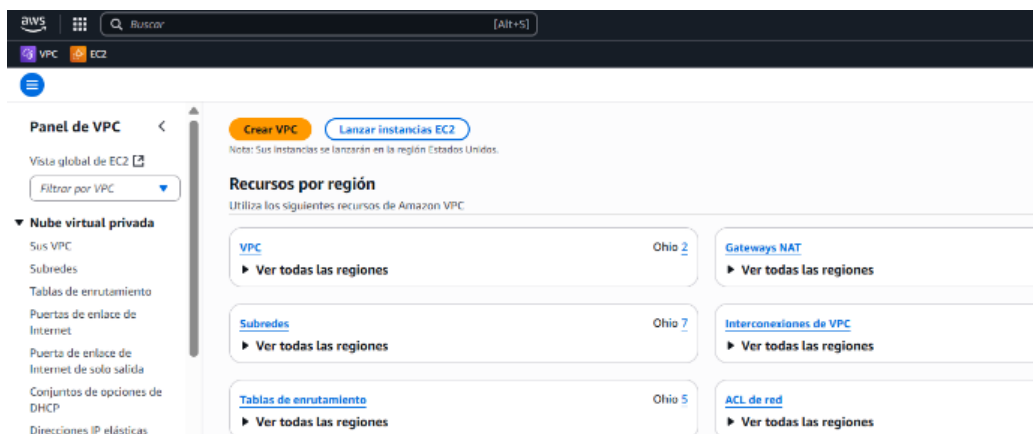
En el buscador escribimos VPC y seleccionamos.

Figura 4 Creación de VPC.



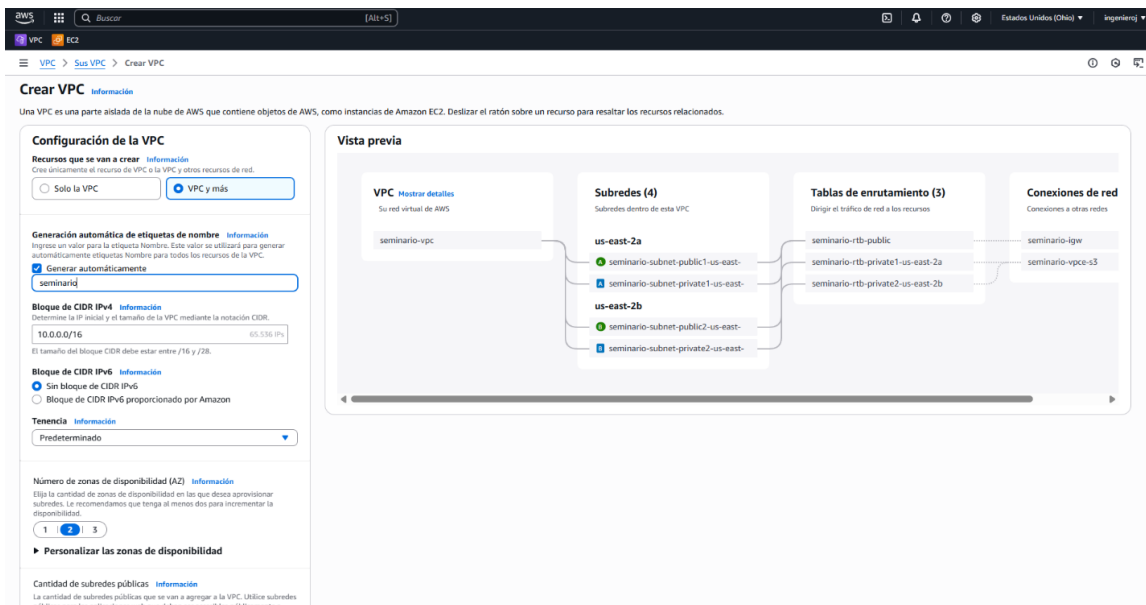
Damos en la opción de crear VPC.

Figura 5 crear VPC.



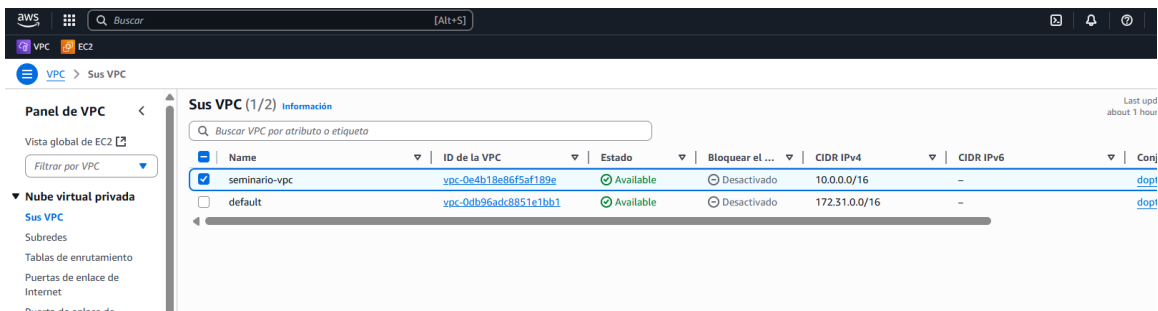
Nombramos nuestra VPC y elegimos la cantidad de subredes que necesitamos, las cuales van a hacer 2 públicas y dos privadas. Le damos en Crear VPC

Figura 6 nombrar VPC.



Evidenciamos que la VPC se creó correctamente

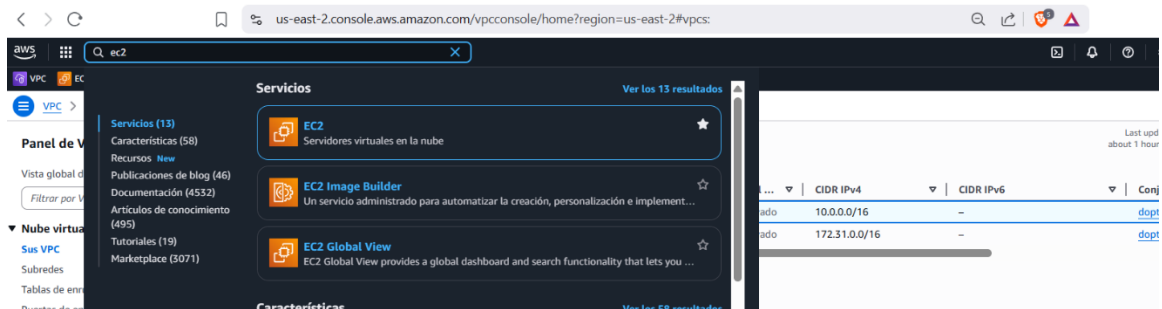
Figura 7 VPC creadas.



Creación de instancia con Windows Server 2016

En el buscador escribimos EC2 y seleccionamos.

Figura 8 Búsqueda de ec2.

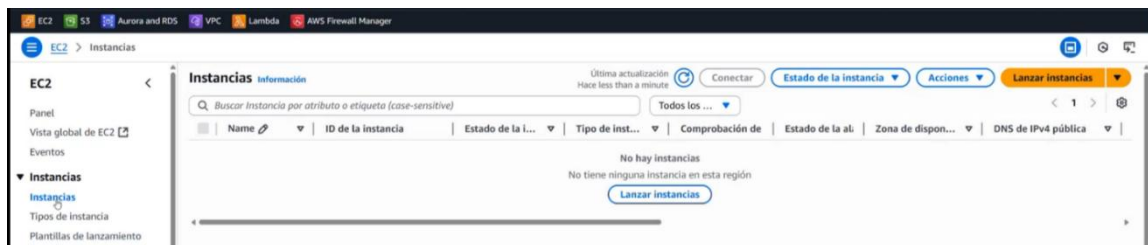


En el panel izquierdo seleccionamos instancias y luego damos lanzar instancia.

Figura 9 servicio instancias.

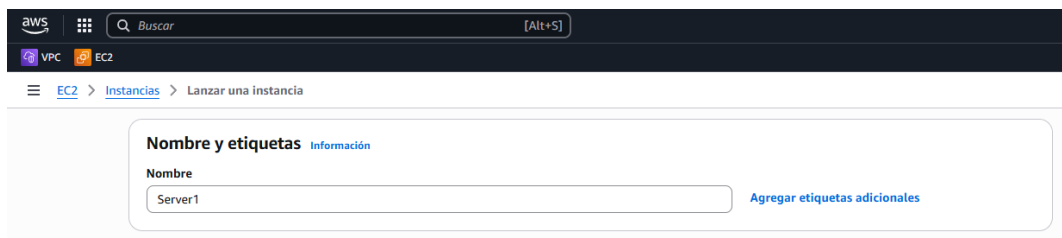


Figura 10 creación de instancia.



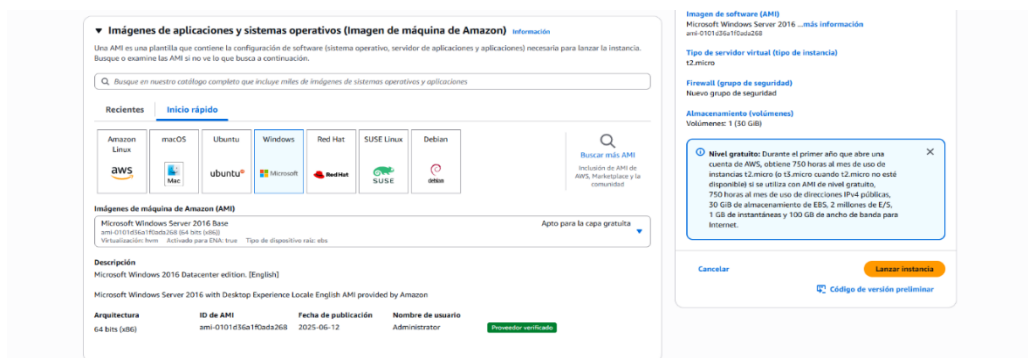
Ingresamos el nombre de nuestra instancia.

Figura 11 nombrar instancia.



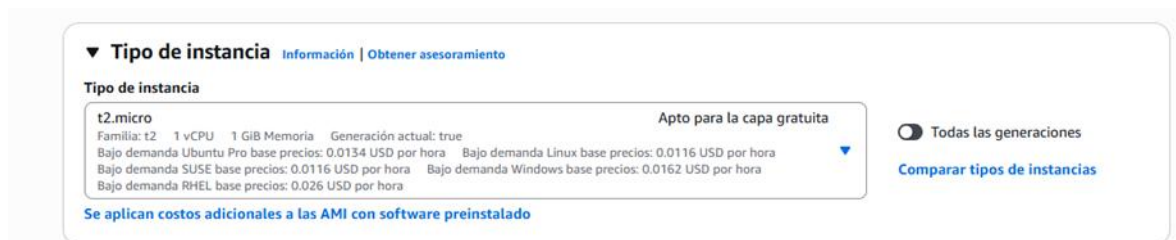
Seleccionamos la AMI para nuestro servidor, en este caso Windows Server 2016 Base

Figura 12 AMI a instalar.



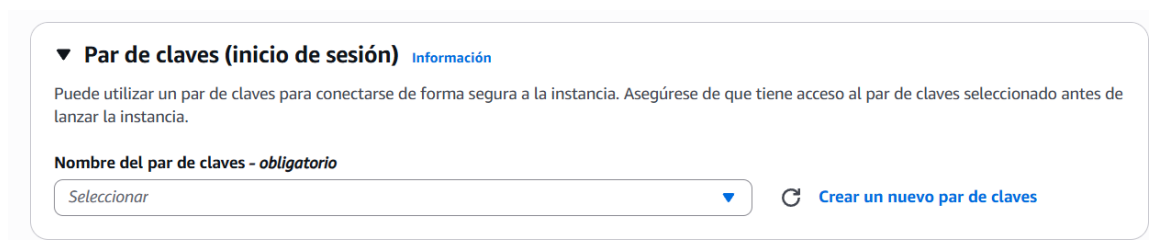
Seleccionamos el tipo de instancia.

Figura 13 tipo de instancia.



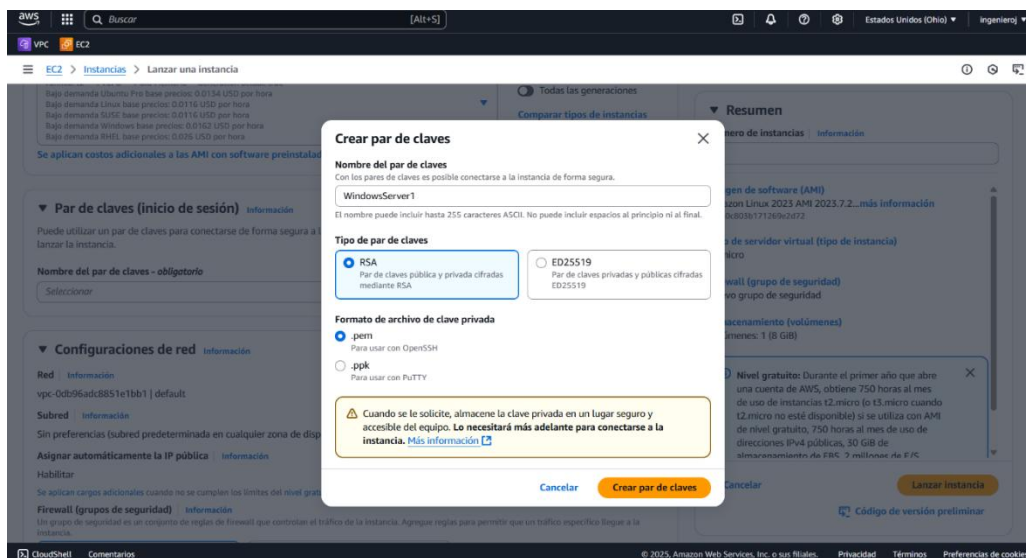
Creamos un par de claves para acceder a nuestra instancia, seleccionamos la opción de crear un nuevo par de claves, para generar un certificado de seguridad.

Figura 14 creación Par de Clave.



Nombramos el par de claves y le damos crear.

Figura 15 Par de claves.



Realizamos la configuración de red: Seleccionamos nuestra VPC y la subred que vamos a utilizar. Ademas habilitamos la opción de asignar IP pública para acceder a la instancia.

Figura 16 configuración de red.



Creamos el grupo de seguridad y revisamos las reglas del grupo de seguridad, que por defecto nos da una regla tipo RDP que nos permite el acceso al protocolo TCP por el puerto 3389. Habilitados el tipo de origen para que se conecte desde cualquier lugar.

Figura 17 grupo de seguridad.

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

Nombre del grupo de seguridad - *obligatorio*

Este grupo de seguridad se agregará a todas las interfaces de red. El nombre no se puede editar después de crear el grupo de seguridad. La longitud máxima es de 255 caracteres. Caracteres válidos: a-z, A-Z, 0-9, espacios y _-;/()#,@[]+=&;!:\$*

Descripción - *obligatorio* | [Información](#)

Reglas de grupos de seguridad de entrada

▼ Regla del grupo de seguridad 1 (TCP, 3389, 0.0.0.0/0) [Eliminar](#)

Tipo Información	Protocolo Información	Intervalo de puertos Información
<input type="text" value="rdp"/>	TCP	3389
Tipo de origen Información	Origen Información	Descripción - <i>opcional</i> Información
<input type="text" value="Cualquier lugar"/>	<input type="text" value="0.0.0.0/0"/> <input type="text" value="Agregue CIDR, lista de prefijos o grupo d"/>	<input type="text" value="por ejemplo, SSH para Admin Desktop"/>

Configuración de almacenamiento, que por defecto nos recomienda unas características.

Figura 18 configuración almacenamiento.

▼ Configurar almacenamiento | [Información](#) [Avanzado](#)

1x GiB Volumen raíz, No cifrado

[Agregar un nuevo volumen](#)

The selected AMI contains instance store volumes, however the instance does not allow any instance store volumes. None of the instance store volumes from the AMI will be accessible from the instance

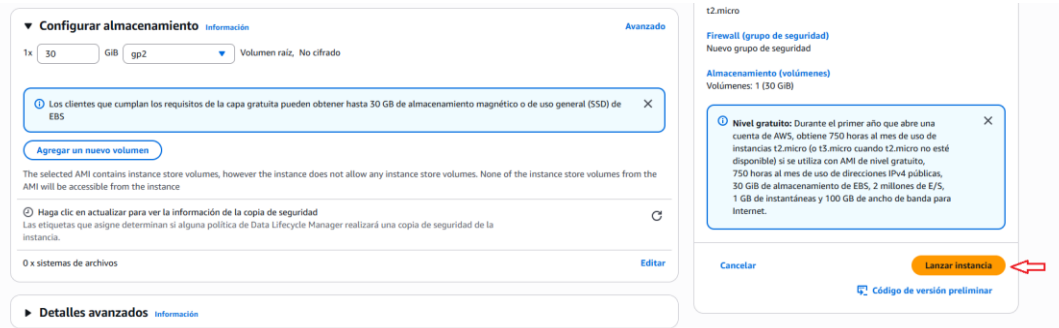
Las etiquetas que asigne determinan si alguna política de Data Lifecycle Manager realizará una copia de seguridad de la instancia. [✕](#)

0 x sistemas de archivos [Editar](#)

▶ Detalles avanzados | [Información](#)

Finalmente le damos Lanzar instancia y esperamos la creación de esta.

Figura 19 lanzar instancia.



Efectivamente observamos que nuestra instancia se creó correctamente.

Figura 20 creación instancia.

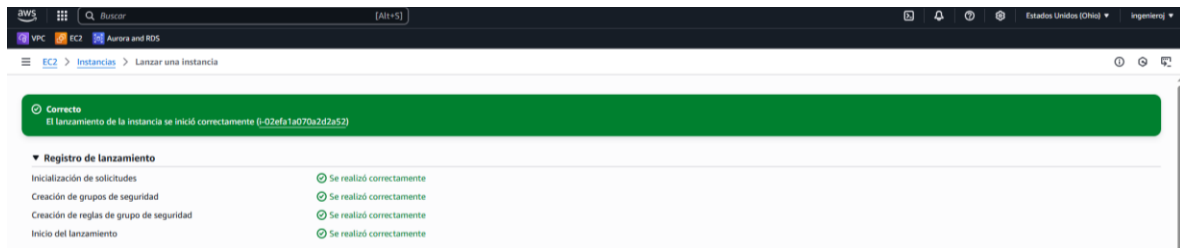
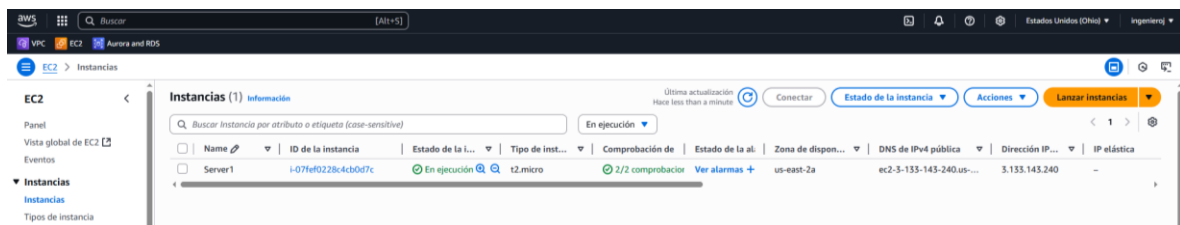
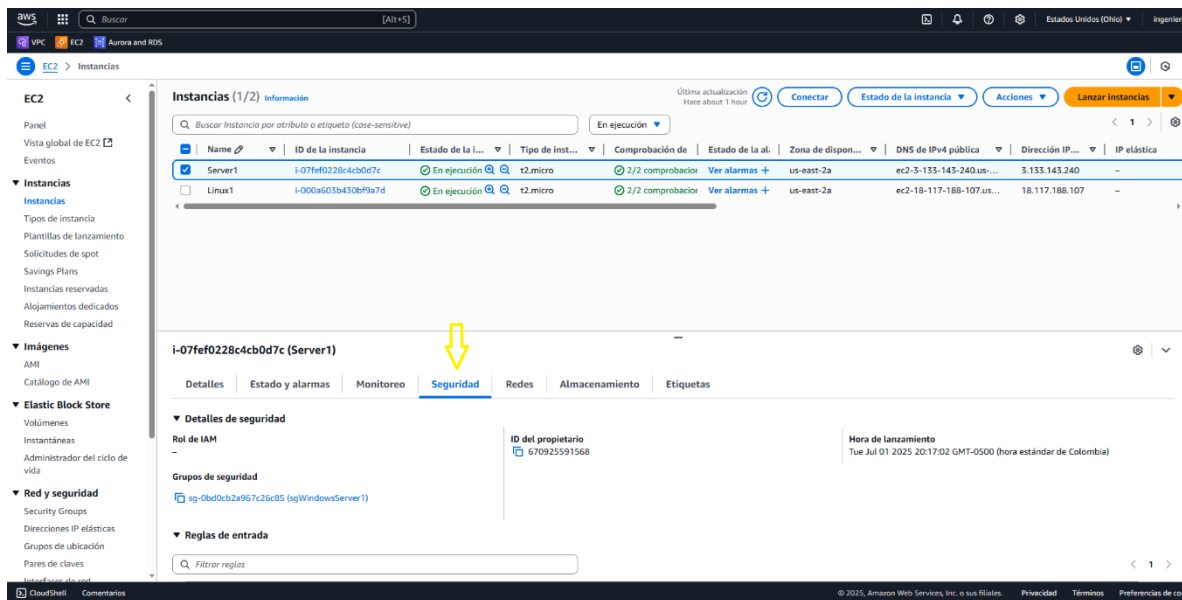


Figura 21 instancia activa.



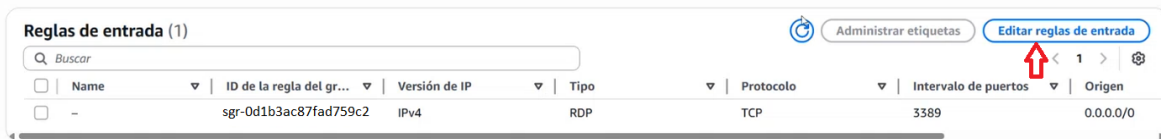
Vamos a habilitar el puerto 80 para acceder al servidor desde la web, entrando en nuestra instancia en la opción de seguridad.

Figura 22 habilitacion del Puerto 80.



Seleccionamos grupo de seguridad y le damos en editar reglas de entrada.

Figura 23 Grupo de seguridad.



Le damos en la opción de agregar reglas.


Figura 24 agregar reglas de entrada.

Editar reglas de entrada Información

Las reglas de entrada controlan el tráfico entrante que puede llegar a la instancia.

Reglas de entrada Información

ID de la regla del grupo de seguridad	Tipo <small>Información</small>	Protocolo <small>Información</small>	Intervalo de puertos <small>Información</small>	Origen <small>Información</small>	Descripción: opcional <small>Información</small>
sgr-0d1b3ac87fad759c2	RDP	TCP	3389	Persona...	0.0.0.0/0

[Agregar regla](#) 

⚠ Las reglas cuyo origen es 0.0.0.0/0 o ::/0 permiten a todas las direcciones IP acceder a la instancia. Recomendamos configurar reglas de grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas.

[Cancelar](#) [Previsualizar los cambios](#) [Guardar reglas](#)

Agregamos el puerto al que se le va a dar acceso en este caso 80, para que se conecte desde cualquier lugar y le damos en guardar regla.

Figura 25 habilitar Puerto 80.

Editar reglas de entrada Información


Las reglas de entrada controlan el tráfico entrante que puede llegar a la instancia.

Reglas de entrada Información

ID de la regla del grupo de seguridad	Tipo <small>Información</small>	Protocolo <small>Información</small>	Intervalo de puertos <small>Información</small>	Origen <small>Información</small>	Descripción: opcional <small>Información</small>
sgr-0d1b3ac87fad759c2	RDP	TCP	3389	Persona...	0.0.0.0/0
-	TCP personalizado	TCP	80	Anywh...	0.0.0.0/0

[Agregar regla](#)

⚠ Las reglas cuyo origen es 0.0.0.0/0 o ::/0 permiten a todas las direcciones IP acceder a la instancia. Recomendamos configurar reglas de grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas.

[Cancelar](#) [Previsualizar los cambios](#) [Guardar reglas](#) 

Evidenciamos que ya se agregó y podremos acceder por medio de ese puerto.

Figura 26 Puerto 80 agregado.

Reglas de entrada (2)

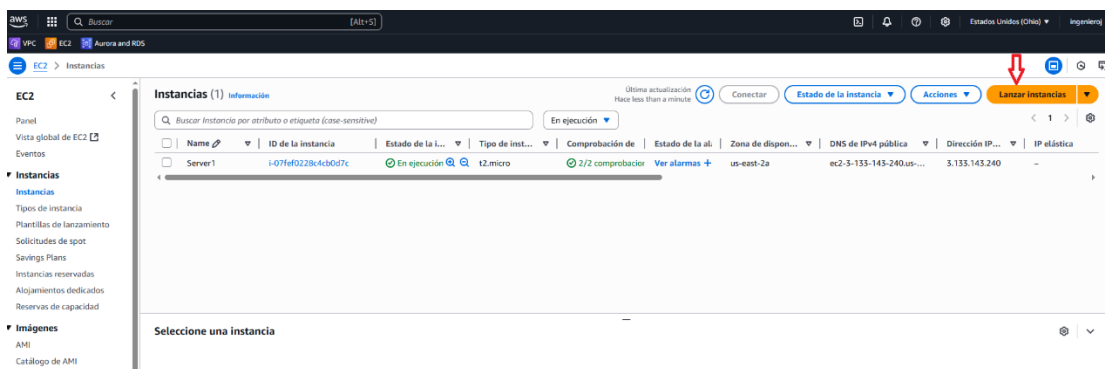
[Administrar etiquetas](#) [Editar reglas de entrada](#)

<input type="checkbox"/>	Name	ID de la regla del gr...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
<input type="checkbox"/>	-	sgr-0a040f6788552ea87	IPv4	HTTP	TCP	80	0.0.0.0/0	-
<input type="checkbox"/>	-	sgr-0d1b3ac87fad759c2	IPv4	RDP	TCP	3389	0.0.0.0/0	-

Creación de instancia con Amazon Linux 2023

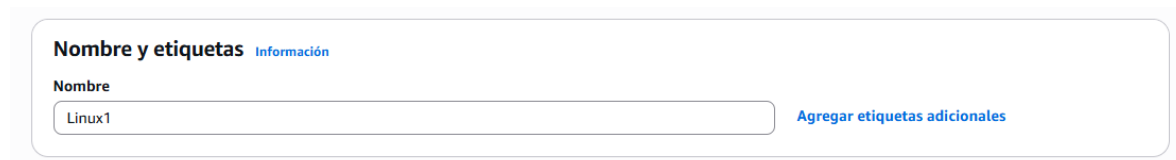
Nos dirigimos al panel de EC2 en la opción de instancias, y seleccionamos lanzar instancia.

Figura 27 creación de instancia Linux.



Nombramos nuestra instancia (en este caso Linux1).

Figura 28 nombrar instancia.



Seleccionamos nuestra AMI para nuestra instancia, en este caso Amazon Linux 2023.

Figura 29 elección de AMI.

▼ **Imágenes de aplicaciones y sistemas operativos (Imagen de máquina de Amazon)** [Información](#)

Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servidor de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Busque o examine las AMI si no ve lo que busca a continuación.

🔍 *Busque en nuestro catálogo completo que incluye miles de imágenes de sistemas operativos y aplicaciones*

Recientes | **Inicio rápido**

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Linux

Debian

[Buscar más AMI](#)
Inclusión de AMI de AWS, Marketplace y la comunidad

Imágenes de máquina de Amazon (AMI)

AMI de Amazon Linux 2023 Apto para la capa gratuita ▼
ami-0c803b171269e2d72 (64 bits (x86), uefi-preferred) / ami-02b2147120fd682bf (64 bits (Arm), uefi)
Virtualización: hvm Activado para ENA: true Tipo de dispositivo raíz: ebs

Descripción

Amazon Linux 2023 es un sistema operativo moderno y de uso general basado en Linux que incluye 5 años de soporte a largo plazo. Está optimizado para AWS y diseñado para proporcionar un entorno de ejecución seguro, estable y de alto desempeño para desarrollar y ejecutar sus aplicaciones en la nube.

Amazon Linux 2023 AMI 2023.7.20250623.1 x86_64 HVM kernel-6.1

Arquitectura	Modo de arranque	ID de AMI	Fecha de publicación	Nombre de usuario	
64 bits (x86) ▼	uefi-preferred	ami-0c803b171269e2d72	2025-06-20	ec2-user	Proveedor verificado

En tipo de instancia lo dejamos por defecto (t2.micro).

Figura 30 tipo de instancia.

▼ **Tipo de instancia** [Información](#) | [Obtener asesoramiento](#)

Tipo de instancia

t2.micro Apto para la capa gratuita

Familia: t2 1 vCPU 1 GiB Memoria Generación actual: true

Bajo demanda Ubuntu Pro base precios: 0.0134 USD por hora Bajo demanda Linux base precios: 0.0116 USD por hora

Bajo demanda SUSE base precios: 0.0116 USD por hora Bajo demanda Windows base precios: 0.0162 USD por hora

Bajo demanda RHEL base precios: 0.026 USD por hora

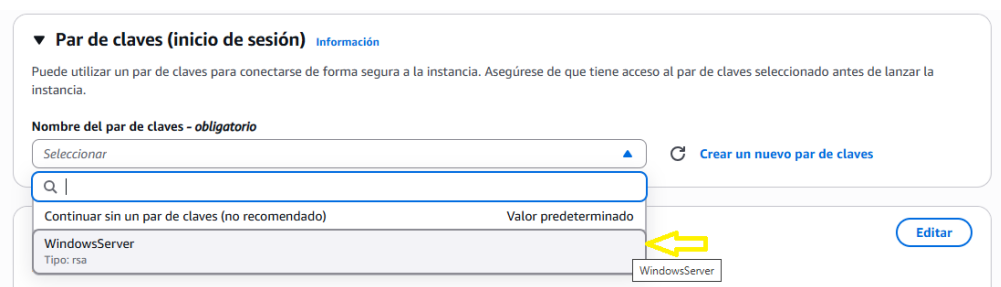
Todas las generaciones

[Comparar tipos de instancias](#)

Se aplican costos adicionales a las AMI con software preinstalado

Para el par de claves usamos el mismo que creamos para Windows y lo seleccionamos.

Figura 31 Autenticación para de calves.



▼ **Par de claves (inicio de sesión)** Información

Puede utilizar un par de claves para conectarse de forma segura a la instancia. Asegúrese de que tiene acceso al par de claves seleccionado antes de lanzar la instancia.

Nombre del par de claves - obligatorio

Seleccionar ▲ [Crear un nuevo par de claves](#)

Q |

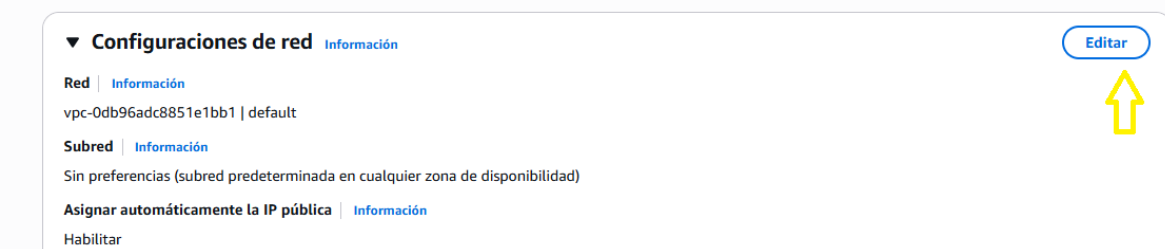
Continuar sin un par de claves (no recomendado) Valor predeterminado Editar

WindowsServer
Tipo: rsa

WindowsServer

Editamos la configuración de red.

Figura 32 configuración de red.



▼ **Configuraciones de red** Información Editar

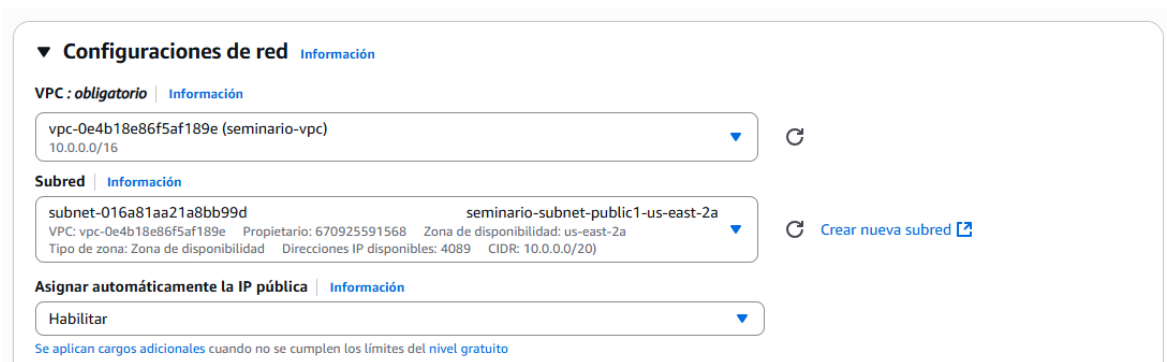
Red Información
vpc-0db96adc8851e1bb1 | default

Subred Información
Sin preferencias (subred predeterminada en cualquier zona de disponibilidad)

Asignar automáticamente la IP pública Información
Habilitar

Seleccionamos la VPC ya creada para que nos asigne la subred pública y habilitamos la opción para que nos cree una IP automáticamente.

Figura 33 eleccion de VPC.



Creamos un nuevo grupo de seguridad y agregamos una regla para acceder por el puerto 80 y que se conecte desde cualquier lugar.

Configuramos el almacenamiento, por defecto nos sugiere unas características.

Figura 36 Almacenamiento instancia.

▼ Configurar almacenamiento Información Avanzado

1x GiB Volumen raíz, 3000 IOPS, No cifrado

ⓘ Los clientes que cumplan los requisitos de la capa gratuita pueden obtener hasta 30 GB de almacenamiento magnético o de uso general (SSD) de EBS ✕

[Agregar un nuevo volumen](#)

ⓘ Haga clic en actualizar para ver la información de la copia de seguridad
 Las etiquetas que asigne determinan si alguna política de Data Lifecycle Manager realizará una copia de seguridad de la instancia. ↻

0 x sistemas de archivos Editar

Presionamos finalmente en lanzar instancia para que se cree.

Figura 37 lanzamiento instancia.

▼ Configurar almacenamiento Información Avanzado

1x GiB Volumen raíz, 3000 IOPS, No cifrado

ⓘ Los clientes que cumplan los requisitos de la capa gratuita pueden obtener hasta 30 GB de almacenamiento magnético o de uso general (SSD) de EBS ✕

[Agregar un nuevo volumen](#)

ⓘ Haga clic en actualizar para ver la información de la copia de seguridad
 Las etiquetas que asigne determinan si alguna política de Data Lifecycle Manager realizará una copia de seguridad de la instancia. ↻

0 x sistemas de archivos Editar

Firewall (grupo de seguridad)
 Nuevo grupo de seguridad

Almacenamiento (volúmenes)
 Volúmenes: 1 (8 GiB)

ⓘ **Nivel gratuito:** Durante el primer año que abre una cuenta de AWS, obtiene 750 horas al mes de uso de instancias t2.micro (o t3.micro cuando t2.micro no esté disponible) si se utiliza con AMI de nivel gratuito, 750 horas al mes de uso de direcciones IPv4 públicas, 30 GiB de almacenamiento de EBS, 2 millones de E/S, 1 GB de instantáneas y 100 GB de ancho de banda para Internet. ✕

Cancelar [Lanzar instancia](#)
[Código de versión preliminar](#)

► Detalles avanzados Información

Observamos que nuestra instancia se creó.

Figura 38 instancia creada.

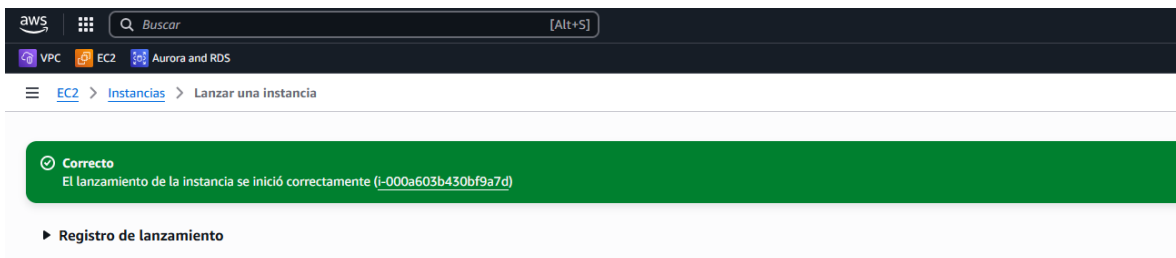
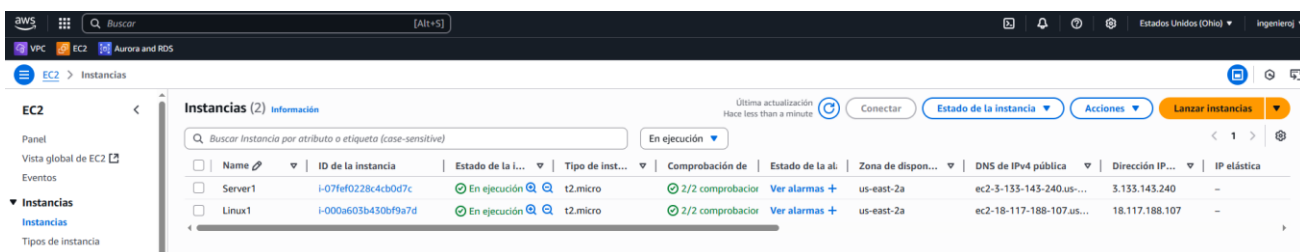


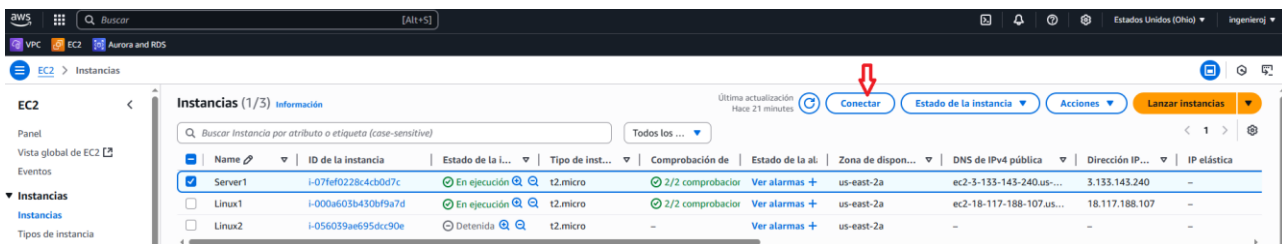
Figura 39 visualización instancia.



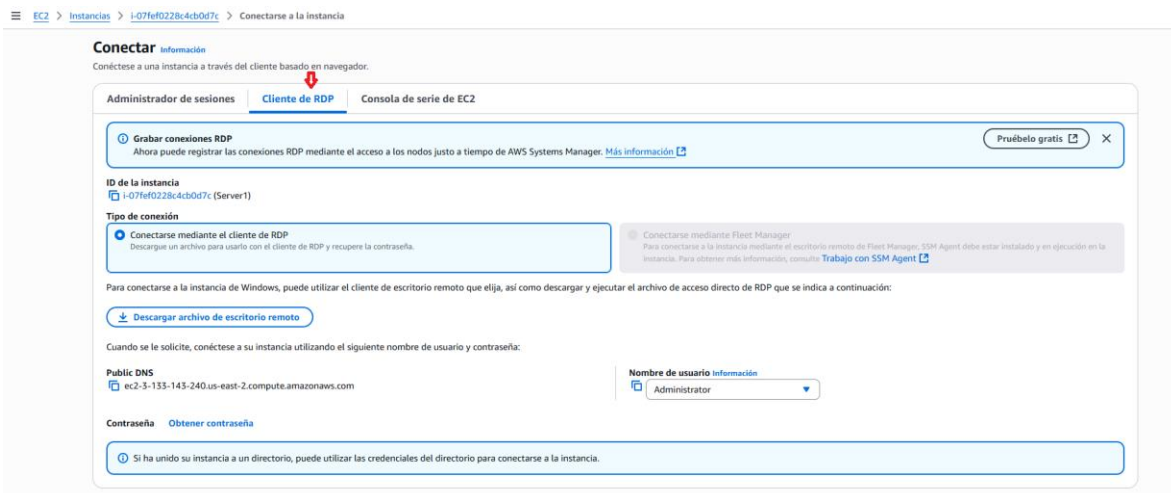
Acceso vía RDP a la instancia Windows

Seleccionamos la instancia y damos en conectar.

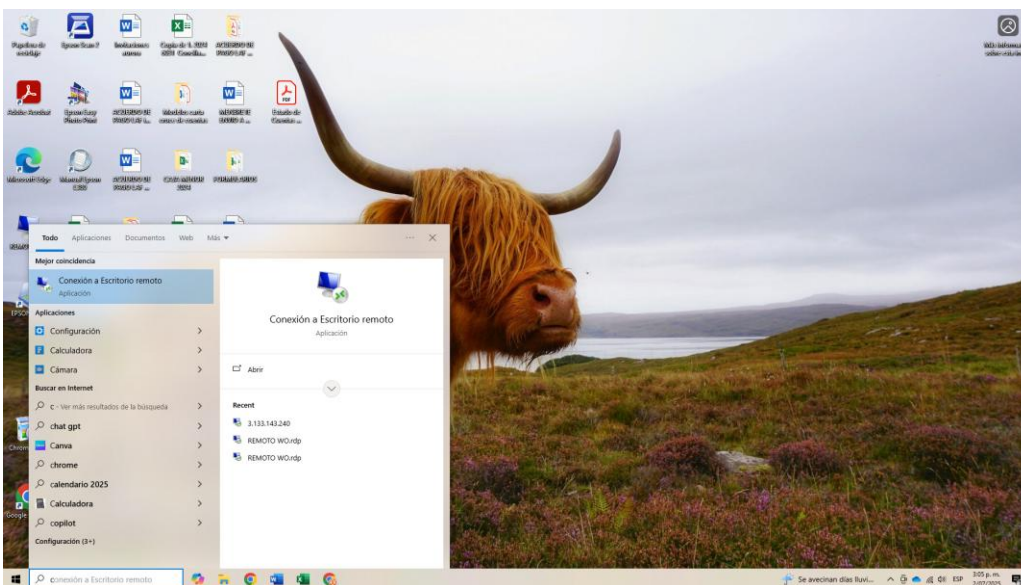
Figura 40 acceso por RDP a windows.



Seleccionamos cliente RDP.

Figura 41 conexión RDP.

Buscamos en nuestro equipo conexión a escritorio remoto.

Figura 42 conexión por escritorio remoto.

Copiamos la dirección IP pública de nuestra instancia.

Figura 43 seleccion IP publica.

The screenshot shows the AWS Management Console interface. At the top, there's a search bar and a table of instances. The table has columns for Name, ID, State, Instance Type, Health, Availability Zone, DNS Public IP, and Elastic IP. The first instance, 'Server1', is selected. Below the table, the details for 'Server1' are shown, including its ID, state (En ejecución), and network information. A red arrow points to the 'Dirección IPv4 pública' field, which contains the IP address '3.133.143.240'.

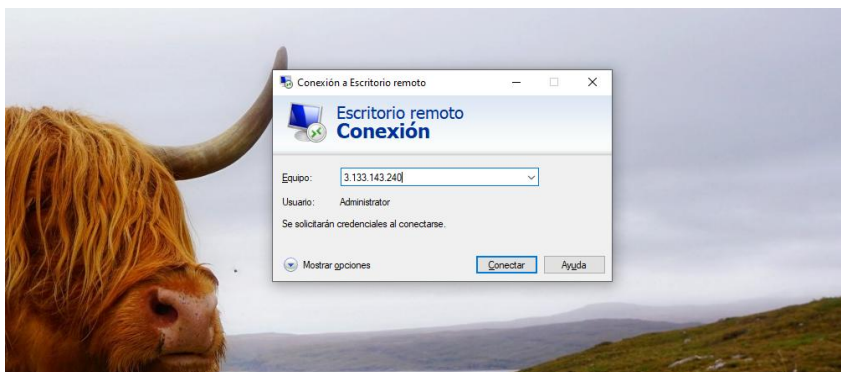
Nombre	ID de la instancia	Estado de la instancia	Tipo de instancia	Comprobación de salud	Estado de la disponibilidad	Zona de disponibilidad	DNS de IPv4 pública	Dirección IP elástica
Server1	i-07fef0228c4cb0d7c	En ejecución	t2.micro	2/2 comprobador	us-east-2a	us-east-2a	ec2-3-133-143-240.us-east-2.compute.amazonaws.com	3.133.143.240
Linux1	i-000a603b430b9a7d	En ejecución	t2.micro	2/2 comprobador	us-east-2a	us-east-2a	ec2-18-117-188-107.us-east-2.compute.amazonaws.com	18.117.188.107
Linux2	i-056039ae695dc90e	Detenida	t2.micro	-	us-east-2a	us-east-2a	-	-

i-07fef0228c4cb0d7c (Server1)

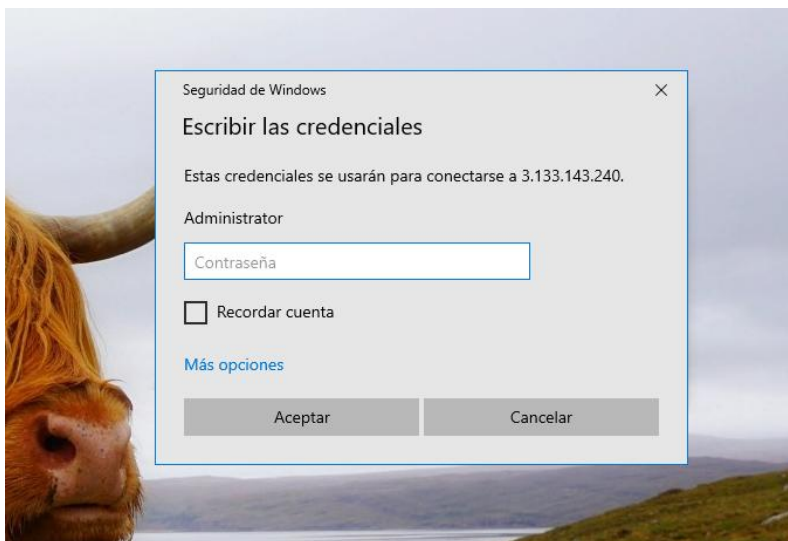
- Dirección IPv4 pública:** 3.133.143.240 | dirección abierta
- Direcciones IPv4 privadas:** 10.0.2.138
- DNS público:** ec2-3-133-143-240.us-east-2.compute.amazonaws.com | dirección abierta
- Direcciones IP elásticas:** -

La pegamos en la venta de conexión a escritorio remoto y damos conectar.

Figura 44 conexion a escritorio remoto.



Nos pide la contraseña de acceso. Para esto nos devolvemos a la conexión de la instancia en cliente RDP.

Figura 45 contraseña de acceso.

Damos en la opción de obtener contraseña.

Figura 46 obtención de contraseña.

Conectar Información
Conéctese a una instancia a través del cliente basado en navegador.

Administrador de sesiones **Cliente de RDP** Consola de serie de EC2

Grabar conexiones RDP Información
Ahora puede registrar las conexiones RDP mediante el acceso a los nodos justo a tiempo de AWS Systems Manager. [Más información](#) Pruébelo gratis X

ID de la instancia
i-071fe0228c4cb0d7c (Server)

Tipo de conexión

- Conectarse mediante el cliente de RDP**
Descargue un archivo para usarlo con el cliente de RDP y recupere la contraseña.
- Conectarse mediante Fleet Manager
Para conectarse a la instancia mediante el escritorio remoto de Fleet Manager, SSH Agent debe estar instalado y en ejecución en la instancia. Para obtener más información, consulte [Trabajo con SSM Agent](#).

Para conectarse a la instancia de Windows, puede utilizar el cliente de escritorio remoto que elija, así como descargar y ejecutar el archivo de acceso directo de RDP que se indica a continuación:

[Descargar archivo de escritorio remoto](#)

Cuando se le solicite, conéctese a su instancia utilizando el siguiente nombre de usuario y contraseña:

Public DNS
ec2-3-133-143-240.us-east-2.compute.amazonaws.com

Nombre de usuario Información
Administrator

Contraseña [Obtener contraseña](#) ←

Obtener contraseña
Si ha unido su instancia a un directorio, puede utilizar las credenciales del directorio para conectarse a la instancia.

Cargamos nuestro archivo del par de claves para que nos proporcione la contraseña.

Figura 47 cargue de par de clave.


Obtener la contraseña de Windows Información

Utilice la clave privada para recuperar y descifrar la contraseña de administrador de Windows inicial correspondiente a esta instancia.

ID de la instancia
 i-07fef0228c4cb0d7c (Server1)

Par de claves asociado a esta instancia
 WindowsServer

Clave privada
 Cargue el archivo de la clave privada o copie y pegue su contenido en el campo que aparece a continuación.



Contenido de la clave privada: *opcional*

Contenido de la clave privada

Una vez cargado, le damos descifrar contraseña.

Figura 48 cifrado de contraseña.

Obtener la contraseña de Windows Información

Utilice la clave privada para recuperar y descifrar la contraseña de administrador de Windows inicial correspondiente a esta instancia.

ID de la instancia
 i-07fef0228c4cb0d7c (Server1)


Par de claves asociado a esta instancia
 WindowsServer

Clave privada
 Cargue el archivo de la clave privada o copie y pegue su contenido en el campo que aparece a continuación.

WindowsServer.pem
 1.678KB

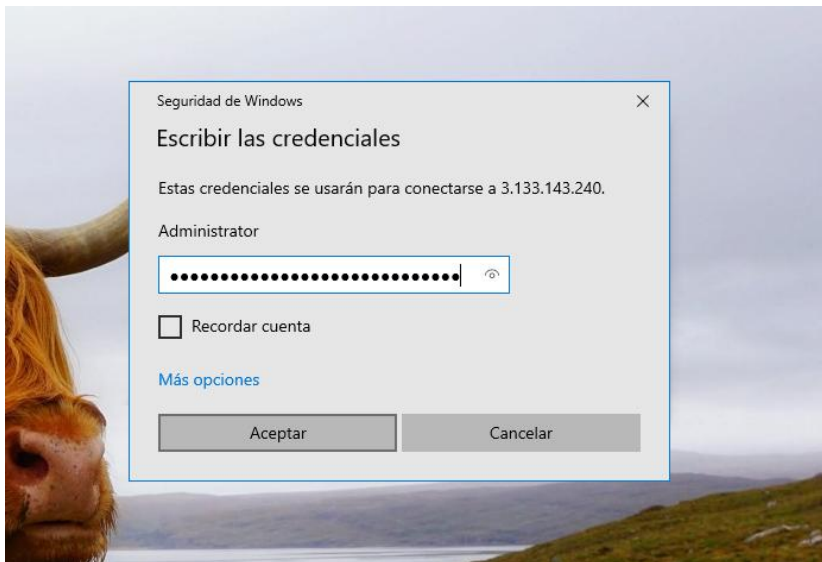
Contenido de la clave privada: *opcional*

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAyBki/mrdIyeUWITV826AqBAII+aKfhpFvDDej5+tTKilg5xv
tEgIQhe+eVmiDm67JEXV1ymi7CVXIV9QM3yEKx8VKppqMuvNrmA95bpJj+dHK+pdp
4KcoOUHERKTOkOLWfpjB/ukKavCOWw/vcpJ4I3ovYfDNNK4HKpmbz/ffovFh6+xbq
55u5IQe9QA3ysCkoojVoaLSjBRg03NWARsjkTTIvbaagG7M4Pm6IPSNdDQun
D+e5KR8wTY8Xo2LFjMj/ZCvdVgan15biqXfo+gbqO7JUP/Wj+cZO9hXmNAdEqg8n
69RjYMXLY6p+KQKnCkufrIDReAqZ0ZkoOFMfQIDAQABAoIBAQC03EJp67Wutq
fdThxtJNRzry8biS2hXIO5asroY7okRJGhaW2ww5YqIPPOuydiD78VtsR7qgLRH
-----
```



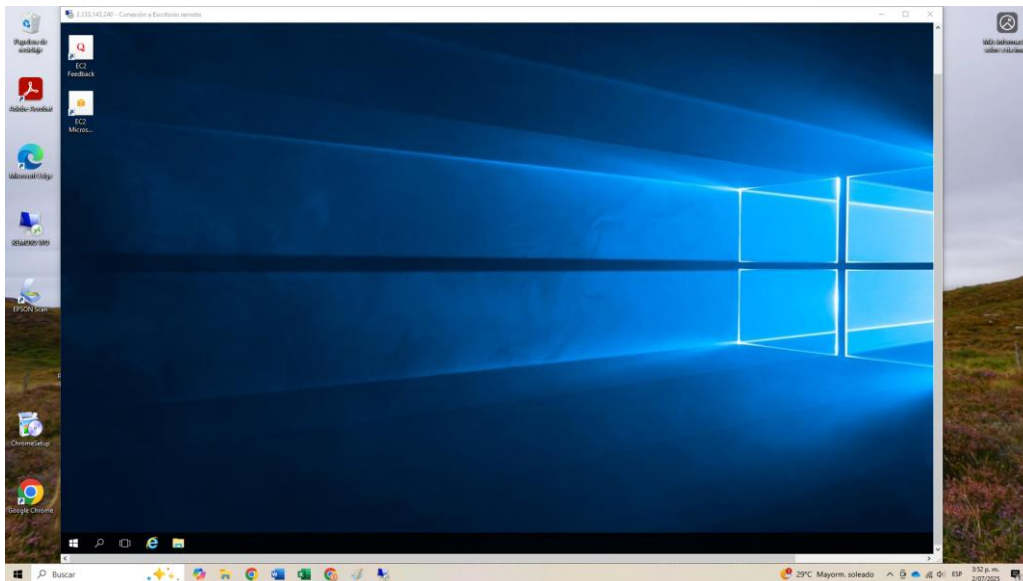
Ingresamos las credenciales y damos aceptar.

Figura 49 credenciales de acceso.



Efectivamente se conecta al servidor.

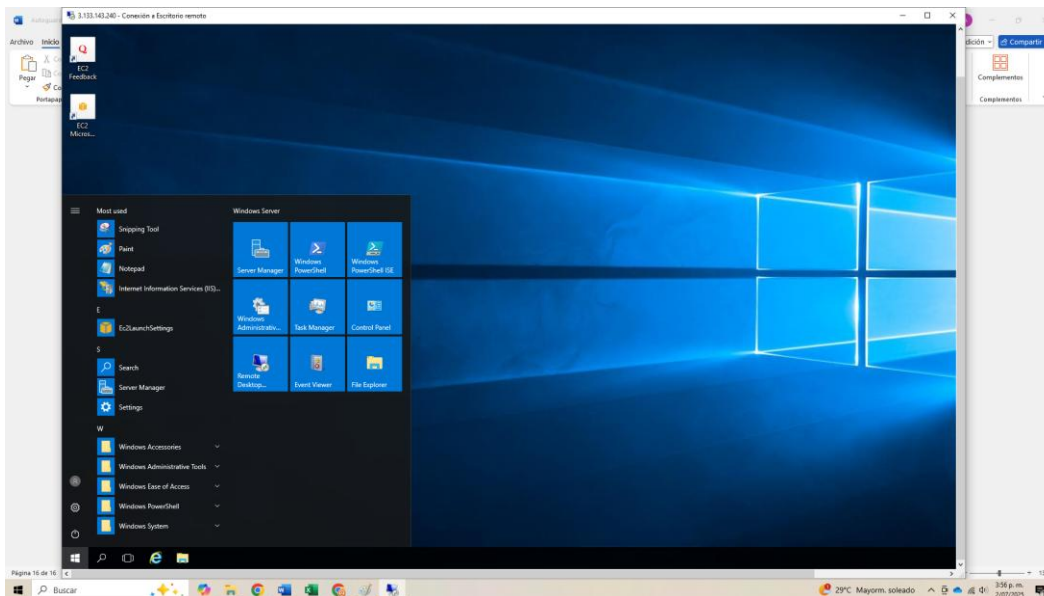
Figura 50 conexión servidor.



Instalación del rol IIS

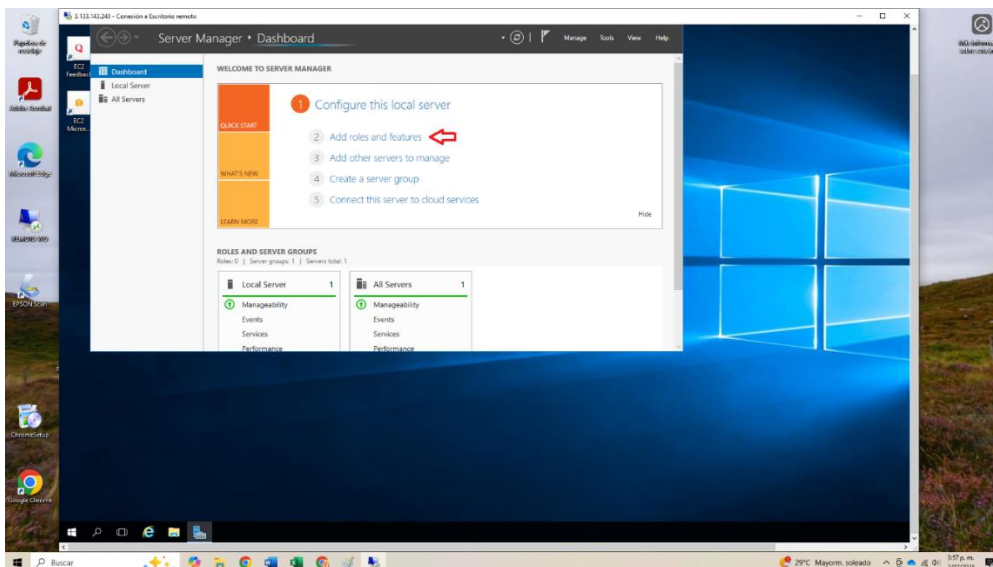
Dentro de nuestro servidor buscamos server manager y damos clic.

Figura 51 Búsqueda server manager.



Para instalar el rol damos clic en añadir roles y características.

Figura 52 instalación de rol.



Iniciamos la instalación y damos siguiente.

Figura 53 proceso instalación.

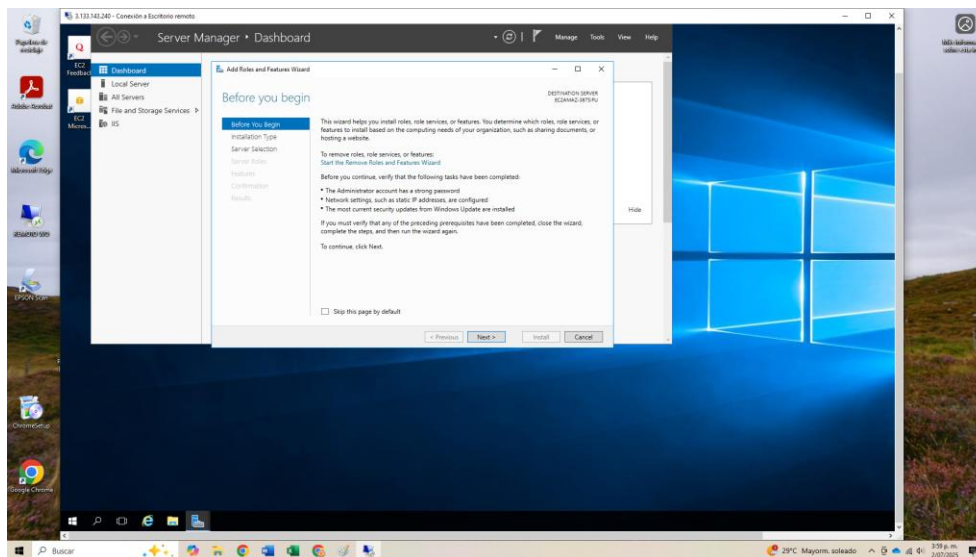


Figura 54 proceso de instalación.

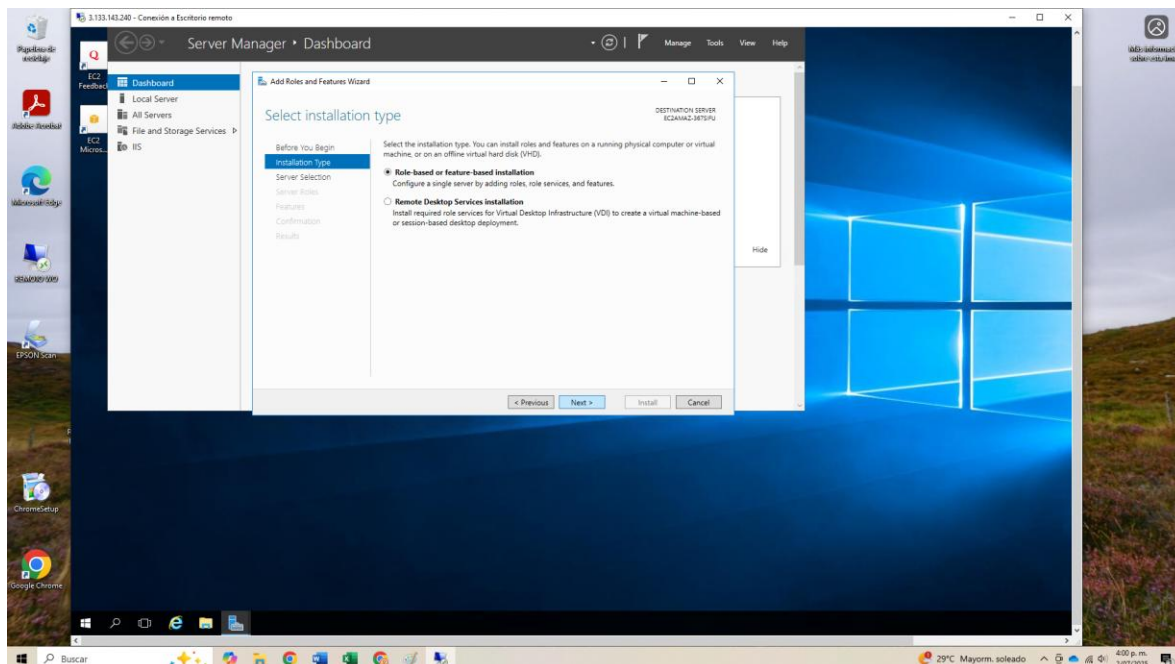
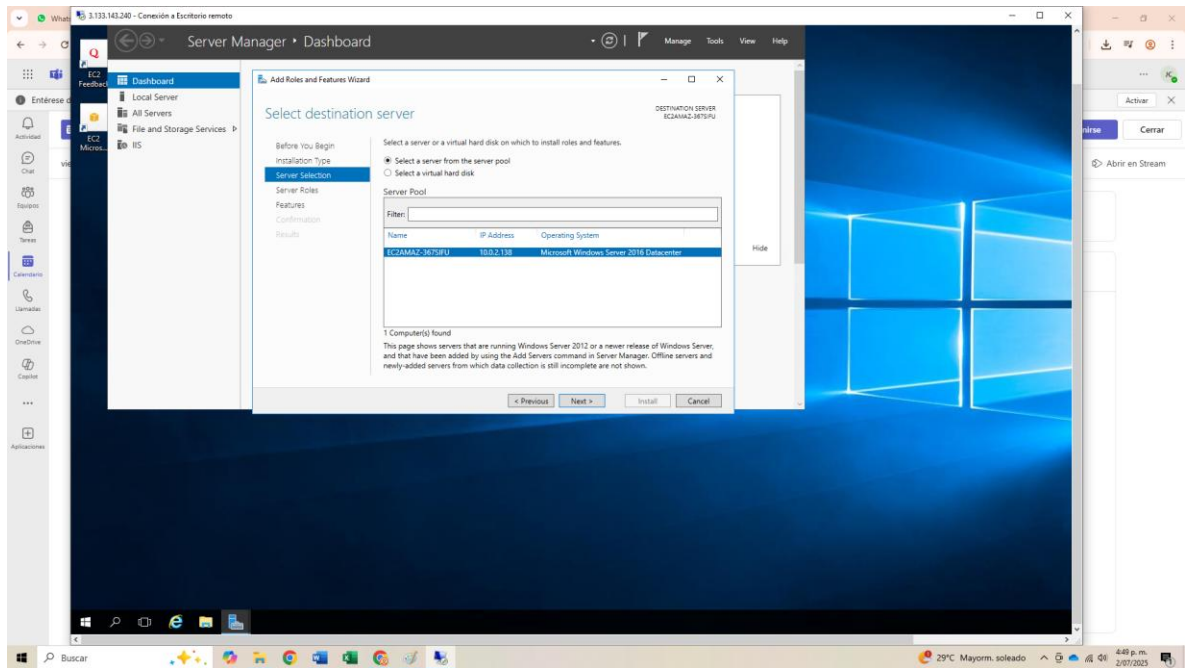


Figura 55 instalación rol.



Instalamos el servicio de web server.

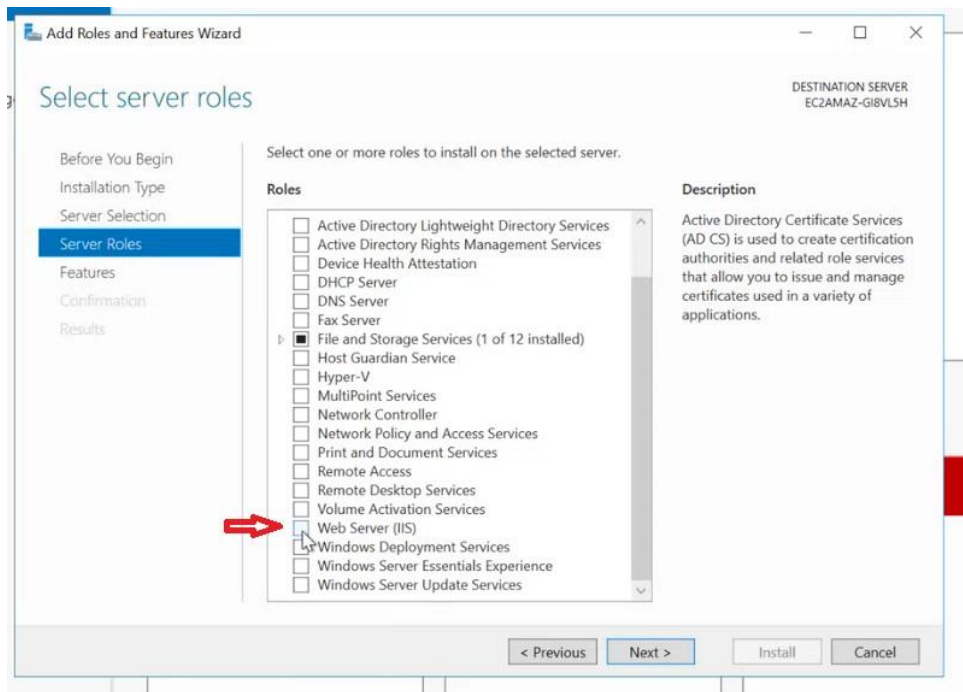


Figura 56 instalación web server.

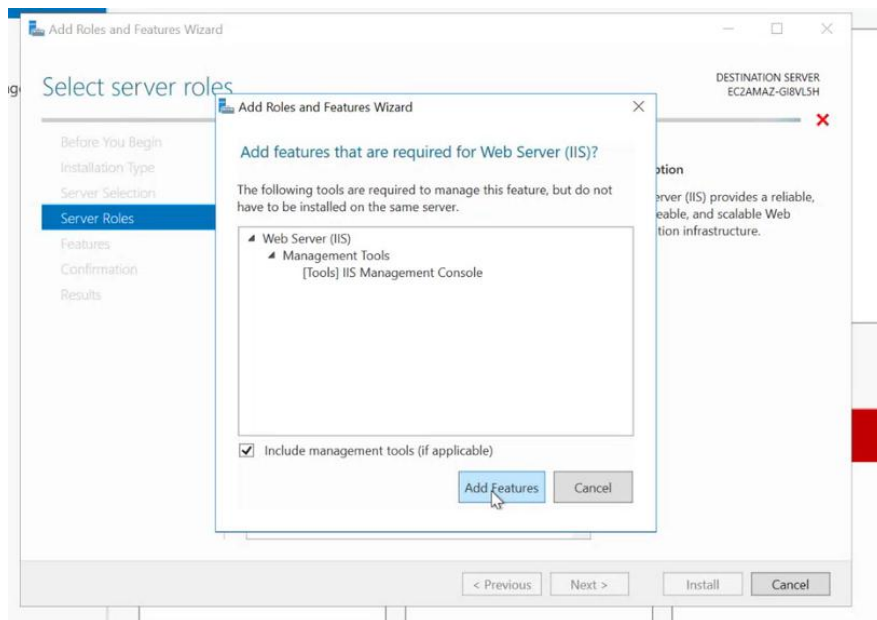
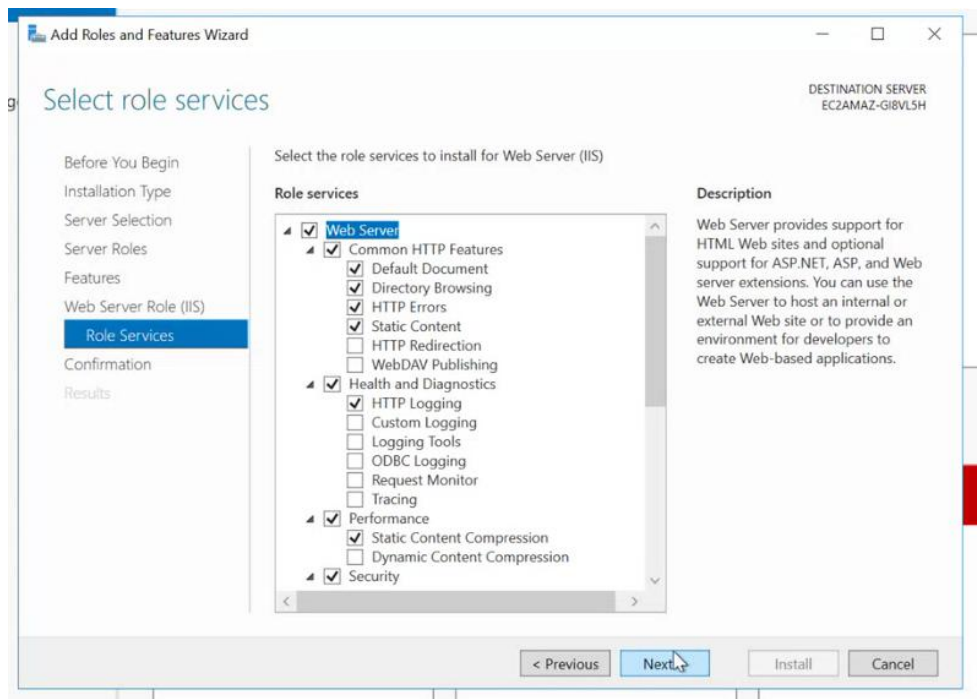


Figura 57 instalación rol.



Instalamos y esperamos que se ejecute la instalación.

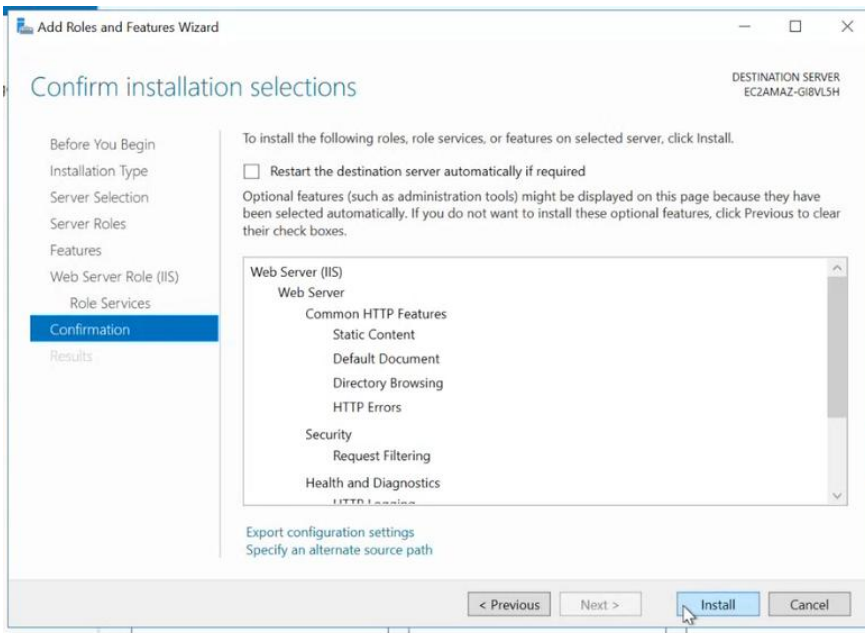
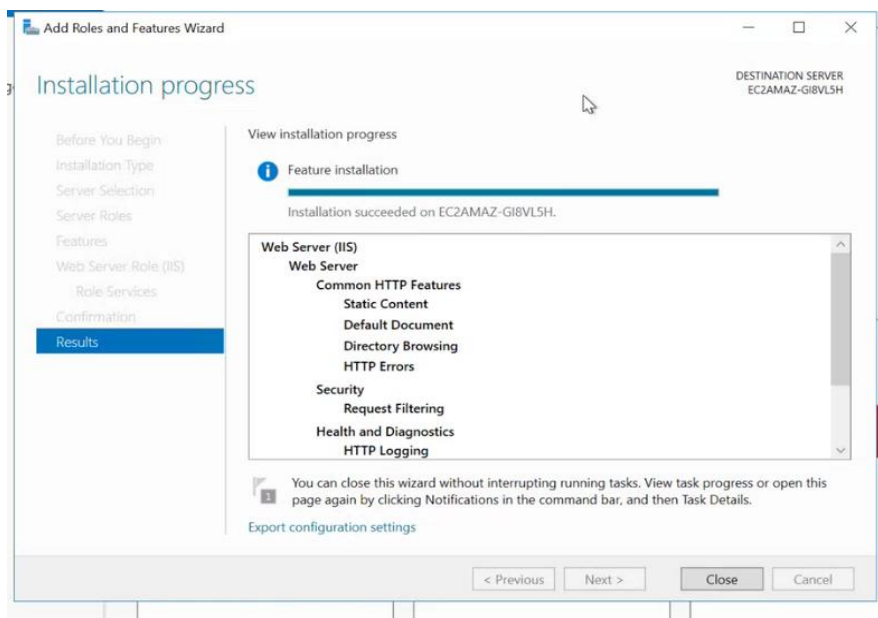
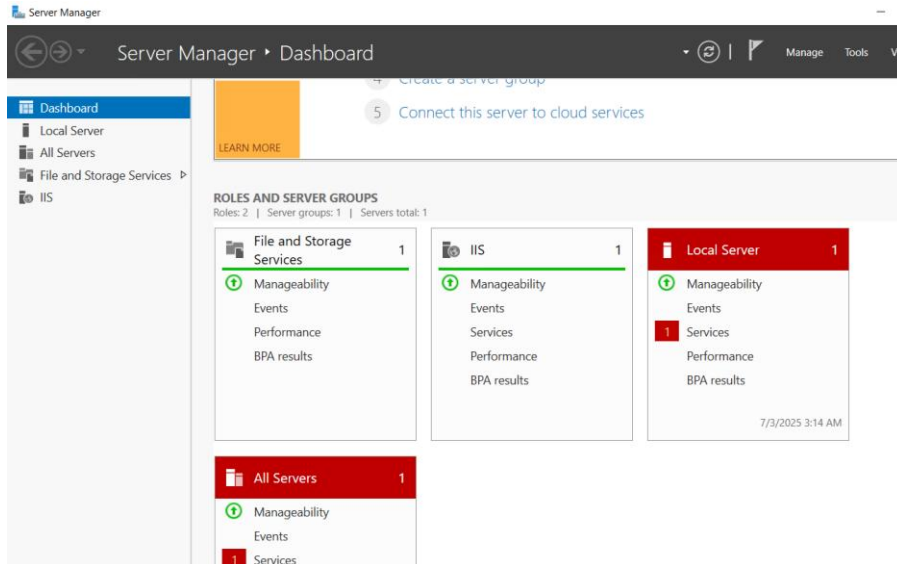


Figura 58 finalización de instalación.



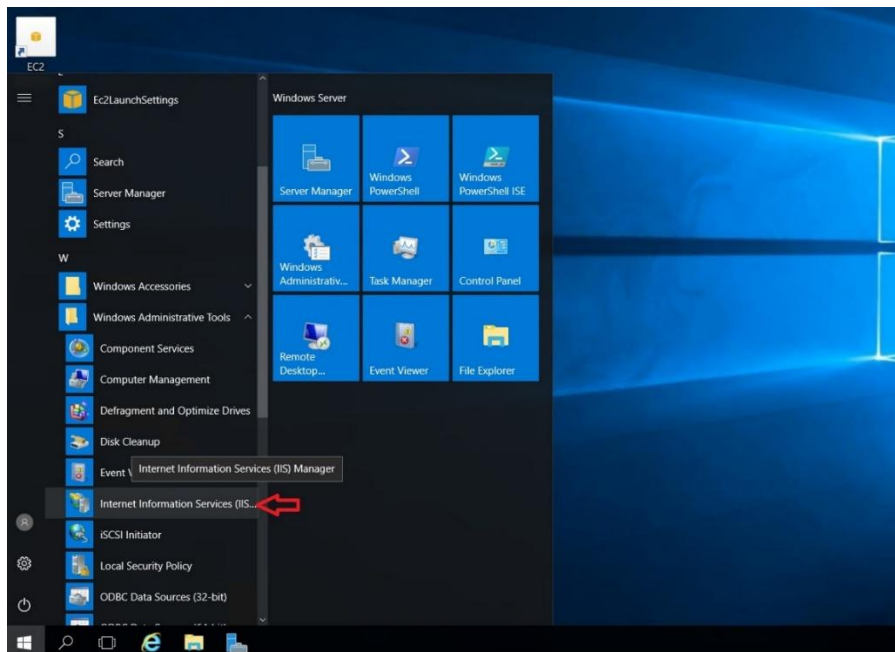
Evidenciamos que ya se instaló correctamente.

Figura 59 visualización instalación.



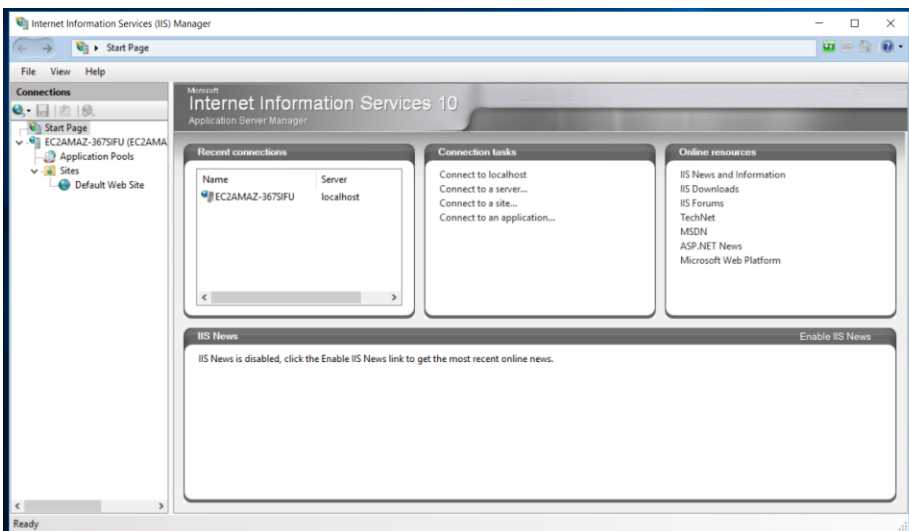
Buscamos el servicio que se instaló y seleccionamos internet information services.

Figura 60 Búsqueda servicio instalado.



Observamos nuestro servidor web creado.

Figura 61 servidor creado.



Probamos nuestro sitio desde el servidor, para comprobar que funciona.

Figura 62 prueba servidor.

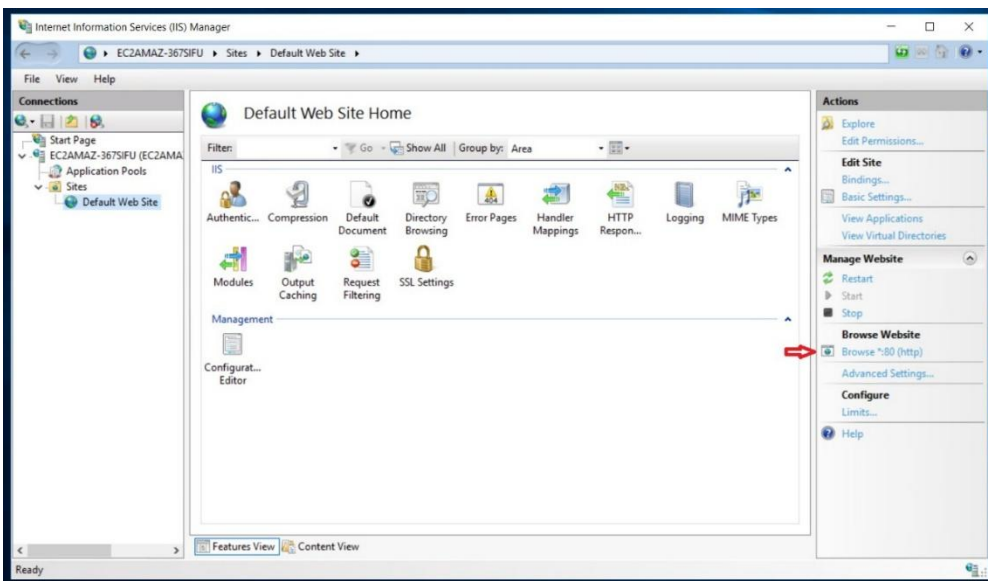
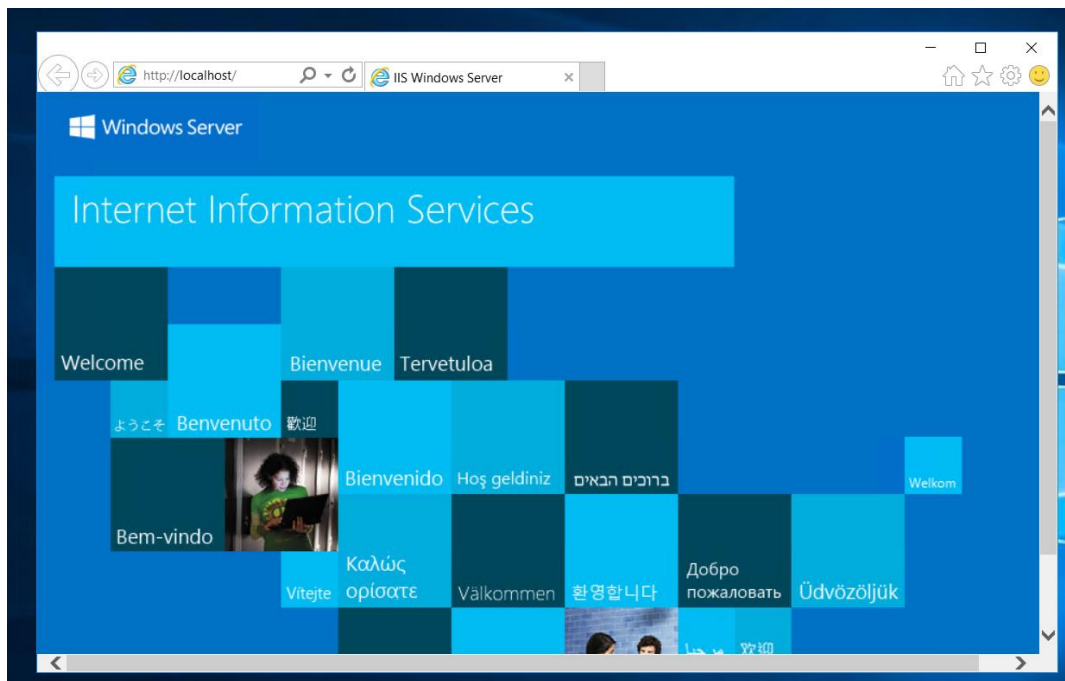
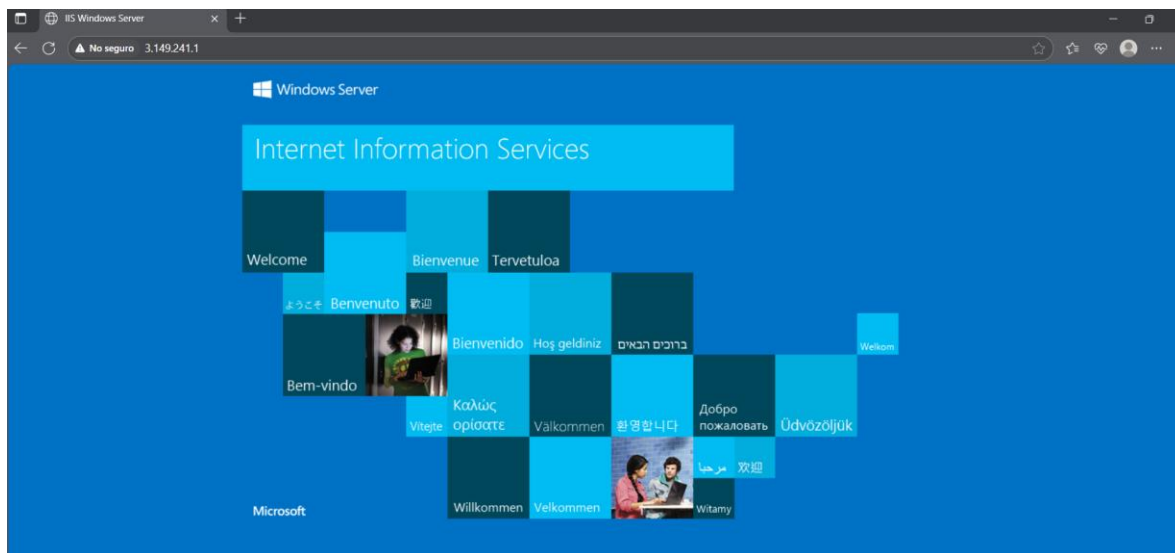


Figura 63 servidor funcionando.



Probamos que nuestro sitio web se vea desde la dirección pública en nuestro navegador.

Figura 64 prueba en navegar web.

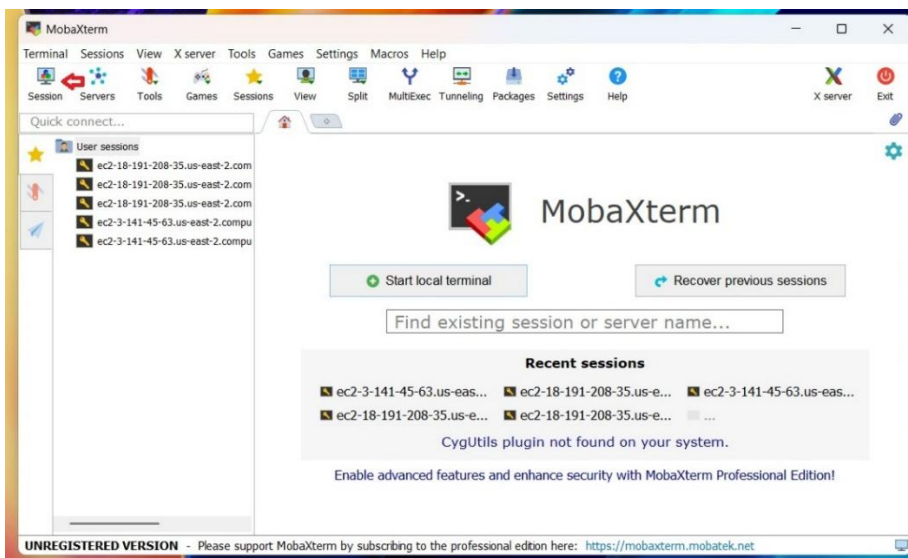


Acceso vía SSH a la instancia Linux

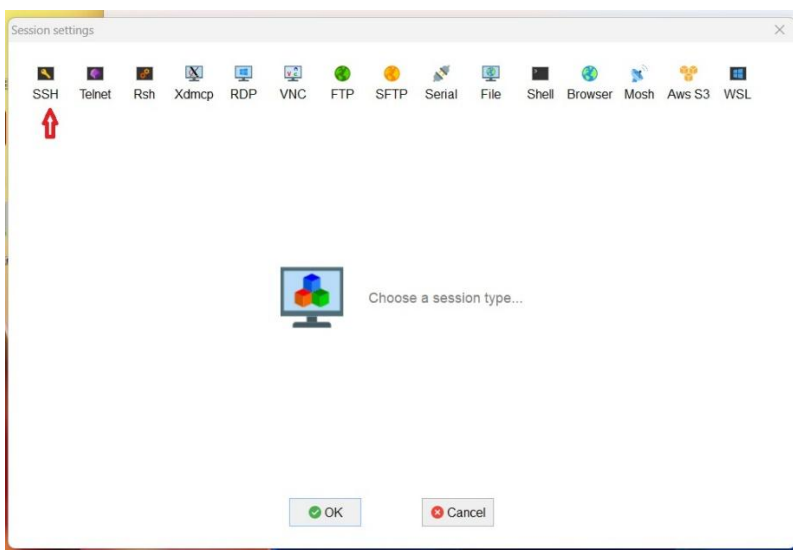
Para conectarnos a la instancia de Linux necesitamos MobaXterm

Abrimos nuestro programa y damos clic en la opción Session.

Figura 65 acceso SSH.



Seleccionamos SSH, colocamos la información que nos pide de nuestra instancia.



Seleccionamos nuestra instancia y le damos clic en conectar.

Figura 66 conexión.

Instancias (1/3) Información Última actualización Hace 1 minute [Conectar](#) [Estado de la instancia](#) [Acciones](#) [Lanzar instancias](#)

Buscar instancia por atributo o etiqueta (case-sensitive) Todos los ...

<input type="checkbox"/>	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación de	Estado de la al:	Zona de dispon...	DNS de IPv4
<input type="checkbox"/>	Server1	i-07fef0228c4cb0d7c	En ejecución	t2.micro	2/2 comprobador	Ver alarmas +	us-east-2a	ec2-3-149-2
<input checked="" type="checkbox"/>	Linux1	i-000a603b430bf9a7d	En ejecución	t2.micro	2/2 comprobador	Ver alarmas +	us-east-2a	ec2-3-16-78
<input type="checkbox"/>	Linux2	i-056039ae695dcc90e	Detenida	t2.micro	-	Ver alarmas +	us-east-2a	-

Seleccionamos cliente SSH.

Figura 67 sección cliente SSH.

Conectar Información

Conéctese a una instancia a través del cliente basado en navegador.

[Conexión de la instancia EC2](#) |
 [Administrador de sesiones](#) |
 [Cliente SSH](#) |
 [Consola de serie de EC2](#)

ID de la instancia

[i-000a603b430bf9a7d](#) (Linux1)

Copiamos la IP Pública y la pegamos en MobaXterm en la opción de Remote Host.

Figura 68 conexión por DNS.

Conectar Información

Conéctese a una instancia a través del cliente basado en navegador.

[Conexión de la instancia EC2](#) |
 [Administrador de sesiones](#) |
 [Cliente SSH](#) |
 [Consola de serie de EC2](#)

ID de la instancia

[i-000a603b430bf9a7d](#) (Linux1)

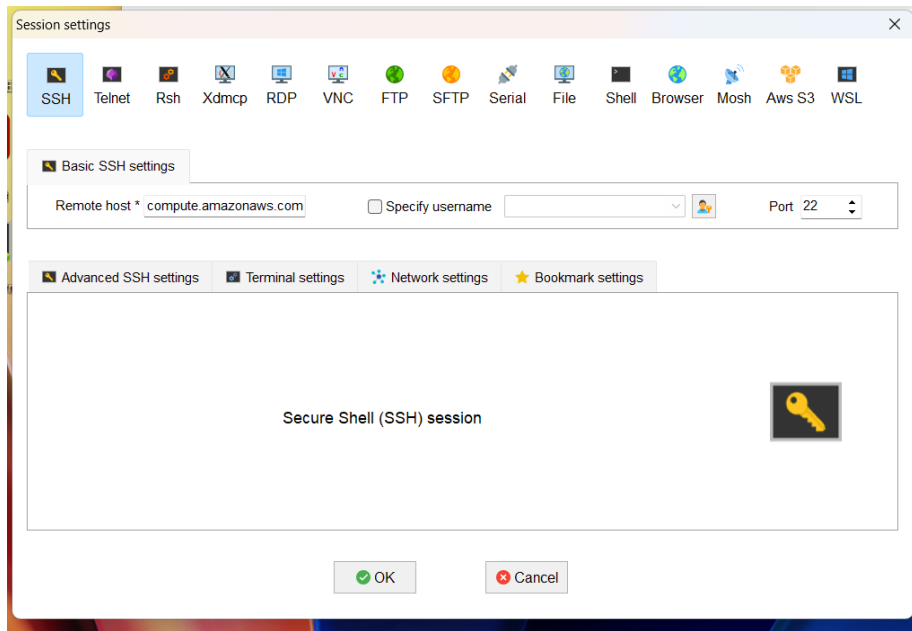
- Abra un cliente SSH.
- Localice el archivo de clave privada. La clave utilizada para lanzar esta instancia es `WindowsServer.pem`
- Ejecute este comando, si es necesario, para garantizar que la clave no se pueda ver públicamente.


```
chmod 400 "WindowsServer.pem"
```
- Conéctese a la instancia mediante su DNS público:

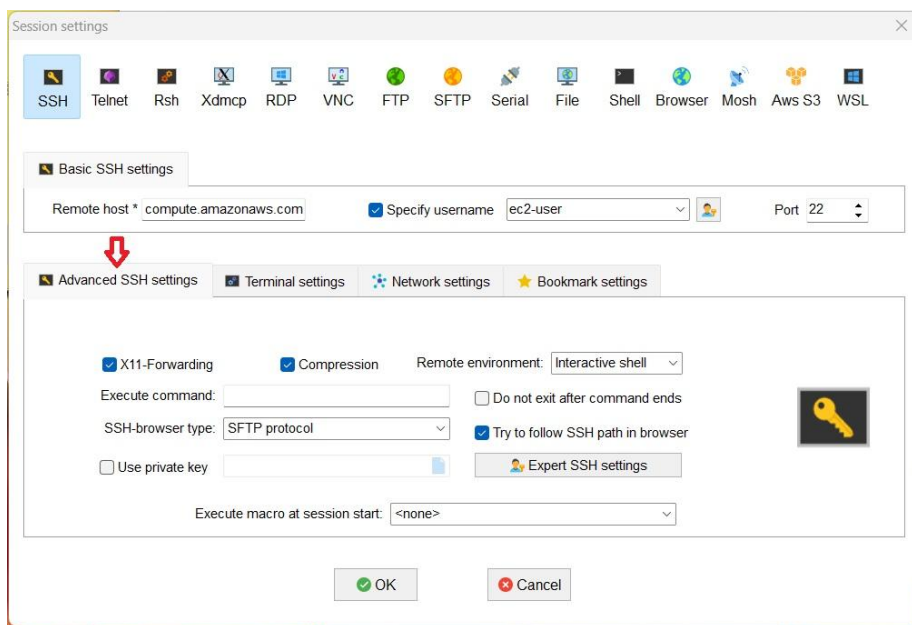

```
ec2-3-16-78-69.us-east-2.compute.amazonaws.com
```

Ejemplo:

```
ssh -i "WindowsServer.pem" ec2-user@ec2-3-16-78-69.us-east-2.compute.amazonaws.com
```

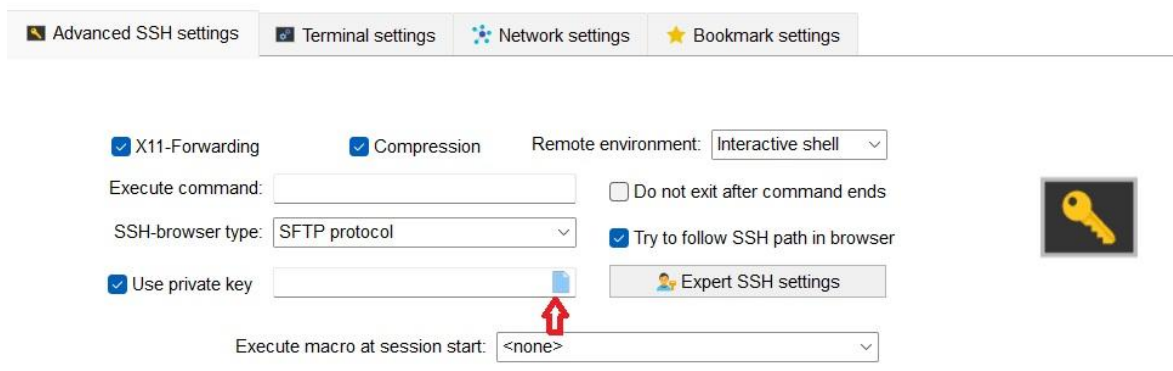
Figura 69 acceso servidor.

Ingresamos nuestro usuario, que en este caso es (ec2-user) y presionamos la opción Advanced SSH settings.

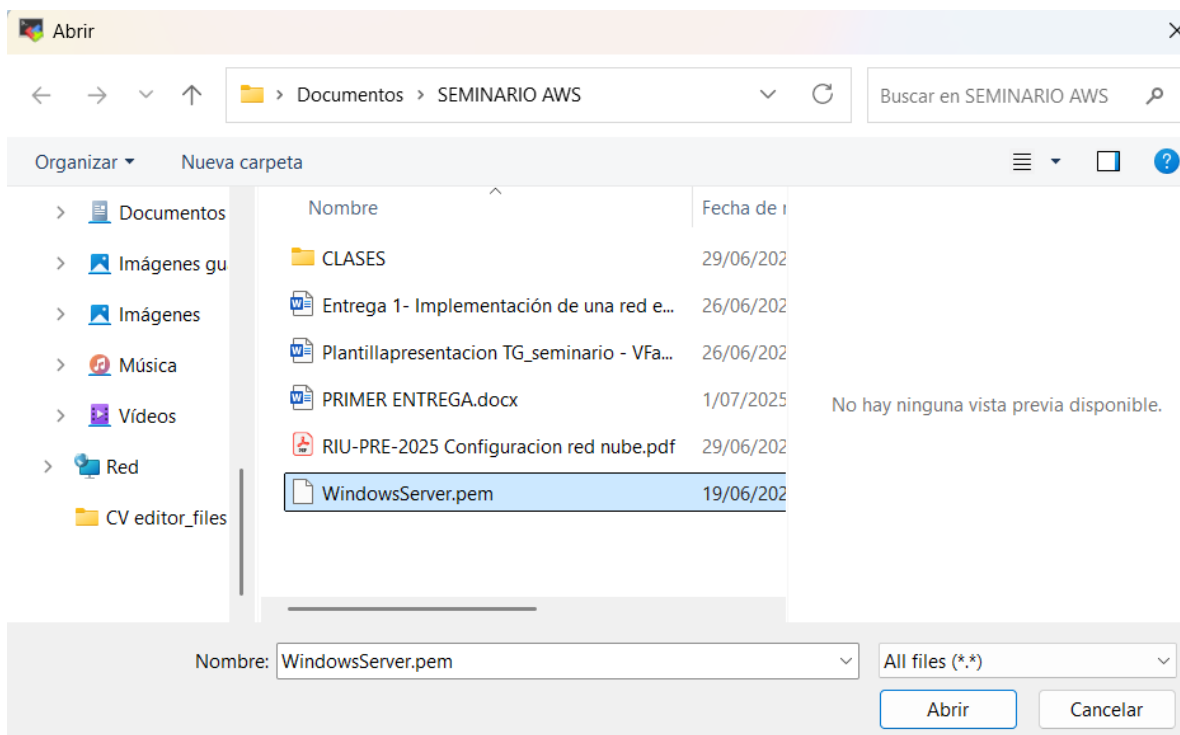
Figura 70 acceso SSH.

Seleccionamos la casilla para usar la clave privada y buscamos nuestro archivo
WindowsServer.pem.

Figura 71 ingreso de archivo .pem.



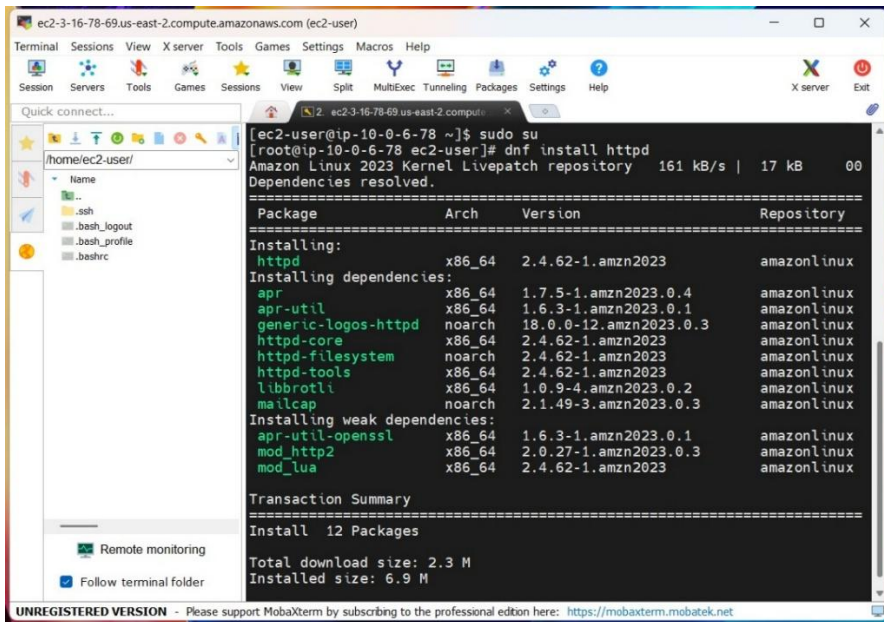
Lo seleccionamos y damos aceptar.



Presionamos OK para acceder.

Ejecutamos el comando (dnf install httpd) para instalar el Apache.

Figura 74 instalación Apache.



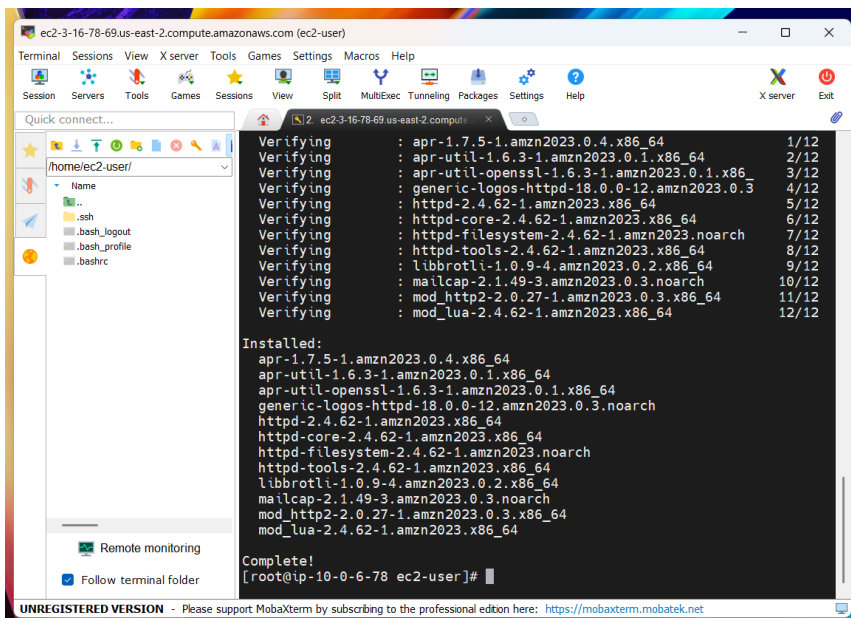
```

[ec2-user@ip-10-0-6-78 ~]$ sudo su
[root@ip-10-0-6-78 ec2-user]# dnf install httpd
Amazon Linux 2023 Kernel Livepatch repository 161 kB/s | 17 kB 00
Dependencies resolved.
=====
Package           Arch      Version      Repository
=====
Installing:
httpd              x86_64    2.4.62-1.amzn2023    amazonlinux
Installing dependencies:
apr                x86_64    1.7.5-1.amzn2023.0.4    amazonlinux
apr-util           x86_64    1.6.3-1.amzn2023.0.1    amazonlinux
generic-logos-httpd noarch    18.0.0-12.amzn2023.0.3    amazonlinux
httpd-core         x86_64    2.4.62-1.amzn2023      amazonlinux
httpd-filesystem  noarch    2.4.62-1.amzn2023      amazonlinux
httpd-tools        x86_64    2.4.62-1.amzn2023      amazonlinux
libbrotli          x86_64    1.0.9-4.amzn2023.0.2    amazonlinux
mailcap            noarch    2.1.49-3.amzn2023.0.3    amazonlinux
Installing weak dependencies:
apr-util-openssl  x86_64    1.6.3-1.amzn2023.0.1    amazonlinux
mod_http2          x86_64    2.0.27-1.amzn2023.0.3    amazonlinux
mod_lua            x86_64    2.4.62-1.amzn2023      amazonlinux
=====
Transaction Summary
-----
Install 12 Packages

Total download size: 2.3 M
Installed size: 6.9 M

```

Figura 75 instalación completa.



```

Verifying          : apr-1.7.5-1.amzn2023.0.4.x86_64           1/12
Verifying          : apr-util-1.6.3-1.amzn2023.0.1.x86_64           2/12
Verifying          : apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64 3/12
Verifying          : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch 4/12
Verifying          : httpd-2.4.62-1.amzn2023.x86_64                5/12
Verifying          : httpd-core-2.4.62-1.amzn2023.x86_64           6/12
Verifying          : httpd-filesystem-2.4.62-1.amzn2023.noarch      7/12
Verifying          : httpd-tools-2.4.62-1.amzn2023.x86_64          8/12
Verifying          : libbrotli-1.0.9-4.amzn2023.0.2.x86_64         9/12
Verifying          : mailcap-2.1.49-3.amzn2023.0.3.noarch          10/12
Verifying          : mod_http2-2.0.27-1.amzn2023.0.3.x86_64        11/12
Verifying          : mod_lua-2.4.62-1.amzn2023.x86_64              12/12

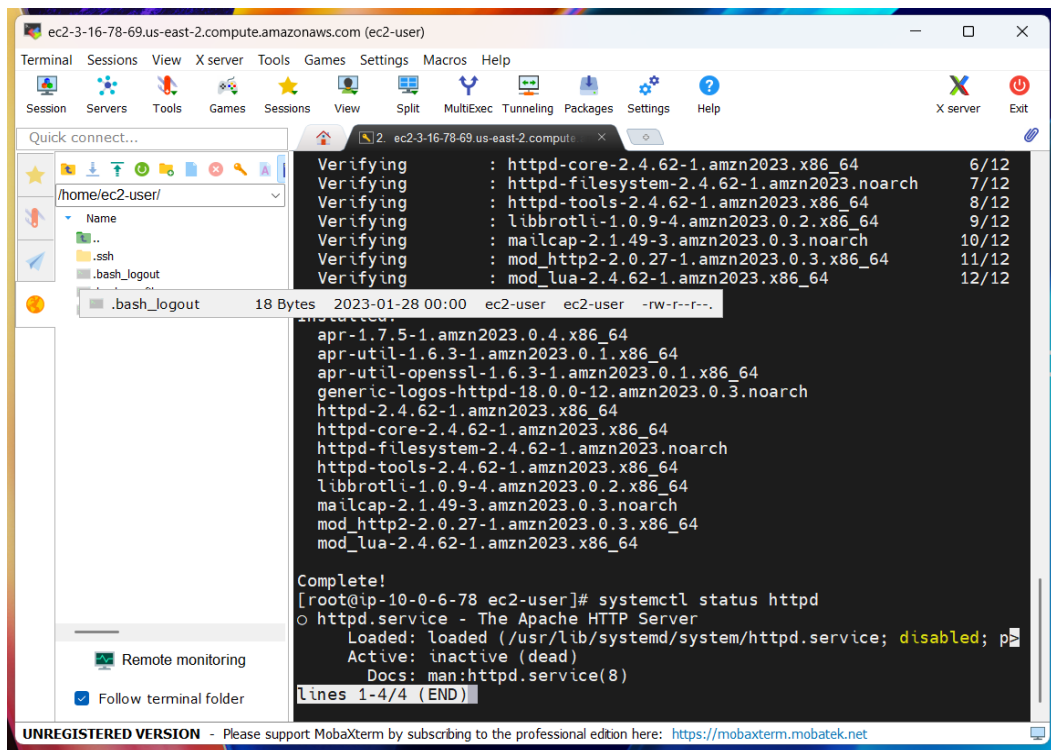
Installed:
apr-1.7.5-1.amzn2023.0.4.x86_64
apr-util-1.6.3-1.amzn2023.0.1.x86_64
apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64
generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch
httpd-2.4.62-1.amzn2023.x86_64
httpd-core-2.4.62-1.amzn2023.x86_64
httpd-filesystem-2.4.62-1.amzn2023.noarch
httpd-tools-2.4.62-1.amzn2023.x86_64
libbrotli-1.0.9-4.amzn2023.0.2.x86_64
mailcap-2.1.49-3.amzn2023.0.3.noarch
mod_http2-2.0.27-1.amzn2023.0.3.x86_64
mod_lua-2.4.62-1.amzn2023.x86_64

Complete!
[root@ip-10-0-6-78 ec2-user]#

```

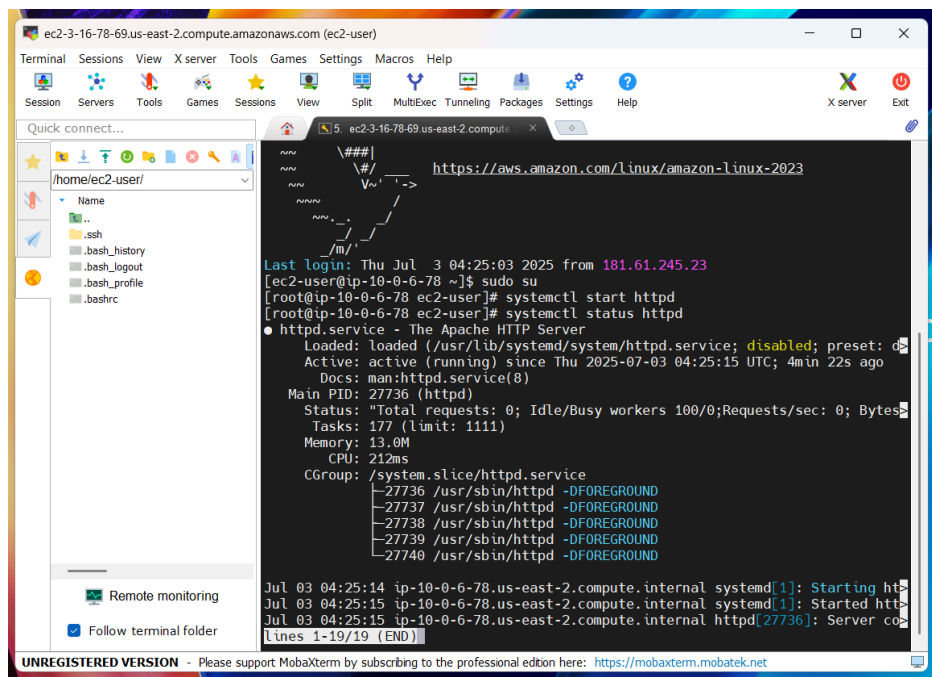
Ingresamos el siguiente comando para verificar que el servidor este corriendo (systemctl status httpd).

Figura 76 verificación estado.



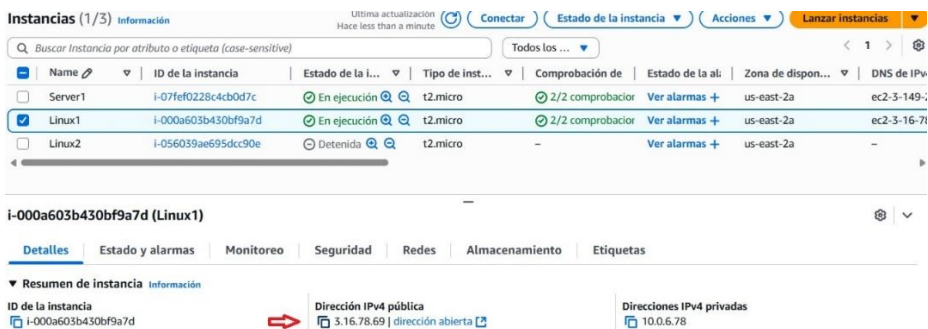
Podemos verificar que esta inactiva. Para activarla usamos el comando(`systemctl start httpd`). Verificamos que la activación con el comando `Systemctl status httpd`.

Figura 77 activación.



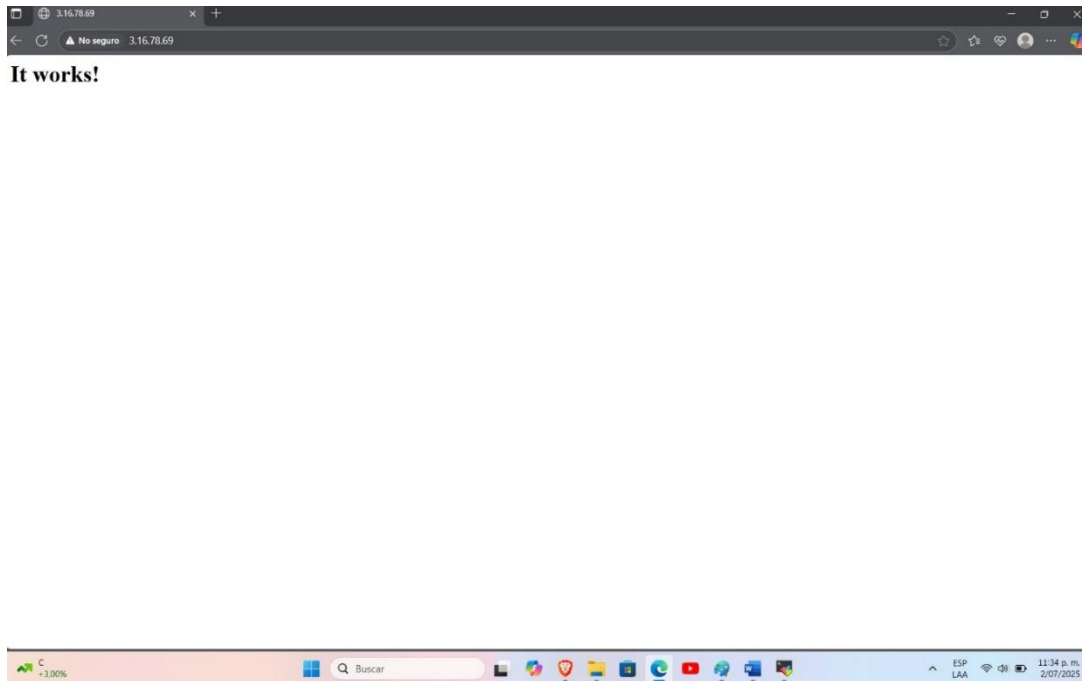
Verificamos el acceso al servidor desde el navegador, copiando nuestra IP pública.

Figura 78 prueba de acceso.



Observamos en nuestro navegador la página que crea por defecto.

Figura 79 prueba en navegador web.

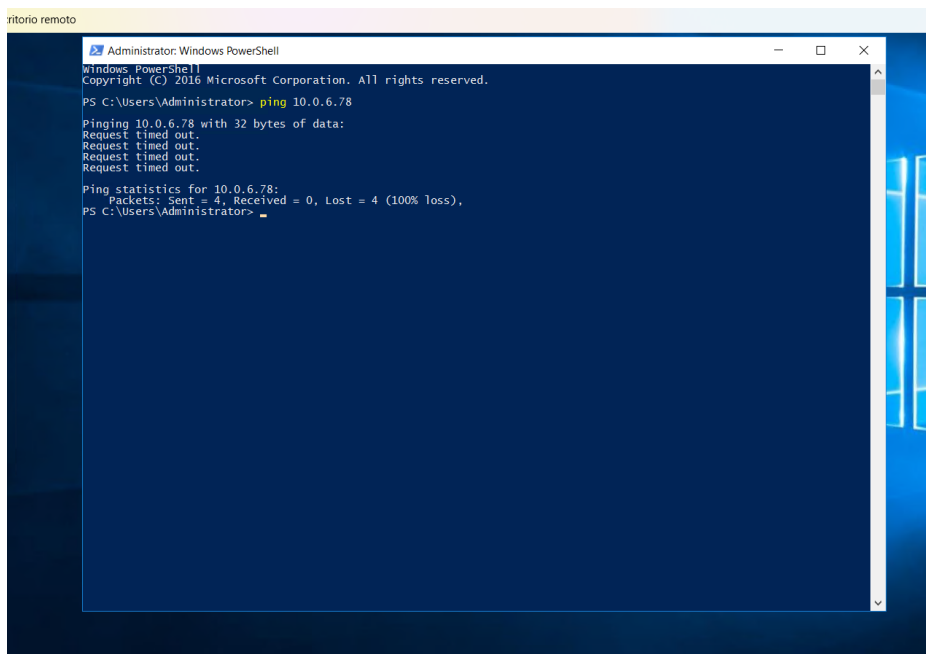


Prueba de conectividad de Windows a Linux.

Para que la conectividad entre ambas instancias por la IP privada sea exitosa, es necesario crear una nueva regla de seguridad con el protocolo ICMP. Sin este no pueden acceder entre ambas.

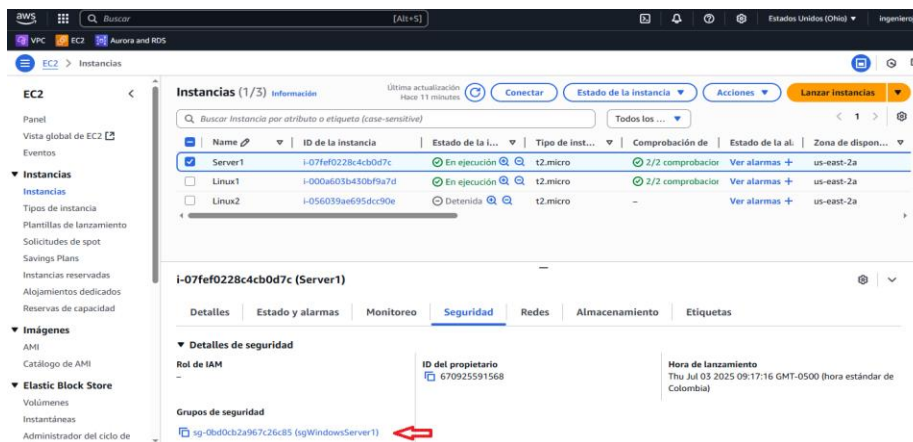
En esta imagen observamos que se ejecuta el ping desde Windows hacia Linux, pero no está establecido el protocolo ICMP y no es exitosa la conexión.

Figura 80 ping sin protocol ICMP.



Para habilitar el protocolo ICMP nos dirigimos a nuestras instancias, en la sección de seguridad y seleccionamos grupo de seguridad. Este proceso es el mismo para ambas instancias.

Figura 81 seleccion grupo de seguridad.



Damos clic en editar reglas de entrada.

Figura 82 regla de entrada.

The screenshot shows the AWS Management Console interface for a security group named 'sg-0bd0cb2a967c26c85 - sgWindowsServer1'. The 'Reglas de entrada' (Inbound Rules) tab is active, displaying a table with 3 rules. A red arrow points to the 'Editar reglas de entrada' button.

Name	ID de la regla del gr...	Versión de IP	Tipo	Protocolo	Intervalo de p
-	sgr-0a040f6788552ea87	IPv4	HTTP	TCP	80
-	sgr-0d1b3ac87fad759c2	IPv4	RDP	TCP	3389

Seleccionamos agregar regla e ingresamos la información para que nos permite realizar la conexión por la IP privada.

The screenshot shows the 'Editar reglas de entrada' (Edit inbound rules) form in the AWS Management Console. The form is titled 'Editar reglas de entrada' and includes a warning message: 'Las reglas cuyo origen es 0.0.0.0 o :::0 permiten a todas las direcciones IP acceder a la instancia. Recomendamos configurar reglas de grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas.' The 'Agregar regla' button is highlighted with a red arrow.

ID de la regla del grupo de seguridad	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción: opcional	Acción
sgr-0a040f6788552ea87	HTTP	TCP	80	Perso...		Eliminar
sgr-0d1b3ac87fad759c2	RDP	TCP	3389	Perso...		Eliminar

Buttons: Agregar regla, Previsualizar los cambios, Guardar reglas, Cancelar.

Damos guardar reglas y ejecutamos ping a la IP para revisar si hay conexión.

Editar reglas de entrada información
Las reglas de entrada controlan el tráfico entrante que puede llegar a la instancia.

ID de la regla del grupo de seguridad	Tipo <small>Información</small>	Protocolo <small>Información</small>	Intervalo de puertos <small>Información</small>	Origen <small>Información</small>	Descripción: opcional <small>Información</small>	
sgr-0a040f6788552ea87	HTTP	TCP	80	Perso...	Q	Eliminar
sgr-0d1b3ac87fad759c2	RDP	TCP	3389	Perso...	Q 0.0.0.0/X	Eliminar
-	Todos los ICMP IPv4	ICMP	Todo	Any...	Q 0.0.0.0/X 0.0.0.0/X	Eliminar

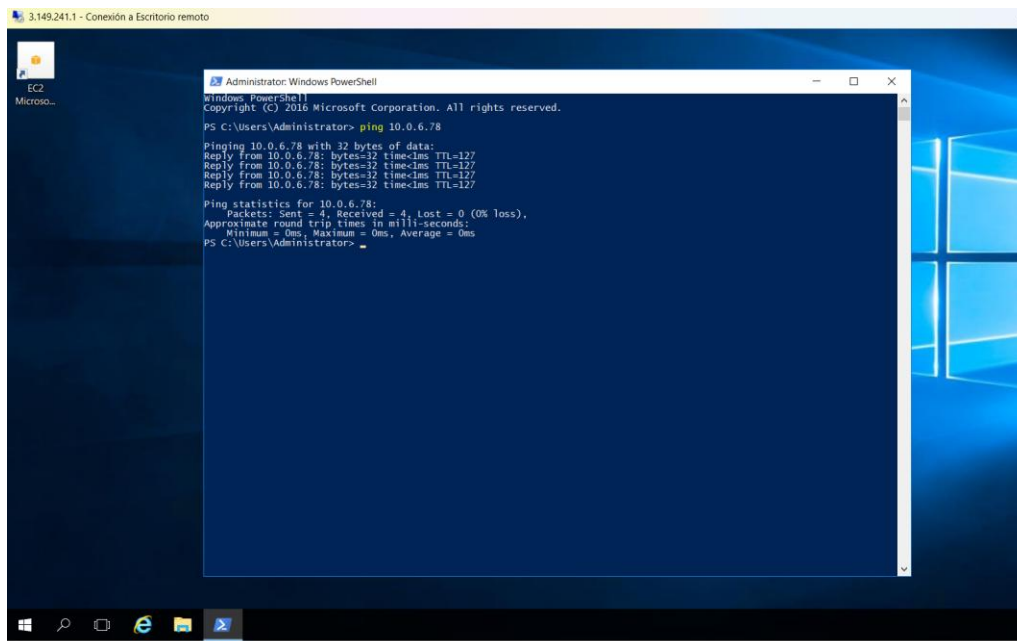
[Agregar regla](#)

⚠ Las reglas cuyo origen es 0.0.0.0/0 o ::/0 permiten a todas las direcciones IP acceder a la instancia. Recomendamos configurar reglas de grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas.

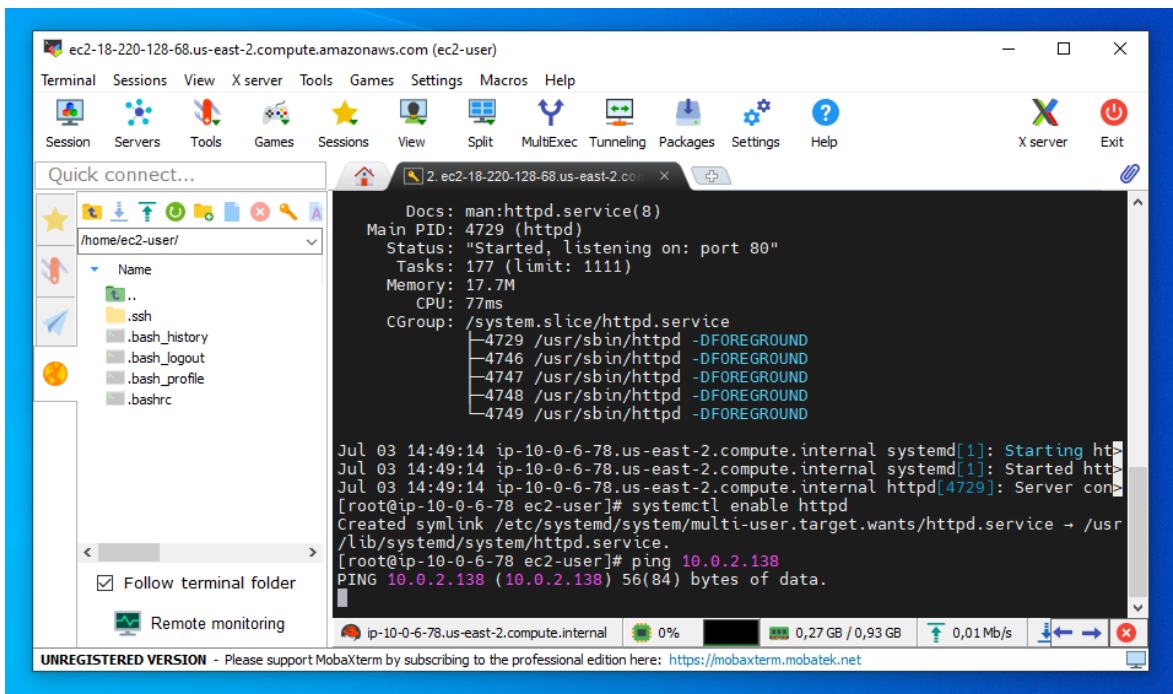
Cancelar [Previsualizar los cambios](#) **Guardar reglas**

Efectivamente la instancia de Windows pudo comunicarse correctamente con la instancia de Linux usando su IP privada.

Figura 83 prueba de conexión entre instancias.

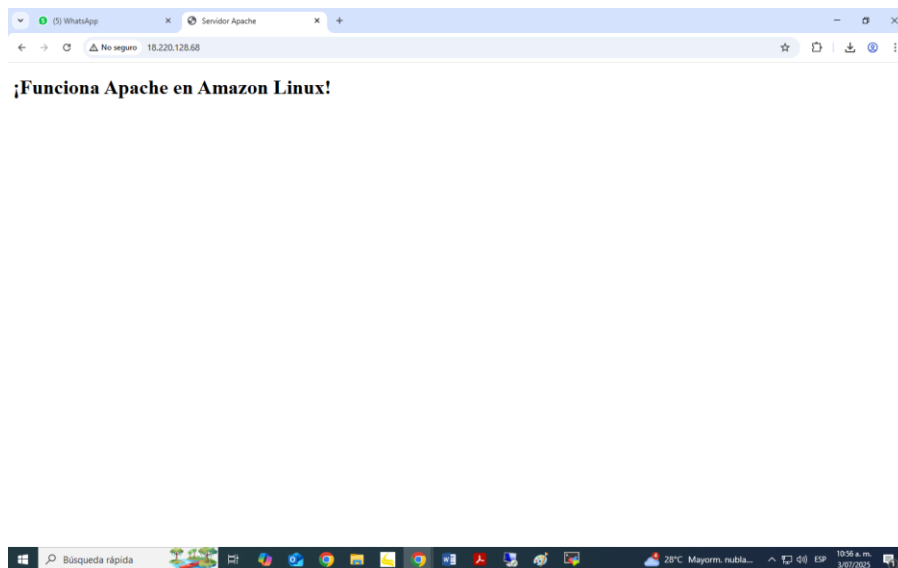


Comprobamos que también hay conexión exitosa de Linux a Windows.



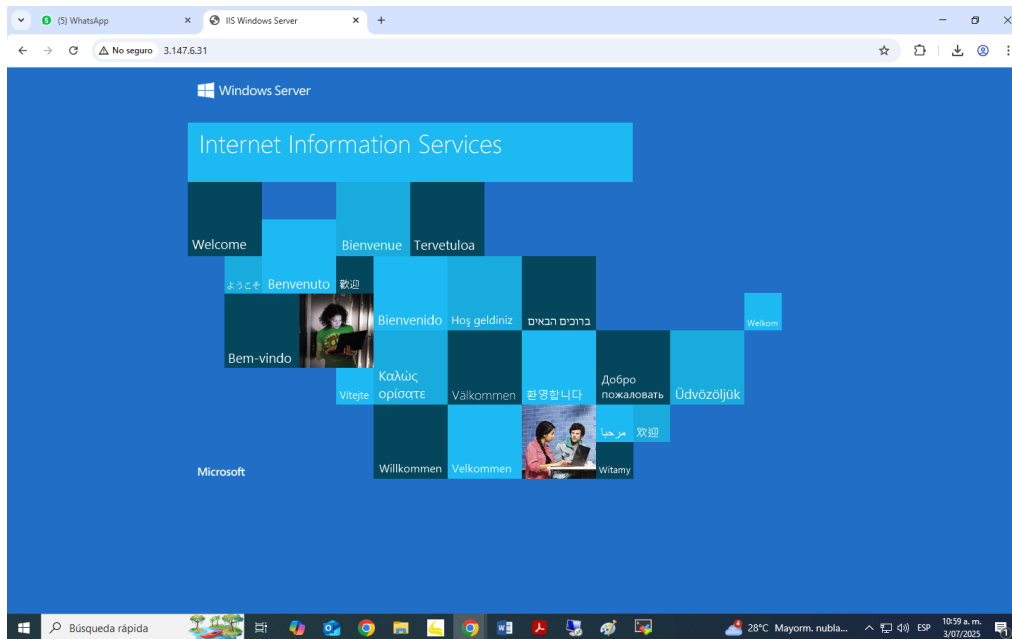
Validación de acceso web desde Linux.

Figura 84 servidor funcionando.



Validación de acceso web desde Windows.

Figura 85 servidor funcionando.



Entrega 2

Para la implementación de Balanceador de Carga (ALB), es necesario contar con al menos 2 instancias EC2 configuradas de manera idéntica, para garantizar que el tráfico se distribuya de manera uniforme sin generar errores; manteniendo la alta disponibilidad y tolerancia a fallos.

Creación de Instancias EC2

Teniendo en cuenta que ya tenemos creado una instancia con Amazon Linux y Apache instalado, vamos a crear una imagen (AMI) de esa instancia, lo que permitirá lanzar una segunda instancia con la misma configuración.

Seleccionamos nuestra ID de la instancia, nos dirigimos a almacenamiento y procedemos a seleccionar nuestro volumen.

Figura 86 selección ID.

The screenshot displays the AWS Management Console interface for an EC2 instance. At the top, there's a navigation bar with 'Instancias (1)' and 'Información'. Below this is a search bar and a table of instances. The table has columns for Name, ID de la instancia, Estado de la instancia, Tipo de instancia, Comprobación de estado, Estado de la alarma, and Zona de disponibilidad. The instance 'Linux1' is highlighted with a red arrow pointing to its ID 'i-000a603b430bf9a7d'. Below the table, the 'Almacenamiento' tab is selected, showing details for the instance's storage configuration. The details are organized into three columns: 'Detalles de la instancia', 'Monitoreo', and 'Detalles de la plataforma'.

Name	ID de la instancia	Estado de la instancia	Tipo de instancia	Comprobación de estado	Estado de la alarma	Zona de disponibilidad
Linux1	i-000a603b430bf9a7d	En ejecución	t2.micro	2/2 comprobador	Ver alarmas +	us-east-2a

Detalles de la instancia	Monitoreo	Detalles de la plataforma
ID de AMI ami-0c803b171269e2d72	Monitoreo desactivado	Detalles de la plataforma Linux/UNIX
Nombre de AMI al2023-ami-2023.7.20250623.1-kernel-6.1-x86_64	Imagen permitida -	Protección de terminación desactivado
Detener la protección desactivado	Hora de lanzamiento Mon Jul 14 2025 12:00:25 GMT-0500 (hora estándar de Colombia) (30 minutos)	Ubicación de AMI amazon/al2023-ami-2023.7.20250623.1-kernel-6.1-x86_64

Figura 87 selección de volumen.

<input checked="" type="checkbox"/>	ID de volumen	Nombre del d...	Tamaño del vol...	Estado del volumen	Estado de la con...	Hora de conexión
<input checked="" type="checkbox"/>	vol-03e111edeac976479	/dev/xvda	8	En uso	Asociado	2025/07/02 13:15 GM

Seleccionamos el volumen, damos en acciones y creamos nuestra instantánea.

Volúmenes (1/1) Información

Conjuntos de filtros guardados
Elegir conjunto de filt... Buscar

ID de volumen = vol-03e111edeac976479

<input checked="" type="checkbox"/>	Name	ID de volumen	Tipo	Tamaño	IOPS
<input checked="" type="checkbox"/>		vol-03e111edeac976479	gp3	8 GiB	3000

Acciones

- Modificar volumen
- Crear instantánea
- Crear política de ciclo de vida de instantáneas
- Eliminar volumen
- Asociar volumen
- Desasociar el volumen
- Desasociar el volumen forzosamente

Crear volumen

Creada: 2025/07/02 13:15 GM

Asignamos el nombre a nuestra instantánea y damos crear.

Figura 88 creación instantánea.

Crear instantánea Información

Cree una instantánea de un momento dado para realizar copias de seguridad de los datos de un volumen de Amazon EBS en Amazon S3.

Volumen de origen

ID de volumen:

Zona de disponibilidad:

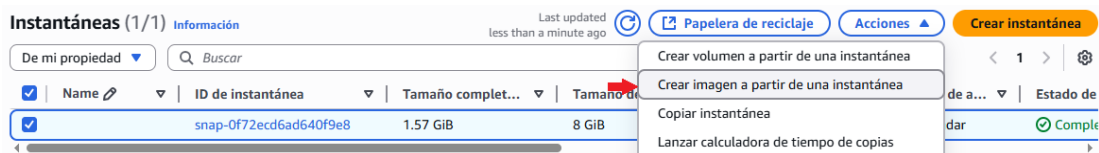
Detalles de la instantánea

Descripción
Agrega una descripción para la instantánea

255 caracteres como máximo

Una vez creada damos en acciones para seleccionar la opción de crear imagen a partir de una instantánea.

Figura 89 creación de imagen.



Le damos un nombre y descripción, revisamos el nombre de dispositivo de raíz que sea el mismo nombre con el que crea los volúmenes, lo copiamos y pegamos.

Figura 90 creación de AMI.

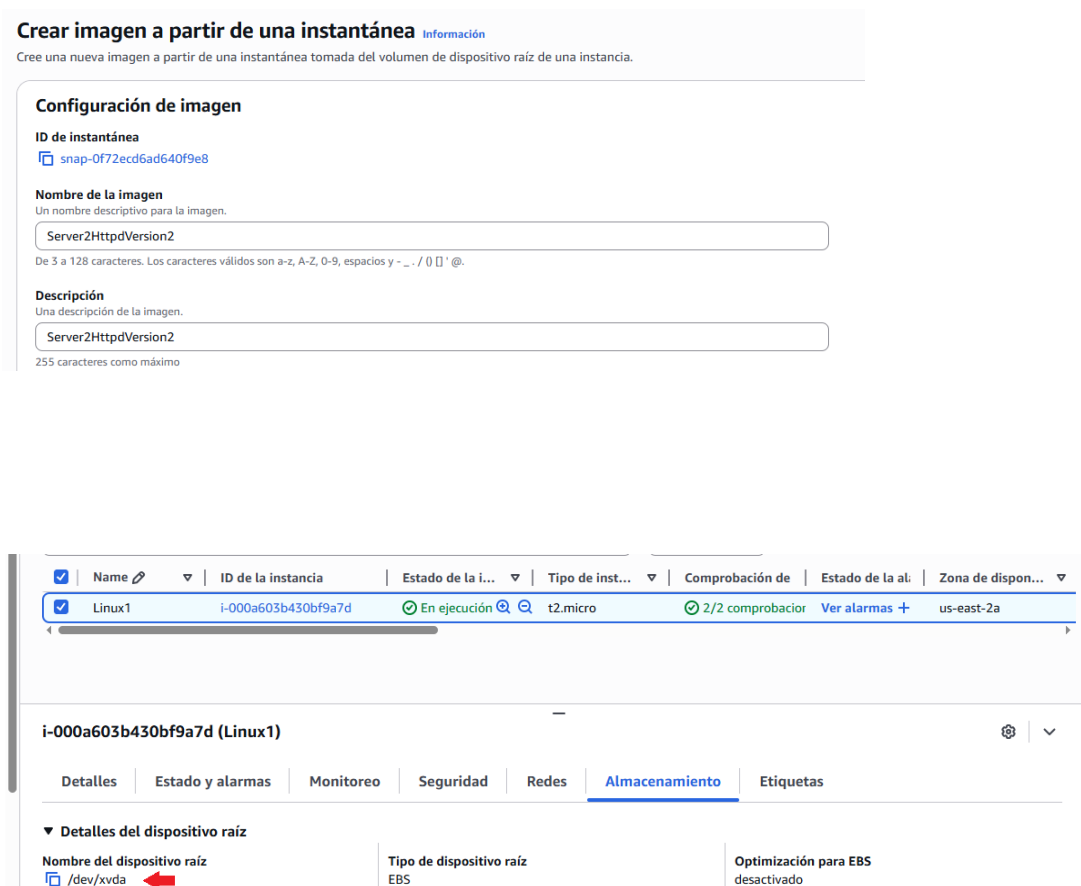


Figura 91 identificación dispositivo raíz .

Nombre del dispositivo raíz | Información
El nombre del dispositivo que está reservado para el volumen raíz.

Tipo de virtualización | Información
El tipo de virtualización que utilizarán las instancias lanzadas desde esta imagen.

Virtualización asistida por hardware

ID de kernel | Información
El kernel del sistema operativo para la AMI.

Usar valor predeterminado

Dejamos por defecto la demás información y damos crear imagen.

volumen

Tipo de dispositivo Raíz	Nombre del dispositivo /dev/xvda	Instantánea snap-0f72ecd6ad640f9e8
Tamaño (GiB) 8	Tipo de volumen SSD de uso general (gp3)	IOPS 3000
Velocidad (MB/s) 125	Comportamiento de terminación <input checked="" type="checkbox"/> Eliminar cuando termine	Cifrado <input type="checkbox"/> Cifrar volumen

[Agregar volumen](#)

Etiquetas - opcional | Información
Las etiquetas son marcas que se asignan a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizarlas para buscar los recursos y filtrarlos, o para hacer un seguimiento de los costos en AWS.

No hay etiquetas correspondientes a este recurso.

[Agregar etiqueta](#)
Puede agregar 50 etiquetas más.

[Cancelar](#) [Crear imagen](#)

Verificamos que nuestra AMI se creó correctamente.

Figura 92 Figura 90 creación de AMI.

Imágenes de Amazon Machine Image (AMI) (1) | Información

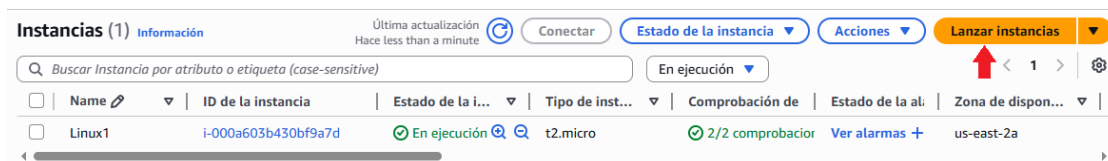
[Papelera de reciclaje](#) [EC2 Image Builder](#) [Acciones](#) [Lanzar instancia a partir de una AMI](#)

De mi propiedad |

<input type="checkbox"/>	Name	Nombre de AMI	ID de AMI	Origen	Propiet...	Visibilidad	Estado
<input type="checkbox"/>	Server2HttpdVersion2		ami-02384b503f037f140	670925591...	670925591...	Privado	Disponibile

Procedemos a crear nuestra segunda instancia con nuestra AMI personalizada.

Figura 93 creación instancia.



Asignamos el nombre, seleccionamos la opción de mis AMI y automáticamente nos aparece a AMI que creamos anteriormente.

Figura 94 seleccion de AMI personalizada.



En el tipo de instancia lo dejamos en t2.micro y elegimos nuestro par de claves que ya tenemos creado.

The screenshot shows the AWS console interface for instance configuration. The 'Tipo de instancia' section is expanded, showing 't2.micro' as the selected instance type. Below it, there are details about the instance type, including family, vCPU, memory, and pricing. To the right, there are options for 'Todas las generaciones' and a link to 'Comparar tipos de instancias'. Below this, there is a search bar and a list of key pairs. The 'WindowsServer' key pair is selected, and a red arrow points to it. There is also a link to 'Crear un nuevo par de claves'.

Configuramos la red, para que tenga acceso a nuestra VPC, asignamos la subred publica y damos habilitar para que se asigne la IP publica automáticamente.

The screenshot shows the AWS console interface for network configuration. The 'Configuraciones de red' section is expanded, showing 'VPC: obligatorio' with a dropdown menu showing 'vpc-0e4b18e86f5af189e (seminario-vpc)'. A red arrow points to this dropdown. Below it, the 'Subred' section is expanded, showing 'subnet-016a81aa21a8bb99d' with a dropdown menu showing 'seminario-subnet-public1-us-east-2a'. A red arrow points to this dropdown. Below this, the 'Asignar automáticamente la IP pública' section is expanded, showing 'Habilitar' as the selected option. A red arrow points to this dropdown. At the bottom, there are two radio buttons: 'Crear grupo de seguridad' (selected) and 'Seleccionar un grupo de seguridad existente'.

Agregamos una nueva regla de seguridad para que podamos acceder al servidor por el puerto 80 desde cualquier lugar.

Figura 95 regla de entrada Puerto 80.

Reglas de grupos de seguridad de entrada

▼ Regla del grupo de seguridad 1 (TCP, 22, 0.0.0.0/0) Eliminar

Tipo | Información: ssh

Protocolo | Información: TCP

Intervalo de puertos | Información: 22

Tipo de origen | Información: Cualquier lugar

Origen | Información: 0.0.0.0/0

Descripción - opcional | Información: por ejemplo, SSH para Admin Desktop

▼ Regla del grupo de seguridad 2 (TCP, 80, 0.0.0.0/0) Eliminar

Tipo | Información: TCP personalizado

Protocolo | Información: TCP

Intervalo de puertos | Información: 80

Tipo de origen | Información: Personalizada

Origen | Información: 0.0.0.0/0

Descripción - opcional | Información: por ejemplo, SSH para Admin Desktop

Dejamos lo demás por defecto y presionamos en lanzar instancia.

Configurar almacenamiento | Información | Avanzado

1x 8 GIB gp3 Volumen raíz, 3000 IOPS, No cifrado

Los clientes que cumplan los requisitos de la capa gratuita pueden obtener hasta 30 GB de almacenamiento magnético o de uso general (SSD) de EBS

Agregar un nuevo volumen

Haga clic en actualizar para ver la información de la copia de seguridad. Las etiquetas que asigne determinan si alguna política de Data Lifecycle Manager realizará una copia de seguridad de la instancia.

0 x sistemas de archivos | Editar

► Detalles avanzados | Información

Imagen de software (AMI)
Server2HttpdVersion2
ami-02384b503f037f140

Tipo de servidor virtual (tipo de instancia)
t2.micro

Firewall (grupo de seguridad)
Nuevo grupo de seguridad

Almacenamiento (volúmenes)
Volúmenes: 1 (8 GIB)

Nivel gratuito: Durante el primer año que abre una cuenta de AWS, obtiene 750 horas al mes de uso de instancias t2.micro (o t3.micro cuando t2.micro no está disponible).

Cancelar ➔ **Lanzar instancia**

🔗 Código de versión preliminar

Efectivamente se creó nuestra instancia Linux 2.

Figura 96 Segunda instancia creada de la AMI.

Instancias (2) | Información | Última actualización: Hace 11 minutos | Conectar | Estado de la instancia | Acciones | Lanzar instancias

Buscar instancia por atributo o etiqueta (case-sensitive) | Todos los ...

	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación de	Estado de la al...	Zona de dispon...
<input type="checkbox"/>	Linux1	i-000a603b430bf9a7d	En ejecución	t2.micro	2/2 comprobador	Ver alarmas +	us-east-2a
<input type="checkbox"/>	Linux2	i-097f72ad3b1b4b016	En ejecución	t2.micro	2/2 comprobador	Ver alarmas +	us-east-2a

Servidor 1 en correcto funcionamiento.

Figura 97 prueba en navegar web.

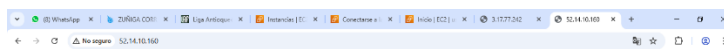


Servidor Apache 1



Servidor 2 en correcto funcionamiento.

Figura 98 prueba en navegar web.



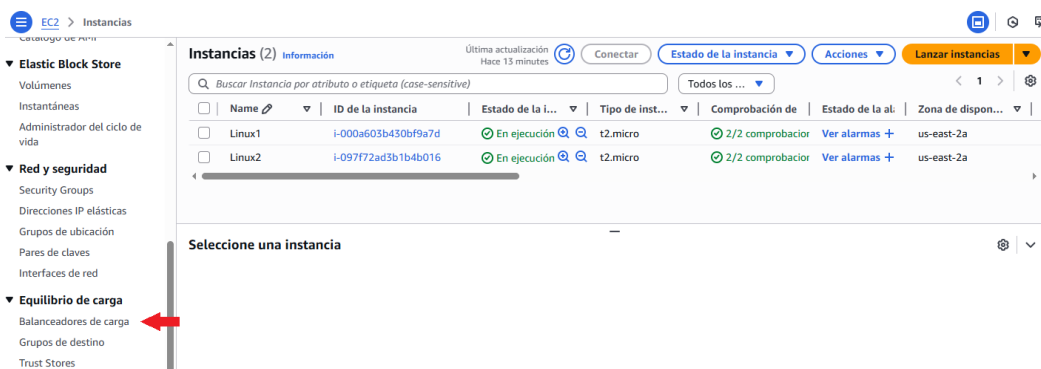
Servidor Apache 2



Con las instancias funcionando de manera correcta, continuamos con la creación del servicio de balanceador de carga(ALB), el cual permitirá balancear el tráfico HTTP a través de múltiples zonas de disponibilidad.

Dentro de EC2 nos dirigimos a equilibrio de carga y seleccionamos Balanceadores de carga.

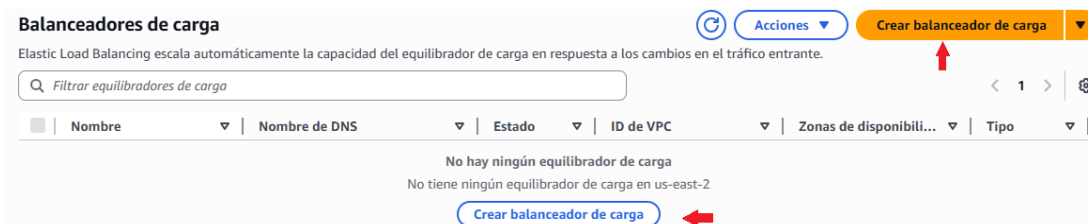
Figura 99 selección balanceadores de carga.



Creación de Balanceador de Carga

Damos en crear Balanceador de carga.

Figura 100 creación balanceador.

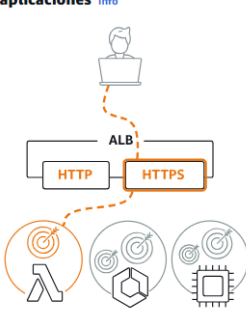


Seleccionamos el tipo de balanceador a crear, que en nuestro caso es balanceador de carga de aplicaciones.

Figura 101 selección tipo balanceador.

EC2 > Balanceadores de carga > Compare y seleccione el tipo de equilibrador de carga

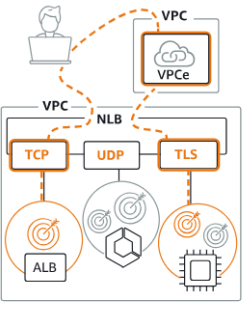
Balancedor de carga de aplicaciones Info



Elija un balanceador de carga de aplicaciones cuando necesite un conjunto de características flexibles para sus aplicaciones con tráfico HTTP y HTTPS. En el nivel de solicitud, los balanceadores de carga de aplicaciones proporcionan características avanzadas de enrutamiento y visibilidad dirigidas a arquitecturas de aplicación, incluidos microservicios y contenedores.

[Crear](#)


Balancedor de carga de red Info



Elija un equilibrador de carga de red cuando necesite un rendimiento ultraalto, descarga de TLS a gran escala, implementación centralizada de certificados, compatibilidad con UDP y direcciones IP estáticas para sus aplicaciones. En el nivel de conexión, los equilibradores de carga de red pueden controlar millones de solicitudes por segundo de forma segura a la vez que mantienen latencias ultrabajas.

[Crear](#)

Equilibrador de carga de gateway Info



Elija un equilibrador de carga de gateway cuando necesite implementar y administrar una flota de dispositivos virtuales de terceros compatibles con GENEVE. Estos dispositivos permiten mejorar los controles de las políticas, la seguridad y la conformidad.

[Crear](#)

Iniciamos con la configuración de nuestro balanceador, asignamos un nombre, elegimos que será expuesto a internet y que el tipo de dirección IP del balanceador será versión 4.

Figura 102 configuración balanceador.

Configuración básica

Nombre del balanceador de carga
Debe ser nombre único dentro de su cuenta de AWS y no puede cambiarse después de crear el equilibrador de carga.

LoadBalancer1

Se permite un máximo de 32 caracteres alfanuméricos, incluidos guiones, pero el nombre no puede comenzar ni terminar por un guión.

Esquema | Info
El esquema no se puede cambiar después de crear el equilibrador de carga.

Expuesto a Internet

- Suministra el tráfico expuesto a Internet.
- Tiene direcciones IP públicas.
- El nombre DNS se resuelve en direcciones IP públicas.
- Requiere una subred pública.

Interno

- Suministra el tráfico interno.
- Tiene direcciones IP privadas.
- El nombre DNS se resuelve en direcciones IP privadas.
- Compatible con los tipos de direcciones IP IPv4 y Dualstack.

Tipo de dirección IP del equilibrador de carga | Info
Seleccione el tipo de dirección IP de frontend que desea asignar al equilibrador de carga. La VPC y las subredes asignadas a este equilibrador de carga deben incluir los tipos de direcciones IP seleccionados. Las direcciones IPv6

IPv4
Incluye solo direcciones IPv4.

Dualstack
Incluye direcciones IPv4 e IPv6.

Dualstack sin IPv4 pública
Incluye una dirección IPv6 pública y direcciones IPv4 e IPv6 privadas. Compatible solo con equilibradores de carga expuestos a Internet.

Para la configuración de red seleccionamos nuestro VPC creado anteriormente y seleccionamos las dos zonas de disponibilidad (data centers) dentro de la región, para distribuir el tráfico entre ambas instancias. Además, elegimos las IP públicas para tener acceso a ellas.

Figura 103 seleccion de VPC y zonas de disponibilidad.

Mapeo de red

El balanceador de carga dirige el tráfico a los destinos de las subredes seleccionadas y en función de la configuración de las direcciones IP.

VPC | Info
El equilibrador de carga existirá y escalará dentro de la VPC seleccionada. La VPC seleccionada también es el lugar donde se alojar los destinos del equilibrador de carga, a menos que se dirijan a destinos de Lambda o locales, o si se utiliza la interconexión de VPC. Para confirmar la VPC para sus objetivos, consulte [los grupos de destino](#). Para una VPC nueva, [Cree una VPC](#).

seminario-vpc
vpc-0e4b18e86f5af189e
CIDR de VPC IPv4: 10.0.0.0/16

Grupos de IP - nuevo | Info
Si lo desea, puede configurar un grupo de IPAM como la fuente preferida para las direcciones IP de sus equilibradores de carga. Cree o visualice los grupos en [la consola del administrador de direcciones IP de Amazon VPC](#).

Use el grupo de IPAM para direcciones IPv4 públicas
El grupo de IPAM que elija será la fuente preferida de direcciones IPv4 públicas. Si el grupo está agotado, AWS asignará las direcciones IPv4.

Zonas de disponibilidad y subredes | Info
Seleccione al menos dos zonas de disponibilidad y una subred para cada zona. Se colocará un nodo de equilibrador de carga en cada zona seleccionada y se escalará de forma automática en respuesta al tráfico. El equilibrador de cargas dirige el tráfico únicamente a los destinos de las zonas de disponibilidad seleccionadas.

us-east-2a (use2-az1)

Subred
Solo se utilizan los bloques CIDR correspondientes al tipo de dirección IP del equilibrador de cargas. Se necesitan al menos 8 direcciones IP disponibles para que el equilibrador de cargas escale de manera eficiente.

subnet-016a81aa21a8bb99d
CIDR de subred IPv4: 10.0.0.0/20

seminario-subnet-public1-us-east-2a

us-east-2b (use2-az2)

Subred
Solo se utilizan los bloques CIDR correspondientes al tipo de dirección IP del equilibrador de cargas. Se necesitan al menos 8 direcciones IP disponibles para que el equilibrador de cargas escale de manera eficiente.

subnet-0b0d0183dcf7f0d37
CIDR de subred IPv4: 10.0.16.0/20

seminario-subnet-public2-us-east-2b

Por seguridad se recomienda crearle su propio grupo de seguridad al balanceador, que permita el tráfico HTTP (puerto 80) desde cualquier IP.

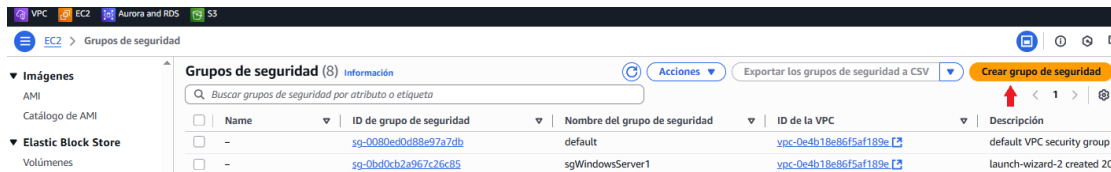
Para esto nos dirigimos en grupos de seguridad.

Figura 104 grupos de seguridad.



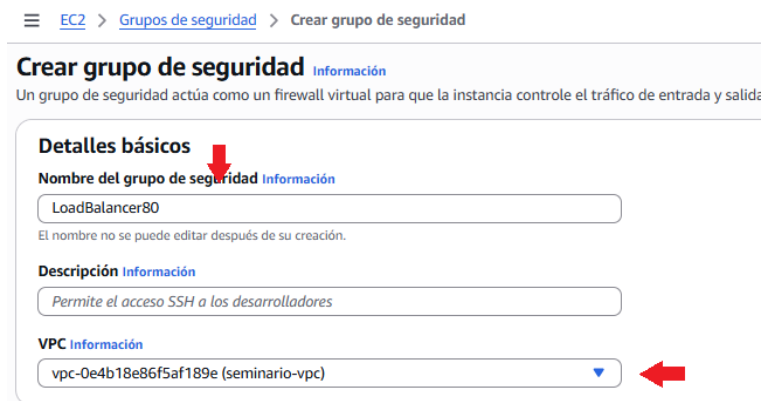
Damos en crear grupo de seguridad.

Figura 105 creación grupo de seguridad.



Le asignamos un nombre a nuestro grupo de seguridad y elegimos nuestra VPC ya creada.

Figura 106 configuración grupo de seguridad.



Agregamos la regla de entrada para que nos permita el acceso por el puerto 80 desde cualquier lugar.

Figura 107

Dejamos por defecto la regla de salida y damos en crear grupo de seguridad.

Una vez creado el grupo de seguridad, continuamos con la elaboración de nuestro balanceador eligiendo el grupo de seguridad que acabamos de realizar.

Figura 108 creación balanceador.

En esta etapa se habilita el acceso por el puerto 80 de forma predeterminada. Además, como aún no existe, se procede a crear un grupo de destino que permitirá al balanceador enrutar el tráfico correctamente hacia las instancias EC2 disponibles.

Figura 109 puerto 80 habilitado.

Agentes de escucha y direccionamiento Info

Un agente de escucha es un proceso que comprueba las solicitudes de conexión mediante el puerto y el protocolo que configure. Las reglas que defina para un agente de escucha det solicitudes a sus destinos registrados.

▼ Agente de escucha **HTTP:80**

Protocolo: HTTP (dropdown) | Puerto: 80 (input) | Acción predeterminada: Info Seleccionar un grupo de destino (dropdown)

Etiquetas del agente de escucha - *opcional*

Considere la posibilidad de agregar etiquetas al agente de escucha. Las etiquetas permiten clasificar los recursos de AWS para que pueda administrarlos con mayor facilidad.

Seleccionamos crear un grupo de destino.

Elegimos nuestro grupo de destino, que en nuestro caso serán nuestras dos instancias creadas y asignamos un nombre.

Figura 110 creación grupo destino.

Configuración básica

La configuración de esta sección no se puede cambiar después de crear el grupo de destino.

Elegir un tipo de destino

- Instancias**
 - Admite el balanceo de carga en instancias dentro de una VPC específica.
 - Facilita el uso de [Amazon EC2 Auto Scaling](#) para administrar y escalar la capacidad de EC2.
- Direcciones IP**
 - Admite el balanceo de carga en recursos de VPC y en las instalaciones.
 - Facilita el direccionamiento a varias direcciones IP e interfaces de red en la misma instancia.
 - Ofrece flexibilidad con arquitecturas basadas en microservicios, lo que simplifica la comunicación entre aplicaciones.
 - Admite destinos IPv6, lo que permite la comunicación IPv6 integral y NAT de IPv4 a IPv6.
- Función Lambda**
 - Facilita el direccionamiento a una única función Lambda.
 - Accesible sólo para balanceadores de carga de aplicaciones.
- Balanceador de carga de aplicaciones**
 - Ofrece la flexibilidad para que un balanceador de carga de red acepte y dirija solicitudes TCP dentro de una VPC específica.
 - Facilita el uso de direcciones IP estáticas y PrivateLink con un balanceador de carga de aplicaciones.

Nombre del grupo de destino

targetGroupSeminario

Se permite un máximo de 32 caracteres alfanuméricos, incluidos guiones, pero el nombre no puede comenzar ni terminar por un guion.

Dejamos por defecto para que las peticiones se envíen por el puerto 80, nuestro tipo de dirección IP es IPv4, nuestro VPC es seminariovpc.

Figura 111 configuración VPC, puerto y tipo dirección.

Protocolo
Protocolo para la comunicación entre el equilibrador de carga y el objetivo. No se puede modificar después de la creación.
HTTP

Puerto
Número de puerto donde los objetivos reciben tráfico. Se puede anular para objetivos individuales durante el registro.
80
1-65535

Tipo de dirección IP
Solo los destinos con el tipo de dirección IP indicado pueden registrarse en este grupo de destino.
 IPv4
Cada instancia tiene una interfaz de red predeterminada (eth0) a la que se le asigna la dirección IPv4 privada principal. La dirección IPv4 privada principal de la instancia es la que se aplicará al destino.
 IPv6
Cada instancia que registre debe tener asignada una dirección IPv6 principal. Ésta se configura en la interfaz de red predeterminada de la instancia (eth0). [Obtenga más información](#)

VPC
Seleccione la VPC con las instancias que desea incluir en el grupo de destino. En esta lista solo están disponibles las VPC que admiten el tipo de dirección IP seleccionado anteriormente.
seminario-vpc
vpc-0e4b18e86f5af189e
CIDR de VPC IPv4: 10.0.0.0/16

Versión del protocolo
 HTTP1
Envíe solicitudes a los destinos con HTTP/1.1. Compatible cuando el protocolo de solicitud es HTTP/1.1 o HTTP/2.
 HTTP2
Envíe solicitudes a los destinos con HTTP/2. Compatible cuando el protocolo de solicitud es HTTP/2 o gRPC, pero las características específicas gRPC no están disponibles.
 gRPC
Envíe solicitudes a los destinos con gRPC. Compatible cuando el protocolo de solicitud es gRPC.

Configuramos los parámetros de comprobación de estado para monitorear la disponibilidad de las instancias. Se utiliza el puerto de tráfico (80), la ruta / y el código de éxito 200, lo que permite al balanceador determinar si una instancia está saludable antes de enviarle tráfico.

Figura 112 parametros de comprobacion de estado.

EC2 > Grupos de destino > Crear un grupo de destino

2

2-10

Tiempo de espera
La cantidad de tiempo, en segundos, durante la cual no hay respuesta significa que se produjo un error en la comprobación de estado.

5 segundos

2-120

Intervalo
Periodo de tiempo aproximado que transcurre entre comprobaciones de estado de un destino individual.

30 segundos

5-300

Códigos de éxito
Códigos HTTP que se deben utilizar al comprobar si se ha recibido una respuesta correcta de un destino. Puede especificar varios valores (por ejemplo, "200,302") o un intervalo de valores (por ejemplo, "200-299").

200

Atributos

Algunos atributos predeterminados se aplicarán al grupo de destino. Puede verlos y editarlos después de crear el grupo de destino.

Etiquetas - opcional
Considere la posibilidad de agregar etiquetas a su grupo de destino. Las etiquetas le permiten clasificar sus recursos de AWS para que pueda administrarlos con mayor facilidad.

Cancelar **Siguiente**

Registramos nuestras dos instancias que están dentro de la VPC y seleccionamos incluir como pendiente a continuación.

Figura 113 registro de destinos.

Paso 1
● Especificar los detalles del grupo

Paso 2
● Registrar destinos

Registrar destinos

Se trata de un paso opcional para crear un grupo de destino. Sin embargo, para asegurarse de que el balanceador de carga dirige el tráfico a este grupo de destino, debe registrar los destinos.

Instancias disponibles (2/2)

Buscar: Filtrar instancias

<input checked="" type="checkbox"/>	ID de instancia	Nombre	Estado	Grupos de seguridad	Zona
<input checked="" type="checkbox"/>	i-097f72ad3b1b4b016	Linux2	Ejecutando	launch-wizard-3	us-east-2a
<input checked="" type="checkbox"/>	i-000a603b430bf9a7d	Linux1	Ejecutando	launch-wizard-2	us-east-2a

2 seleccionados

Puertos para las instancias seleccionadas
Puertos para dirigir el tráfico a las instancias seleccionadas.

80

1-65535 (separe puertos múltiples con comas)

Incluir como pendiente a continuación

Seleccionamos crear grupo de destino.

Figura 114 creación grupo de destino.

Revisar destinos

Destinos (2) [Eliminar todos los pendientes](#)

Mostrar solo pendientes

ID de instancia	Nombre	Puerto	Estado	Grupos de seguridad	Zona	Dirección IPv4 privada	ID de subred
i-097f72ad3b1b4b016	Linux2	80	✔ Ejecutando	launch-wizard-3	us-east-2a	10.0.13.114	subnet-016a81aa21a8bb95
i-000a603b430bf9a7d	Linux1	80	✔ Ejecutando	launch-wizard-2	us-east-2a	10.0.6.78	subnet-016a81aa21a8bb95

2 pendientes

[Cancelar](#) [Anterior](#) [Crear un grupo de destino](#)

De esa manera se crea nuestro grupo de destino y podemos continuar con la creación del balanceador de carga y seleccionar el grupo de destino creado.

▼ Agente de escucha HTTP:80

Protocolo **Puerto**
1-65535

Acción predeterminada [Info](#)

Reenviar a [Crear un grupo de destino](#)

Damos crear balanceador de carga y esperamos a que se ejecute la creación.

Figura 115 creación balanceador.

Estado y flujo de trabajo de creación

► **Estado y tareas del lado del servidor**
Tras completar y enviar los pasos anteriores, todas las tareas del servidor y sus estados estarán disponibles para su supervisión.

[Cancelar](#) [Crear balanceador de carga](#)

Se creó correctamente nuestro balanceador y grupo de destino.

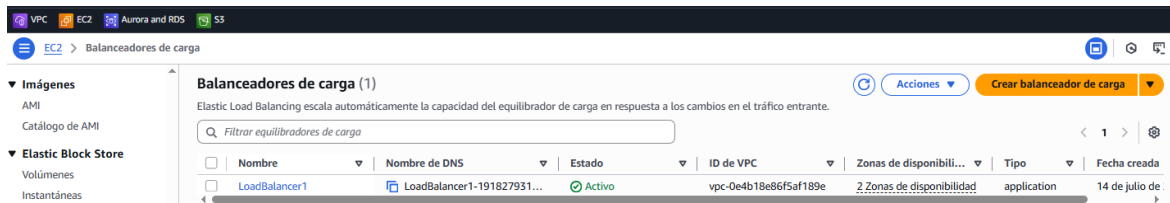
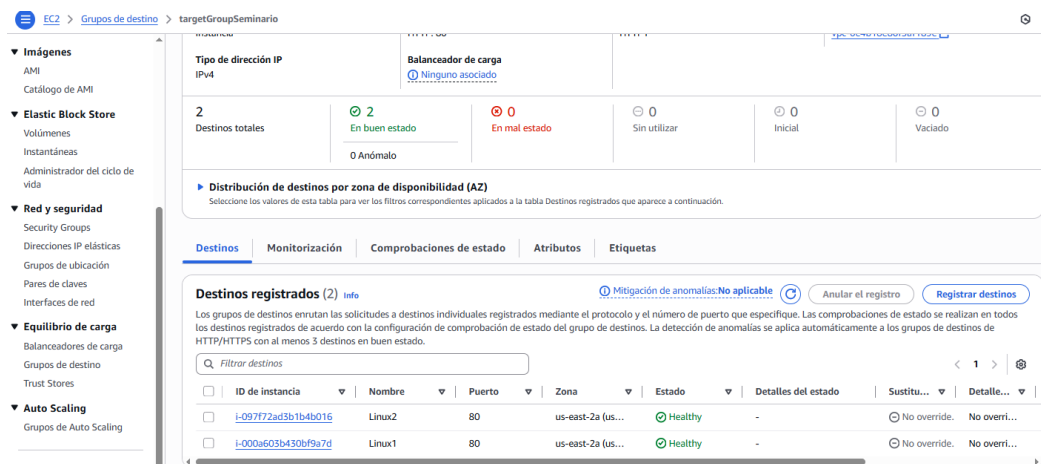


Figura 116 visualización de balanceador.



Para verificar que nuestro balanceador funciona correctamente, desde nuestro navegador web accedemos con el nombre DNS que crea nuestro balanceador y evidenciamos que desde ese mismo DNS se puede acceder a los dos servidores cargando la página con `ctrl+r`.

Balancedores de carga (1/1) Acciones Crear balanceador de carga

Elastic Load Balancing escala automáticamente la capacidad del equilibrador de carga en respuesta a los cambios en el tráfico entrante.

Q *Filtrar equilibradores de carga* < 1 > ⚙

✓	Nombre	Nombre de DNS	Estado	ID de VPC	Zonas de disponibilit...	Tipo	Fecha creada
✓	LoadBalancer1	LoadBalancer1-191827931...	Activo	vpc-0e4b18e86f5af189e	2 Zonas de disponibilidad	application	14 de julio de 2025, 16:49 (UTC-05:00)

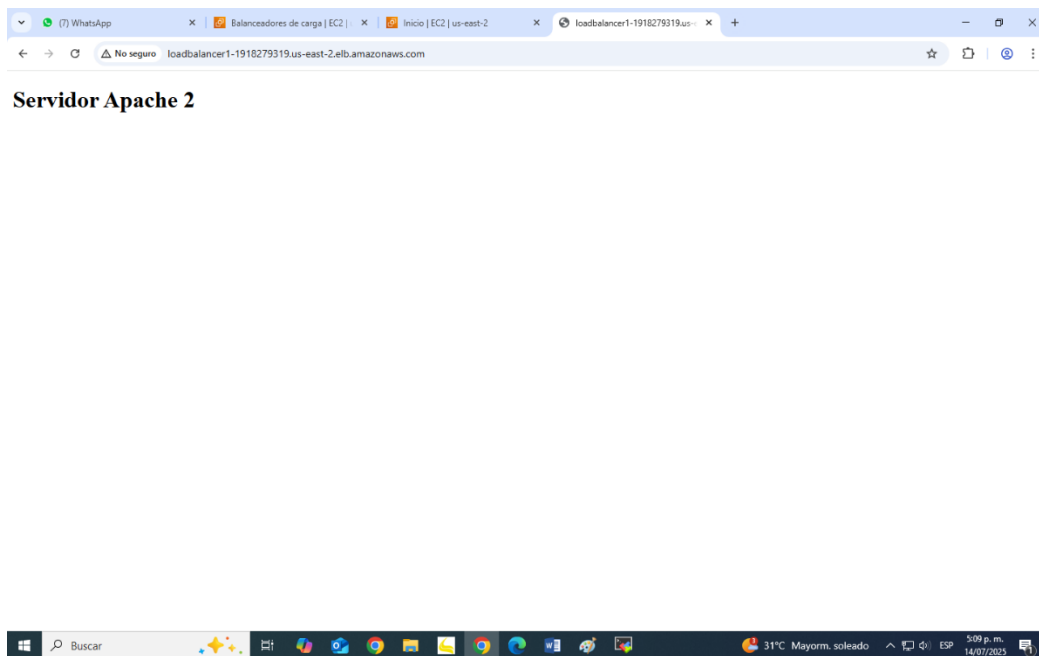
Equilibrador de carga: LoadBalancer1

Tipo de equilibrador de carga Aplicación	Estado Activo	VPC vpc-0e4b18e86f5af189e	Tipo de dirección IP del equilibrador de carga IPv4
Esquema Internet-facing	Zona hospedada Z3AADJG6KTTL2	Zonas de disponibilidad subnet-016a81aa21a8bb99d us-east-2a (use2-az1) subnet-0b0d0183dcf7f0d37 us-east-2b (use2-az2)	Fecha creada 14 de julio de 2025, 16:49 (UTC-05:00)
ARN del equilibrador de carga arn:aws:elasticloadbalancing:us-east-2:670925591568:loadbalancer/app/LoadBalancer1/03a466f50a9d8469		Nombre de DNS info LoadBalancer1-1918279319.us-east-2.elb.amazonaws.com (Registro A)	

Figura 117 prueba de balanceador en navegador web.

Servidor Apache 1

Figura 118 prueba balanceador en navegador web.

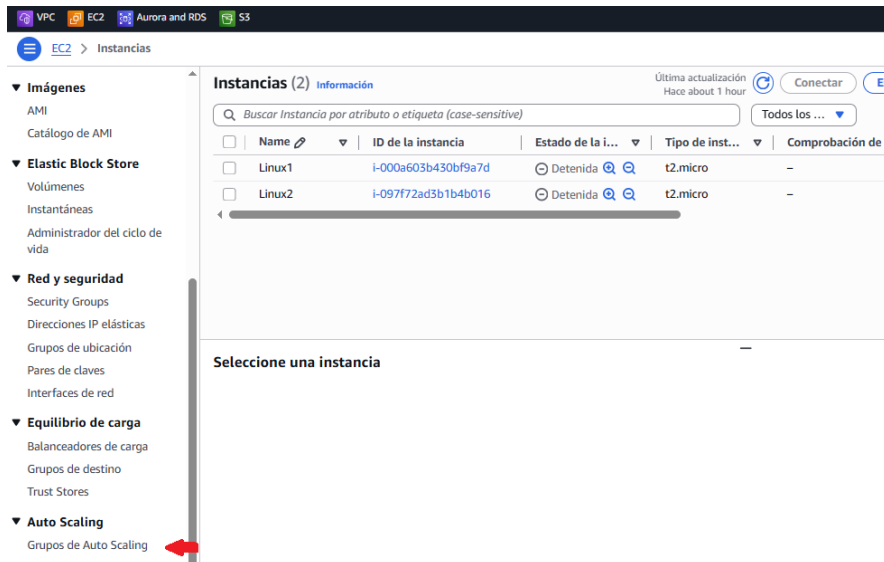


Creación del Auto Scaling

Procedemos con la configuración del Auto Scaling, teniendo en cuenta que este servicio permite ajustar la cantidad de instancias según la demanda, asegurando la disponibilidad.

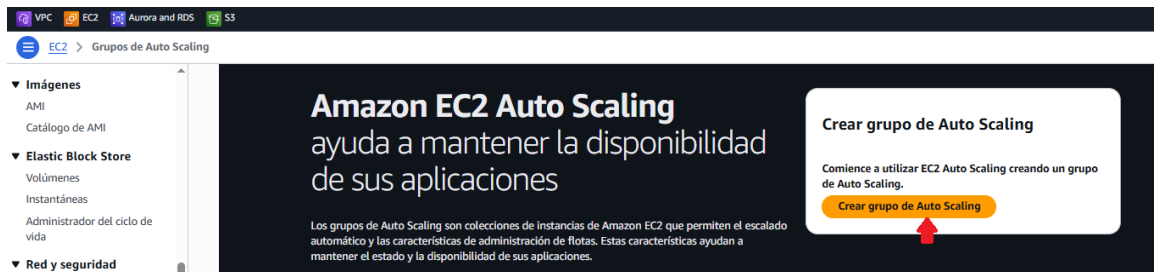
Dentro del servicio EC2 seleccionamos la opción de grupo de Auto Scaling.

Figura 119 servicio auto scaling.



Damos clic en crear grupo de auto scaling e iniciamos la configuración.

Figura 120 creación de servicio auto scaling.



Asignamos un nombre a nuestro auto scaling y como no hemos creado una plantilla de lanzamiento donde va a estar la configuración de las nuevas instancias que se van a crear, damos clic en crear configuración de lanzamiento.

Figura 121 nombrar auto scaling.

Elegir plantilla de lanzamiento Info

Especifique una plantilla de lanzamiento que contenga configuraciones comunes a todas las instancias de EC2 lanzadas por este grupo de escalado automático.

Nombre

Nombre del grupo de Auto Scaling
Escriba un nombre para identificar el grupo.

AutoScalingSeminario

Debe ser único para esta cuenta en la región actual y no puede superar los 255 caracteres.

Plantilla de lanzamiento Info

Para las cuentas creadas después del 31 de mayo de 2023, la consola de EC2 solo admite la creación de grupos de escalado automático con plantillas de lanzamiento se recomienda crear grupos de escalado automático con configuraciones de lanzamiento, pero aún se podrá hacer a través de la CLI y la API hasta el 31 de diciembre.

Plantilla de lanzamiento
Elija una configuración de lanzamiento que contenga la configuración de nivel de instancia, como la imagen de máquina de Amazon (AMI), el tipo de instancia, el par de claves y los grupos de seguridad.

Seleccionar una plantilla de lanzamiento

Crear una configuración de lanzamiento Info

Ingresamos nombre y descripción a nuestra plantilla.

Figura 122 creación Plantilla de lanzamiento.

Crear plantilla de lanzamiento

La creación de una plantilla de lanzamiento le permite crear una configuración de instancia guardada que se puede reutilizar, compartir y lanzar más adelante. Las plantillas pueden tener varias versiones.

Nombre y descripción de la plantilla de lanzamiento

Nombre de la plantilla de lanzamiento - *obligatorio*

PlantillaServerLinux

Debe ser única para esta cuenta. Máximo de 128 caracteres. Sin espacios ni caracteres especiales, como "&", "*", "@", "#".

Descripción de la versión de la plantilla

PlantillaServerLinux

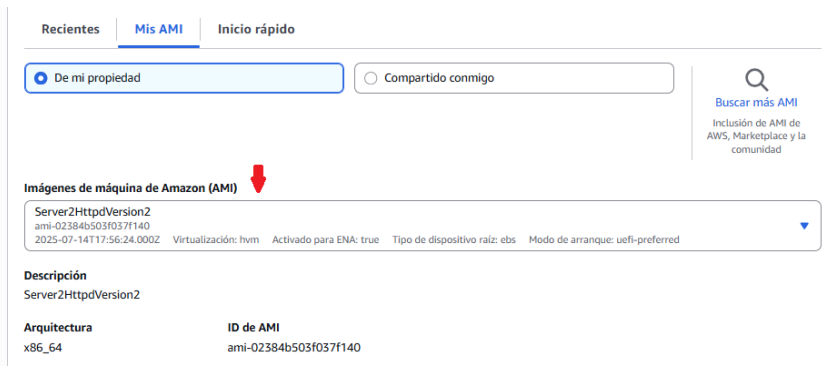
Máximo de 255 caracteres

Orientación sobre Auto Scaling Información
Selecciónelo si va a utilizar esta plantilla con EC2 Auto Scaling

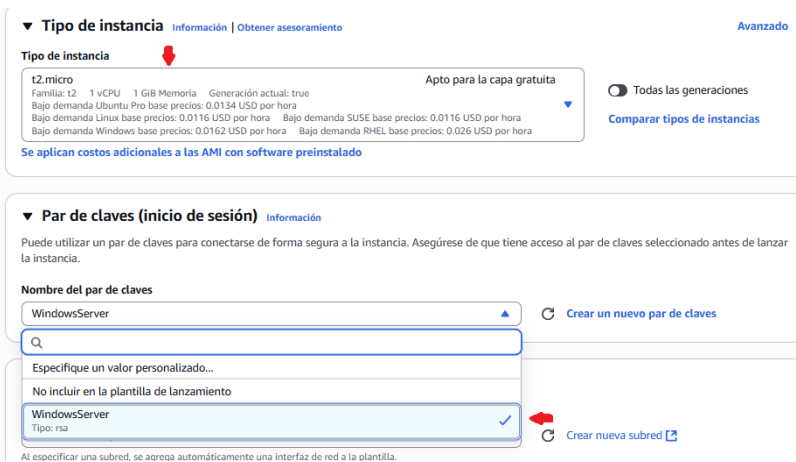
Proporcionar orientación que me ayude a configurar una plantilla que pueda utilizar con EC2 Auto Scaling

Seleccionamos nuestra AMI creada anteriormente.

Figura 123 selección de AMI.



En tipo de instancia seleccionamos la capa gratuita t2.micro y elegimos nuestro par de claves creado anteriormente.



En la configuración de la red elegimos no incluir en la plantilla de lanzamiento, porque ya está incluido en el balanceador, creamos el grupo de seguridad, asignamos un nombre y seleccionamos nuestra VPC.

Figura 124 configuración de la red.

▼ Configuraciones de red [Información](#)

Subred | [Información](#)

No incluir en la plantilla de lanzamiento [Crear nueva subred](#)

Al especificar una subred, se agrega automáticamente una interfaz de red a la plantilla.

Zona de disponibilidad [Información](#)

No incluir en la plantilla de lanzamiento [Enable additional zones](#)

No aplicable a EC2 Auto Scaling

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.

Seleccionar un grupo de seguridad existente **Crear grupo de seguridad**

Nombre del grupo de seguridad - obligatorio

Servers80LoadBalancer

Este grupo de seguridad se agregará a todas las interfaces de red. El nombre no se puede editar después de crear el grupo de seguridad. La longitud máxima es de 255 caracteres. Caracteres válidos: a-z, A-Z, 0-9, espacios y _-./[!@#%&*~!]*

Descripción - obligatorio | [Información](#)

Permite el acceso SSH a los desarrolladores

VPC | [Información](#)

vpc-Oe4b18e86f5af189e (seminario-vpc) 10.0.0.0/16

En la regla del grupo de seguridad agregamos el puerto 80 para que permita el acceso desde cualquier lugar.

Figura 125 puerto 80 agregado.

Reglas de grupos de seguridad de entrada

▼ Regla del grupo de seguridad 1 (TCP; 80, 0.0.0.0/0) [Eliminar](#)

Tipo | [Información](#)

TCP personalizado

Protocolo | [Información](#)

TCP

Intervalo de puertos | [Información](#)

80

Tipo de origen | [Información](#)

Personalizada

Origen | [Información](#)

0.0.0.0/0

Descripción - opcional | [Información](#)

por ejemplo, SSH para Admin Desktop

En la sección de configuración de red, damos clic en eliminar porque no vamos a usar segunda tarjeta de red.

▼ Configuración de red avanzada

Interfaz de red 1 Eliminar

Índice de dispositivos Información
0

Interfaz de red Información
Nueva interfaz
No se recomienda utilizar las interfaces de red existentes al crear una plantilla para el escalamiento automático.

Descripción Información

Subred Información
No incluir en la plantilla de lanzamiento
No aplicable a EC2 Auto Scaling

Grupos de seguridad Información
Nuevo grupo de seguridad

Asignar automáticamente la IP pública Información
No incluir en la plantilla de lanzamiento

IP principal Información
No aplicable a EC2 Auto Scaling

IP secundaria Información
No incluir en la plantilla de lanzamiento
No aplicable a EC2 Auto Scaling

Direcciones IP IPv6 Información
No incluir en la plantilla de lanzamiento
No aplicable a EC2 Auto Scaling

Dejamos la información del almacenamiento que nos sugiere, la cual es la misma que tiene la AMI y damos clic en crear plantilla de lanzamiento.

Figura 126 almacenamiento por defecto y creación.

▼ Almacenamiento (volúmenes) Información

Volúmenes de EBS Ocultar detalles

► Volumen 1 (Raíz de AMI) : 8 GiB, EBS, SSD de uso general (gp3), 3000 IOPS
Los volúmenes de la AMI no se incluirán en la plantilla a menos que se modifiquen

Los clientes que cumplan los requisitos de la capa gratuita pueden obtener hasta 30 GiB de almacenamiento magnético o de uso general (SSD) de EBS

Agregar un nuevo volumen

▼ Etiquetas de recursos Información

Actualmente, no hay ninguna etiqueta de recursos incluida en esta plantilla. Agregue una etiqueta de recursos para incluirla en la plantilla de lanzamiento.

Agregar nueva etiqueta
Puede agregar hasta 50 etiquetas más.

Imagen de software (AMI)
Server2HttpdVersion2
ami-02384b503f057f140

Tipo de servidor virtual (tipo de instancia)
t2.micro

Firewall (grupo de seguridad)
Nuevo grupo de seguridad

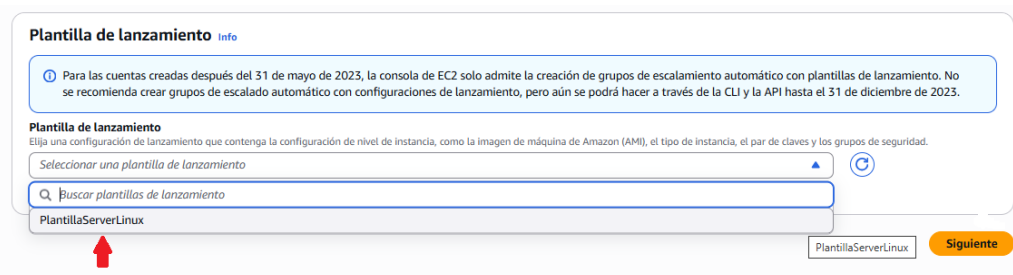
Almacenamiento (volúmenes)
Volúmenes: 1 (8 GiB)

Nivel gratuito: Durante el primer año que abre una cuenta de AWS, obtiene 750 horas al mes de uso de instancias t2.micro (o t3.micro cuando t2.micro no está disponible) si se utiliza con AMI de nivel gratuito, 750 horas al mes de uso de direcciones IPv4 públicas, 30 GiB de almacenamiento de EBS, 2 millones de E/S, 1 GB de instantáneas y 100 GB de ancho de banda para Internet.

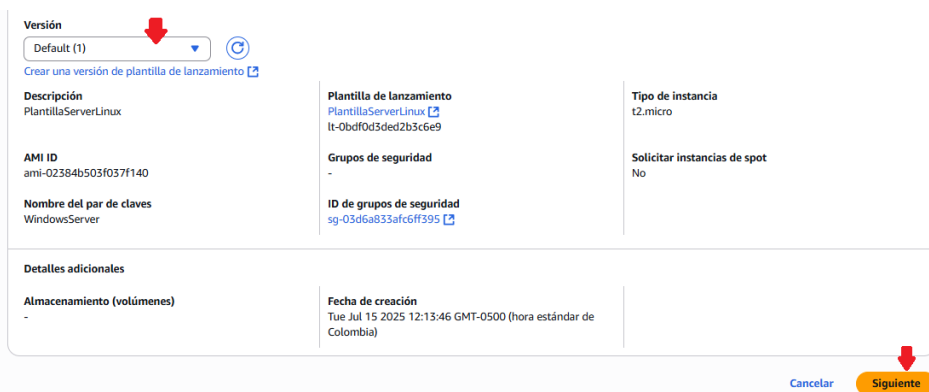
Cancelar Crear plantilla de lanzamiento

Una vez creada nos aparece efectivamente la plantilla para continuar con la creación del auto scaling.

Figura 127 plantilla disponible.



Dejamos la versión que nos muestra por defecto y damos siguiente.



En la configuración de red seleccionamos nuestra VPC y las subredes privadas que se recomienda como buena práctica para que las instancias no tengan acceso desde internet. Además, seleccionamos en mejor esfuerzo equilibrado para que las instancias que se van a crear se distribuyan entre las dos data centers.

Figura 128 configuración de red.

VPC
Elija la VPC que define la red virtual para el grupo de Auto Scaling.

vpc-0e4b18e86f5af189e (seminario-vpc)
10.0.0.0/16

[Crear una VPC](#)

Zonas de disponibilidad y subredes
Defina qué zonas de disponibilidad y subredes puede utilizar el grupo de Auto Scaling en la VPC elegida.

Seleccionar zonas de disponibilidad y subredes

use2-az2 (us-east-2b) | subnet-066a51619e5ed3266 (seminario-subnet-private2-us-east-2b)
10.0.144.0/20

use2-az1 (us-east-2a) | subnet-0685683ec81433125 (seminario-subnet-private1-us-east-2a)
10.0.128.0/20

[Crear una subred](#)

Distribución de zonas de disponibilidad - nueva
El escalamiento automático equilibra automáticamente las instancias en todas las zonas de disponibilidad. Si se producen errores de lanzamiento en una zona, seleccione una estrategia.

Mejor esfuerzo equilibrado
Si los lanzamientos fallan en una zona de disponibilidad, el escalamiento automático intentará lanzarse en otra zona de disponibilidad en buen estado.

Solo equilibrado
Si los lanzamientos fallan en una zona de disponibilidad, el escalamiento automático seguirá intentando lanzarse en la zona de disponibilidad en mal estado para mantener una distribución equilibrada.

Cancelar [Omitir para revisar](#) [Anterior](#) **Siguiente**

Continuamos con la configuración asociando nuestro auto scaling al balanceador previamente creado.

Seleccionamos asociar balanceador existente y elegimos nuestro grupo de destino de nuestro balanceador.

Figura 129 asociar balanceador y grupo de destino.

Balance de carga info

Utilice las siguientes opciones para asociar su grupo de Auto Scaling a un balanceador de carga existente o a uno nuevo que defina.

No se encontró ningún balanceador de carga
El tráfico a su grupo de Auto Scaling no se llevará a cabo por un balanceador de carga.

Asociar a un balanceador de carga existente
Elija entre los balanceadores de carga existentes.

Asociar a un nuevo balanceador de carga
Cree rápidamente un balanceador de carga básico para asociarlo al grupo de Auto Scaling.

↑

Asociar a un balanceador de carga existente

Seleccione los balanceadores de carga que desea asociar al grupo de Auto Scaling.

Elegir entre los grupos de destino del balanceador de carga
Esta opción le permite asociar balanceadores de carga de puerta de enlace, red o aplicaciones.

Elegir entre balanceadores de carga clásicos

Grupos de destino del balanceador de carga existentes

Solo están disponibles para su selección los grupos de destino de instancias que pertenecen a la misma VPC que el grupo de Auto Scaling.

Seleccionar grupos de destino
▼
C

targetGroupSeminario | HTTP
X

Application Load Balancer: LoadBalancer1

←

Activamos las comprobaciones de estado de las instancias para que realice monitoreo de las mismas y continuamos.

Figura 130 activación de comprobación de estado.

Comprobaciones de estado

Las comprobaciones de estado aumentan la disponibilidad reemplazando instancias en mal estado. Cuando se utilizan varias comprobaciones de estado, se evalúan todas y, si se produce un error en al menos una, se lleva a cabo la sustitución de instancias.

Comprobaciones de estado de EC2

[Siempre habilitadas](#)

Tipos de comprobaciones de estado adicionales - opcional info

Activar las comprobaciones de estado de Elastic Load Balancing Recomendado

Elastic Load Balancing puede monitorear si las instancias están disponibles para gestionar solicitudes. Cuando informa de una instancia en mal estado, EC2 Auto Scaling puede sustituirla en la siguiente comprobación periódica.

i EC2 Auto Scaling comenzará a detectar y actuar en función de las comprobaciones de estado realizadas por Elastic Load Balancing. Para evitar terminaciones inesperadas, primero verifique la configuración de estas comprobaciones de estado en la [consola del equilibrador de carga](#).

X

Activar las comprobaciones de estado de VPC Lattice
VPC Lattice puede supervisar si las instancias están disponibles para administrar solicitudes. Si considera que un destino no ha superado una comprobación de estado, EC2 Auto Scaling lo sustituye después de la siguiente comprobación periódica.

Activar las comprobaciones de estado de Amazon EBS
EBS monitorea si el volumen vinculado o el volumen raíz de una instancia se detiene. Cuando informa de un volumen en mal estado, EC2 Auto Scaling puede sustituir la instancia en la siguiente comprobación de estado periódica.

Período de gracia de la comprobación de estado info

Este período de tiempo retrasa la primera comprobación de estado hasta que las instancias terminen de inicializarse. No impide que una instancia termine cuando se establece en un estado que no sea de ejecución.

300

 segundos

Cancelar
Omitir para revisar
Anterior
Siguiente

Ingresamos la capacidad de instancias deseadas, en este caso 2 y agregamos la capacidad mínima y máxima deseada.

Figura 131 capacidad instancias creadas.

Tamaño del grupo [Info](#)
 Defina el tamaño inicial del grupo de escalamiento automático. Después de crear el grupo, puede cambiar su tamaño de escalamiento automático.

Tipo de capacidad deseado
 Elija la unidad de medida para el valor de capacidad deseado. Las vCPU y la memoria (GiB) solo son compatibles con grupos de instancias.

Unidades (número de instancias) ▼

Capacidad deseada
 Especifique el tamaño de su grupo.

2

Escalado [Info](#)
 Puede cambiar el tamaño de su grupo de escalamiento automático de forma manual o automática para cumplir con los requisitos de capacidad.

Límites de escalamiento
 Establezca límites sobre cuánto puede aumentarse o disminuirse la capacidad deseada.

Capacidad deseada mínima **Capacidad deseada máxima**

1 5 ▼

Capacidad igual o inferior a la deseada Capacidad igual o superior a la deseada

Creamos nuestra política de escalado y continuamos.

Figura 132 creación política de escalado.

Escalamiento automático - opcional
Elija si desea utilizar una política de seguimiento de destino [Info](#)
 Puede configurar otras políticas de escalado basadas en métricas y un escalado programado después de crear su grupo de escalamiento automático.

Sin políticas de escalamiento
 Su grupo de escalamiento automático mantendrá su tamaño inicial y no se redimensionará de forma dinámica para satisfacer la demanda.

Política de escalado de seguimiento de destino
 Elija una métrica y un valor objetivo de CloudWatch y deje que la política de escalamiento ajuste la capacidad deseada en proporción al valor de la métrica.

Nombre de la política de escalado

política 80 cpu

Tipo de métrica [Info](#)
 Métrica supervisada que determina si la utilización de recursos es demasiado baja o alta. Si utiliza métricas de EC2, considere la posibilidad de habilitar la supervisión detallada para obtener un mejor rendimiento de escalado.

Utilización promedio de la CPU ▼

Valor de destino

80

Preparación de la instancia [Info](#)

300 segundos

Deshabilite el escalado descendente para crear solo una política de escalado ascendente

No configuramos notificaciones ni etiquetas por el momento, para continuar con la creación del auto scaling.

Paso 1
● Elegir plantilla de lanzamiento

Paso 2
● Elegir las opciones de lanzamiento de instancias

Paso 3 - opcional
● Integrar en otros servicios

Paso 4 - opcional
● Configurar escalamiento y tamaño de grupo

Paso 5 - opcional
● **Añadir notificación**

Añadir notificación - opcional info
Envíe notificaciones a temas de SNS siempre que Amazon EC2 Auto Scaling lance o termine las instancias EC2 de su grupo de Auto Scaling.

[Añadir notificación](#)

[Cancelar](#) [Omitir para revisar](#) [Anterior](#) [Siguiente](#)

Paso 1
● Elegir plantilla de lanzamiento

Paso 2
● Elegir las opciones de lanzamiento de instancias

Paso 3 - opcional
● Integrar en otros servicios

Paso 4 - opcional
● Configurar escalamiento y tamaño de grupo

Paso 5 - opcional
● Añadir notificación

Paso 6 - opcional
● **Añadir etiquetas**

Paso 7
○ Revisar

Añadir etiquetas - opcional info
Añada etiquetas que le ayuden a buscar, filtrar y realizar un seguimiento de su grupo de Auto Scaling en AWS. También puede optar por añadir automáticamente estas etiquetas a las instancias cuando se lancen.

Si lo desea, puede optar por agregar etiquetas a las instancias (y a sus volúmenes de EBS adjuntos) si especifica etiquetas en la plantilla de lanzamiento. Sin embargo, recomendamos que tenga precaución, ya que los valores de etiqueta de las instancias de la plantilla de lanzamiento se invalidarán si hay claves duplicadas especificadas para el grupo de Auto Scaling.

Etiquetas (0)

[Agregar etiqueta](#)
50 restante

[Cancelar](#) [Anterior](#) [Siguiente](#)

Posteriormente nos muestra un resumen de la configuración y damos clic en crear grupo de auto scaling.

Figura 133 resumen de la configuración.

Configuración adicional

Protección de escalado descendente de instancias Deshabilitado	Monitoreo Deshabilitado	Calentamiento predeterminado de la instancia Deshabilitado
---	----------------------------	---

Preferencia de reserva de capacidad

Preferencia Predeterminado	ID de reserva de capacidad -	Grupos de recursos -
-------------------------------	---------------------------------	-------------------------

Paso 5: Añadir notificaciones [Editar](#)

Notificaciones
Sin notificaciones

Paso 6: Añadir etiquetas [Editar](#)

Etiquetas (0)

Clave	Valor	Etiquetar instancias nuevas
No hay etiquetas		

[Vista previa del código](#) [Cancelar](#) [Anterior](#) [Crear grupo de Auto Scaling](#)

Efectivamente nuestro grupo de auto scaling se creó de forma correcta, creando en nuestro balanceador 2 nuevas instancias de destino.

Figura 134 prueba de auto scaling funcionando.

4 Destinos totales

4 En buen estado

0 En mal estado

0 Sin utilizar

0 Inicial

0 Vaciado

0 Anómalo

Distribución de destinos por zona de disponibilidad (AZ)
 Seleccione los valores de esta tabla para ver los filtros correspondientes aplicados a la tabla Destinos registrados que aparece a continuación.

Destinos | Monitorización | Comprobaciones de estado | Atributos | Etiquetas

Destinos registrados (4) [info](#) [Mitigación de anomalías: No aplicable](#) [Anular el registro](#) [Registrar destinos](#)

Los grupos de destinos enrutan las solicitudes a destinos individuales registrados mediante el protocolo y el número de puerto que especifique. Las comprobaciones de estado se realizan en todos los destinos registrados de acuerdo con la configuración de comprobación de estado del grupo de destinos. La detección de anomalías se aplica automáticamente a los grupos de destinos de HTTP/HTTPS con al menos 3 destinos en buen estado.

<input type="checkbox"/>	ID de instancia	Nombre	Puerto	Zona	Estado	Detalles del estado	Sustitu...	Detalle...
<input checked="" type="checkbox"/>	i-Oa66941a652117821		80	us-east-2b (us...)	Healthy	-	No override	No overri...
<input checked="" type="checkbox"/>	i-O9d148f1e3c894e3a		80	us-east-2a (us...)	Healthy	-	No override	No overri...
<input type="checkbox"/>	i-000a603b430bf9a7d	Linux1	80	us-east-2a (us...)	Healthy	-	No override	No overri...
<input type="checkbox"/>	i-O97f72ad3b1b4b016	Linux2	80	us-east-2a (us...)	Healthy	-	No override	No overri...

Para comprobar que esté funcionando nos dirigimos a nuestro balanceador de carga, copiamos nuestro DNS para hacer la prueba en nuestro navegador.

Figura 135 prueba en navegar web.

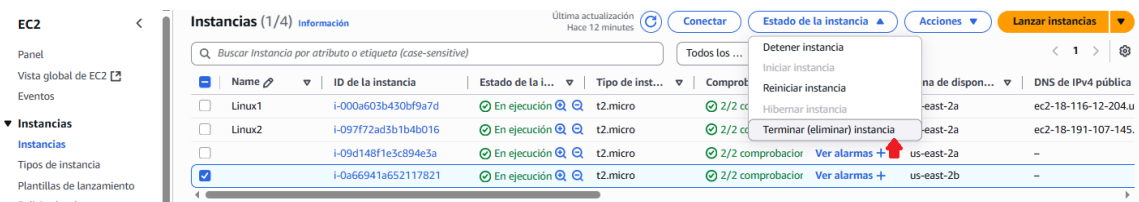
¡Funciona Apache en Amazon Linux!

Efectivamente al recargar la imagen los dos servidores me muestran la misma imagen y no se nota el cambio, ya que se sacó la imagen de mi servidor 1.

Probamos que nuestro auto scaling funcione correctamente, eliminando una instancia, este servicio al notar ese proceso, lo que hace es generar automáticamente una nueva instancia con las mismas características.

Damos terminar a una de nuestras instancias.

Figura 136 prueba auto scaling .



Revisamos en nuestro grupo de destino evidenciando que queda una instancia y esperamos que el auto scaling cree una nueva.

Figura 137 prueba auto scaling.



Efectivamente creó una nueva.

Figura 138 prueba creación auto scaling.

2 Destinos totales

- 2 En buen estado
- 0 Anómalo
- 0 En mal estado
- 0 Sin utilizar
- 0 Inicial
- 0 Vaciado

Distribución de destinos por zona de disponibilidad (AZ)
 Seleccione los valores de esta tabla para ver los filtros correspondientes aplicados a la tabla Destinos registrados que aparece a continuación.

Destinos | Monitorización | Comprobaciones de estado | Atributos | Etiquetas

Destinos registrados (2) Info Mitigación de anomalías: No aplicable Anular el registro Registrar destinos

Los grupos de destinos enrutan las solicitudes a destinos individuales registrados mediante el protocolo y el número de puerto que especifique. Las comprobaciones de estado se realizan en todos los destinos registrados de acuerdo con la configuración de comprobación de estado del grupo de destinos. La detección de anomalías se aplica automáticamente a los grupos de destinos de HTTP/HTTPS con al menos 3 destinos en buen estado.

Buscar:

ID de instancia	Nombre	Puerto	Zona	Estado	Detalles del estado	Sustitu...	Detalle...
i-02d322eba5cb045d9		80	us-east-2b (us...)	Healthy	-	No override	No overri...
i-09d148f1e3c894e3a		80	us-east-2a (us...)	Healthy	-	No override	No overri...

Historial de actividad (4) Info

Buscar:

Estado	Descripción	Causa	Hora de inicio	Hora de finalización
Correcto	Launching a new EC2 instance: i-02d322eba5cb045d9	At 2025-07-15T18:22:06Z an instance was launched in response to an unhealthy instance needing to be replaced.	2025 July 15, 01:22:08 PM -05:00	2025 July 15, 01:22:1 PM -05:00
Drenaje de conexiones en curso	Terminating EC2 instance: i-0a66941a652117821 - Waiting For ELB Connection Draining.	At 2025-07-15T18:22:06Z an instance was taken out of service in response to an EC2 health check indicating it has been terminated or stopped.	2025 July 15, 01:22:06 PM -05:00	
Correcto	Launching a new EC2 instance: i-09d148f1e3c894e3a	At 2025-07-15T17:55:46Z a user request created an AutoScalingGroup changing the desired capacity from 0 to 2. At 2025-07-15T17:58:41Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 0 to 2.	2025 July 15, 12:58:43 PM -05:00	2025 July 15, 12:59:1 PM -05:00
Correcto	Launching a new EC2 instance: i-0a66941a652117821	At 2025-07-15T17:55:46Z a user request created an AutoScalingGroup changing the desired capacity from 0 to 2. At 2025-07-15T17:58:41Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 0 to 2.	2025 July 15, 12:58:43 PM -05:00	2025 July 15, 12:59:1 PM -05:00

EC2

Panel
 Vista global de EC2
 Eventos

Instancias

Tipos de instancia
 Plantillas de lanzamiento
 Solicitudes de spot
 Savings Plans
 Instancias reservadas

Instancias (5) Información Última actualización: Hace less than a minute Conectar Estado de la instancia Acciones Lanzar instancias

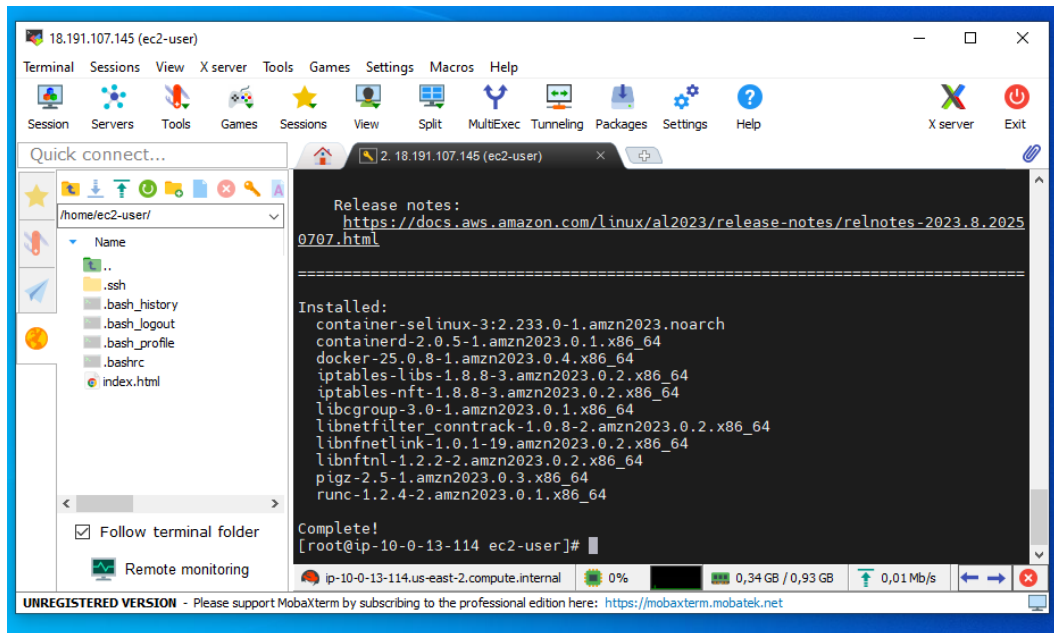
Buscar instancia por atributo o etiqueta (case-sensitive)

Todos los ...

Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación de	Estado de la al...	Zona de dispon...	DNS de IPv4 pública
Linux1	i-000a603b430bf9a7d	En ejecución	t2.micro	2/2 comprobador	Ver alarmas +	us-east-2a	ec2-18-116-12-204.u
Linux2	i-097f72ad3b1b4b016	En ejecución	t2.micro	2/2 comprobador	Ver alarmas +	us-east-2a	ec2-18-191-107-145.
	i-09d148f1e3c894e3a	En ejecución	t2.micro	2/2 comprobador	Ver alarmas +	us-east-2a	-
	i-0a66941a652117821	Terminada	t2.micro	-	Ver alarmas +	us-east-2b	-
	i-02d322eba5cb045d9	En ejecución	t2.micro	2/2 comprobador	Ver alarmas +	us-east-2b	-

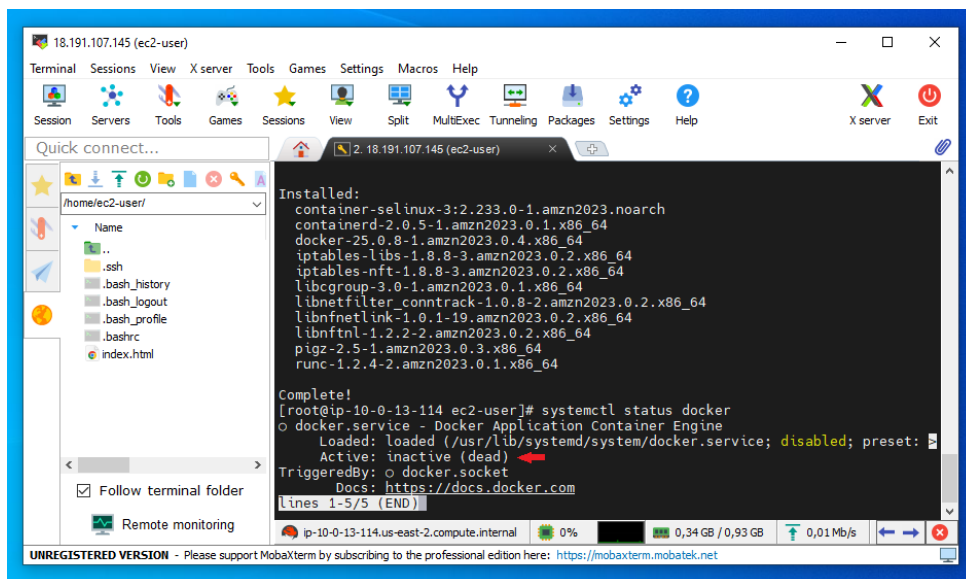
Ingresamos el comando (sudo su) para obtener el rol de administrador y procedemos a usar el comando (yum install Docker) para la instalación del Docker.

Figura 141 rol administrador.



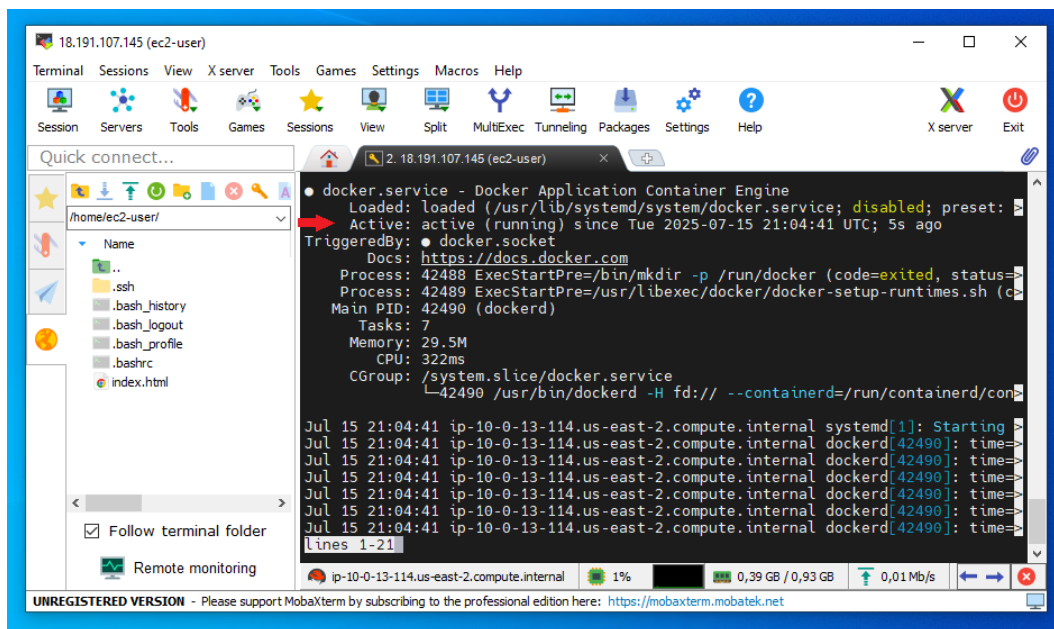
Visualizamos en qué estado está el servicio con el comando (systemctl status Docker).

Figura 142 estado del servidor.



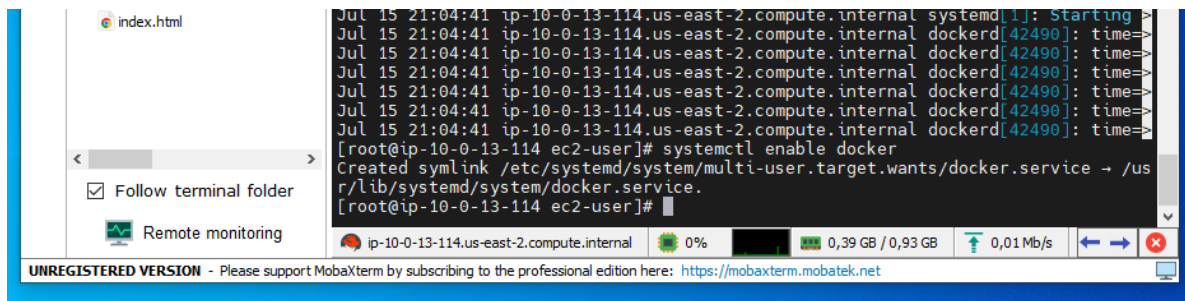
Para activar el servicio escribimos (systemctl start Docker) y volvemos a verificar el estado con el comando anterior.

Figura 143 servidor activado.



Procedemos a ingresar el comando (systemctl enable docker) para que este servicio arranque de forma automática.

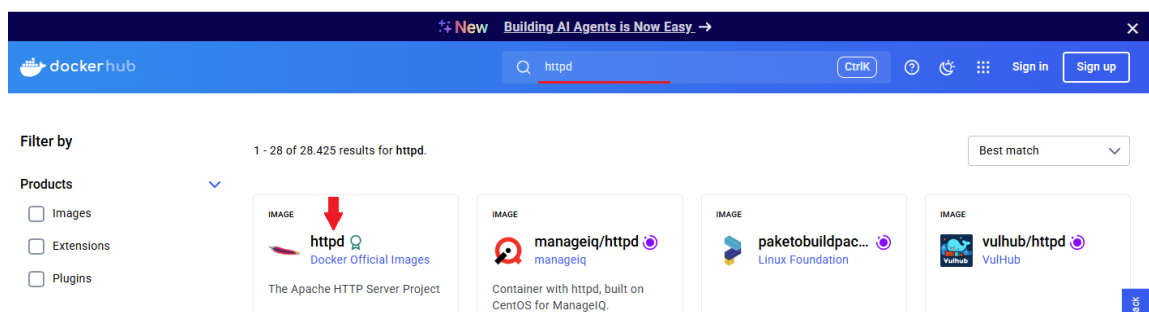
Figura 144 comando de arranque automatico.



Procedemos a crear nuestro contenedor, pero para eso necesitamos una imagen que va a funcionar dentro del mismo. Para esto vamos a descargar una imagen desde el repositorio de docker, el cual se llama docker hub.

Dentro del repositorio de docker, buscamos httpd y seleccionamos el más actualizado.

Figura 145 Búsqueda desde el navegador docker hub.



Para descargar la imagen usamos el comando que nos proporciona.

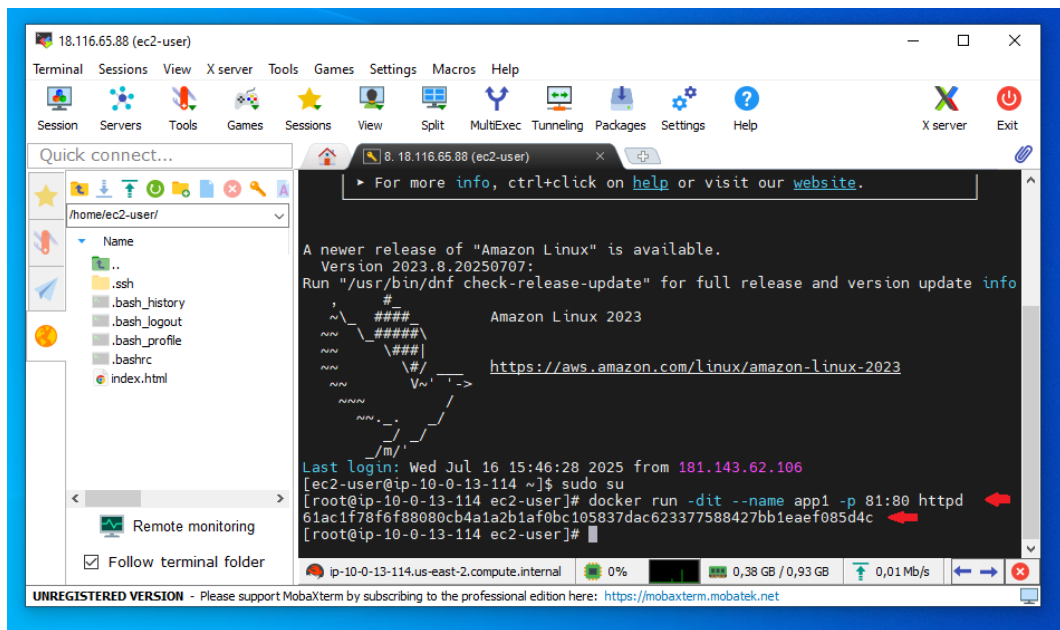
Figura 146 descarga del sitio.



Ejecutamos ese comando en el servidor y esperamos la instalación de la imagen.

Una vez instalada la imagen, iniciamos a crear nuestro primer contenedor con el comando (docker run -dit --name app1 -p 81:80 httpd).

Figura 149 creación de contenedor.



Observamos los contenedores tenemos con el comando (docker ps).

Figura 150 contenedores disponibles

```

_/m/'
Last login: Wed Jul 16 15:46:28 2025 from 181.143.62.106
[ec2-user@ip-10-0-13-114 ~]$ sudo su
[root@ip-10-0-13-114 ec2-user]# docker run -dit --name app1 -p 81:80 httpd
61ac1f78f6f88080cb4a1a2b1af0bc105837dac623377588427bb1eaeaf085d4c
[root@ip-10-0-13-114 ec2-user]# docker ps
CONTAINER ID   IMAGE     COMMAND                  CREATED    STATUS    PORTS
TS
61ac1f78f6f8   httpd    "httpd-foreground"     2 minutes ago    Up 2 minutes    0.0:81->80/tcp, :::81->80/tcp
app1
[root@ip-10-0-13-114 ec2-user]#

```

Para verificar que nuestro contenedor esté funcionando desde el puerto 81, debemos agregarlo en el grupo de seguridad de nuestra instancia y luego probarlo.

En las reglas de entrada damos editar para agregar el puerto 81.

Figura 151 puerto 81 agregado a las reglas de entrada.

The screenshot shows the 'Reglas de entrada' (Inbound Rules) configuration page in the AWS IAM console. It displays a table of existing rules and a form to add a new rule. The new rule is configured with the following details:

ID de la regla del grupo de seguridad	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción: opcional	Acción
sgr-0cc5c5e27a0a12aca	HTTP	TCP	80	Person...	0.0.0.0/0	Eliminar
sgr-0075ca9142f9bf825	SSH	TCP	22	Person...	0.0.0.0/0	Eliminar
-	TCP personalizado	TCP	81	Anywh...	0.0.0.0/0	Eliminar

At the bottom of the configuration form, there is a warning message: "Las reglas cuyo origen es 0.0.0.0/0 o ::/0 permiten a todas las direcciones IP acceder a la instancia. Recomendamos configurar reglas de grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas." Below this message are buttons for 'Cancelar', 'Previsualizar los cambios', and 'Guardar reglas'.

Probamos nuestro contenedor ingresando la IP pública seguida del puerto habilitado para el contenedor y efectivamente está funcionando.

Figura 152 prueba en navegar web del contenedor.

The screenshot shows a web browser window with the address bar containing the URL `18.116.65.88:81`. A red arrow points to the port number `81` in the address bar.

It works!

Continuamos ingresando una aplicación propia en la ubicación en la ubicación de la carpeta del servidor.

Para la administración de nuestro docker debemos tener en cuenta el identificar que se genera al momento de crear los contenedores.

Para detener el contenedor ingresamos el comando (docker stop #idcontenedor).

Figura 153 detener contenedor.

```
cbe747411fd3  httpd      "httpd-foreground"   3 seconds ago   Up 2 seconds   0.0.0
.0:82->80/tcp, :::82->80/tcp   app2
61ac1f78f6f8  httpd      "httpd-foreground"   6 minutes ago   Up 6 minutes   0.0.0
.0:81->80/tcp, :::81->80/tcp   app1
[root@ip-10-0-13-114 ec2-user]# docker stop 61ac1f78f6f8
61ac1f78f6f8
[root@ip-10-0-13-114 ec2-user]#
```

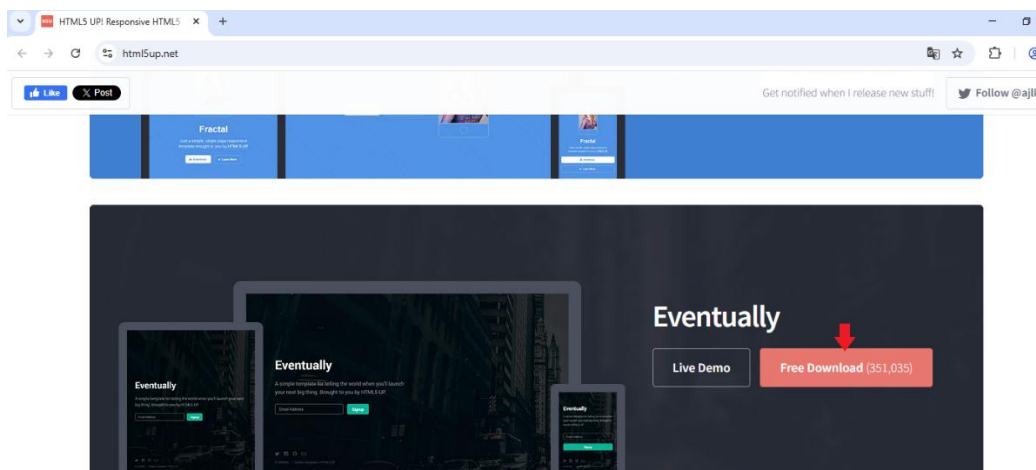
Para revisar que nuestro contenedor se detuvo ingresamos el comando (docker ps -a).

Figura 154 observar contenedor detenido.

```
[root@ip-10-0-13-114 ec2-user]# docker ps -a
CONTAINER ID   IMAGE    COMMAND                  CREATED        STATUS
PORTS          NAMES
cbe747411fd3   httpd    "httpd-foreground"      28 minutes ago   Up 28 minutes
0.0.0.0:82->80/tcp, :::82->80/tcp   app2
61ac1f78f6f8   httpd    "httpd-foreground"      34 minutes ago   Exited (0) 2 minutes ago
app1
[root@ip-10-0-13-114 ec2-user]#
```

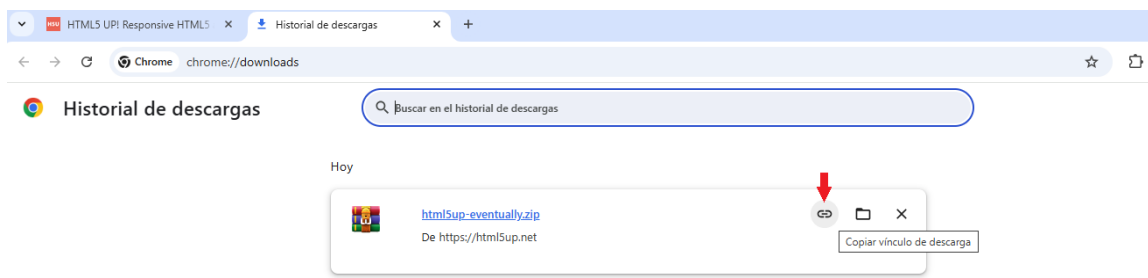
Vamos a probar montando una página en nuestro contenedor, buscamos en nuestro navegador web html5 template y elegimos una descargando el archivo.

Figura 155 prueba montando imagen.



Una vez se descarga necesitamos copiar el enlace de descargar para utilizarlo en nuestra instancia de Linux.

Figura 156 copiar el enlace de la imagen descargada.



Creamos la carpeta para ingresar el archivo con el comando (mkdir app1) y accedemos a la carpeta con el comando (cd app1/), para descargar el sitio.

Figura 157 creación de carpeta.

```
[root@ip-10-0-13-114 ec2-user]# mkdir app1
[root@ip-10-0-13-114 ec2-user]# cd app1/
[root@ip-10-0-13-114 app1]#
```

Descargamos el sitio ingresando el comando (wget) y pegando el enlace de descarga del sitio.

Figura 158 descarga de sitio.

```
[root@ip-10-0-13-114 ec2-user]# mkdir app1
[root@ip-10-0-13-114 ec2-user]# cd app1/
[root@ip-10-0-13-114 app1]# wget https://html5up.net/eventually/download
--2025-07-16 16:46:59-- https://html5up.net/eventually/download
Resolving html5up.net (html5up.net)... 172.67.195.190, 104.21.76.136, 2606:4700:30
30:6815:4c88, ...
Connecting to html5up.net (html5up.net)|172.67.195.190|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-zip]
Saving to: 'download'

download          [ <=>          ] 1.72M  --.-KB/s   in 0.1s
2025-07-16 16:47:00 (18.1 MB/s) - 'download' saved [1799395]
[root@ip-10-0-13-114 app1]#
```

Comprobamos que es un archivo Zip con el comando (file download) y lo descomprimos con el comando (unzip download).

Figura 159 comprobacion de tipo de archivo.

```
inflating: assets/sass/main.scss
  creating: assets/sass/components/
inflating: assets/sass/components/_icons.scss
inflating: assets/sass/components/_button.scss
inflating: assets/sass/components/_form.scss
inflating: assets/sass/components/_icon.scss
inflating: assets/sass/components/_list.scss
inflating: assets/sass/components/_section.scss
  creating: assets/sass/libs/
inflating: assets/sass/libs/_functions.scss
inflating: assets/sass/libs/_mixins.scss
inflating: assets/sass/libs/_vars.scss
inflating: assets/sass/libs/_vendor.scss
inflating: assets/sass/libs/_breakpoints.scss
inflating: README.txt
inflating: index.html
  creating: images/
inflating: images/bg03.jpg
inflating: images/bg02.jpg
inflating: images/bg01.jpg
[root@ip-10-0-13-114 app1]# ls
LICENSE.txt  README.txt  assets  download  images  index.html
[root@ip-10-0-13-114 app1]#
```

Luego agregamos el archivo a la carpeta creada anteriormente para que los contenedores puedan acceder a él.

Para eso vamos a crear un nuevo contenedor y a este le vamos a agregar el archivo que descargamos para que este dentro de la carpeta del contenedor y pueda mostrar el sitio que descargamos.

Figura 160 creación de contenedor con el archivo descargado.

```
Create and run a new container from an image
[root@ip-10-0-13-114 app1]# docker run -dit --name app3 -p 83:80 -v /home/ec2-user
/app1/:/usr/local/apache2/htdocs/ httpd
2abc4bdf0c4831e36003f5f0b0761c766094face9d4bc8a37b6cfd9de8cb2cd2
[root@ip-10-0-13-114 app1]#
```

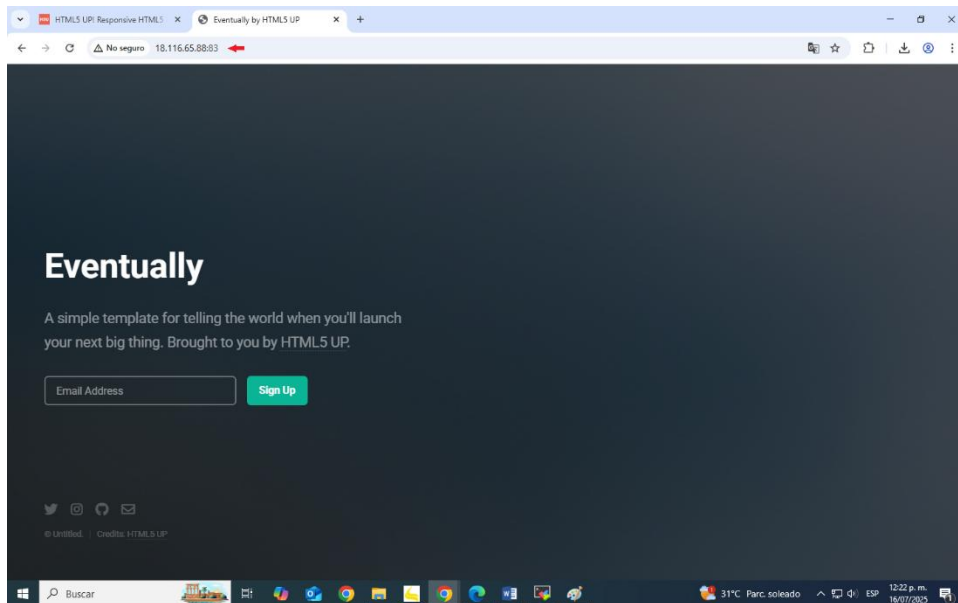
Verificamos en nuestro navegador, pero antes le damos el acceso a nuestro puerto 83 desde la instancia en grupos de seguridad, reglas de entrada.

Figura 161 acceso a puerto para prueba.

Reglas de entrada <small>Información</small>	Tipo <small>Información</small>	Protocolo <small>Información</small>	Intervalo de puertos <small>Información</small>	Origen <small>Información</small>	Descripción: opcional <small>Información</small>	
sgr-0cc5c5e27a0a12aca	HTTP	TCP	80	Person...	Q	Eliminar
sgr-0e9058eeac626b62b	TCP personalizado	TCP	83	Person...	Q 0.0.0.0 X	Eliminar
sgr-0075ca9142f9bf825	SSH	TCP	22	Person...	Q 0.0.0.0 X	Eliminar

Efectivamente nos carga el contenedor con la aplicación.

Figura 162 prueba del contenedor en el navegador web.



Creamos otro contenedor, pero en este caso ingresamos un nuevo comando para garantizar que, aunque se apague el servidor, el contenedor vuelva a arrancar de manera automática.

Figura 163 creación de contenedor y comando de inicio automáticamente.

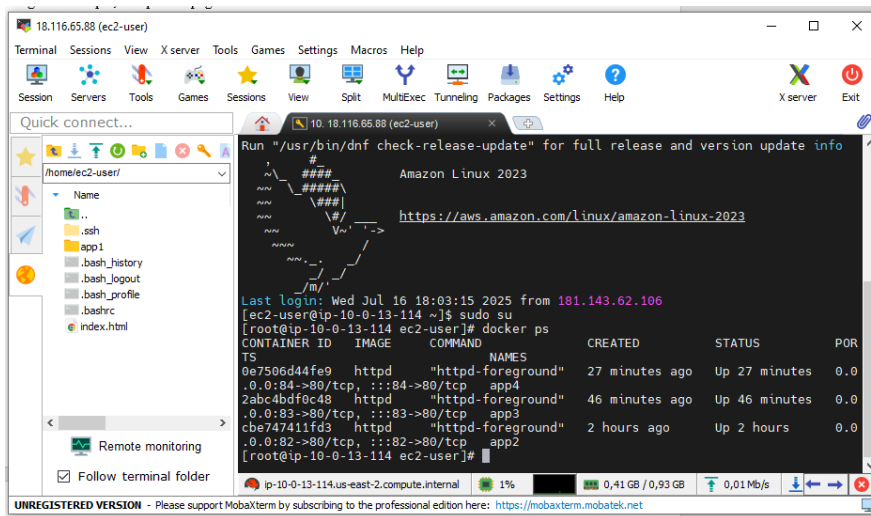
```
[root@ip-10-0-13-114 app1]# docker run -dit --name app4 -d --restart always -p 84:80 -v /home/ec2-user/app1:/usr/local/apache2/htdocs/ httpd 0e7506d44fe9f18b83508bd7338aedbe6de3713eed7b555e90fc33045cd4c6a7 [root@ip-10-0-13-114 app1]#
```

Proxy Reverso con instancias

Implementación del proxy inverso para que gestione el tráfico entrante entre los servidores.

Verificamos los contenedores que tenemos creados, con el comando (Docker ps).

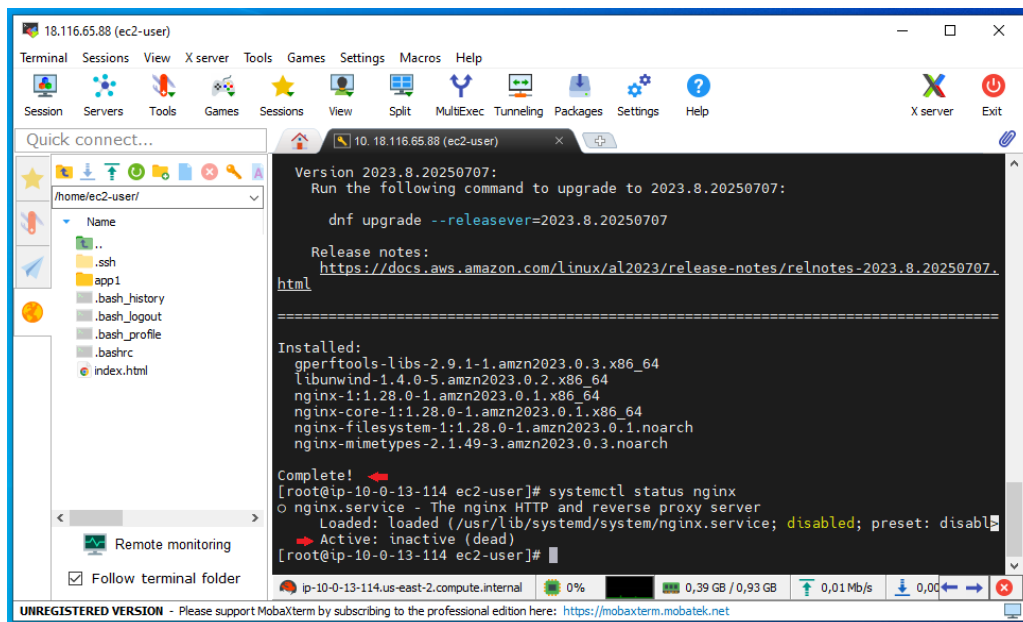
Figura 164 comprobacion de contenedores.



Ponemos a funcionar varios contenedores dentro de la misma instancia con la misma aplicación, para tener acceso desde una URL sin puertos y necesitamos instalar el servicio de Nginx.

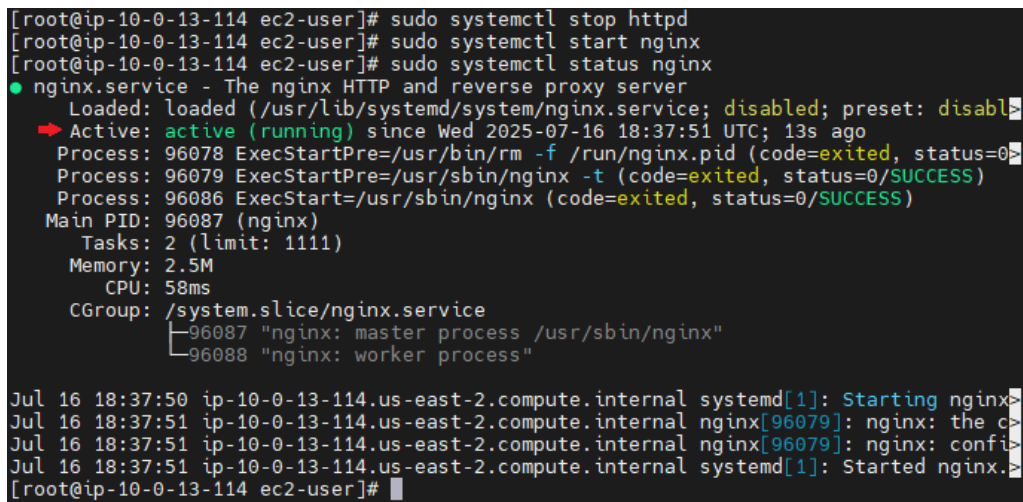
Instalamos el servicio de Nginx ejecutando el comando (dnf install nginx) y verificamos el estado.

Figura 165 instalación del servicio Nginx.



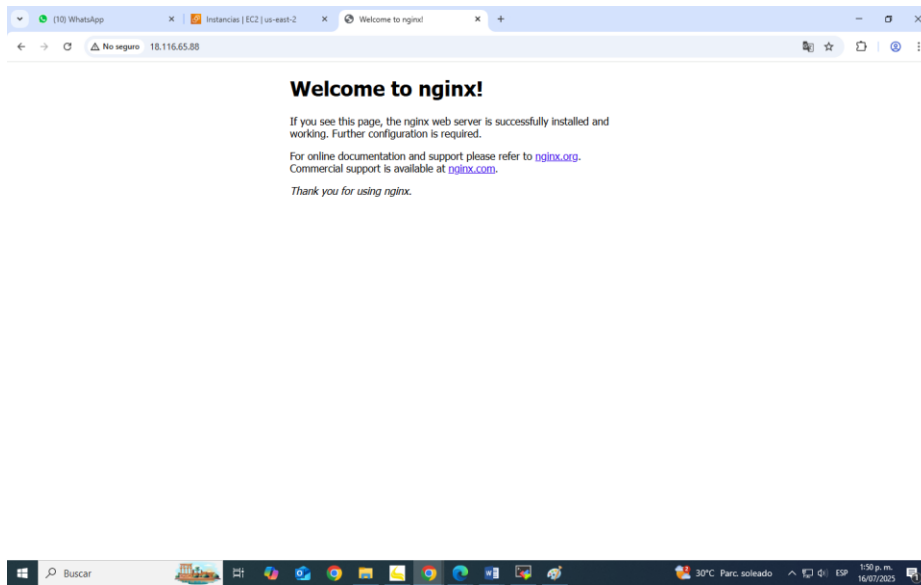
Activamos el servicio con (systemctl start nginx).

Figura 166 activación del servicio.



Verificamos que este corriendo, accediendo desde internet por medio del puerto 80, usando la IP publica de nuestra instancia.

Figura 167 prueba de acceso.



Seguimos con la configuración para poner a funcionar el servicio como un proxy inverso.

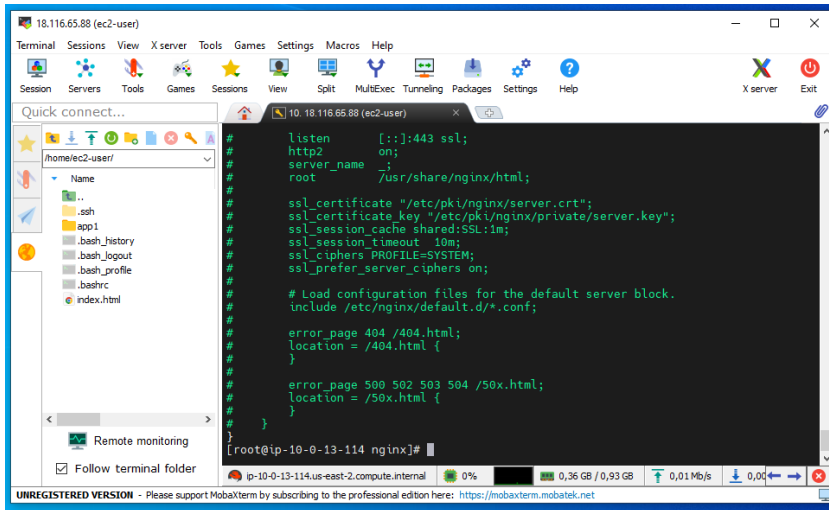
Ingresamos a la carpeta de Nginx para acceder a la configuración con la ruta (`cd /etc/nginx/`) y escribimos `ls` para ver que lo que está dentro.

Figura 168 configuración de la ruta.

```
[root@ip-10-0-13-114 ec2-user]# cd /etc/nginx/
[root@ip-10-0-13-114 nginx]# ls
conf.d          koi-utf          scgi_params
default.d      koi-win          scgi_params.default
fastcgi.conf   mime.types       uwsgi_params
fastcgi.conf.default  mime.types.default  uwsgi_params.default
fastcgi_params  nginx.conf       win-utf
fastcgi_params.default  nginx.conf.default
[root@ip-10-0-13-114 nginx]#
```

Revisamos el funcionamiento del servidor ingresando (cat nginx.conf)

Figura 169 revisar funcionamiento.



```

# listen      [::]:443 ssl;
# http2      on;
# server_name _;
# root       /usr/share/nginx/html;

# ssl_certificate "/etc/pki/nginx/server.crt";
# ssl_certificate_key "/etc/pki/nginx/private/server.key";
# ssl_session_cache shared:SSL:1m;
# ssl_session_timeout 10m;
# ssl_ciphers PROTOCOL=SYSTEM;
# ssl_prefer_server_ciphers on;

# Load configuration files for the default server block.
# include /etc/nginx/default.d/*.conf;

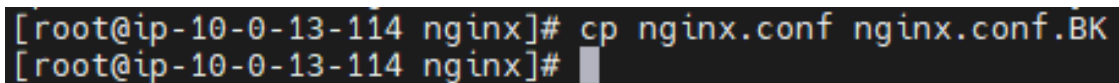
# error_page 404 /404.html;
# location = /404.html {
# }

# error_page 500 502 503 504 /50x.html;
# location = /50x.html {
# }

```

Realizamos una copia del archivo por si deseamos regresar al estado como estaba el archivo.

Figura 170 Copia de seguridad.



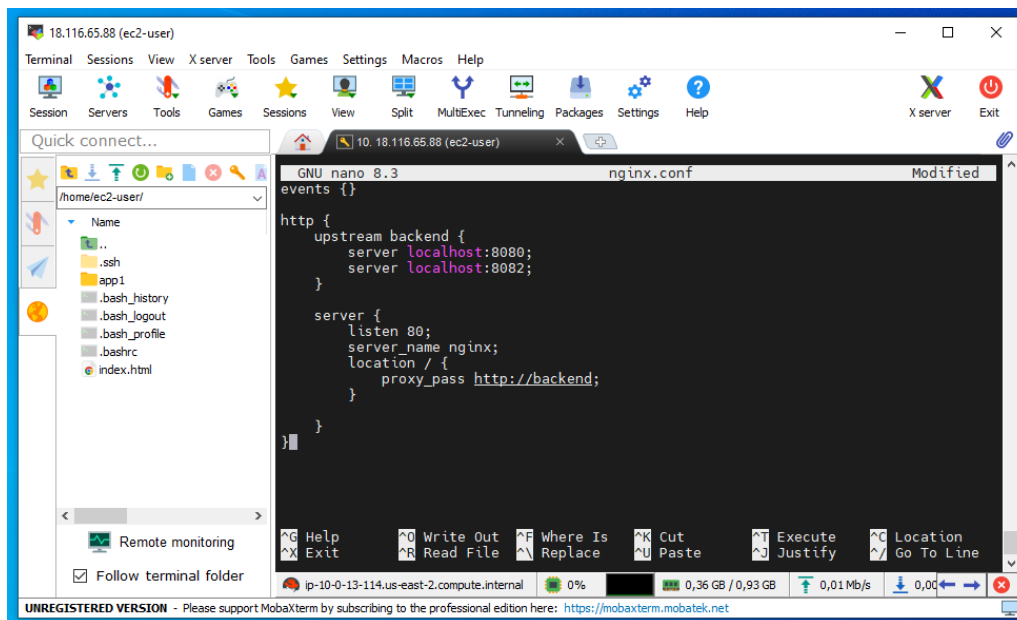
```

[root@ip-10-0-13-114 nginx]# cp nginx.conf nginx.conf.BK
[root@ip-10-0-13-114 nginx]#

```

Entramos al archivo para modificarlo con (nano nginx). Borramos la información y pegamos la documentación del sitio.

Figura 171 modificación de archivo para sitio.



Esa es la configuración que se debe usar para que funcione el servicio como proxy reverso.

Modificamos el nombre del servidor y las urls para que cuando llegue una petición al puerto 80 las redireccione al grupo de urls donde están mis contenedores.

Figura 172 modificación nombre del servidor y url.

```
events {
    worker_connections 1024;
}

http {
    upstream seminario {
        server localhost:83; ←
        server localhost:82; ←
        server localhost:84; ←
    }

    server {
        listen 80;
        server_name nginx;

        location / {
            proxy_pass http://seminario; ←
        }
    }
}
```

Prueba de proxy reverso desde cada una de las IP

Figura 173 prueba de contenedor con el puerto 85.

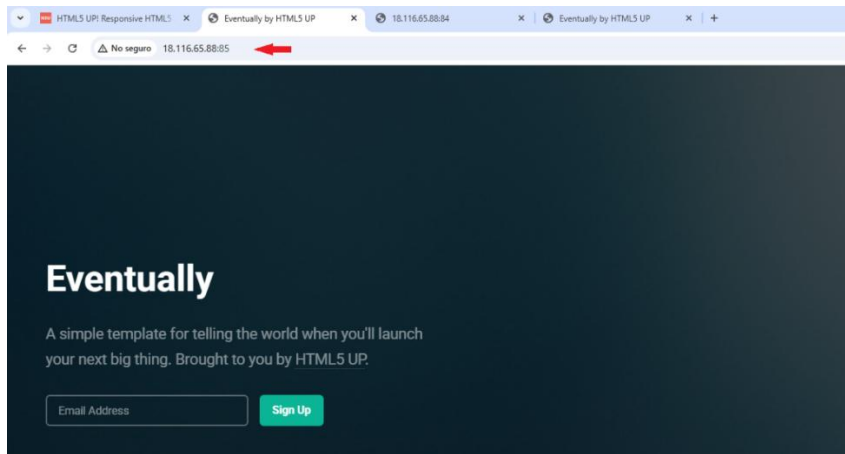
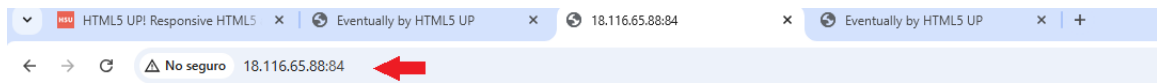
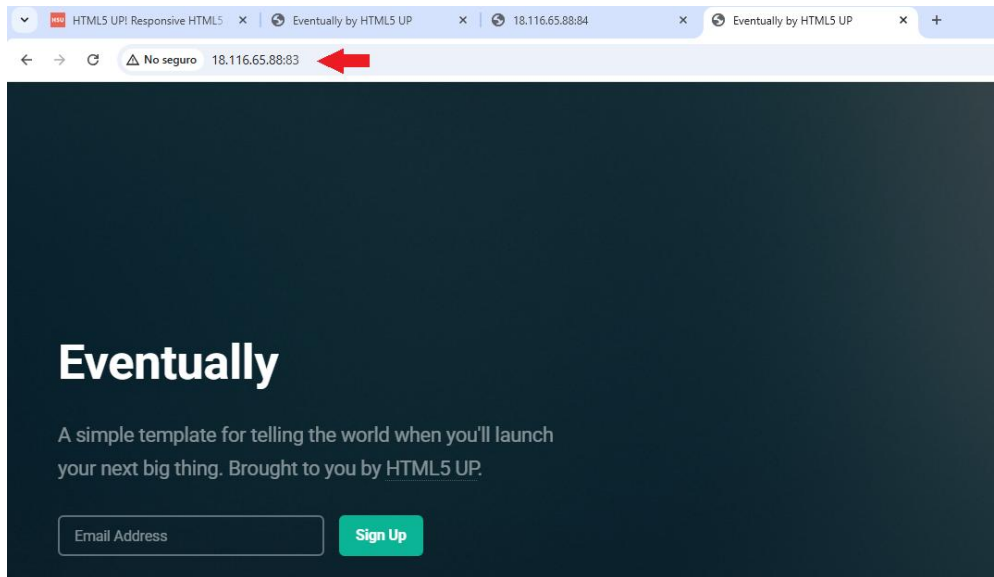


Figura 174 prueba de contenedor con el puerto 84.



It works!

Figura 175 prueba de contenedor con el puerto 83.



Para que nuestro proxy reverso funcione de manera adecuada y muestre lo que tienen los contenedores sin acceder a cada uno desde la IP individual es necesario abrir el archivo de configuración y editar para agregar los puertos de los contenedores que tenemos disponibles.

Figura 176 aplicación del proxy reverso en el archivo.

```

GNU nano 8.3 /etc/nginx/nginx.conf
events {
    worker_connections 1024;
}

http {
    upstream seminario {
        server localhost:85;
        server localhost:83;
        server localhost:84;
        server localhost:86;
    }

    server {
        listen 80;
        server_name nginx;

        location / {
            proxy_pass http://seminario;
            proxy_set_header Host $host;
            proxy_set_header X-Real-IP $remote_addr;
            proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        }
    }
}
  
```

Verificación del funcionamiento del proxy reverso con la IP pública

Para verificar que está funcionando ingresamos la IP pública de nuestra instancia y desde ahí debemos observar el cambio de contenedores al recargar la página desde el mismo puerto 80.

Efectivamente carga la información que está en el index.html del contenedor al que corresponde el puerto.

Figura 177 prueba del proxy reverso.

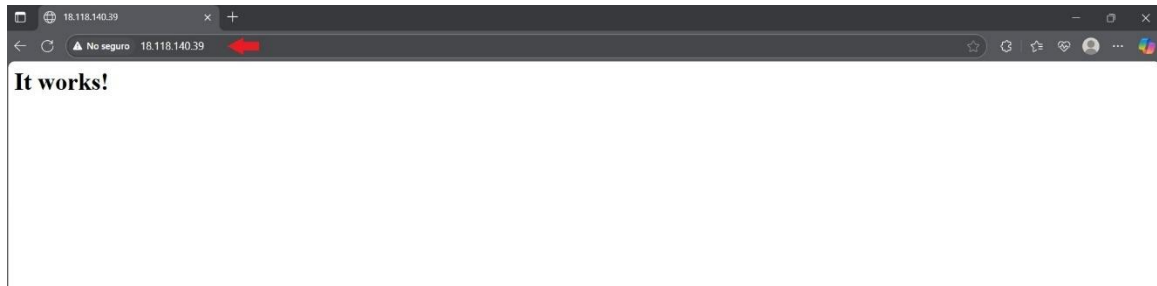


Figura 178 prueba del proxy reverso.

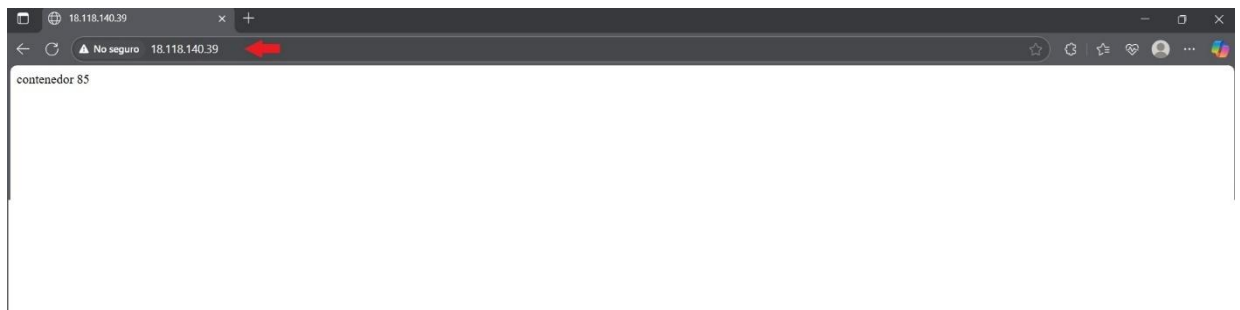


Figura 179 prueba del proxy reverso.

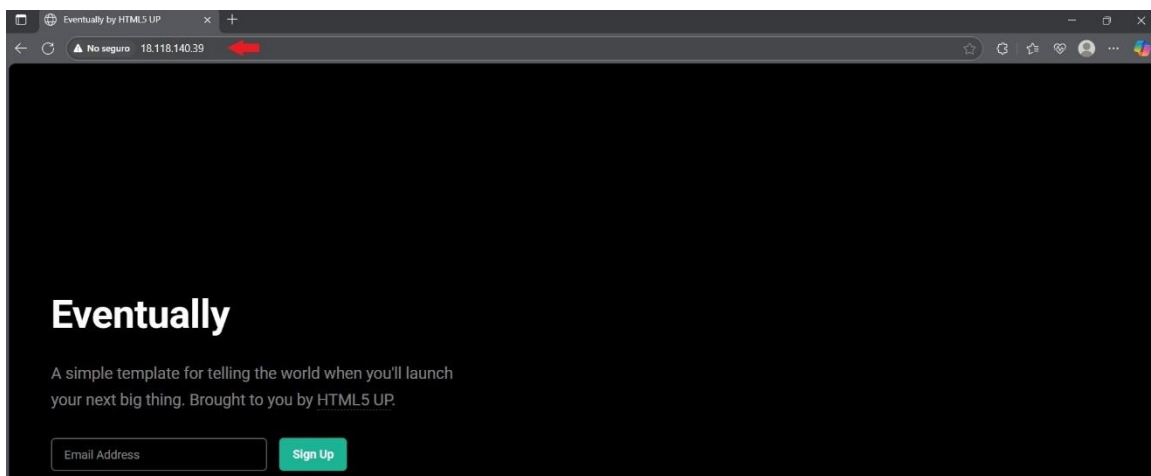
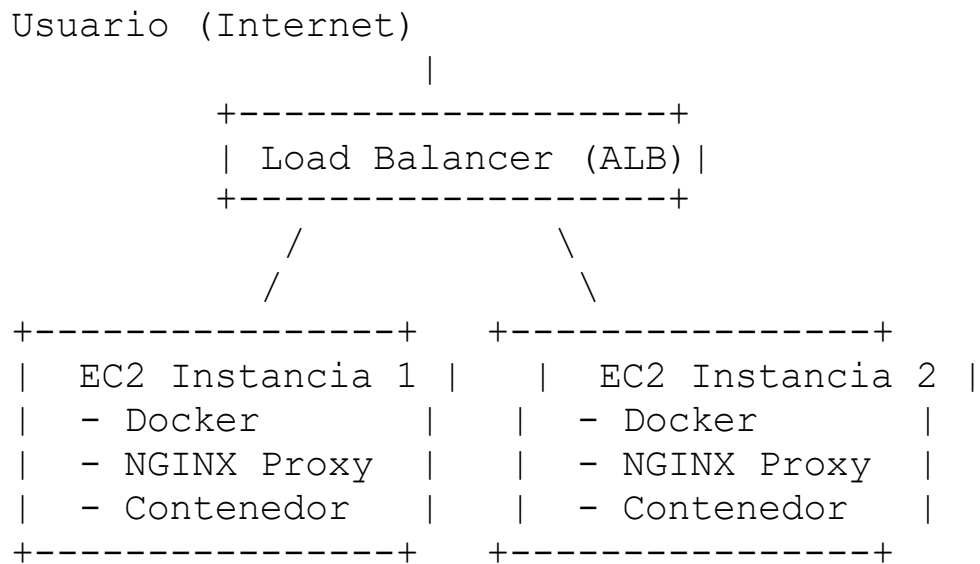


Diagrama de los servicios usados

Indice de figuras

Figura 1 Diseño general de la red en AWS.....	9
Figura 2 Servidor IIS operativo.	13
Figura 3 Servidor Apache activo	13
Figura 4 Creación de VPC.	14
Figura 5 crear VPC.	14
Figura 6 nombrar VPC.....	15
Figura 7 VPC creadas.	15
Figura 8 Búsqueda de ec2.....	16
Figura 9 servicio instancias.....	16
Figura 10 creación de instancia.....	17
Figura 11 nombrar instancia.	17
Figura 12 AMI a instalar.....	17
Figura 13 tipo de instancia.....	18
Figura 14 creación Par de Clave.	18
Figura 15 Par de claves.....	19
Figura 16 configuración de red.....	19
Figura 17 grupo de seguridad.	20
Figura 18 configuración almacenamiento.....	20
Figura 19 lanzar instancia.	21
Figura 20 creación instancia.	21
Figura 21 instancia activa.	21
Figura 22 habilitacion del Puerto 80.....	22
Figura 23 Grupo de seguridad.....	22
Figura 24 agregar reglas de entrada.....	23
Figura 25 habilitar Puerto 80.	23
Figura 26 Puerto 80 agregado.	23
Figura 27 creación de instancia Linux.....	24
Figura 28 nombrar instancia.	24
Figura 29 elección de AMI.	25
Figura 30 tipo de instancia.....	25
Figura 31 Autenticacion para de calves.....	26
Figura 32 configuración de red.....	26
Figura 33 eleccion de VPC.	27
Figura 34 nuevo Grupo de seguridad.....	28
Figura 35 habilitacion Puerto 80.....	28
Figura 36 Almacenamiento instancia.....	29
Figura 37 lanzamiento instancia.	29
Figura 38 instancia creada.	30
Figura 39 visualización instancia.....	30
Figura 40 acceso por RDP a windows.....	30
Figura 41 conexión RDP.....	31
Figura 42 conexion por escritorio remoto.....	31

Figura 43 seleccion IP publica.....	32
Figura 44 conexion a escritorio remoto.....	32
Figura 45 contraseña de acceso.....	33
Figura 46 obtención de contraseña.....	33
Figura 47 cargue de par de clave.....	34
Figura 48 cifrado de contraseña.....	34
Figura 49 credenciales de acceso.....	35
Figura 50 conexion servidor.....	35
Figura 51 Busqueda server manager.....	36
Figura 52 instalación de rol.....	36
Figura 53 proceso instalación.....	37
Figura 54 proceso de instalación.....	37
Figura 55 instalación rol.....	38
Figura 56 instalación web server.....	39
Figura 57 instalación rol.....	39
Figura 58 finalización de instalación.....	40
Figura 59 visualización instalación.....	41
Figura 60 Busqueda servicio instalado.....	41
Figura 61 servidor creado.....	42
Figura 62 prueba servidor.....	42
Figura 63 servidor funcionando.....	43
Figura 64 prueba en navegar web.....	43
Figura 65 acceso SSH.....	44
Figura 66 conexión.....	45
Figura 67 sección cliente SSH.....	45
Figura 68 conexión por DNS.....	45
Figura 69 acceso servidor.....	46
Figura 70 acceso SSH.....	46
Figura 71 ingreso de archivo .pem.....	47
Figura 72 acceso servidor Linux.....	48
Figura 73 modo administración.....	48
Figura 74 instalación Apache.....	49
Figura 75 instalación completa.....	49
Figura 76 verificación estado.....	50
Figura 77 activación.....	51
Figura 78 prueba de acceso.....	51
Figura 79 prueba en navegador web.....	52
Figura 80 ping sin protocol ICMP.....	53
Figura 81 seleccion grupo de seguridad.....	53
Figura 82 regla de entrada.....	54
Figura 83 prueba de conexión entre instancias.....	55
Figura 84 servidor funcionando.....	56
Figura 85 servidor funcionando.....	57
Figura 86 selección ID.....	58
Figura 87 selección de volumen.....	59

Figura 88 creación instantánea.....	59
Figura 89 creación de imagen.....	60
Figura 90 creación de AMI.....	60
Figura 91 identificación dispositivo raíz.....	61
Figura 92 Figura 90 creación de AMI.....	61
Figura 93 creación instancia.....	62
Figura 94 selección de AMI personalizada.....	62
Figura 95 regla de entrada Puerto 80.....	64
Figura 96 Segunda instancia creada de la AMI.....	64
Figura 97 prueba en navegar web.....	65
Figura 98 prueba en navegar web.....	65
Figura 99 selección balanceadores de carga.....	66
Figura 100 creación balanceador.....	66
Figura 101 selección tipo balanceador.....	67
Figura 102 configuración balanceador.....	68
Figura 103 selección de VPC y zonas de disponibilidad.....	68
Figura 104 grupos de seguridad.....	69
Figura 105 creación grupo de seguridad.....	69
Figura 106 configuración grupo de seguridad.....	69
Figura 107.....	70
Figura 108 creación balanceador.....	70
Figura 109 puerto 80 habilitado.....	71
Figura 110 creación grupo destino.....	71
Figura 111 configuración VPC, puerto y tipo dirección.....	72
Figura 112 parametros de comprobación de estado.....	73
Figura 113 registro de destinos.....	73
Figura 114 creación grupo de destino.....	74
Figura 115 creación balanceador.....	74
Figura 116 visualización de balanceador.....	75
Figura 117 prueba de balanceador en navegador web.....	76
Figura 118 prueba balanceador en navegador web.....	77
Figura 119 servicio auto scaling.....	78
Figura 120 creación de servicio auto scaling.....	78
Figura 121 nombrar auto scaling.....	79
Figura 122 creación Plantilla de lanzamiento.....	79
Figura 123 selección de AMI.....	80
Figura 124 configuración de la red.....	81
Figura 125 puerto 80 agregado.....	81
Figura 126 almacenamiento por defecto y creación.....	82
Figura 127 plantilla disponible.....	83
Figura 128 configuración de red.....	84
Figura 129 asociar balanceador y grupo de destino.....	85
Figura 130 activación de comprobación de estado.....	85
Figura 131 capacidad instancias creadas.....	86
Figura 132 creación política de escalado.....	86

	116
Figura 133 resumen de la configuración.....	87
Figura 134 prueba de auto scaling funcionando.	88
Figura 135 prueba en navegar web.	88
Figura 136 prueba auto scaling	89
Figura 137 prueba auto scaling.	89
Figura 138 prueba creación auto scaling.	90
Figura 139 seleccion de instancia.	91
Figura 140 acceso al servidor.	91
Figura 141 rol administrador.	92
Figura 142 estado del servidor.	92
Figura 143 servidor activado.	93
Figura 144 comando de arranque automatico.	93
Figura 145 Busqueda desde el navegador docker hub.	94
Figura 146 descarga del sitio.	94
Figura 147 instalación de la imagen.	95
Figura 148 comprobacion de imagen instalada.	95
Figura 149 creación de contenedor.	96
Figura 150 contenedores disponibles.	96
Figura 151 puerto 81 agregado a las reglas de entrada.	97
Figura 152 prueba en navegar web del contenedor.	97
Figura 153 detener contenedor.	98
Figura 154 observar contenedor detenido.	98
Figura 155 prueba montando imagen.	99
Figura 156 copiar el enlace de la imagen descargada.	99
Figura 157 creación de carpeta.	99
Figura 158 descarga de sitio.	100
Figura 159 comprobacion de tipo de archivo.	100
Figura 160 creación de contenedor con el archivo descargado.	101
Figura 161 acceso a puerto para prueba.	101
Figura 162 prueba del contenedor en el navegador web.	102
Figura 163 creación de contenedor y comando de inicio automáticamente.	102
Figura 164 comprobacion de contenedores.	103
Figura 165 instalación del servicio Nginx.	104
Figura 166 activación del servicio.	104
Figura 167 prueba de acceso.	105
Figura 168 configuración de la ruta.	105
Figura 169 revisar funcionamiento.	106
Figura 170 Copia de seguridad.	106
Figura 171 modificación de archivo para sitio.	107
Figura 172 modificacion nombre del servidor y url.	107
Figura 173 prueba de contenedor con el puerto 85.	108
Figura 174 prueba de contenedor con el puerto 84.	108
Figura 175 prueba de contenedor con el puerto 83.	109
Figura 176 aplicación del proxy reverso en el archivo.	110
Figura 177 prueba del proxy reverso.	111

	117
Figura 178 prueba del proxy reverso.	111
Figura 179 prueba del proxy reverso.	111

Conclusiones

La arquitectura implementada durante el seminario AWS garantiza alta disponibilidad gracias al uso de los balanceadores de carga y la distribución en múltiples zonas de disponibilidad; además el uso de Docker permite un despliegue eficaz de las aplicaciones, optimizando los tiempos de configuración. Cabe destacar que el auto scaling asegura que la infraestructura puede adaptarse automáticamente a variaciones en la demanda, contribuyendo a una mayor eficiencia en el uso de recursos.

Finalmente, el uso del proxy reverso permite manejar múltiples contenedores en una sola instancia de manera ordenada y escalable. Los servicios de AWS demuestran ser herramientas sólidas y en constante evolución, para desplegar infraestructuras modernas, robustas y preparadas para el crecimiento dinámico de las aplicaciones.

Referencias

- AWS, A. (s.f.). *Amazon AWS*. Obtenido de https://docs.aws.amazon.com/es_es/elasticloadbalancing/latest/userguide/what-is-load-balancing.html
- AWS, A. (s.f.). *Amazon AWS*. Obtenido de https://docs.aws.amazon.com/es_es/elasticloadbalancing/latest/userguide/what-is-load-balancing.html
- AWS, A. (s.f.). *AWS Amazon*. Obtenido de https://docs.aws.amazon.com/es_es/ebs/latest/userguide/ebs-volumes.html
- C, D. (30 de Julio de 2022). *Medium* . Obtenido de Medium.com: <https://medium.com/@diego.coder/introducci%C3%B3n-a-aws-vpc-amazon-virtual-private-cloud-a8e8bd614e24>
- Mallón, X. (25 de Octubre de 2024). Obtenido de <https://keepcoding.io/blog/que-es-una-imagen-de-maquina-de-amazon-ami/>
- Mallón, X. (17 de Mayo de 2024). *Keep Coding*. Obtenido de Keepcoding.io: <https://keepcoding.io/blog/que-es-amazon-ec2/>
- Mendieta, A. d. (17 de Marzo de 2017). *OpenWebinars*. Obtenido de OpenWebinars.net: <https://openwebinars.net/blog/que-es-aws/>
- Morales, E. V. (11 de Marzo de 2022). *Pragma*. Obtenido de pragma.co: <https://www.pragma.co/es/blog/contenedores-de-aws-que-son-y-cuales-son-sus-usos-y-ventajas>
- NAKIVO, E. (6 de Mayo de 2024). *Naviko*. Obtenido de naviko.com: <https://www.nakivo.com/es/blog/aws-ebs-snapshot-explained/>
- Susnjara, S., & Smalley, I. (10 de Febrero de 2025). *IBM*. Obtenido de IBM.COM: <https://www.ibm.com/es-es/think/topics/cloud-computing>
- Takami, K. (25 de Julio de 2024). *Squads Ventures*. Obtenido de <https://squads.ventures/la-importancia-de-la-escalabilidad-en-el-desarrollo-de-software/>