



PRÁCTICA 6 AWS

Paloma Pérez de Madrid

ÍNDICE

1. Ejecución de Instancias EC2

- 1.1 Acceso a la Consola y Creación de Claves
- 1.2 Creación de Grupo de Seguridad
- 1.3 Comprobación de VPC y Subredes
- 1.4 Lanzamiento de Instancia PruebasWeb
- 1.5 Configuración de la Instancia y Tareas de Mantenimiento
- 1.6 Efecto de Reinicio y Detención de la Instancia
- 1.7 Generación de Imagen de la Instancia
- 1.8 Terminación de la Instancia

2. Balanceador de Carga ELB (Elastic Load Balancer)

- 2.1 Lanzamiento de Instancias y Creación de Grupo de Seguridad
- 2.2 Creación de Grupo de Destinatarios
- 2.3 Creación de Balanceador de Carga
- 2.4 Pruebas de Acceso y Balanceo
- 2.5 Acceso por SSH a Instancias Internas
- 2.6 Terminación de Instancias y Recursos Asociados

3. Subredes Públicas/Privadas y NAT Gateway

- 3.1 Creación de Subredes y Lanzamiento de Instancias
- 3.2 Configuración de NAT Gateway y Tablas de Rutas
- 3.3 Configuración de Network ACLs
- 3.4 Terminación de Instancias, NAT Gateway y Recursos Asociados

4. Almacenamiento S3

- 4.1 Creación de Bucket S3 y Subida de Archivos
- 4.2 Configuración para Hosting Web Estático
- 4.3 Pruebas de Acceso y Descarga de Archivos
- 4.4 Eliminación del Bucket

5. Autoescalado para Aplicaciones Web

- 5.1 Creación de Grupo de Destinatarios y Balanceador
- 5.2 Creación de Plantilla de Lanzamiento y Grupo de Autoescalado
- 5.3 Configuración de Escalado Automático
- 5.4 Pruebas de Funcionamiento del Escalado
- 5.5 Eliminación de Recursos de Autoescalado

ÍNDICE

1. Ejecución de Instancias EC2

- 1.1 Acceso a la Consola y Creación de Claves
- 1.2 Creación de Grupo de Seguridad
- 1.3 Comprobación de VPC y Subredes
- 1.4 Lanzamiento de Instancia PruebasWeb
- 1.5 Configuración de la Instancia y Tareas de Mantenimiento
- 1.6 Efecto de Reinicio y Detención de la Instancia
- 1.7 Generación de Imagen de la Instancia
- 1.8 Terminación de la Instancia

2. Balanceador de Carga ELB (Elastic Load Balancer)

- 2.1 Lanzamiento de Instancias y Creación de Grupo de Seguridad
- 2.2 Creación de Grupo de Destinatarios
- 2.3 Creación de Balanceador de Carga
- 2.4 Pruebas de Acceso y Balanceo
- 2.5 Acceso por SSH a Instancias Internas
- 2.6 Terminación de Instancias y Recursos Asociados

3. Subredes Públicas/Privadas y NAT Gateway

- 3.1 Creación de Subredes y Lanzamiento de Instancias
- 3.2 Configuración de NAT Gateway y Tablas de Rutas
- 3.3 Configuración de Network ACLs
- 3.4 Terminación de Instancias, NAT Gateway y Recursos Asociados

4. Almacenamiento S3

- 4.1 Creación de Bucket S3 y Subida de Archivos
- 4.2 Configuración para Hosting Web Estático
- 4.3 Pruebas de Acceso y Descarga de Archivos
- 4.4 Eliminación del Bucket

5. Autoescalado para Aplicaciones Web

- 5.1 Creación de Grupo de Destinatarios y Balanceador
- 5.2 Creación de Plantilla de Lanzamiento y Grupo de Autoescalado
- 5.3 Configuración de Escalado Automático
- 5.4 Pruebas de Funcionamiento del Escalado
- 5.5 Eliminación de Recursos de Autoescalado

1. EJECUCIÓN INSTANCIAS EC2

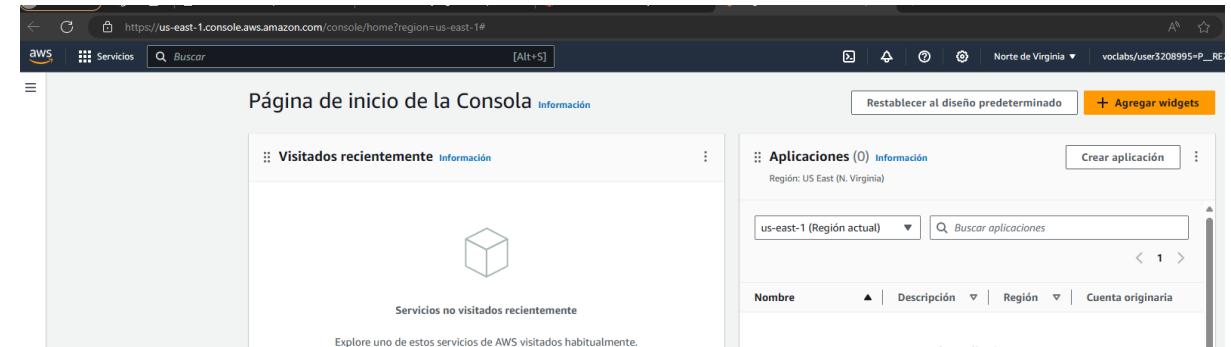
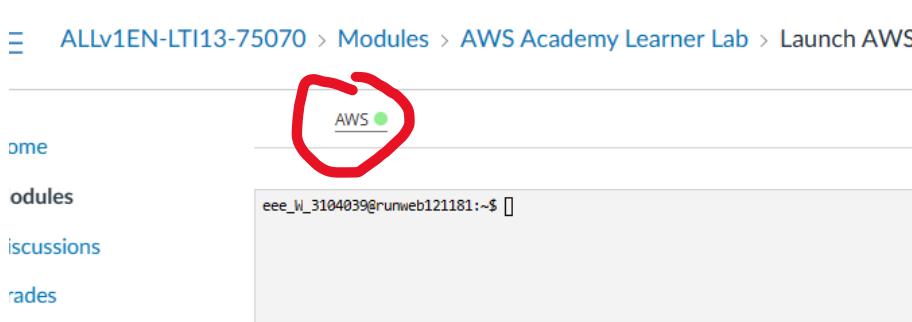
Acceder a la consola de administración web y seleccionar una Región AWS para realizar la práctica. Si accedemos con la cuenta de AWS Academy usaremos la región us-east-1. Si lo hacemos con nuestra cuenta particular, se recomienda trabajar en una región europea. Vamos a crear en primer lugar una pareja de claves pública/privada. Si accedemos con la cuenta de AWS Academy las claves ya existen (sección AWS Details), y sólo tenemos que descargarlas, en formatos .pem y .ppk. En ese caso no es necesario crear nuevas claves, aunque también podemos hacerlo para reproducir el proceso a seguir con una cuenta AWS. En la consola de computación EC2 (Services → Compute → EC2) acceder a la sección de claves (Network & Security → Key Pairs) y crear una nueva pareja de claves RSA en formato .pem (ClavesPractica). Guardar la clave privada descargada en un lugar seguro. Si va a utilizarse el cliente Putty para acceder a las instancias será necesario convertir la clave a formato .ppk (botones Load y Save Private Key de la utilidad Puttygen; el archivo de claves se guardará en formato .ppk). Nota: para usar la clave privada generada (archivo .pem) en un cliente SSH de Linux o Mac tendremos que llevar una copia del archivo al equipo, asignar derechos exclusivos al archivo para el propietario (chmod 400) y usar la opción -i en la llamada al cliente.

1. EJECUCIÓN INSTANCIAS EC2

1.1 Acceso a la Consola y Creación de Claves

Acceder a la consola de administración web y seleccionar una Región AWS para realizar la práctica. Si accedemos con la cuenta de AWS Academy usaremos la región **us-east-1**. Si lo hacemos con nuestra cuenta particular, se recomienda trabajar en una región europea. Vamos a crear en primer lugar una pareja de claves pública/privada. Si accedemos con la cuenta de AWS Academy las claves ya existen (sección AWS Details), y sólo tenemos que descargarlas, en formatos .pem y .ppk. En ese caso no es necesario crear nuevas claves, aunque también podemos hacerlo para reproducir el proceso a seguir con una cuenta AWS. En la consola de computación EC2 (Services → Compute → EC2) acceder a la sección de claves (Network & Security → Key Pairs) y crear una nueva pareja de claves RSA en formato .pem (ClavesPractica). Guardar la clave privada descargada en un lugar seguro. Si va a utilizarse el cliente Putty para acceder a las instancias será necesario convertir la clave a formato .ppk (botones Load y Save Private Key de la utilidad Puttygen; el archivo de claves se guardará en formato .ppk). Nota: para usar la clave privada generada (archivo .pem) en un cliente SSH de Linux o Mac tendremos que llevar una copia del archivo al equipo, asignar derechos exclusivos al archivo para el propietario (chmod 400) y usar la opción -i en la llamada al cliente.

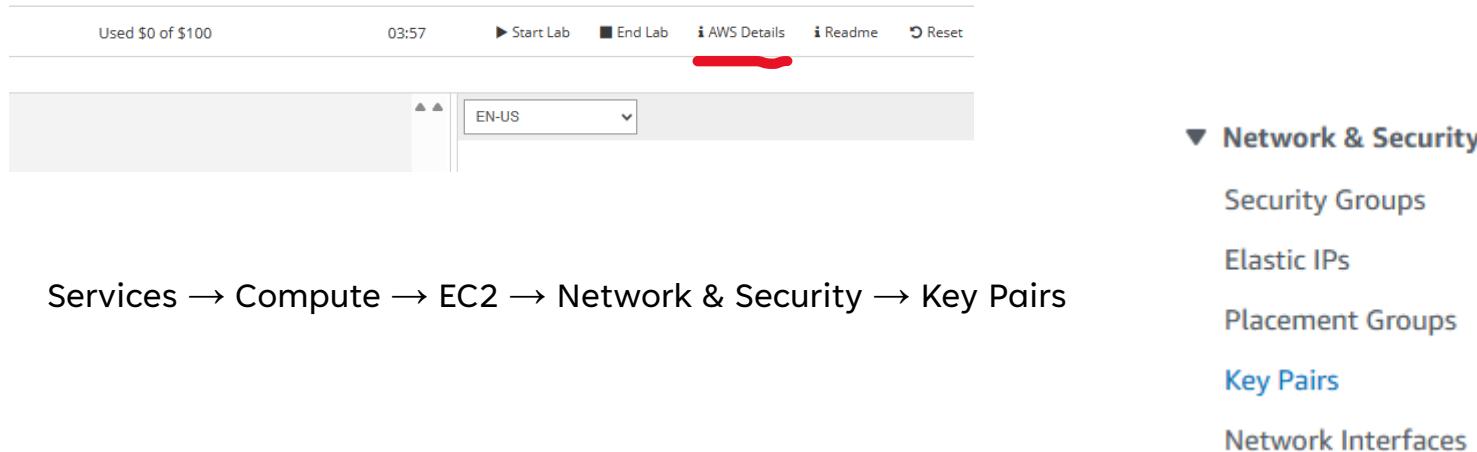
AWS Academy Learner Lab >> Modules >> Launch AWS Learner Lab >> start lab >> icono AWS verde



1. EJECUCIÓN INSTANCIAS EC2

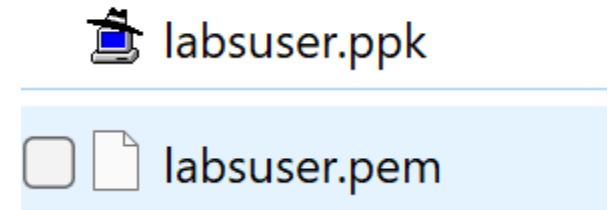
1.1 Acceso a la Consola y Creación de Claves

Vamos a **crear** en primer lugar una **pareja de claves pública/privada**. Si accedemos con la cuenta de AWS Academy las claves ya existen (sección AWS Details), y sólo tenemos que descargarlas, en formatos .pem y .ppk. En ese caso no es necesario crear nuevas claves, aunque también podemos hacerlo para reproducir el proceso a seguir con una cuenta AWS. En la consola de computación EC2 (Services → Compute → EC2) acceder a la sección de claves (Network & Security → Key Pairs) y crear una nueva pareja de claves RSA en formato .pem (ClavesPractica). Guardar la clave privada descargada en un lugar seguro. Si va a utilizarse el cliente Putty para acceder a las instancias será necesario convertir la clave a formato .ppk (botones Load y Save Private Key de la utilidad Puttygen; el archivo de claves se guardará en formato .ppk). Nota: para usar la clave privada generada (archivo .pem) en un cliente SSH de Linux o Mac tendremos que llevar una copia del archivo al equipo, asignar derechos exclusivos al archivo para el propietario (chmod 400) y usar la opción -i en la llamada al cliente.



The screenshot shows the AWS Lambda console interface. At the top, there are navigation links: Used \$0 of \$100, 03:57, Start Lab, End Lab, AWS Details, Readme, and Reset. Below this is a search bar with the placeholder 'EN-US'. On the left, there's a sidebar with 'Lambda' and 'CloudWatch Metrics' sections. The main content area has a heading 'Network & Security' with a dropdown arrow. Underneath are several links: Security Groups, Elastic IPs, Placement Groups, Key Pairs (which is highlighted in blue), and Network Interfaces.

Services → Compute → EC2 → Network & Security → Key Pairs



1. EJECUCIÓN INSTANCIAS EC2

1.1 Acceso a la Consola y Creación de Claves

*En su momento no creé las claves, las crearé ahora pero no estará reflejado en las próximas trasparencias

Services → Compute → EC2 → Network & Security → Key Pairs

▼ Network & Security

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Create key pair Info

Key pair

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name

ClavePractica

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type Info

RSA

ED25519

Private key file format

.pem

For use with OpenSSH

.ppk

For use with PuTTY

Tags - optional

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Create key pair

1. EJECUCIÓN INSTANCIAS EC2

1.2 Creación de Grupo de Seguridad

Acceder a la sección Network & Security → Security Groups. Crear un nuevo grupo de seguridad (SSH_HTTP_Any) para permitir el acceso a las instancias (inbound) por los puertos 22/tcp y 80/tcp desde cualquier dirección IP. Comprobar que se acepta todo el tráfico en las conexiones salientes (outbound).

The screenshot shows the AWS Management Console interface for creating a new security group. The top section, titled 'Inbound rules', displays two rules:

- Rule 1:** Type: SSH, Protocol: TCP, Port range: 22, Source: Anywhere..., Description: optional (empty). The source field contains '0.0.0.0/0' with a delete button.
- Rule 2:** Type: HTTP, Protocol: TCP, Port range: 80, Source: Anywhere..., Description: optional (empty). The source field contains '0.0.0.0/0' with a delete button.

A 'Delete' button is located at the bottom right of the rule list. Below this, a 'Details' section provides summary information:

Security group name	Security group ID	Description	VPC ID
PR6_SecurityGroup	sg-0720b0ae0ed758ea5	permitir el acceso a las instancias (inbound) por los puertos 22/tcp y 80/tcp desde cualquier dirección IP.	vpc-00a5dfc0664ac615a
Owner	Inbound rules count	Outbound rules count	
958486390477	2 Permission entries	1 Permission entry	

1. EJECUCIÓN INSTANCIAS EC2

1.2 Creación de Grupo de Seguridad

Acceder a la sección Network & Security → Security Groups. Crear un nuevo grupo de seguridad (SSH_HTTP_Any) para permitir el acceso a las instancias (inbound) por los puertos 22/tcp y 80/tcp desde cualquier dirección IP. Comprobar que se acepta todo el tráfico en las conexiones salientes (outbound).

Edit inbound rules [Info](#)

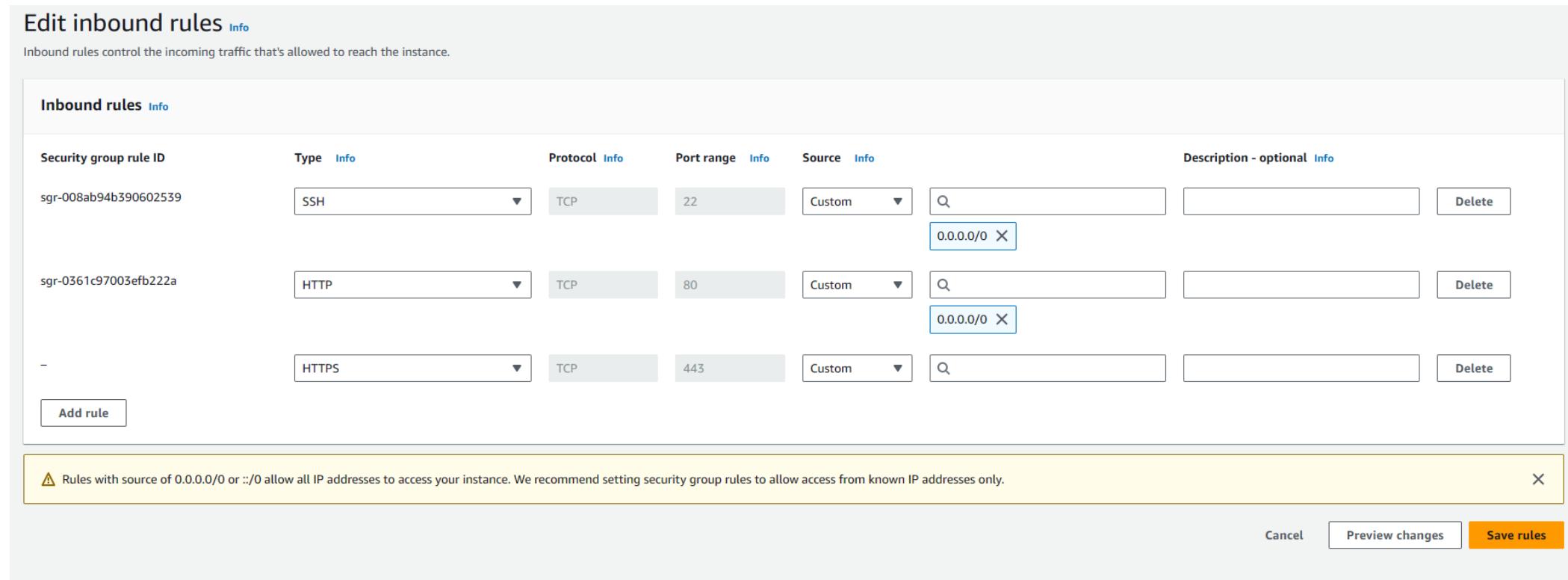
Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
sgr-008ab94b390602539	SSH	TCP	22	Custom	<input type="text" value="0.0.0.0"/> X
sgr-0361c97003efb222a	HTTP	TCP	80	Custom	<input type="text" value="0.0.0.0"/> X
-	HTTPS	TCP	443	Custom	<input type="text"/>

[Add rule](#)

⚠ Rules with source of 0.0.0.0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. X

[Cancel](#) [Preview changes](#) [Save rules](#)



1. EJECUCIÓN INSTANCIAS EC2

1.2 Creación de Grupo de Seguridad

Acceder a la sección Network & Security → Security Groups. Crear un nuevo grupo de seguridad (SSH_HTTP_Any) para permitir el acceso a las instancias (inbound) por los puertos 22/tcp y 80/tcp desde cualquier dirección IP. **Comprobar que se acepta todo el tráfico en las conexiones salientes (outbound).**

Details

Security group name PR6_SecurityGroup	Security group ID sg-0720b0ae0ed758ea5	Description permitir el acceso a las instancias (inbound) por los puertos 22/tcp y 80/tcp desde cualquier dirección IP.	VPC ID vpc-00a5dfc0664ac615a
Owner 958486390477	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

[Inbound rules](#) [Outbound rules](#) [Tags](#)

Outbound rules (1)

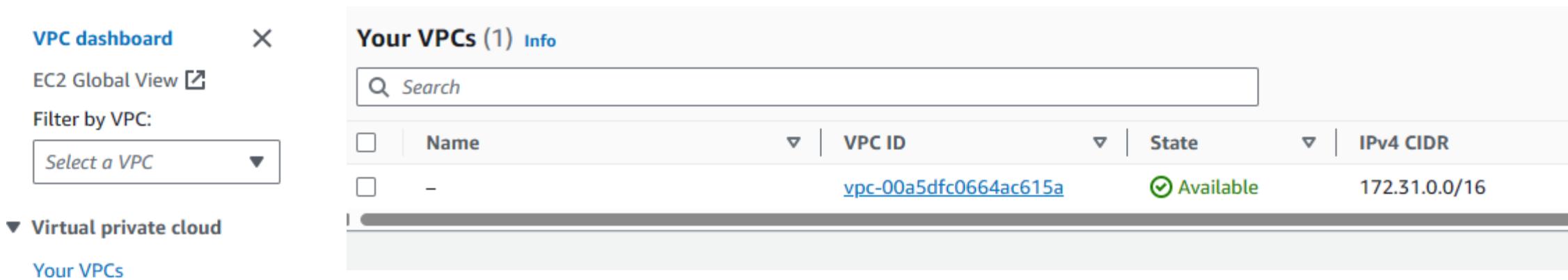
<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	Port range	Destination	Description
<input type="checkbox"/>	-	sgr-0e3ef92dce34a8e12	IPv4	All traffic	All	All	0.0.0.0/0	-

1. EJECUCIÓN INSTANCIAS EC2

1.3 Comprobación de VPC y Subredes

En la consola VPC (Services → Networking & Content Delivery → VPC) comprobar el direccionamiento IPv4 asignado a nuestra VPC y a las subredes definidas (una por cada zona de disponibilidad de la Región). Consultar también la tabla de rutas existente y el nombre del router por defecto en la VPC existente.

Comprobar direccionamiento de mi VPC



The screenshot shows the AWS VPC Dashboard. On the left, there's a sidebar with 'VPC dashboard' (selected), 'EC2 Global View' (with a refresh icon), and a dropdown 'Filter by VPC:' containing 'Select a VPC'. Below that is a section for 'Virtual private cloud' with 'Your VPCs' (selected). The main area is titled 'Your VPCs (1)' with an 'Info' link. It features a search bar and a table with columns: Name, VPC ID, State, and IPv4 CIDR. The table contains one row: Name '-' (checkbox), VPC ID [vpc-00a5dfc0664ac615a](#), State Available (checkbox checked), and IPv4 CIDR 172.31.0.0/16.

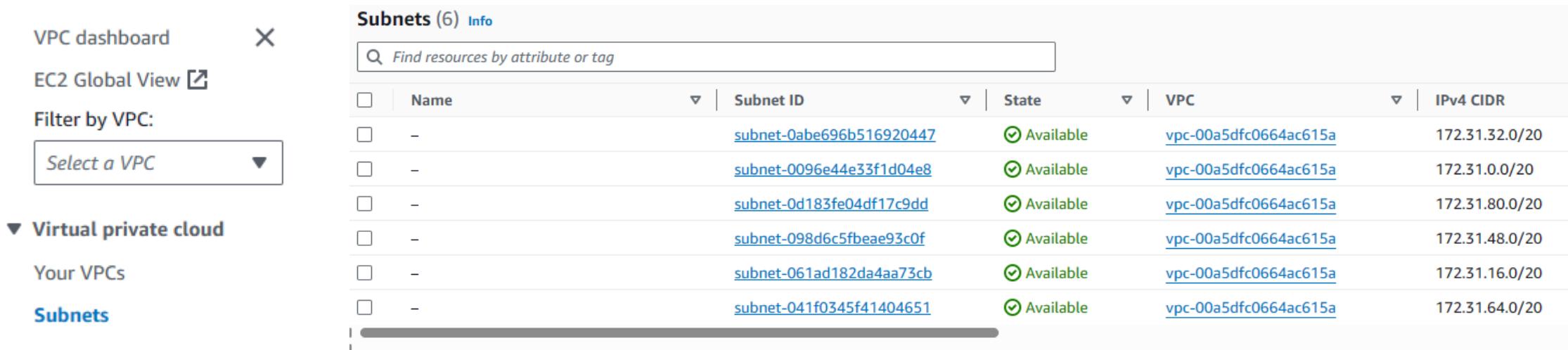
	Name	VPC ID	State	IPv4 CIDR
<input type="checkbox"/>	-	vpc-00a5dfc0664ac615a	Available <input checked="" type="checkbox"/>	172.31.0.0/16

1. EJECUCIÓN INSTANCIAS EC2

1.3 Comprobación de VPC y Subredes

En la consola VPC (Services → Networking & Content Delivery → VPC) comprobar el direccionamiento IPv4 asignado a nuestra VPC y a las subredes definidas (una por cada zona de disponibilidad de la Región). Consultar también la tabla de rutas existente y el nombre del router por defecto en la VPC existente.

Comprobar subredes definidas



The screenshot shows the AWS VPC dashboard with the 'Subnets' section selected. The table lists six subnets, each associated with a specific VPC and a range of IPv4 addresses. All subnets are currently available.

Subnets (6) Info					
<input type="text"/> Find resources by attribute or tag					
	Name	Subnet ID	State	VPC	IPv4 CIDR
<input type="checkbox"/>	-	subnet-0abe696b516920447	Available	vpc-00a5dfc0664ac615a	172.31.32.0/20
<input type="checkbox"/>	-	subnet-0096e44e33f1d04e8	Available	vpc-00a5dfc0664ac615a	172.31.0.0/20
<input type="checkbox"/>	-	subnet-0d183fe04df17c9dd	Available	vpc-00a5dfc0664ac615a	172.31.80.0/20
<input type="checkbox"/>	-	subnet-098d6c5fbeae93c0f	Available	vpc-00a5dfc0664ac615a	172.31.48.0/20
<input type="checkbox"/>	-	subnet-061ad182da4aa73cb	Available	vpc-00a5dfc0664ac615a	172.31.16.0/20
<input type="checkbox"/>	-	subnet-041f0345f41404651	Available	vpc-00a5dfc0664ac615a	172.31.64.0/20

1. EJECUCIÓN INSTANCIAS EC2

1.3 Comprobación de VPC y Subredes

En la consola VPC (Services → Networking & Content Delivery → VPC) comprobar el direccionamiento IPv4 asignado a nuestra VPC y a las subredes definidas (una por cada zona de disponibilidad de la Región). Consultar también la tabla de rutas existente y el nombre del router por defecto en la VPC existente.

Tabla de rutas existentes

The screenshot shows the AWS VPC Route Tables page. On the left, there's a sidebar with 'VPC dashboard' and 'EC2 Global View'. Under 'Virtual private cloud', it says 'Your VPCs' and 'Route tables'. A dropdown menu 'Select a VPC' is open. The main area shows a table of existing route tables:

Name	Route table ID	Explicit subnet assoc...	Edge associations	Main	VPC	Owner ID
-	rtb-02f32a46096dd1164	-	-	Yes	vpc-00a5dfc0664ac615a	958486390477

Below this, a 'Details' section shows the route table's configuration:

Route table ID rtb-02f32a46096dd1164	Main <input type="checkbox"/> Yes	Explicit subnet associations -
VPC vpc-00a5dfc0664ac615a	Owner ID 958486390477	

At the bottom, there are tabs for 'Routes', 'Subnet associations', 'Edge associations', 'Route propagation', and 'Tags'. The 'Routes' tab is selected, showing two routes:

Destination	Target	Status
0.0.0.0/0	igw-0f67c8b7b5fb5bb82	Active
172.31.0.0/16	local	Active

A red arrow points from the text 'Router por defecto' to the target column of the first route entry.

1. EJECUCIÓN INSTANCIAS EC2

1.4 Lanzamiento de Instancia PruebasWeb

Nuevamente en la consola EC2 lanzar una primera instancia PruebasWeb con una Amazon Linux AMI y tipo t2.micro (forma parte de la capa gratuita), con almacenamiento EBS de 8 GB (el contenido es persistente, aunque podemos eliminarlo automáticamente al finalizar la instancia). Arrancaremos la instancia en una de las redes “públicas” existentes (son las subredes predeterminadas, y existe una por zona de disponibilidad), y tendrá asociada un IP pública (elástica). Usará el grupo de seguridad SSH_HTTP_Any y la pública de ClavesPractica. Lanzar la instancia. Tras un par de minutos la máquina estará operativa.

Services → Compute → EC2 → Instances → Launch Instances



Amazon Machine Image (AMI)

Amazon Linux 2023 AMI
ami-051f8a213df8bc089 (64-bit (x86), uefi-preferred) / ami-05adadbbe8cf9fb48 (64-bit)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.4.20240401.1 x86_64 HVM kernel-6.1

Architecture

64-bit (x86) ▾

Boot mode

uefi-preferred

AMI ID

ami-051f8a213df8bc089

The screenshot shows the 'Code' section of the Lambda function configuration. It displays the ARN of the Lambda function and the S3 bucket and key for the uploaded zip file. Below this, there are sections for 'Handler' (lambda_function.lambda_handler), 'Runtime' (Python 3.9), 'Memory limit' (128 MB), 'Timeout' (3 seconds), and 'Environment variables'. A large 'Create function' button is at the bottom.

The screenshot shows the 'Configuration' section of the Lambda function configuration. It includes sections for 'Lambda function' (Function name: PruebasWeb, Description: PruebasWeb), 'Function settings' (Memory: 128 MB, Timeout: 3 seconds, Role: arn:aws:iam::123456789012:role/lambdaBasicExecutionRole), 'Logs' (CloudWatch Logs Log group: /aws/lambda/PruebasWeb), and 'Metrics' (CloudWatch Metrics Metric prefix: PruebasWeb). A large 'Save changes' button is at the bottom.

1. EJECUCIÓN INSTANCIAS EC2

1.4 Lanzamiento de Instancia PruebasWeb

Nuevamente en la consola EC2 lanzar una primera instancia PruebasWeb con una Amazon Linux AMI y tipo t2.micro (forma parte de la capa gratuita), con almacenamiento EBS de 8 GB (el contenido es persistente, aunque podemos eliminarlo automáticamente al finalizar la instancia). Arrancaremos la instancia en una de las redes “públicas” existentes (son las subredes predeterminadas, y existe una por zona de disponibilidad), y tendrá asociada un IP pública (elástica). Usará el grupo de seguridad SSH_HTTP_Any y la pública de ClavesPractica. Lanzar la instancia. Tras un par de minutos la máquina estará operativa.

Services → Compute → EC2 → Instances → Launch Instances



Amazon Machine Image (AMI)

Amazon Linux 2023 AMI
ami-051f8a213df8bc089 (64-bit (x86), uefi-preferred) / ami-05adadbbe8cf9fb48 (64-bit)
Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Amazon Linux 2023 AMI 2023.4.20240401.1 x86_64 HVM kernel-6.1

Architecture

64-bit (x86)

Boot mode

uefi-preferred

AMI ID

ami-051f8a213df8bc089

The screenshot shows the 'Code' section of the AWS Lambda function configuration page. It displays the ARN of the Lambda function and the S3 bucket and key for the uploaded code. Below this, there are sections for 'Handler' (lambda_function.lambda_handler), 'Runtime' (Python 3.9), 'Memory limit' (128 MB), 'Timeout' (3 seconds), and 'Environment variables'. A large 'Create function' button is at the bottom.

The screenshot shows the 'Configuration' section of the AWS Lambda function configuration page. It includes sections for 'Function name' (PruebasWeb), 'Function description' (PruebasWeb), 'Function runtime' (Python 3.9), 'Memory limit' (128 MB), 'Timeout' (3 seconds), and 'Environment variables'. A large 'Create function' button is at the bottom.

1. EJECUCIÓN INSTANCIAS EC2

1.4 Lanzamiento de Instancia PruebasWeb

Nuevamente en la consola EC2 lanzar una primera instancia PruebasWeb con una Amazon Linux AMI y tipo t2.micro (forma parte de la capa gratuita), con almacenamiento EBS de 8 GB (el contenido es persistente, aunque podemos eliminarlo automáticamente al finalizar la instancia). Arrancaremos la instancia en una de las redes “públicas” existentes (son las subredes predeterminadas, y existe una por zona de disponibilidad), y tendrá asociada un IP pública (elástica). Usará el grupo de seguridad SSH_HTTP_Any y la pública de ClavesPractica. Lanzar la instancia. Tras un par de minutos la máquina estará operativa.

Success
Successfully initiated launch of instance ([i-0c8e1e6db4a1f42cb](#))

Instances (1) Info										
C Connect Instance state ▾ Actions ▾ Launch ins...										
<input type="text"/> Find Instance by attribute or tag (case-sensitive)										
All states ▾										
Clear filters										
<input type="checkbox"/>	Name ✎	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Public IPv4 ...
<input type="checkbox"/>	PruebasWeb	i-0c8e1e6db4a1f42cb	Running 🕒 ⟳	t2.micro	Initializing View alarms +	us-east-1c	ec2-107-20-114-189.co...	107.20.114.189		

1. EJECUCIÓN INSTANCIAS EC2

1.4 Lanzamiento de Instancia PruebasWeb

Nuevamente en la consola EC2 lanzar una primera instancia PruebasWeb con una Amazon Linux AMI y tipo t2.micro (forma parte de la capa gratuita), con almacenamiento EBS de 8 GB (el contenido es persistente, aunque podemos eliminarlo automáticamente al finalizar la instancia). Arrancaremos la instancia en una de las redes “públicas” existentes (son las subredes predeterminadas, y existe una por zona de disponibilidad), y tendrá asociada un IP pública (elástica). Usará el grupo de seguridad SSH_HTTP_Any y la pública de ClavesPractica. Lanzar la instancia. Tras un par de minutos la máquina estará operativa.

Instance: i-0c8e1e6db4a1f42cb (PruebasWeb)

=

Details | Status and alarms New | Monitoring | Security | Networking | Storage | Tags

▼ Instance summary Info

Instance ID i-0c8e1e6db4a1f42cb (PruebasWeb)	Public IPv4 address 107.20.114.189 [open address]	Private IPv4 addresses 172.31.17.210
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-107-20-114-189.compute-1.amazonaws.com [open address]
Hostname type IP name: ip-172-31-17-210.ec2.internal	Private IP DNS name (IPv4 only) ip-172-31-17-210.ec2.internal	Elastic IP addresses -
Answer private resource DNS name IPv4 (A)	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto-assigned IP address 107.20.114.189 [Public IP]	VPC ID vpc-00a5dfc0664ac615a	Auto Scaling Group name -
IAM Role -	Subnet ID subnet-061ad182da4aa73cb	

1. EJECUCIÓN INSTANCIAS EC2

1.5 Lanzamiento de Instancia PruebasWeb

Identificar las direcciones IP asignadas (privada y pública), así como los nombres de dominio asociados a la instancia. Usando un cliente SSH y la clave privada descargada abrir una conexión a la instancia. La información de conexión está disponible pulsando en el botón superior Connect (el usuario será ec2-user para la Amazon Linux, aunque este nombre puede cambiar en otras distribuciones). Realizar algunas tareas de mantenimiento y configuración en la máquina virtual: promover a superusuario (sudo su -), comprobar la dirección IP privada asignada y la tabla de encaminamiento, actualizar el SO (yum -y update), instalar el servidor apache (httpd) y configurar su arranque automático. Instalar también el intérprete php, y crear una página de inicio predeterminada (index.php) que nos presentará la dirección IP privada de la máquina virtual. Comprobar que se visualiza la página de inicio con la dirección IP de la instancia accediendo desde un navegador web con la dirección IP pública y el nombre de dominio externo asignado. Instalar también el programa stress, que usaremos en el apartado de auto escalado.

' Network Interfaces (1) [Info](#)

Filter network interfaces						
Interface ID	Description	IPv4 Prefixes	IPv6 Prefixes	Public IPv4 address	Private IPv4 address	Private IPv4 DNS
eni-0436d4c8b604c4005	-	-	-	107.20.114.189	172.31.17.210	ip-172-31-17-210.ec2...

Private IPv4 addresses
[172.31.17.210](#)

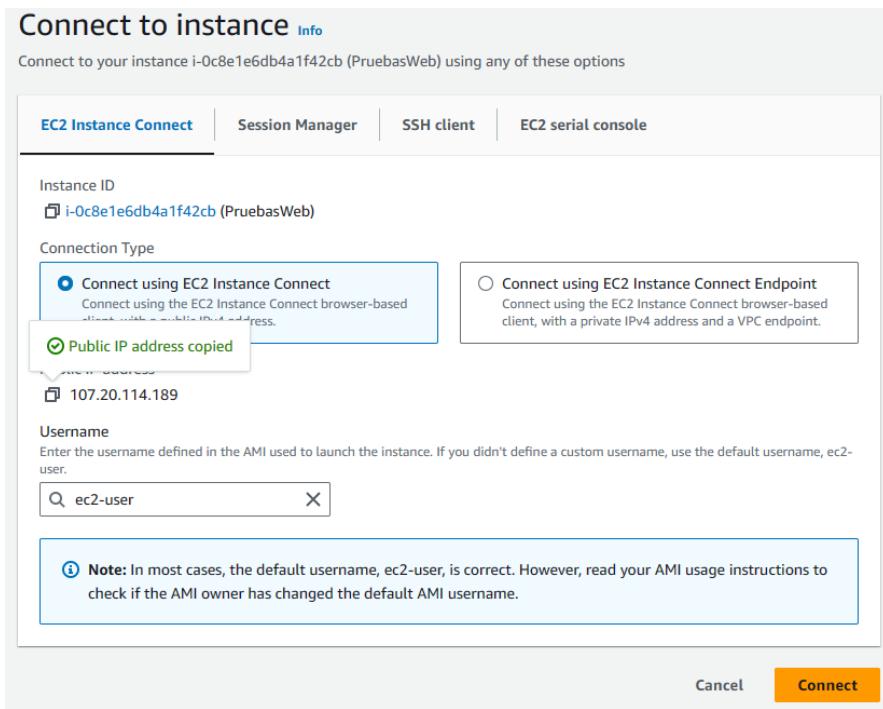
Public IPv4 DNS
[ec2-107-20-114-189.compute-1.amazonaws.com](#) | [open address](#)

Nombre de dominio

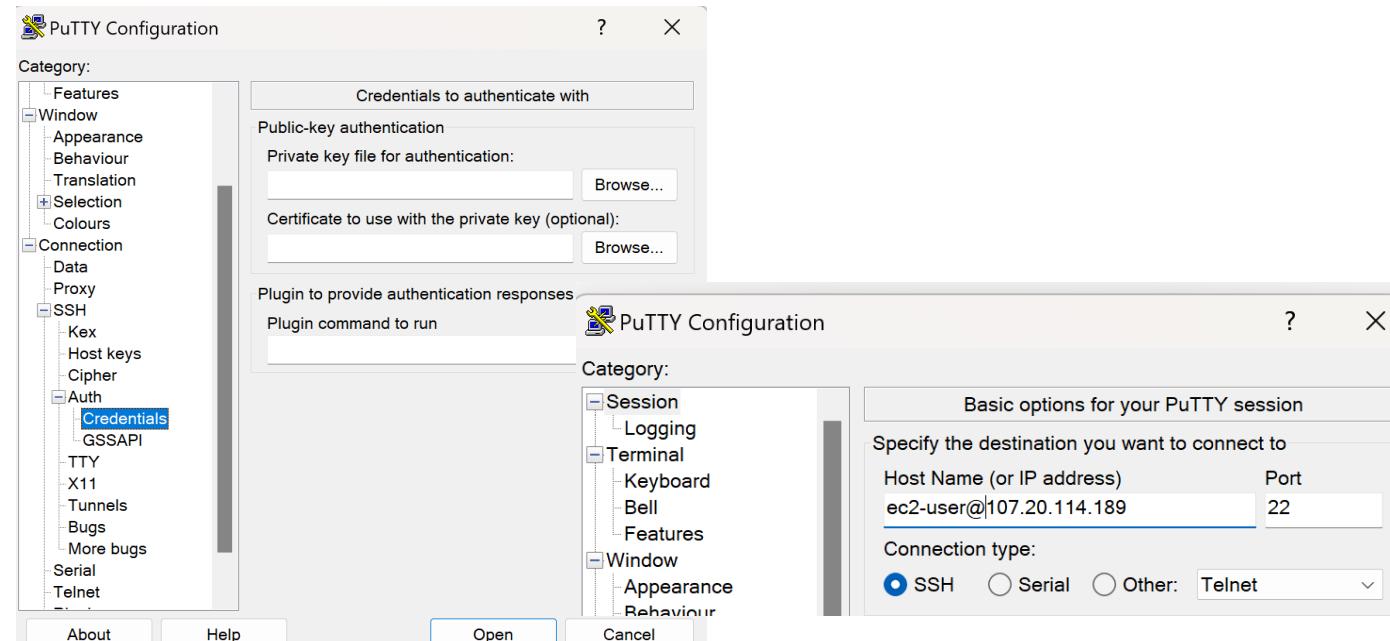
1. EJECUCIÓN INSTANCIAS EC2

1.5 Lanzamiento de Instancia PruebasWeb

Usando un cliente SSH y la clave privada descargada abrir una conexión a la instancia. La información de conexión está disponible pulsando en el botón superior Connect (el usuario será ec2-user para la Amazon Linux, aunque este nombre puede cambiar en otras distribuciones).



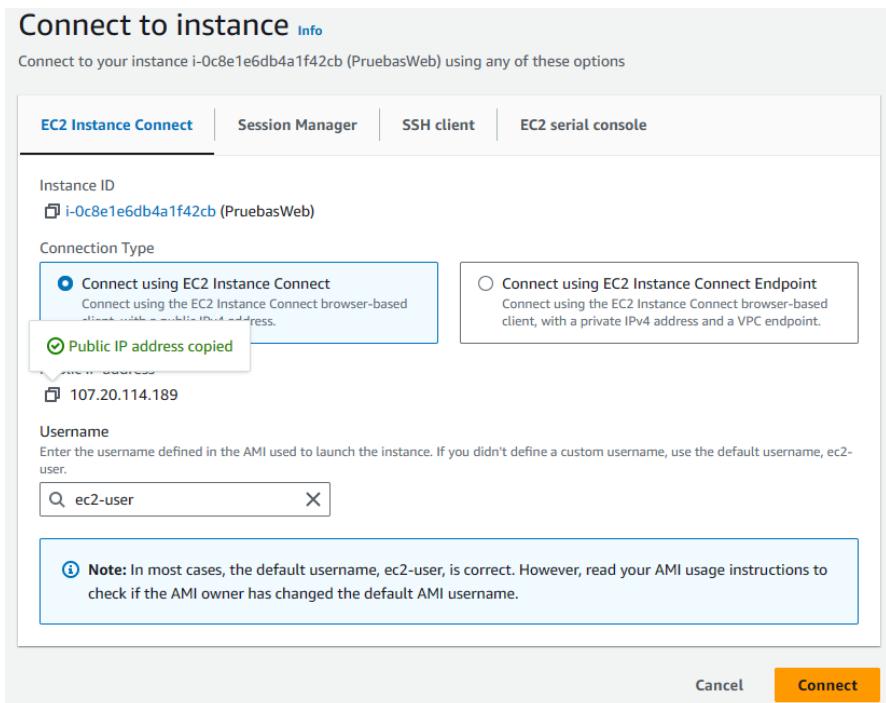
En Putty → SSH → Auth → Credentials → Private Key (subimos archivo ppk)



1. EJECUCIÓN INSTANCIAS EC2

1.5 Lanzamiento de Instancia PruebasWeb

Usando un cliente SSH y la clave privada descargada abrir una conexión a la instancia. La información de conexión está disponible pulsando en el botón superior Connect (el usuario será ec2-user para la Amazon Linux, aunque este nombre puede cambiar en otras distribuciones).



Desde la terminal:

`ssh -i archivo_claves usuario@ip_maquina`

En mi caso:

`ssh -i labsuser.pem ec2-user@107.20.114.189`

1. EJECUCIÓN INSTANCIAS EC2

1.5 Lanzamiento de Instancia PruebasWeb

Realizar algunas tareas de mantenimiento y configuración en la máquina virtual: **promover a superusuario** (`sudo su -`), comprobar la **dirección IP privada asignada** y la **tabla de encaminamiento**, actualizar el SO (`yum -y update`), instalar el servidor apache (`httpd`) y configurar su arranque automático. Instalar también el intérprete php, y crear una página de inicio predeterminada (`index.php`) que nos presentará la dirección IP privada de la máquina virtual. Comprobar que se visualiza la página de inicio con la dirección IP de la instancia accediendo desde un navegador web con la dirección IP pública y el nombre de dominio externo asignado. Instalar también el programa stress, que usaremos en el apartado de auto escalado.

Tabla encaminamiento: `ip routes`

```
default via 172.31.16.1 dev enX0 proto dhcp src 172.31.17.210 metric 512
172.31.0.2 via 172.31.16.1 dev enX0 proto dhcp src 172.31.17.210 metric 512
172.31.16.0/20 dev enX0 proto kernel scope link src 172.31.17.210 metric 512
172.31.16.1 dev enX0 proto dhcp scope link src 172.31.17.210 metric 512
[root@ip-172-31-17-210 ~]#
```

1. EJECUCIÓN INSTANCIAS EC2

1.5 Lanzamiento de Instancia PruebasWeb

Realizar algunas tareas de mantenimiento y configuración en la máquina virtual: promover a superusuario (sudo su -), comprobar la dirección IP privada asignada y la tabla de encaminamiento, **actualizar el SO** (yum -y update), **instalar el servidor apache (httpd)** y **configurar su arranque automático**. Instalar también el intérprete php, y crear una página de inicio predeterminada (index.php) que nos presentará la dirección IP privada de la máquina virtual. Comprobar que se visualiza la página de inicio con la dirección IP de la instancia accediendo desde un navegador web con la dirección IP pública y el nombre de dominio externo asignado. Instalar también el programa stress, que usaremos en el apartado de auto escalado.

```
[root@ip-172-31-17-210 ~]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr
/lib/systemd/system/httpd.service.
[root@ip-172-31-17-210 ~]# systemctl is-enabled httpd
enabled
1 [root@ip-172-31-17-210 ~]#
```

```
172.31.10.1 dev enx0 proto dhcp scope link src ...
[root@ip-172-31-17-210 ~]# yum -y update
Last metadata expiration check: 1:12:30 ago on Sat Apr 13 08:26:48 2024.
Dependencies resolved.
Nothing to do.
Complete!
```

```
[root@ip-172-31-17-210 ~]# yum install httpd
Last metadata expiration check: 1:13:00 ago on Sat Apr 13 08:26:48 2024.
Dependencies resolved.
=====
 Package           Arch      Version          Repository      Size
=====
Installing:
 httpd            x86_64    2.4.58-1.amzn2023   amazonlinux   47 k
Installing dependencies:
 apr              x86_64    1.7.2-2.amzn2023.0.2   amazonlinux   129 k
 apr-util         x86_64    1.6.3-1.amzn2023.0.1   amazonlinux   98 k
 generic-logos-httpd noarch   18.0.0-12.amzn2023.0.3   amazonlinux   19 k
 httpd-core       x86_64    2.4.58-1.amzn2023   amazonlinux   1.4 M
 httpd-filesystem noarch   2.4.58-1.amzn2023   amazonlinux   14 k
 httpd-tools       x86_64    2.4.58-1.amzn2023   amazonlinux   81 k
 libbrotli        x86_64    1.0.9-4.amzn2023.0.2   amazonlinux   315 k
 mailcap          noarch   2.1.49-3.amzn2023.0.3   amazonlinux   33 k
Installing weak dependencies:
 apr-util-openssl x86_64    1.6.3-1.amzn2023.0.1   amazonlinux   17 k
 mod_http2        x86_64    2.0.11-2.amzn2023   amazonlinux   150 k
 mod_lua          x86_64    2.4.58-1.amzn2023   amazonlinux   61 k
=====
Transaction Summary
=====
Install 12 Packages

Total download size: 2.3 M
Installed size: 6.9 M
Is this ok [y/N]:
```

1. EJECUCIÓN INSTANCIAS EC2

1.5 Lanzamiento de Instancia PruebasWeb

Realizar algunas tareas de mantenimiento y configuración en la máquina virtual: promover a superusuario (sudo su -), comprobar la dirección IP privada asignada y la tabla de encaminamiento, actualizar el SO (yum -y update), instalar el servidor apache (httpd) y configurar su arranque automático.

Instalar también el intérprete php, y crear una página de inicio predeterminada (index.php) que nos presentará la dirección IP privada de la máquina virtual. Comprobar que se visualiza la página de inicio con la dirección IP de la instancia accediendo desde un navegador web con la dirección IP pública y el nombre de dominio externo asignado. Instalar también el programa stress, que usaremos en el apartado de auto escalado.

Yum install php

Vim /var/www/html/index.php

```
<?php  
$ip_privada = $_SERVER['SERVER_ADDR'];  
echo "La dirección IP privada de esta instancia es: $ip_privada";  
?>  
|
```

```
[root@ip-172-31-17-210 ~]# yum install php  
Last metadata expiration check: 1:18:46 ago on Sat Apr 13 08:26:44 UTC 2019  
Dependencies resolved.  
=====  
 Package           Architecture   Version  
=====  
Installing:  
  php8.2           x86_64        8.2.15-1.amzn2  
Installing dependencies:  
  libsodium         x86_64        1.0.19-4.amzn2  
  libxml2          x86_64        1.1.34-5.amzn2  
  nginx-filesystem noarch       1:1.24.0-1.amzn2  
  php8.2-cli        x86_64        8.2.15-1.amzn2  
  php8.2-common     x86_64        8.2.15-1.amzn2  
  php8.2-process    x86_64        8.2.15-1.amzn2  
  php8.2-xml        x86_64        8.2.15-1.amzn2  
Installing weak dependencies:  
  php8.2-fpm        x86_64        8.2.15-1.amzn2  
  php8.2-mbstring   x86_64        8.2.15-1.amzn2  
  php8.2-opcache    x86_64        8.2.15-1.amzn2  
  php8.2-pdo         x86_64        8.2.15-1.amzn2  
  php8.2-sodium     x86_64        8.2.15-1.amzn2  
=====  
 Transaction Summary  
=====  
 Install 13 Packages  
=====  
 Total download size: 7.8 M  
 Installed size: 37 M  
 Is this ok [y/N]: |
```

1. EJECUCIÓN INSTANCIAS EC2

1.5 Lanzamiento de Instancia PruebasWeb

Realizar algunas tareas de mantenimiento y configuración en la máquina virtual: promover a superusuario (sudo su -), comprobar la dirección IP privada asignada y la tabla de encaminamiento, actualizar el SO (yum -y update), instalar el servidor apache (httpd) y configurar su arranque automático. Instalar también el intérprete php, y crear una página de inicio predeterminada (index.php) que nos presentará la dirección IP privada de la máquina virtual. **Comprobar que se visualiza la página de inicio con la dirección IP de la instancia accediendo desde un navegador web con la dirección IP pública y el nombre de dominio externo asignado. Instalar también el programa stress, que usaremos en el apartado de auto escalado.**

La IP Pública actual (tuve que apagar la instancia): 54.91.132.15
Dominio Externo: ec2-54-91-132-15.compute-1.amazonaws.com

Nota: Tuve que permitir el acceso por https en el grupo de seguridad porque mi navegador no usa el protocolo HTTP sino HTTPS

```
[root@ip-172-31-17-210 ~]# yum install stress
Last metadata expiration check: 1:42:21 ago on Sat Apr 13 08:26:48 2024.
Dependencies resolved.
=====
 Package           Architecture      Version       Repository      Size
=====
 Installing:
  stress            x86_64          1.0.4-28.amzn2023.0.2    amazonlinux   37 k
Transaction Summary
=====
 Install 1 Package
```



Descarga de stress

1. EJECUCIÓN INSTANCIAS EC2

1.6 Efecto de Reinicio y Detención de la Instancia

Comprobar el efecto sobre las direcciones IP pública y privada de un reinicio de la máquina (shutdown -r now) y una detención (shutdown -h now, equivalente a Actions → Instance Settings → Stop desde la consola EC2) y arranque posterior (Actions → Instance Settings → Start). Nota: verificar también que el servidor web se inicia automáticamente.

```
[root@ip-172-31-17-210 ~]# shutdown -r now
Broadcast message from root@ip-172-31-17-210.ec2.internal on pts/1 (Sat 2024-04-13 10:11:39 UTC):
The system will reboot now!
[root@ip-172-31-17-210 ~]# Connection to 54.91.132.15 closed by remote host.
Connection to 54.91.132.15 closed.
C:\Users\ppere\Desktop\AdminSist\Practicas\PR6_aws>
```

shutdown -r now → reinicia el sistema, las IPs siguen siendo las mismas

Public IPv4 address
54.91.132.15 |open address ↗

Instance state
Running

Private IP DNS name (IPv4 only)
ip-172-31-17-210.ec2.internal

Private IPv4 addresses
172.31.17.210

Public IPv4 DNS
ec2-54-91-132-15.compute-1.amazonaws.com |open address ↗

1. EJECUCIÓN INSTANCIAS EC2

1.6 Efecto de Reinicio y Detención de la Instancia

Comprobar el efecto sobre las direcciones IP pública y privada de un reinicio de la máquina (shutdown -r now) y una detención (shutdown -h now, equivalente a Actions → Instance Settings → Stop desde la consola EC2) y arranque posterior (Actions → Instance Settings → Start). Nota: verificar también que el servidor web se inicia automáticamente.

```
[root@ip-172-31-17-210 ~]# shutdown -h now
Broadcast message from root@ip-172-31-17-210.ec2.internal on pts/1 (Sat 2024-04-13 10:14:47 UTC):
The system will power off now!
[root@ip-172-31-17-210 ~]# Connection to 54.91.132.15 closed by remote host.
Connection to 54.91.132.15 closed.
```

shutdown –h now → Apaga el sistema, la IP pública cambia al volverla a iniciar pero la IP privada se mantiene

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
PruebasWeb	i-0c8e1e6db4a1f42cb	Stopping	t2.micro	-	View alarms +	us-east-1c	ec2-54-91-132-15.amazonaws.com...	54.91.132.15

Instance State >> Start Instance

Public IPv4 address
[34.228.165.29](#) | [open address](#)

Instance state
✓ Running

Private IP DNS name (IPv4 only)
[ip-172-31-17-210.ec2.internal](#)

Private IPv4 addresses
[172.31.17.210](#)

Public IPv4 DNS
[ec2-34-228-165-29.compute-1.amazonaws.com](#) | [open address](#)

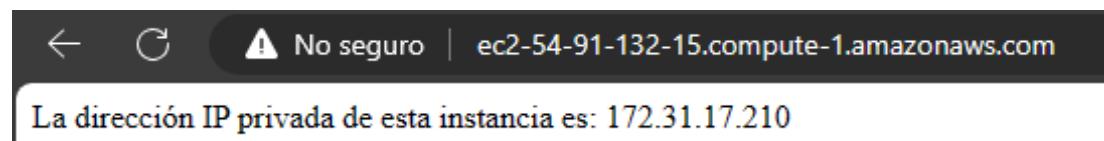
1. EJECUCIÓN INSTANCIAS EC2

1.6 Efecto de Reinicio y Detención de la Instancia

Comprobar el efecto sobre las direcciones IP pública y privada de un reinicio de la máquina (shutdown -r now) y una detención (shutdown -h now, equivalente a Actions → Instance Settings → Stop desde la consola EC2) y arranque posterior (Actions → Instance Settings → Start).
Nota: verificar también que el servidor web se inicia automáticamente.

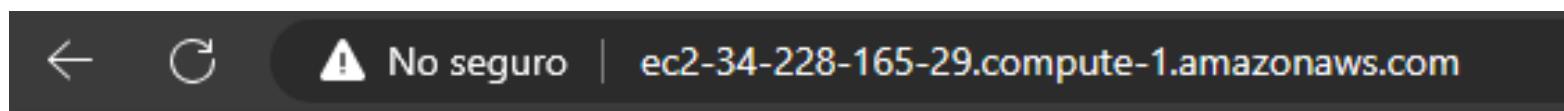
Verificar que el servidor web se iniciar automáticamente:

shutdown -r now



Verificar que el servidor web se iniciar automáticamente:

shutdown -h now



La dirección IP privada de esta instancia es: 172.31.17.210

1. EJECUCIÓN INSTANCIAS EC2

1.7 Generación de Imagen de la Instancia

Generar una imagen de la instancia con nombre ServidorWeb (Actions → Image → Create Image) con los valores por defecto. Podemos comprobar que se genera una nueva imagen privada (sección Images → AMIs). Por defecto, para generar la imagen AMI la instancia se reinicia. Cuando necesitemos un servidor Web podremos lanzar una instancia de esta imagen. Nota: esta AMI creada la mantendremos hasta el final de la práctica.

Create image Info

An image (also referred to as an AMI) defines the programs and settings for your instances.

Instance ID

Image name

Maximum 127 characters. Can't be modified after creation.

Image description - optional

Maximum 255 characters

▼ Images

AMIs

AMI Catalog

Amazon Machine Images (AMIs) (1) info

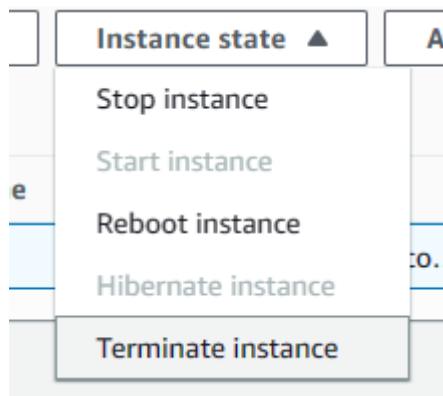
<input type="checkbox"/>	Name <small>edit</small>	AMI name	AMI ID	Source	Owner	Visibility
<input type="checkbox"/>	ServidorWeb	ami-0f71cdad87729a0b5	958486390477/ServidorWeb	958486390477	958486390477	Private

Nota: No soporta tildes

1. EJECUCIÓN INSTANCIAS EC2

1.8 Terminación de la Instancia

Cuando concluya la generación de la imagen, terminar la ejecución de la instancia PruebasWeb (Actions → Instance Settings → Terminate). Podemos comprobar que también se elimina el volumen EBS de la instancia, pero no la imagen creada (y el snapshot asociado).



En mi caso se termina la instancia con Instances → Instance State → Terminate Instance

Name	Instance ID	Instance state
PruebasWeb	i-0c8e1e6db4a1f42cb	Terminated
AMI name	AMI ID	
ServidorWeb	ami-0f71cdad87729a0b5	

La imagen “ServidorWeb” no se ha borrado

Se ha eliminado el volumen EBS: Elastic Block Storage→ Volumes

Volumes Info									
<input type="text"/> Search									
	Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot		
You currently have no volumes in this region									

ÍNDICE

1. Ejecución de Instancias EC2

- 1.1 Acceso a la Consola y Creación de Claves
- 1.2 Creación de Grupo de Seguridad
- 1.3 Comprobación de VPC y Subredes
- 1.4 Lanzamiento de Instancia PruebasWeb
- 1.5 Configuración de la Instancia y Tareas de Mantenimiento
- 1.6 Efecto de Reinicio y Detención de la Instancia
- 1.7 Generación de Imagen de la Instancia
- 1.8 Terminación de la Instancia

2. Balanceador de Carga ELB (Elastic Load Balancer)

- 2.1 Lanzamiento de Instancias y Creación de Grupo de Seguridad
- 2.2 Creación de Grupo de Destinatarios
- 2.3 Creación de Balanceador de Carga
- 2.4 Pruebas de Acceso y Balanceo
- 2.5 Acceso por SSH a Instancias Internas
- 2.6 Terminación de Instancias y Recursos Asociados

3. Subredes Públicas/Privadas y NAT Gateway

- 3.1 Creación de Subredes y Lanzamiento de Instancias
- 3.2 Configuración de NAT Gateway y Tablas de Rutas
- 3.3 Configuración de Network ACLs
- 3.4 Terminación de Instancias, NAT Gateway y Recursos Asociados

4. Almacenamiento S3

- 4.1 Creación de Bucket S3 y Subida de Archivos
- 4.2 Configuración para Hosting Web Estático
- 4.3 Pruebas de Acceso y Descarga de Archivos
- 4.4 Eliminación del Bucket

5. Autoescalado para Aplicaciones Web

- 5.1 Creación de Grupo de Destinatarios y Balanceador
- 5.2 Creación de Plantilla de Lanzamiento y Grupo de Autoescalado
- 5.3 Configuración de Escalado Automático
- 5.4 Pruebas de Funcionamiento del Escalado
- 5.5 Eliminación de Recursos de Autoescalado

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.1 Lanzamiento de Instancias y Creación de Grupo de Seguridad

En la consola de computación (Services → Compute → EC2) lanzar dos instancias t2.micro usando la imagen ServidorWeb creada en el apartado anterior (ServidorWeb1 y ServidorWeb2). Las instancias se ejecutarán en dos zonas de disponibilidad distintas (a y b), y sólo tendrán asociada una IP privada (no usaremos direcciones elásticas). Crearemos un nuevo grupo de seguridad, (SSH_HTTP_Internal), con acceso a los servicios SSH y HTTP, pero sólo desde la red VPC. Por último, inyectaremos nuestra pareja de claves (ClavesPractica) en cada instancia, aunque no vamos a poder alcanzar las instancias desde el exterior.

Creamos el grupo de seguridad SSH_HTTP_Internal → Reglas de entrada: SSH & HTTPS , source: VPC

The screenshot shows the AWS Management Console interface for creating a security group named 'SSH_HTTP_Internal'. On the left, there's a sidebar titled 'VPC Información' showing a single VPC entry: 'vpc-00a5dfc0664ac615a'. The main area is titled 'Reglas de entrada' (Inbound Rules) and lists three rules:

Tipo	Protocolo	Intervalo de puertos	Origen
SSH	TCP	22	Personaliz... 172.131.0.0/16
HTTP	TCP	80	Personaliz... 172.131.0.0/16
HTTPS	TCP	443	Personaliz... 172.131.0.0/16

Each rule has a search bar next to its target IP range, and the first two rows have their ranges highlighted in yellow.

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.1 Lanzamiento de Instancias y Creación de Grupo de Seguridad

En la consola de computación (Services → Compute → EC2) lanzar dos instancias t2.micro usando la imagen ServidorWeb creada en el apartado anterior (ServidorWeb1 y ServidorWeb2). Las instancias se ejecutarán en dos zonas de disponibilidad distintas (a y b), y sólo tendrán asociada una IP privada (no usaremos direcciones elásticas). Crearemos un nuevo grupo de seguridad, (SSH_HTTP_Internal), con acceso a los servicios SSH y HTTP, pero sólo desde la red VPC. Por último, inyectaremos nuestra pareja de claves (ClavesPractica) en cada instancia, aunque no vamos a poder alcanzar las instancias desde el exterior.

Lanzamos Instancias ServidorWeb1 y ServidorWeb2 → seguimos los mismos pasos que en el punto 1

The screenshot shows the AWS EC2 Instances launch wizard. On the left, there's a sidebar with 'Mis AMI' selected. The main area has two tabs: 'De mi propiedad' (selected) and 'Compartido conmigo'. Below these tabs, there's a search bar labeled 'Buscar más AMI' and a note about including AMIs from AWS Marketplace and the community. The main configuration section includes:

- Número de instancias:** 1
- Imagen de software (AMI):** ServidorWeb de la práctica 6 d...[más información](#)
ami-0f71cdad87729a0b5
- Tipo de servidor virtual (tipo de instancia):** t2.micro
- Firewall (grupo de seguridad):** SSH_HTTP_Internal
- Almacenamiento (volúmenes):** Volúmenes: 1 (8 GiB)

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.1 Lanzamiento de Instancias y Creación de Grupo de Seguridad

En la consola de computación (Services → Compute → EC2) lanzar dos instancias t2.micro usando la imagen ServidorWeb creada en el apartado anterior (ServidorWeb1 y ServidorWeb2). Las instancias se ejecutarán en dos **zonas de disponibilidad distintas (a y b)**, y sólo tendrán asociada una IP privada (no usaremos direcciones elásticas). Crearemos un nuevo grupo de seguridad, (SSH_HTTP_Internal), con acceso a los servicios SSH y HTTP, pero sólo desde la red VPC. Por último, inyectaremos nuestra pareja de claves (ClavesPractica) en cada instancia, aunque no vamos a poder alcanzar las instancias desde el exterior.

Deshabilitamos IP Pública (Config. Red → Editar)

The screenshot shows the 'Configuraciones de red' (Network Settings) section of the EC2 instance creation wizard. Under 'VPC', the VPC is set to 'vpc-00a5dfc0664ac615a' (CIDR: 172.31.0.0/16). In the 'Subred' (Subnet) dropdown, 'Sin preferencias' (No preferences) is selected. Under 'Asignar automáticamente la IP pública' (Assign Public IP automatically), the option 'Desactivar' (Disable) is chosen. A large 'C' icon is positioned to the right of the subnet dropdown.

Elegimos la zona de disponibilidad en el apartado de subredes

The screenshot shows a list of subnets in a VPC. The first subnet listed is 'subnet-0abe696b516920447' (VPC: vpc-00a5dfc0664ac615a, Propietario: 958486390477, Zona de disponibilidad: us-east-1d, Direcciones IP disponibles: 4091, CIDR: 172.31.32.0/20). Other subnets listed include 'subnet-0096e44e33f1d04e8', 'subnet-0d183fe04df17c9dd', 'subnet-098d6c5fbeae93cf0f', 'subnet-061ad182da4aa73cb', and 'subnet-041f0345f41404651'. A large 'C' icon is positioned to the right of the subnet list. At the bottom, there is a 'Sin preferencias' (No preferences) button.

Subnet ID	VPC	Propietario	Zona de disponibilidad	Direcciones IP disponibles	CIDR
subnet-0abe696b516920447	vpc-00a5dfc0664ac615a	Propietario: 958486390477	Zona de disponibilidad: us-east-1d	Direcciones IP disponibles: 4091	CIDR: 172.31.32.0/20
subnet-0096e44e33f1d04e8	vpc-00a5dfc0664ac615a	Propietario: 958486390477	Zona de disponibilidad: us-east-1a	Direcciones IP disponibles: 4091	CIDR: 172.31.0.0/20
subnet-0d183fe04df17c9dd	vpc-00a5dfc0664ac615a	Propietario: 958486390477	Zona de disponibilidad: us-east-1b	Direcciones IP disponibles: 4091	CIDR: 172.31.80.0/20
subnet-098d6c5fbeae93cf0f	vpc-00a5dfc0664ac615a	Propietario: 958486390477	Zona de disponibilidad: us-east-1e	Direcciones IP disponibles: 4091	CIDR: 172.31.48.0/20
subnet-061ad182da4aa73cb	vpc-00a5dfc0664ac615a	Propietario: 958486390477	Zona de disponibilidad: us-east-1c	Direcciones IP disponibles: 4091	CIDR: 172.31.16.0/20
subnet-041f0345f41404651	vpc-00a5dfc0664ac615a	Propietario: 958486390477	Zona de disponibilidad: us-east-1f	Direcciones IP disponibles: 4091	CIDR: 172.31.64.0/20

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.1 Lanzamiento de Instancias y Creación de Grupo de Seguridad

En la consola de computación (Services → Compute → EC2) lanzar dos instancias t2.micro usando la imagen ServidorWeb creada en el apartado anterior (ServidorWeb1 y ServidorWeb2). Las instancias se ejecutarán en dos zonas de disponibilidad distintas (a y b), y sólo tendrán asociada una IP privada (no usaremos direcciones elásticas). Crearemos un nuevo grupo de seguridad, (SSH_HTTP_Internal), con acceso a los servicios SSH y HTTP, pero sólo desde la red VPC. Por último, inyectaremos nuestra pareja de claves (ClavesPractica) en cada instancia, aunque no vamos a poder alcanzar las instancias desde el exterior.

<input type="checkbox"/>	ServidorWeb2	i-01bdb47bd05044d25	✓ En ejecución		t2.micro		Ver alarmas +	us-east-1b
<input type="checkbox"/>	ServidorWeb1	i-0c8fff65903491e0e	✓ En ejecución		t2.micro		Ver alarmas +	us-east-1a

Dirección IPv4 pública

-

Estado de la instancia

✓ En ejecución

Dirección IPv4 pública

-

Estado de la instancia

✓ En ejecución

Direcciones IPv4 privadas

172.31.5.177

ServidorWeb1

DNS de IPv4 pública

-

Direcciones IPv4 privadas

172.31.92.51

ServidorWeb2

DNS de IPv4 pública

-

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.2 Creación de Grupo de Destinatarios

Ir a la sección Load Balancing → Target Groups. Crear un nuevo grupo de destinatarios (ServidoresWeb) con el protocolo HTTP (puerto 80). Establecer el check que nos propone el asistente (una consulta a la raíz del servidor). Registrar en el grupo de destinatarios las dos instancias de nuestro servidor Web (ServidorWeb1 y ServidorWeb2).

The screenshot shows the AWS Lambda console interface. On the left, a sidebar menu is open under the 'Load Balancing' section, with 'Target Groups' selected. The main area displays a table for the target group 'ServidoresWeb'. The table includes columns for 'Details', 'Protocol', 'Protocol version', and 'VPC'. Under 'Details', the ARN is listed as arn:aws:elasticloadbalancing:us-east-1:958486390477:targetgroup/ServidoresWeb/558eb8fcabb2120a. The 'Protocol' is set to 'HTTP: 80' and 'Protocol version' to 'HTTP1'. The 'VPC' section shows 'vpc-00a5dfc0664ac615a'. Below this, a summary row shows '2 Total targets' with 0 healthy, 0 unhealthy, 2 unused, 0 initial, and 0 draining targets. A note at the bottom says 'Include as pending below'.

Cuando se añaden las instancias es importante darle a este botón

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.3 Creación de Balanceador de Carga

Ir a la sección Load Balancing → Load Balancers. Crear un balanceador de carga de Aplicación HTTP/HTTPS con nombre Balanceador1, con esquema expuesto a Internet (Internet-facing), sólo para tráfico IPv4 y HTTP (puerto 80/TCP). El balanceador trabajará sobre las dos primeras zonas de disponibilidad (a y b), en las que se encuentran las instancias. Usaremos el grupo de seguridad SSH_HTTP_Any (aunque sólo necesitamos HTTP). Establecer el grupo de destinatarios (ServidoresWeb) con el protocolo HTTP (puerto 80) y fijar el check que nos proponen por defecto (una consulta a la página de inicio). Por último, lanzar el balanceador.

Load balancer types

Application Load Balancer [Info](#)

Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architecture, including microservices and containers.

Create

Network Load Balancer [Info](#)

Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Create

Gateway Load Balancer [Info](#)

Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

Create

Subnet

us-east-1a (use1-az1)
Subnet: subnet-0096e44e33f1d04e8

us-east-1b (use1-az2)
Subnet: subnet-0d183fe04df17c9dd

IPv4 address

Assigned by AWS

Listeners and routing [Info](#)

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP:80

Protocol	Port	Default action	Info
HTTP	: 80	Forward to	ServidorWeb Target type: Instance, IPv4
1-65535		HTTP	

[Create target group](#)

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.3 Creación de Balanceador de Carga

Ir a la sección Load Balancing → Load Balancers. Crear un balanceador de carga de Aplicación HTTP/HTTPS con nombre Balanceador1, con esquema expuesto a Internet (Internet-facing), sólo para tráfico IPv4 y HTTP (puerto 80/TCP). El balanceador trabajará sobre las dos primeras zonas de disponibilidad (a y b), en las que se encuentran las instancias. Usaremos el grupo de seguridad SSH_HTTP_Any (aunque sólo necesitamos HTTP). Establecer el grupo de destinatarios (ServidoresWeb) con el protocolo HTTP (puerto 80) y fijar el check que nos proponen por defecto (una consulta a la página de inicio). Por último, lanzar el balanceador.

Balanceador1			
Actions ▾			
▼ Details			
Load balancer type	Status	VPC	IP address type
Application	Provisioning	vpc-00a5dfc0664ac615a	IPv4
Scheme	Hosted zone	Availability Zones	Date created
Internet-facing	Z35SXDOTRQ7X7K	subnet-0096e44e33f1d04e8 us-east-1a (use1-az1) subnet-0d183fe04df17c9dd us-east-1b (use1-az2)	April 14, 2024, 17:11 (UTC+02:00)
Load balancer ARN	DNS name Info		
am:aws:elasticloadbalancing:us-east-1:958486390477:loadbalancer/app/Balanceador1/ad60fab7d52f9d35	Balanceador1-503309084.us-east-1.elb.amazonaws.com (A Record)		

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.4 Pruebas de Acceso y Balanceo

Lanzar consultas desde el exterior al nombre de dominio asociado al balanceador creado. Debería mostrarse la página de inicio y el balanceo que se está produciendo (mediante las direcciones IP de la página de inicio). Podemos comprobar el estado de las instancias en la sección de Load Balancing → Target Groups.

The image consists of three vertically stacked screenshots from an AWS interface.

- Screenshot 1:** Shows a table with a single row for "Balanceador1". A tooltip "DNS name copied" is shown over the "Name" column header. The row details show "Balanceador1" and "Balanceador1-503309084....".
- Screenshot 2:** Shows a browser window with the address bar containing "balanceador1-236265637.us-east-1.elb.amazonaws.com". Below the address bar, a message says "La dirección IP privada de esta instancia es: 172.31.5.177".
- Screenshot 3:** Shows a browser window with the same address bar. Below the address bar, a message says "La dirección IP privada de esta instancia es: 172.31.81.223".

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.4 Pruebas de Acceso y Balanceo

Lanzar consultas desde el exterior al nombre de dominio asociado al balanceador creado. Debería mostrarse la página de inicio y el balanceo que se está produciendo (mediante las direcciones IP de la página de inicio). Podemos comprobar el estado de las instancias en la sección de Load Balancing → Target Groups.

=

Target group: ServidoresWeb

arn:aws:elasticloadbalancing:us-east-1:958486390477:targetgroup/ServidoresWeb/558eb8fcabb2120a					
Target type Instance		Protocol : Port HTTP: 80	Protocol version HTTP1	VPC vpc-00a5dfc0664ac615a	
IP address type IPv4		Load balancer Balanceador1			
2 Total targets	2 Healthy	0 Unhealthy	0 Unused	0 Initial	0 Draining
	0 Anomalous				
▼ Distribution of targets by Availability Zone (AZ)					
Select values in this table to see corresponding filters applied to the Registered targets table below.					
Last fetched 1 minute					
Zone	Total targets	Healthy	Unhealthy	Unused	Initial
us-east-1a	1	1	0	0	0
us-east-1b	1	1	0	0	0

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.4 Pruebas de Acceso y Balanceo

Targets

Instance ID	Name	Port	Zone	Health status	Health status details	Launch time	Anomaly detection
i-0c8fff65903491e0e	ServidorWeb1	80	us-east-1a	Healthy	-	April 14, 2024, 18:28 (UTC+02:00)	Normal
i-039dfefe288f8576f	ServidorWeb2	80	us-east-1b	Healthy	-	April 14, 2024, 18:28 (UTC+02:00)	Normal

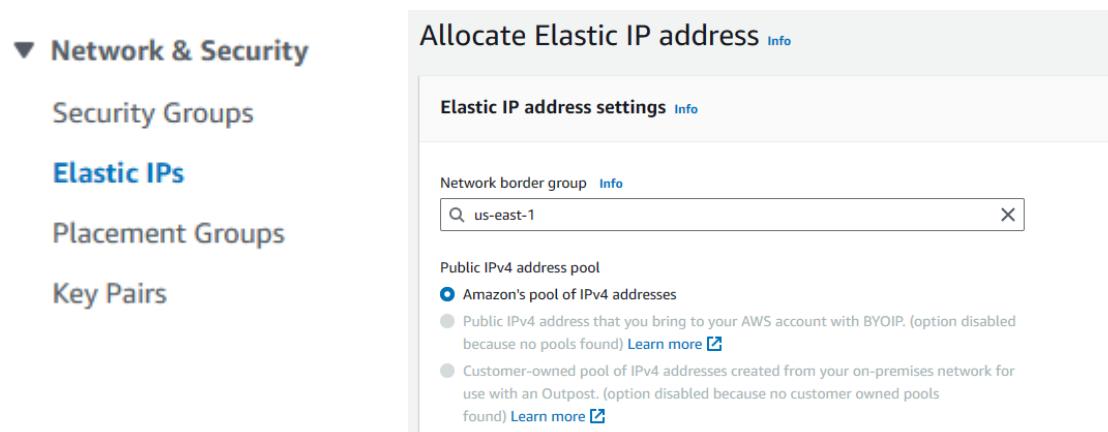
Health checks

Protocol	Path	Port	Healthy threshold
HTTP	/	Traffic port	5 consecutive health check successes
Unhealthy threshold	Timeout	Interval	Success codes
2 consecutive health check failures	5 seconds	30 seconds	200

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.5 Acceso por SSH a Instancias Internas

Los servidores web ofrecen sus contenidos a través del balanceador, pero no están accesibles desde el exterior para su administración. Para acceder por SSH a estos servidores podemos usar distintas técnicas. Por ejemplo, adquirir una dirección IP elástica (pública) y a continuación asociarla a una de las instancias internas (igualmente será necesario modificar la política de seguridad para permitir el acceso SSH desde cualquier dirección IP). También es posible levantar una nueva instancia auxiliar con una IP pública y, una vez conectados por SSH a esta nueva instancia, abrir nuevas conexiones SSH desde ella a las máquinas internas (será necesario copiar la clave privada a esa nueva instancia). Otras opciones: podemos usar la instancia auxiliar anterior y crear túneles SSH, o configurar en esa instancia la función de routing y reglas de port-forwarding hacia las máquinas internas. Probar al menos el primer modo: Reservar una IP elástica (Network & Security → Elastic IPs) y asociarla a una de las máquinas internas (ServidorWeb1). También hay que cambiar el grupo de seguridad para poder acceder por SSH desde el exterior. Una vez sea posible acceder a la instancia mediante SSH, detener el servicio Apache y comprobar su efecto al lanzar nuevas peticiones al balanceador.



2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.5 Acceso por SSH a Instancias Internas

- a) Reservar una IP elástica (Network & Security → Elastic IPs) y asociarla a una de las máquinas internas (ServidorWeb1).

Elastic IP addresses (1/1)

Name	Allocated IPv4 address	Type	Allocation ID	Reverse DNS record
-	23.23.33.51	Public IP	eipalloc-0c104d4eb85fa20f2	-

Actions ▲ Allocate Elastic IP address

- [View details](#)
- [Release Elastic IP addresses](#)
- [Associate Elastic IP address](#)
- [Disassociate Elastic IP address](#)
- [Update reverse DNS](#)
- [Enable transfers](#)
- [Disable transfers](#)
- [Accept transfers](#)

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.5 Acceso por SSH a Instancias Internas

- a) Reservar una IP elástica (Network & Security → Elastic IPs) y asociarla a una de las máquinas internas (ServidorWeb1).

Associate Elastic IP address Info

Choose the instance or network interface to associate to this Elastic IP address (23.23.33.51)

Elastic IP address: 23.23.33.51

Resource type
Choose the type of resource with which to associate the Elastic IP address.

Instance
 Network interface

⚠ If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. [Learn more](#)

If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

Instance
  ServidorWeb1

Private IP address
The private IP address with which to associate the Elastic IP address.

Reassociation
Specify whether the Elastic IP address can be reassigned with a different resource if it is already associated with a resource.

Allow this Elastic IP address to be reassigned

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.5 Acceso por SSH a Instancias Internas

- a) Reservar una IP elástica (Network & Security → Elastic IPs) y asociarla a una de las máquinas internas (ServidorWeb1).

The screenshot shows the AWS EC2 Instances page with the following details:

- Instances (1/4) Info**: Shows four instances: ServidorWeb2 (terminated), ServidorWeb2 (running), ServidorWeb1 (running), and ServidorWeb2 (terminated). The "ServidorWeb1" row is selected.
- Actions** dropdown menu:
 - Connect
 - View details
 - Manage instance state
 - Instance settings
 - Networking
 - Security** (highlighted)
 - Get Windows password
 - Image and templates
 - Modify IAM role
 - Monitor and troubleshoot
- Associated security groups**: A search bar shows "sg-0720b0ae0ed758ea5". Below it, a list includes "Use: sg-0720b0ae0ed758ea5", "SSH_HTTP_internal (sg-07356cfcd7cfcdff)", "default (sg-0fc9a5d7808026dd9)", and "PR6_SecurityGroup (sg-0720b0ae0ed758ea5)". A red circle highlights the "Add security group" button.
- Associated security groups**: A search bar shows "sg-07356cfcd7cfcdff". Below it, a table lists security groups associated with the network interface:

Security group name	Security group ID
PR6_SecurityGroup	sg-0720b0ae0ed758ea5
SSH_HTTP_internal	sg-07356cfcd7cfcdff

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.5 Acceso por SSH a Instancias Internas

- a) Reservar una IP elástica (Network & Security → Elastic IPs) y asociarla a una de las máquinas internas (ServidorWeb1).

```
C:\Users\ppere\Desktop\AdminSist\Practicas\PR6_aws>ssh -i labsuser.pem ec2-user@23.23.33.51
'_
~\_ ####_          Amazon Linux 2023
~~ \#####\
~~ \###|
~~ \#/ ___ https://aws.amazon.com/linux/amazon-linux-2023
~~ \~' '-->
~~ /
~~ ._. /_/
~/m/' 

Last login: Sat Apr 13 10:14:38 2024 from 81.41.169.152
[ec2-user@ip-172-31-5-177 ~]$ |
```

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.5 Acceso por SSH a Instancias Internas

- a) Reservar una IP elástica (Network & Security → Elastic IPs) y asociarla a una de las máquinas internas (ServidorWeb1).

```
_7 ""
Last login: Sat Apr 13 10:14:38 2024 from 81.41.169.152
[ec2-user@ip-172-31-5-177 ~]$ systemctl status httpd
● httpd.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
  Drop-In: /usr/lib/systemd/system/httpd.service.d
            └─php-fpm.conf
    Active: active (running) since Sun 2024-04-14 16:29:26 UTC; 31min ago
      Docs: man:httpd.service(8)
   Main PID: 1979 (httpd)
     Status: "Total requests: 111; Idle/Busy workers 100/0;Requests/sec: 0.059; Bytes served/sec: 23 B/sec"
        Tasks: 177 (limit: 1114)
       Memory: 19.9M
          CPU: 1.187s
        CGroup: /system.slice/httpd.service
                  ├─1979 /usr/sbin/httpd -DFOREGROUND
                  ├─2016 /usr/sbin/httpd -DFOREGROUND
                  ├─2019 /usr/sbin/httpd -DFOREGROUND
                  ├─2020 /usr/sbin/httpd -DFOREGROUND
                  └─2039 /usr/sbin/httpd -DFOREGROUND

Apr 14 16:29:25 ip-172-31-5-177.ec2.internal systemd[1]: Starting httpd.service - The Apache HTTP Server...
Apr 14 16:29:26 ip-172-31-5-177.ec2.internal systemd[1]: Started httpd.service - The Apache HTTP Server.
Apr 14 16:29:26 ip-172-31-5-177.ec2.internal httpd[1979]: Server configured, listening on: port 80
[ec2-user@ip-172-31-5-177 ~]$
```

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.5 Acceso por SSH a Instancias Internas

- a) Reservar una IP elástica (Network & Security → Elastic IPs) y asociarla a una de las máquinas internas (ServidorWeb1).

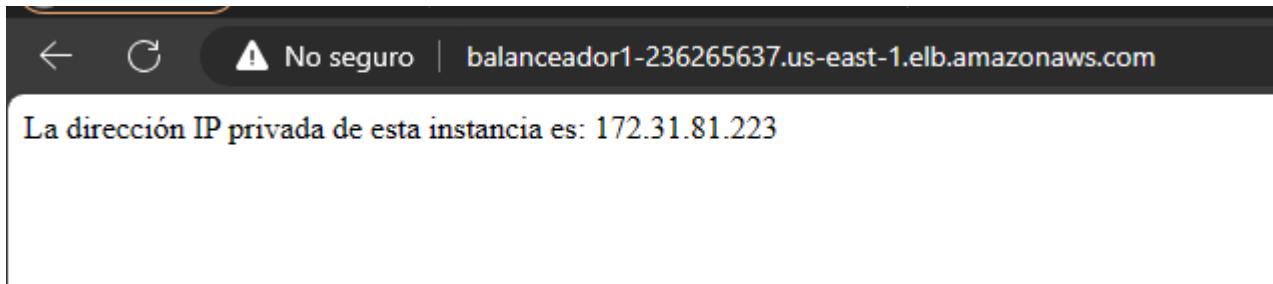
```
[ec2-user@ip-172-31-5-177 ~]$ sudo systemctl stop httpd
[ec2-user@ip-172-31-5-177 ~]$ systemctl status httpd
● httpd.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
  Drop-In: /usr/lib/systemd/system/httpd.service.d
            └─php-fpm.conf
    Active: inactive (dead) since Sun 2024-04-14 17:02:06 UTC; 4s ago
      Duration: 32min 39.007s
        Docs: man:httpd.service(8)
    Process: 1979 ExecStart=/usr/sbin/httpd $OPTIONS -DFOREGROUND (code=exited, status=0/SUCCESS)
   Main PID: 1979 (code=exited, status=0/SUCCESS)
     Status: "Total requests: 115; Idle/Busy workers 100/0;Requests/sec: 0.0589; Bytes served/sec: 23 B/sec"
        CPU: 1.242s

Apr 14 16:29:25 ip-172-31-5-177.ec2.internal systemd[1]: Starting httpd.service - The Apache HTTP Server...
Apr 14 16:29:26 ip-172-31-5-177.ec2.internal systemd[1]: Started httpd.service - The Apache HTTP Server.
Apr 14 16:29:26 ip-172-31-5-177.ec2.internal httpd[1979]: Server configured, listening on: port 80
Apr 14 17:02:05 ip-172-31-5-177.ec2.internal systemd[1]: Stopping httpd.service - The Apache HTTP Server...
Apr 14 17:02:06 ip-172-31-5-177.ec2.internal systemd[1]: httpd.service: Deactivated successfully.
Apr 14 17:02:06 ip-172-31-5-177.ec2.internal systemd[1]: Stopped httpd.service - The Apache HTTP Server.
Apr 14 17:02:06 ip-172-31-5-177.ec2.internal systemd[1]: httpd.service: Consumed 1.242s CPU time.
[ec2-user@ip-172-31-5-177 ~]$
```

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.5 Acceso por SSH a Instancias Internas

- a) Reservar una IP elástica (Network & Security → Elastic IPs) y asociarla a una de las máquinas internas (ServidorWeb1).



Ya no sale la IP 172.31.5.177 del ServidorWeb1

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.5 Acceso por SSH a Instancias Internas

- a) También es posible levantar una nueva instancia auxiliar con una IP pública y, una vez conectados por SSH a esta nueva instancia, abrir nuevas conexiones SSH desde ella a las máquinas internas (será necesario copiar la clave privada a esa nueva instancia)

Grupos de seguridad asociados
Agregue uno o varios grupos de seguridad a la interfaz de red. También puede eliminar grupos de seguridad.

Seleccionar grupos de seguridad Agregar grupo de seguridad

Los grupos de seguridad asociados a la interfaz de red (eni-099dd394e6601fce6)

Nombre del grupo de seguridad	ID de grupo de seguridad	
PR6_SecurityGroup	sg-0720b0ae0ed758ea5	Eliminar
SSH_HTTP_internal	sg-07356cfcd7cfdcff	Eliminar

Eliminamos el grupo SSH_HTTP_Any (en mi caso PR6_SecurityGroup) para volver a tener las directivas que teníamos antes



No tenemos acceso

```
C:\Users\ppere\Desktop\AdminSist\Practicas\PR6_aws>ssh ec2-user@23.23.33.51 -i labsuser.pem  
ssh: connect to host 23.23.33.51 port 22: Connection timed out
```

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.5 Acceso por SSH a Instancias Internas

- a) También es posible levantar una nueva instancia auxiliar con una IP pública y, una vez conectados por SSH a esta nueva instancia, abrir nuevas conexiones SSH desde ella a las máquinas internas (será necesario copiar la clave privada a esa nueva instancia)

Creamos una instancia auxiliar:

Número de instancias	Información
1	Más información
Imagen de software (AMI)	
ServidorWeb de la practica 6 d...	más información
ami-0f71cdad87729a0b5	
Tipo de servidor virtual (tipo de instancia)	
t2.micro	
Firewall (grupo de seguridad)	
PR6_SecurityGroup	
Almacenamiento (volúmenes)	
Volúmenes: 1 (8 GiB)	

Nos conectamos por SSH:

```
C:\Users\ppere\Desktop\AdminSist\Practicas\PR6_aws>ssh ec2-user@107.23.177.63 -i labsuser.pem
The authenticity of host '107.23.177.63 (107.23.177.63)' can't be established.
ED25519 key fingerprint is SHA256:FGemm3v66SdI+lk4WQJPa9NFPym4MkELe458r2v7hCA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '107.23.177.63' (ED25519) to the list of known hosts.

          #_
  ~\_\_ #####_      Amazon Linux 2023
~~  ~\_\#####\
~~   \###|
~~     \#/ ___> https://aws.amazon.com/linux/amazon-linux-2023
~~       V~! '-->
~~     /
~~ ._. / \
~~   /_/
~/m/`'

Last login: Sat Apr 13 10:14:38 2024 from 81.41.169.152
[ec2-user@ip-172-31-30-66 ~]$ |
```

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.5 Acceso por SSH a Instancias Internas

- a) También es posible levantar una nueva instancia auxiliar con una IP pública y, una vez conectados por SSH a esta nueva instancia, abrir nuevas conexiones SSH desde ella a las máquinas internas (será necesario copiar la clave privada a esa nueva instancia)

Copiamos la clave:

```
PS C:\Users\ppere\Desktop\AdminSist\Practicas\PR6_aws> sftp -i labsuser.pem ec2-user@107.23.177.63:/  
Connected to 107.23.177.63.  
Changing to: /  
sftp> put ./labsuser.pem /home/ec2-user  
Uploading ./labsuser.pem to /home/ec2-user/labsuser.pem  
./labsuser.pem  
sftp> |
```

Máquina Principal (Windows)

```
[ec2-user@ip-172-31-30-66 ~]$ pwd  
/home/ec2-user  
[ec2-user@ip-172-31-30-66 ~]$ ls  
labsuser.pem
```

instanciaAuxiliar

Acceso desde instanciaAuxiliar a ServidorWeb1

```
[ec2-user@ip-172-31-30-66 ~]$ ssh -i labsuser.pem ec2-user@172.31.5.177  
The authenticity of host '172.31.5.177 (172.31.5.177)' can't be established.  
ED25519 key fingerprint is SHA256:pQLSF3Lr3abuaoh+Im9U5ely9zwuX7GR0sG1Cjk5TCA.  
This key is not known by any other names  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '172.31.5.177' (ED25519) to the list of known hosts.  
@@@@@@@  
@      WARNING: UNPROTECTED PRIVATE KEY FILE! @  
@  
Permissions 0664 for 'labsuser.pem' are too open.  
It is required that your private key files are NOT accessible by others.  
This private key will be ignored.  
Load key "labsuser.pem": bad permissions Hay que darle permisos a la clave  
ec2-user@172.31.5.177: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).  
[ec2-user@ip-172-31-30-66 ~]$ chmod 400 labsuser.pem  
[ec2-user@ip-172-31-30-66 ~]$ ssh -i labsuser.pem ec2-user@172.31.5.177  
#  
~\_\_ ##### Amazon Linux 2023  
~~ \_\#\#\#\|  
~~ \#\#\|  
~~ \#/ ___ https://aws.amazon.com/linux/amazon-linux-2023  
~~ V~' '--->  
~~ /  
~~ .-./  
~/m/  
Last login: Sun Apr 14 16:59:45 2024 from 81.41.169.152
```

2. BALANCEADOR DE CARGA ELB (ELASTIC LOAD BALANCER)

2.6 Terminación de Instancias y Recursos Asociados

Terminar la ejecución de las instancias (ServidorWeb1, ServidorWeb2) y eliminar la dirección IP elástica, el balanceador y el grupo de destinatarios.

<input checked="" type="checkbox"/>	Name 	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación de	Estado de la al:	Zona de dispon...
<input checked="" type="checkbox"/>	ServidorWeb1	i-0c8fff65903491e0e	 Cerrándose  	t2.micro	 2/2 comprobacion	Ver alarmas 	us-east-1a
<input checked="" type="checkbox"/>	instanciaAuxiliar	i-0da09552094441f59	 Cerrándose  	t2.micro	 Inicializando	Ver alarmas 	us-east-1c
<input checked="" type="checkbox"/>	ServidorWeb2	i-039dfefe288f8576f	 Cerrándose  	t2.micro	 2/2 comprobacion	Ver alarmas 	us-east-1b

✓ Se eliminó correctamente el equilibrador de carga: arn:aws:elasticloadbalancing:us-east-1:958486390477:loadbalancer/app/Balanceador1/da1b81e799e4c254

Se liberará			
Si libera las siguientes direcciones IP elásticas, ya no estarán asignadas a su cuenta ni podrá asociarlas a sus recursos.			
Nombre	Dirección IPv4	ID de asignación	Tipo de dir
-	23.23.33.51	eipalloc-0c104d4eb85fa20f2	Public

Grupos de destino (1/1) Info					
<input type="text"/> Filtrar grupos de destino					
<input checked="" type="checkbox"/>	Nombre	ARN	Puerto	Protocolo	Acciones 
<input checked="" type="checkbox"/>	ServidoresWeb	arn:aws:elasticloadbalanci...	80	HTTP	 Eliminar  Registrar destinos  Editar la configuraci...  Editar atributos de ...  Administrar etiquet...

ÍNDICE

1. Ejecución de Instancias EC2

- 1.1 Acceso a la Consola y Creación de Claves
- 1.2 Creación de Grupo de Seguridad
- 1.3 Comprobación de VPC y Subredes
- 1.4 Lanzamiento de Instancia PruebasWeb
- 1.5 Configuración de la Instancia y Tareas de Mantenimiento
- 1.6 Efecto de Reinicio y Detención de la Instancia
- 1.7 Generación de Imagen de la Instancia
- 1.8 Terminación de la Instancia

2. Balanceador de Carga ELB (Elastic Load Balancer)

- 2.1 Lanzamiento de Instancias y Creación de Grupo de Seguridad
- 2.2 Creación de Grupo de Destinatarios
- 2.3 Creación de Balanceador de Carga
- 2.4 Pruebas de Acceso y Balanceo
- 2.5 Acceso por SSH a Instancias Internas
- 2.6 Terminación de Instancias y Recursos Asociados

3. Subredes Públicas/Privadas y NAT Gateway

- 3.1 Creación de Subredes y Lanzamiento de Instancias
- 3.2 Configuración de NAT Gateway y Tablas de Rutas
- 3.3 Configuración de Network ACLs
- 3.4 Terminación de Instancias, NAT Gateway y Recursos Asociados

4. Almacenamiento S3

- 4.1 Creación de Bucket S3 y Subida de Archivos
- 4.2 Configuración para Hosting Web Estático
- 4.3 Pruebas de Acceso y Descarga de Archivos
- 4.4 Eliminación del Bucket

5. Autoescalado para Aplicaciones Web

- 5.1 Creación de Grupo de Destinatarios y Balanceador
- 5.2 Creación de Plantilla de Lanzamiento y Grupo de Autoescalado
- 5.3 Configuración de Escalado Automático
- 5.4 Pruebas de Funcionamiento del Escalado
- 5.5 Eliminación de Recursos de Autoescalado

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.1 Creación de Subredes y Lanzamiento de Instancias

Normalmente las instancias privadas se ubican en subredes privadas, aisladas de las subredes “publicas”, cuyos recursos pueden estar accesibles desde el exterior mediante direcciones elásticas. Todas las subredes definidas en la VPC, públicas y privadas, tendrán asociado un bloque de direcciones IP libres dentro del rango asociado a la VPC.

Crear en primer lugar una nueva subred con direccionamiento /24 (el primero disponible) en una de las zonas de disponibilidad de la región. Para ello es necesario revisar en primer lugar la asignación de direcciones a las subredes ya definidas, accediendo a la sección Subnets del panel de control de VPC. A continuación, dentro de esta sección, añadir la nueva subred en una zona de disponibilidad, con nombre Red Interna y el bloque /24 seleccionado previamente.

▼ Virtual private cloud

Your VPCs

Subnets

Subredes existentes:

1. Subred en us-east-1d: 172.31.32.0/20
2. Subred en us-east-1a: 172.31.0.0/20
3. Subred en us-east-1b: 172.31.80.0/20
4. Subred en us-east-1e: 172.31.48.0/20
5. Subred en us-east-1c: 172.31.16.0/20
6. Subred en us-east-1 (sin zona especificada): 172.31.64.0/20

Red Interna: 172.31.128.0/24 (la hemos elegido porque está libre)

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.1 Creación de Subredes y Lanzamiento de Instancias

Crear en primer lugar una nueva subred con direccionamiento /24 (el primero disponible) en una de las zonas de disponibilidad de la región. Para ello es necesario revisar en primer lugar la asignación de direcciones a las subredes ya definidas, accediendo a la sección Subnets del panel de control de VPC. A continuación, dentro de esta sección, añadir la nueva subred en una zona de disponibilidad, con nombre Red Interna y el bloque /24 seleccionado previamente.

Details					
Subnet ID	subnet-08d02e8354c0873eb	Subnet ARN	arn:aws:ec2:us-east-1:958486390477:subnet/subnet-08d02e8354c0873eb	State	Available
Available IPv4 addresses	251	IPv6 CIDR	-	Availability Zone	us-east-1a
Network border group	us-east-1	Route table	rtb-02f32a46096dd1164	Availability Zone ID	use1-az1
Default subnet	No	VPC	vpc-00a5dfc0664ac615a	Network ACL	acl-0fe7990f7641f689d
				Auto-assign IPv6 address	No
				Auto-assign customer-owned IPv4 address	

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 256 IPs
[<](#) [>](#) [^](#) [v](#)

▼ Tags - optional

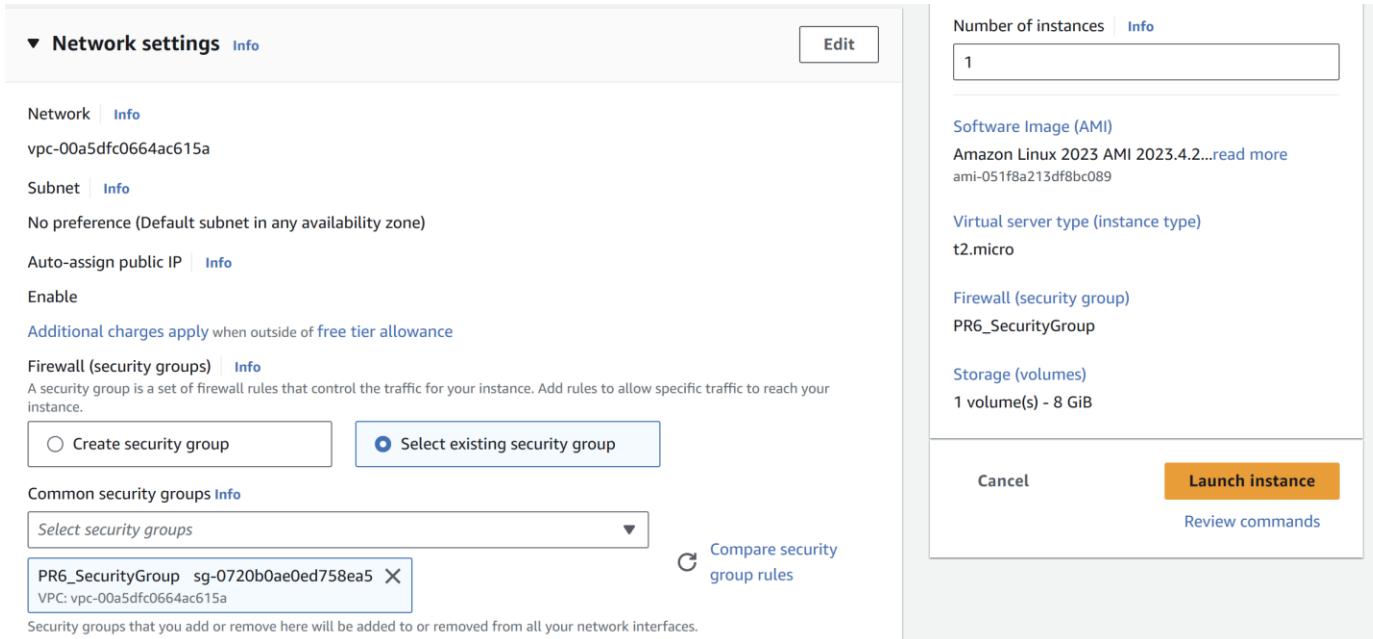
Key	Value - optional	Remove
<input type="text" value="Name"/> X	<input type="text" value="Red Interna"/> X	Remove

[Add new tag](#)

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.1 Creación de Subredes y Lanzamiento de Instancias

En la consola de administración de EC2 lanzar dos nuevas instancias Amazon Linux AMI de tipo t2.micro (ServidorPublico y ServidorPrivado), la primera ubicada en una de las subredes públicas y con dirección IP elástica asociada, y la segunda en la nueva subred y sin dirección elástica (sólo tendrá IP privada). En el grupo de seguridad permitir el acceso a los servicios SSH y HTTP. Acceder a la instancia pública por SSH y conectar desde ella a la instancia privada (es necesario contar con la clave privada ClavesPractica.pem en el cliente ssh). Comprobar que no es posible acceder al exterior desde la red privada.



ServidorPublico

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.1 Creación de Subredes y Lanzamiento de Instancias

En la consola de administración de EC2 lanzar dos nuevas instancias Amazon Linux AMI de tipo t2.micro (ServidorPublico y ServidorPrivado), la primera ubicada en una de las subredes públicas y con dirección IP elástica asociada, y la segunda en la nueva subred y sin dirección elástica (sólo tendrá IP privada). En el grupo de seguridad permitir el acceso a los servicios SSH y HTTP. Acceder a la instancia pública por SSH y conectar desde ella a la instancia privada (es necesario contar con la clave privada ClavesPractica.pem en el cliente ssh). Comprobar que no es posible acceder al exterior desde la red privada.

The screenshot shows the AWS EC2 Launch Instance wizard. On the left, under 'Network settings', a VPC is selected (vpc-00a5dfc0664ac615a, default subnet 172.31.0.0/16). A new subnet 'Red Interna' is being created with CIDR 172.31.128.0/24. Under 'Auto-assign public IP', 'Disable' is selected. Under 'Firewall (security groups)', 'Select existing security group' is chosen, and 'PR6_SecurityGroup' is selected. On the right, under 'Summary', the instance type is 't2.micro' and the AMI is 'Amazon Linux 2023 AMI 2023.4.2...'. The 'Launch instance' button is highlighted in orange.

ServidorPrivado

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.1 Creación de Subredes y Lanzamiento de Instancias

En la consola de administración de EC2 lanzar dos nuevas instancias Amazon Linux AMI de tipo t2.micro (ServidorPublico y ServidorPrivado), la primera ubicada en una de las subredes públicas y con dirección IP elástica asociada, y la segunda en la nueva subred y sin dirección elástica (sólo tendrá IP privada). En el grupo de seguridad permitir el acceso a los servicios SSH y HTTP. **Acceder a la instancia pública por SSH y conectar desde ella a la instancia privada** (es necesario contar con la clave privada ClavesPractica.pem en el cliente ssh). Comprobar que no es posible acceder al exterior desde la red privada.

Public IPv4 address 54.85.161.136 open address	Private IPv4 addresses 172.31.128.45
ServidorPublico	ServidorPrivado

```
PS C:\Users\ppere\Desktop\AdminSist\Practicas\PR6_aws> ssh -i ./labsuser.pem ec2-user@54.85.161.136
The authenticity of host '54.85.161.136 (54.85.161.136)' can't be established.
ED25519 key fingerprint is SHA256:L4+S+3QteEogVp670EBMuxaMNe726ZaS8hYtzztwEAc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '54.85.161.136' (ED25519) to the list of known hosts.

#_
/_###_
~~ \#####
~~ \###|
~~ \#/ ___ https://aws.amazon.com/linux/amazon-linux-2023
~~ V~' '-->
~~ ._. /_
~~ /_/
~~ /m/
[ec2-user@ip-172-31-24-129 ~]$ |
```

```
Connected to 54.85.161.136.
sftp> put ./labsuser.pem /home/ec2-user
Uploading ./labsuser.pem to /home/ec2-user/labsuser.pem
./labsuser.pem
```

Conexión desde ServidorPublico a ServidorPrivado:

```
[ec2-user@ip-172-31-24-129 ~]$ chmod 400 labsuser.pem
[ec2-user@ip-172-31-24-129 ~]$ ssh -i labsuser.pem ec2-user@172.31.128.45
#_
/_###_
~~ \#####
~~ \###|
~~ \#/ ___ https://aws.amazon.com/linux/amazon-linux-2023
~~ V~' '-->
~~ ._. /_
~~ /_/
~~ /m/
[ec2-user@ip-172-31-128-45 ~]$ |
```

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.1 Creación de Subredes y Lanzamiento de Instancias

En la consola de administración de EC2 lanzar dos nuevas instancias Amazon Linux AMI de tipo t2.micro (ServidorPublico y ServidorPrivado), la primera ubicada en una de las subredes públicas y con dirección IP elástica asociada, y la segunda en la nueva subred y sin dirección elástica (sólo tendrá IP privada). En el grupo de seguridad permitir el acceso a los servicios SSH y HTTP. Acceder a la instancia pública por SSH y conectar desde ella a la instancia privada (es necesario contar con la clave privada ClavesPractica.pem en el cliente ssh). **Comprobar que no es posible acceder al exterior desde la red privada.**

Conexión desde ServidorPublico a ServidorPrivado:

```
[ec2-user@ip-172-31-128-45 ~]$ ping google.com
PING google.com (142.251.16.138) 56(84) bytes of data.
^C
--- google.com ping statistics ---
44 packets transmitted, 0 received, 100% packet loss, time 44748ms

[ec2-user@ip-172-31-128-45 ~]$ |
```

```
[ec2-user@ip-172-31-128-45 ~]$ ping www.ceu.es
PING www.ceu.es (104.18.9.169) 56(84) bytes of data.
^C
--- www.ceu.es ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7267ms
```

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.2 Configuración de NAT Gateway y Tablas de Rutas

▼ Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Configurar un NAT Gateway en la subred pública de la misma zona de disponibilidad donde se encuentra la subred privada (es necesario configurar este servicio en cada Zona de Disponibilidad donde existan subredes privadas). Para ello, en la consola de VPC (Services → Compute → VPC) vamos a la sección NAT Gateways y creamos uno nuevo en la subred pública de la zona de disponibilidad deseada. Se le asociará una IP pública.

NAT gateway settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.

Zona de disponibilidad: us-east-1b

Connectivity type
Select a connectivity type for the NAT gateway.
 Public
 Private

Elastic IP allocation ID [Info](#)
Assign an Elastic IP address to the NAT gateway.

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.2 Configuración de NAT Gateway y Tablas de Rutas

Crear una nueva tabla de rutas para encaminar el tráfico saliente (0.0.0.0/0) hacia el nuevo NAT Gateway. Contaremos con dos tablas de encaminamiento: una para las redes “publicas” (salida a través del igw), y otra para la red privada creada (a través del nuevo NAT Gateway).

Route table settings

Name - optional

Create a tag with a key of 'Name' and a value that you specify.

VPC

The VPC to use for this route table.

▼

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key

Value - optional

 X X

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.2 Configuración de NAT Gateway y Tablas de Rutas

Crear una nueva tabla de rutas para encaminar el tráfico saliente (0.0.0.0/0) hacia el nuevo NAT Gateway. Contaremos con dos tablas de encaminamiento: una para las redes “publicas” (salida a través del igw), y otra para la red privada creada (a través del nuevo NAT Gateway).

Edit routes

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
0.0.0.0/0	NAT Gateway	-	No

A valid resource id has to be specified.

nat-0ba73419cc69022fd (Mi Nat Gateway)

Add route

Cancel Preview Save changes

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.2 Configuración de NAT Gateway y Tablas de Rutas

Asignar la nueva tabla de encaminamiento a la subred privada (sección Subnets de VPC). A continuación, acceder a la instancia lanzada en la subred privada y comprobar que es posible alcanzar recursos externos. ¿Cómo podemos conocer desde la instancia qué dirección IP pública se está usando para las conexiones exteriores? Comprobar que dicha dirección coincide con la IP elástica asociada al NAT Gateway.

Edit route table association [Info](#)

Subnet route table settings

Subnet ID
 subnet-08d02e8354c0873eb

Route table ID
rtb-0a1f73ec544ed757d (tabla de rutas Mi Gateway) ▾ C

Routes (2)

Filter routes

Destination	Target
172.31.0.0/16	local
0.0.0.0/0	nat-0ba73419cc69022fd

Comprobación de que accede al exterior:

```
[ec2-user@ip-172-31-128-45 ~]$ ping google.com
PING google.com (142.251.16.138) 56(84) bytes of data.
64 bytes from bl-in-f138.1e100.net (142.251.16.138): icmp_seq=1 ttl=54 time=3.18 ms
64 bytes from bl-in-f138.1e100.net (142.251.16.138): icmp_seq=2 ttl=54 time=2.36 ms
64 bytes from bl-in-f138.1e100.net (142.251.16.138): icmp_seq=3 ttl=54 time=2.37 ms
64 bytes from bl-in-f138.1e100.net (142.251.16.138): icmp_seq=4 ttl=54 time=2.39 ms
64 bytes from bl-in-f138.1e100.net (142.251.16.138): icmp_seq=5 ttl=54 time=2.39 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 2.358/2.535/3.177/0.321 ms
[ec2-user@ip-172-31-128-45 ~]$
```

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.2 Configuración de NAT Gateway y Tablas de Rutas

Asignar la nueva tabla de encaminamiento a la subred privada (sección Subnets de VPC). A continuación, acceder a la instancia lanzada en la subred privada y comprobar que es posible alcanzar recursos externos. ¿Cómo podemos conocer desde la instancia qué dirección IP pública se está usando para las conexiones exteriores? Comprobar que dicha dirección coincide con la IP elástica asociada al NAT Gateway.

Devuelve la dirección IP pública que la instancia está utilizando para las conexiones externas:

```
[ec2-user@ip-172-31-128-45 ~]$ curl ifconfig.me  
3.226.131.34[ec2-user@ip-172-31-128-45 ~]$ |
```

Name	NAT gateway ID	Connectivity...	State	State message	Primary public I...
Mi Nat Gateway	nat-0ba73419cc69022fd	Public	Available	-	3.226.131.34

3.226.131.34

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.3 Configuración de Network ACLs

Es posible limitar el tráfico que entra o sale de las subredes mediante Network ACLs. Verificar en primer lugar la estructura de la ACL predeterminada asociada a las subredes, y sus reglas Inbound y Outbound. ¿Se limita de alguna manera el tráfico de red con esta ACL? A continuación, crear una ACL de prueba para la red privada que impida el acceso por HTTP desde la red “publica” donde se encuentra el ServidorPublico, pero que sí permita el acceso por SSH desde esa red (será el único servicio permitido). A continuación, activar la ACL en la red privada y verificar su funcionamiento. Indicar las reglas usadas.

The screenshot shows the AWS Network ACL configuration interface. At the top, there's a table listing Network ACLs. One row is selected, showing details: Name (-), Network ACL ID (acl-0fe7990f7641f689d), Associated with (7 Subnets), Default (Yes), and VPC ID (vpc-00a5dfc0664ac615a). Below this, a modal window displays the details for the selected ACL (acl-0fe7990f7641f689d). The 'Inbound rules' tab is active, showing two rules:

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

- 1º Regla: permite todo el tráfico entrante desde cualquier dirección IP externa (0.0.0.0/0)
2º Regla: deniega todo el tráfico entrante desde cualquier dirección IP externa (0.0.0.0/0).
La regla número 100, al estar antes que la regla “*”, permitirá que todo el tráfico entre a menos que sea denegado explícitamente por la segunda regla.

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.3 Configuración de Network ACLs

Es posible limitar el tráfico que entra o sale de las subredes mediante Network ACLs. Verificar en primer lugar la estructura de la ACL predeterminada asociada a las subredes, y sus reglas Inbound y Outbound. ¿Se limita de alguna manera el tráfico de red con esta ACL? A continuación, crear una ACL de prueba para la red privada que impida el acceso por HTTP desde la red “publica” donde se encuentra el ServidorPublico, pero que sí permita el acceso por SSH desde esa red (será el único servicio permitido). A continuación, activar la ACL en la red privada y verificar su funcionamiento. Indicar las reglas usadas.

Outbound rules (2)							Edit outbound rules			
<input type="text"/> Filter outbound rules							<<	1	>	
Rule number	Type	Protocol	Port range	Destination	Allow/Deny					
100	All traffic	All	All	0.0.0.0/0	Allow					
*	All traffic	All	All	0.0.0.0/0	Deny					

1º Regla: la regla número 100 permite todo el tráfico saliente desde cualquier dirección IP externa (0.0.0.0/0).

2º Regla, "*", deniega todo el tráfico saliente desde cualquier dirección IP externa (0.0.0.0/0).

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.3 Configuración de Network ACLs

Es posible limitar el tráfico que entra o sale de las subredes mediante Network ACLs. Verificar en primer lugar la estructura de la ACL predeterminada asociada a las subredes, y sus reglas Inbound y Outbound. ¿Se limita de alguna manera el tráfico de red con esta ACL? A continuación, crear una ACL de prueba para la red privada que impida el acceso por HTTP desde la red “publica” donde se encuentra el ServidorPublico, pero que sí permita el acceso por SSH desde esa red (será el único servicio permitido). A continuación, activar la ACL en la red privada y verificar su funcionamiento. Indicar las reglas usadas.

Outbound rules (2)							Edit outbound rules
<input type="text"/> Filter outbound rules							
Rule number	Type	Protocol	Port range	Destination	Allow/Deny		
100	All traffic	All	All	0.0.0.0/0	Allow		
*	All traffic	All	All	0.0.0.0/0	Deny		

1º Regla: la regla número 100 permite todo el tráfico saliente desde cualquier dirección IP externa (0.0.0.0/0).

2º Regla, "*", deniega todo el tráfico saliente desde cualquier dirección IP externa (0.0.0.0/0).

Mientras que el tráfico de entrada está siendo permitido, el tráfico de salida está siendo limitado y en su mayoría denegado

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.3 Configuración de Network ACLs

Es posible limitar el tráfico que entra o sale de las subredes mediante Network ACLs. Verificar en primer lugar la estructura de la ACL predeterminada asociada a las subredes, y sus reglas Inbound y Outbound. ¿Se limita de alguna manera el tráfico de red con esta ACL? **A continuación, crear una ACL de prueba para la red privada que impida el acceso por HTTP desde la red “publica” donde se encuentra el ServidorPublico, pero que sí permita el acceso por SSH desde esa red (será el único servicio permitido).** A continuación, activar la ACL en la red privada y verificar su funcionamiento. Indicar las reglas usadas.

Network ACL settings

Name - *optional*
Creates a tag with a key of 'Name' and a value that you specify.

acl-prueba

VPC
VPC to use for this network ACL.

vpc-00a5dfc0664ac615a

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - <i>optional</i>
<input type="text" value="Name"/> X	<input type="text" value="acl-prueba"/> X Remove tag

Add tag

You can add 49 more tags

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.3 Configuración de Network ACLs

Es posible limitar el tráfico que entra o sale de las subredes mediante Network ACLs. Verificar en primer lugar la estructura de la ACL predeterminada asociada a las subredes, y sus reglas Inbound y Outbound. ¿Se limita de alguna manera el tráfico de red con esta ACL? **A continuación, crear una ACL de prueba para la red privada que impida el acceso por HTTP desde la red “publica” donde se encuentra el ServidorPublico, pero que sí permita el acceso por SSH desde esa red (será el único servicio permitido).** A continuación, activar la ACL en la red privada y verificar su funcionamiento. Indicar las reglas usadas.

VPC > Network ACLs > acl-0e5c917b1863e3277 / acl-prueba > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the VPC.

Rule number Info	Type Info	Protocol Info	Port range Info	Source Info	Allow/Deny Info	
1	SSH (22)	TCP (6)	22	3.226.131.34/32	Allow	Remove
2	HTTP (80)	TCP (6)	80	3.226.131.34/32	Deny	Remove
*	All traffic	All	All	0.0.0.0/0	Deny	

[Add new rule](#) [Sort by rule number](#)

[Cancel](#) [Preview changes](#) [Save changes](#)

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.3 Configuración de Network ACLs

Es posible limitar el tráfico que entra o sale de las subredes mediante Network ACLs. Verificar en primer lugar la estructura de la ACL predeterminada asociada a las subredes, y sus reglas Inbound y Outbound. ¿Se limita de alguna manera el tráfico de red con esta ACL? A continuación, crear una ACL de prueba para la red privada que impida el acceso por HTTP desde la red “publica” donde se encuentra el ServidorPublico, pero que sí permita el acceso por SSH desde esa red (será el único servicio permitido). **A continuación, activar la ACL en la red privada y verificar su funcionamiento. Indicar las reglas usadas.**

The screenshot shows the AWS Network ACL configuration interface for a subnet named 'Red Interna'. At the top, there are two entries: 'subnet-08d02e8354c0873eb' associated with 'vpc-00a5dfc0664ac615a' (172.31.128.0/24) and 'subnet-0096e44e33f1d04e8' associated with 'vpc-00a5dfc0664ac615a' (172.31.0.0/20). Below this, the subnet details are shown: 'subnet-08d02e8354c0873eb / Red Interna'. The 'Network ACL' tab is selected, showing the Network ACL ID 'acl-0fe7990f7641f689d'. A red circle highlights the 'Edit network ACL association' button. The 'Inbound rules (2)' section lists two rules:

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.3 Configuración de Network ACLs

Es posible limitar el tráfico que entra o sale de las subredes mediante Network ACLs. Verificar en primer lugar la estructura de la ACL predeterminada asociada a las subredes, y sus reglas Inbound y Outbound. ¿Se limita de alguna manera el tráfico de red con esta ACL? A continuación, crear una ACL de prueba para la red privada que impida el acceso por HTTP desde la red “publica” donde se encuentra el ServidorPublico, pero que sí permita el acceso por SSH desde esa red (será el único servicio permitido). **A continuación, activar la ACL en la red privada y verificar su funcionamiento. Indicar las reglas usadas.**

subnet-08d02e8354c0873eb / Red Interna

Network ACL: [acl-0e5c917b1863e3277 / acl-prueba](#) Edit network ACL association

Inbound rules (3)						
<input type="text"/> Filter inbound rules						
Rule number	Type	Protocol	Port range	Source	Allow/Deny	
1	SSH (22)	TCP (6)	22	172.31.16.0/20	<input checked="" type="checkbox"/> Allow	
2	HTTP (80)	TCP (6)	80	172.31.16.0/20	<input type="checkbox"/> Deny	
*	All traffic	All	All	0.0.0.0/0	<input type="checkbox"/> Deny	

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.3 Configuración de Network ACLs

Es posible limitar el tráfico que entra o sale de las subredes mediante Network ACLs. Verificar en primer lugar la estructura de la ACL predeterminada asociada a las subredes, y sus reglas Inbound y Outbound. ¿Se limita de alguna manera el tráfico de red con esta ACL? A continuación, crear una ACL de prueba para la red privada que impida el acceso por HTTP desde la red “publica” donde se encuentra el ServidorPublico, pero que sí permita el acceso por SSH desde esa red (será el único servicio permitido). **A continuación, activar la ACL en la red privada y verificar su funcionamiento. Indicar las reglas usadas.**

Deberíamos poder conectarnos al ServidorPublico y de ahí al ServidorPrivado por ssh

Public IPv4 address

 174.129.183.244 | [open address](#) 

ServidorPublico

Private IPv4 addresses

 172.31.128.45

ServidorPrivado

No deberíamos poder conectarnos por http (como por ejemplo haciendo curl [IP_MAQUINA])

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.3 Configuración de Network ACLs

```
C:\Users\ppere\Desktop\AdminSist\Practicas\PR6_aws>ssh -i labsuser.pem ec2-user@174.129.183.244
The authenticity of host '174.129.183.244 (174.129.183.244)' can't be established.
ED25519 key fingerprint is SHA256:L4+S+3QteEogVp670EBMuxaMNe726ZaS8hYtzztwEAc.
This host key is known by the following other names/addresses:
  C:\Users\ppere/.ssh/known_hosts:26: 54.85.161.136
  C:\Users\ppere/.ssh/known_hosts:28: 34.228.68.15
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '174.129.183.244' (ED25519) to the list of known hosts.
```

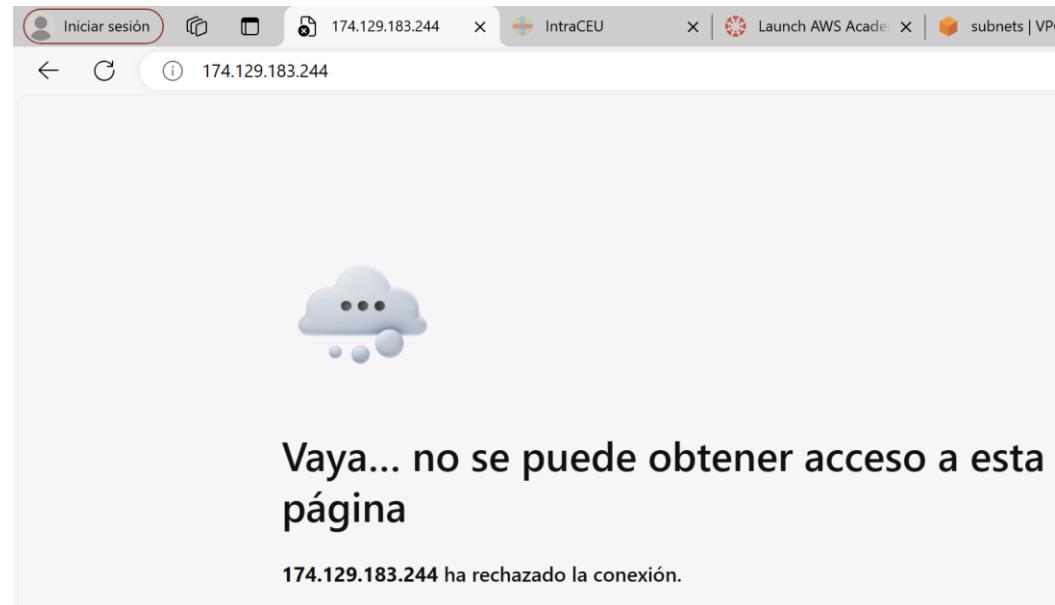
Conexión ssh a ServidorPublico exitosa

```
#_
~\_\_ #####_      Amazon Linux 2023
~~ \_\#####\
~~  \###|
~~   \#/ ___> https://aws.amazon.com/linux/amazon-linux-2023
~~    V~' '-->
~~     /
~~ ._. /_
~~  _/ _/
~~ /m/'  
Last login: Tue Apr 16 12:24:18 2024 from 188.86.160.110
[ec2-user@ip-172-31-24-129 ~]$ ssh ec2-user@172.31.128.45 -i labsuser.pem
#_
~\_\_ #####_      Amazon Linux 2023
~~ \_\#####\
~~  \###|
~~   \#/ ___> https://aws.amazon.com/linux/amazon-linux-2023
~~    V~' '-->
~~     /
~~ ._. /_
~~  _/ _/
~~ /m/'  
Last login: Tue Apr 16 12:27:03 2024 from 172.31.24.129
[ec2-user@ip-172-31-128-45 ~]$ |
```

Conexión ssh desde ServidorPublico a ServidorPrivado exitosa

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.3 Configuración de Network ACLs



Conexión HTTP al ServidorPublico **fallida**

```
Connection to 172.31.128.45 closed.  
[ec2-user@ip-172-31-24-129 ~]$ curl 172.31.128.45  
curl: (28) Failed to connect to 172.31.128.45 port 80 after 133713 ms: Couldn't connect to server
```

Conexión HTTP desde ServidorPublico a ServidorPrivado **fallida**

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.4 Terminación de Instancias, NAT Gateway y Recursos Asociados

Terminar la ejecución de las instancias usadas, el NAT Gateway, la subred privada, la Network ACL y la tabla de encaminamiento. Indicar el orden seguido en la eliminación de estos recursos. Nota: hay que tener en cuenta las dependencias. Por ejemplo, para eliminar una tabla de encaminamiento no puede estar asignada a ninguna subred.

- 1) Eliminar ACLs de la RedInterna →
- 2) Eliminar ACL ←
- 3) Eliminar Gateway
- 4) Eliminar Instancias
- 5) Eliminar RedInterna
- 6) Eliminar Tabla de rutas

subnet-08d02e8354c0873eb / Red Interna

Details | Flow logs | Route table | **Network ACL** | CIDR reservations | Sharing | Tags

Network ACL: [acl-0fe7990f7641f689d](#) Edit network ACL association

Inbound rules (2)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Name Network ACL ID Associated with Del

<input checked="" type="checkbox"/> acl-prueba	acl-0e5c917b1863e3277	-	No
<input type="checkbox"/> -	acl-0fe7990f7641f689d	7 Subnets	Yes

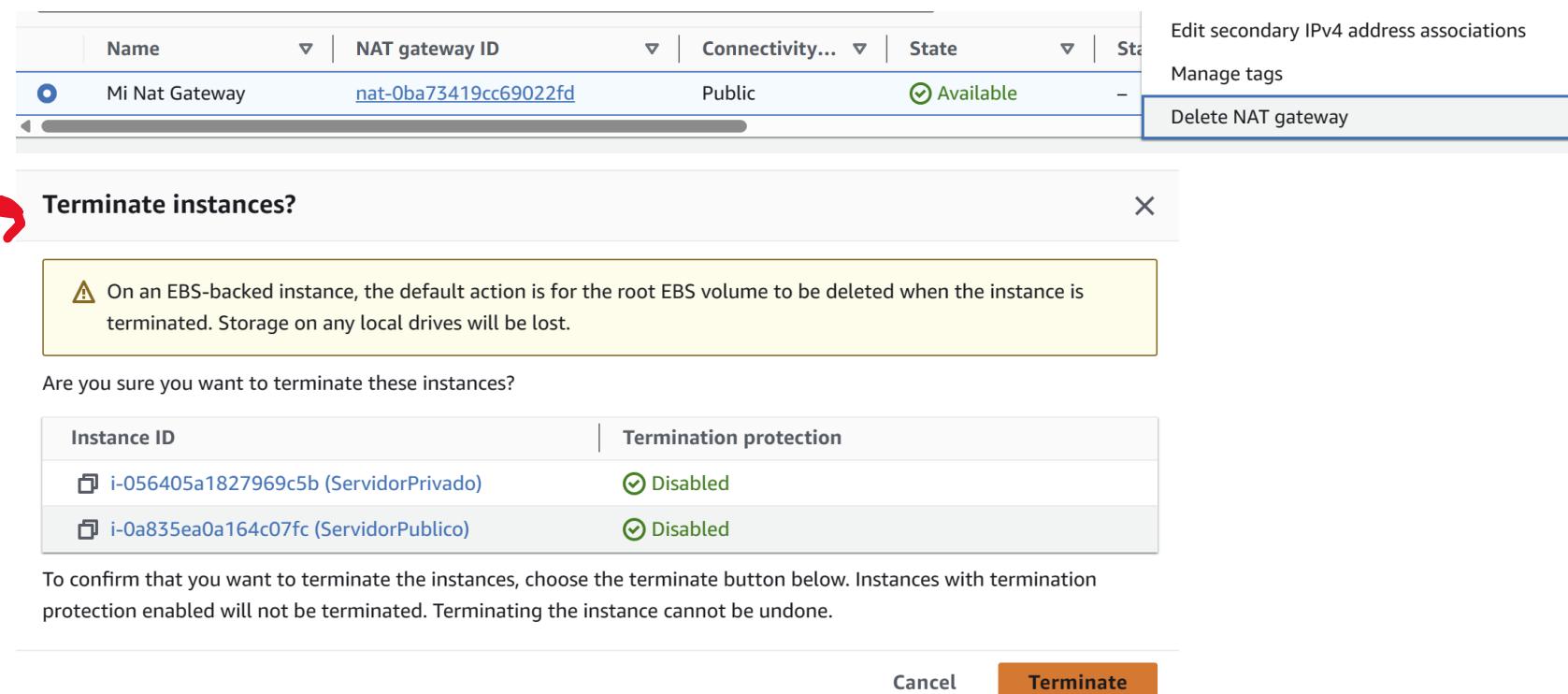
Edit inbound rules
Edit outbound rules
Edit subnet associations
Manage tags
Delete network ACLs

3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.4 Terminación de Instancias, NAT Gateway y Recursos Asociados

Terminar la ejecución de las instancias usadas, el NAT Gateway, la subred privada, la Network ACL y la tabla de encaminamiento. Indicar el orden seguido en la eliminación de estos recursos. Nota: hay que tener en cuenta las dependencias. Por ejemplo, para eliminar una tabla de encaminamiento no puede estar asignada a ninguna subred.

- 1) Eliminar ACLs de la RedInterna
- 2) Eliminar ACL
- 3) Eliminar Gateway
- 4) Eliminar Instancias
- 5) Eliminar RedInterna
- 6) Eliminar Tabla de rutas

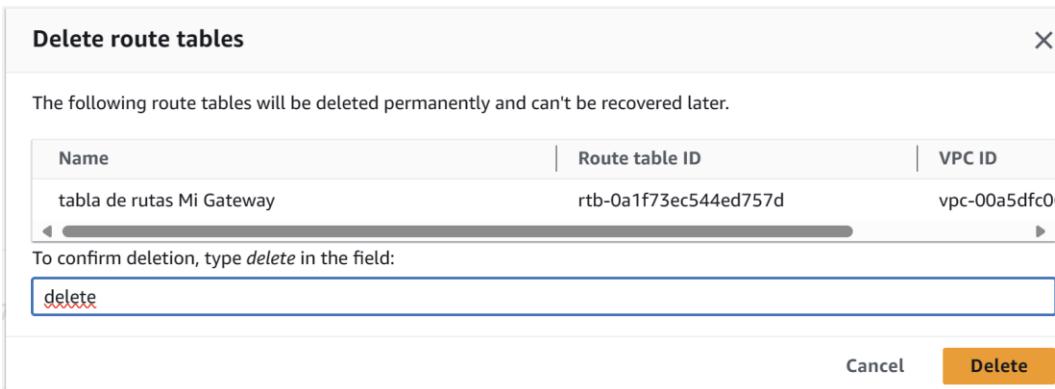


3. SUBREDES PÚBLICAS/PRIVADAS Y NAT GATEWAY

3.4 Terminación de Instancias, NAT Gateway y Recursos Asociados

Terminar la ejecución de las instancias usadas, el NAT Gateway, la subred privada, la Network ACL y la tabla de encaminamiento. Indicar el orden seguido en la eliminación de estos recursos. Nota: hay que tener en cuenta las dependencias. Por ejemplo, para eliminar una tabla de encaminamiento no puede estar asignada a ninguna subred.

- 1) Eliminar ACLs de la RedInterna
- 2) Eliminar ACL
- 3) Eliminar Gateway
- 4) Eliminar Instancias
- 5) Eliminar RedInterna
- 6) Eliminar Tabla de rutas



The screenshot shows a table titled "Subnets (6) Info" with a search bar above it. The table has two columns: "Name" and "Subnet ID". There are six rows, each with a checkbox and a link to the subnet ID. The subnets listed are:

Name	Subnet ID
-	subnet-0abe696b516920447
-	subnet-0096e44e33f1d04e8
-	subnet-0d183fe04df17c9dd
-	subnet-098d6c5fbeae93c0f
-	subnet-061ad182da4aa73cb
-	subnet-041f0345f41404651

ÍNDICE

1. Ejecución de Instancias EC2

- 1.1 Acceso a la Consola y Creación de Claves
- 1.2 Creación de Grupo de Seguridad
- 1.3 Comprobación de VPC y Subredes
- 1.4 Lanzamiento de Instancia PruebasWeb
- 1.5 Configuración de la Instancia y Tareas de Mantenimiento
- 1.6 Efecto de Reinicio y Detención de la Instancia
- 1.7 Generación de Imagen de la Instancia
- 1.8 Terminación de la Instancia

2. Balanceador de Carga ELB (Elastic Load Balancer)

- 2.1 Lanzamiento de Instancias y Creación de Grupo de Seguridad
- 2.2 Creación de Grupo de Destinatarios
- 2.3 Creación de Balanceador de Carga
- 2.4 Pruebas de Acceso y Balanceo
- 2.5 Acceso por SSH a Instancias Internas
- 2.6 Terminación de Instancias y Recursos Asociados

3. Subredes Públicas/Privadas y NAT Gateway

- 3.1 Creación de Subredes y Lanzamiento de Instancias
- 3.2 Configuración de NAT Gateway y Tablas de Rutas
- 3.3 Configuración de Network ACLs
- 3.4 Terminación de Instancias, NAT Gateway y Recursos Asociados

4. Almacenamiento S3

- 4.1 Creación de Bucket S3 y Subida de Archivos
- 4.2 Configuración para Hosting Web Estático
- 4.3 Pruebas de Acceso y Descarga de Archivos
- 4.4 Eliminación del Bucket

5. Autoescalado para Aplicaciones Web

- 5.1 Creación de Grupo de Destinatarios y Balanceador
- 5.2 Creación de Plantilla de Lanzamiento y Grupo de Autoescalado
- 5.3 Configuración de Escalado Automático
- 5.4 Pruebas de Funcionamiento del Escalado
- 5.5 Eliminación de Recursos de Autoescalado

4. ALMACENAMIENTO S3

4.1 Creación de Bucket S3 y Subida de Archivos

Acceder a la consola de administración de S3 (Storage → S3) y crear un nuevo bucket. Utilizar un nombre significativo (por ejemplo, mi_nombre_y_apellido) y ubicarlo en la región de trabajo. Usar las opciones por defecto (ACLs disabled, bloquear todo el acceso público, encriptado, ...) salvo el control de versiones, que lo activaremos. Identificar la clase de almacenamiento S3 usada en este nuevo bucket (Storage class).

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar titled 'General configuration' with fields for 'AWS Region' (set to 'US East (N. Virginia) us-east-1') and 'Bucket type' (set to 'General purpose'). Below these are sections for 'Bucket name' (set to 'palomapmlbucket'), 'Copy settings from existing bucket - optional' (with a note about only bucket settings being copied), and a 'Choose bucket' button. At the bottom of the sidebar, it says 'Format: s3://bucket/prefix'. The main area is titled 'General purpose buckets (1)' and shows a single bucket named 'palomapmlbucket'. A red circle highlights the 'Name' column for this bucket, and a red arrow points from this circle to a 'Bucket Versioning' section below. This section contains a note about versioning and a toggle switch for 'Bucket Versioning' which is set to 'Enable'. To the right of the bucket list, there are tabs for 'Objects', 'Properties', 'Permissions', and 'Metrics' (which is selected). Below these tabs, there's a 'Storage Class Analysis (0)' section with a note about analyzing access patterns and a 'Create analytics configuration' button. At the top right of the main area, there are buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'.

4. ALMACENAMIENTO S3

4.1 Creación de Bucket S3 y Subida de Archivos

Subir algún archivo al nuevo bucket creado (botón Upload). Crear alguna carpeta para organizar los archivos (es posible usar Cut / Paste para mover los archivos entre las carpetas). Estudiar las propiedades de los archivos subidos al bucket (pulsando sobre la casilla de selección)

The screenshot shows the AWS S3 console interface. On the left, there is a list of objects in a bucket named 'practica-6'. The 'Upload' button is highlighted with a red circle. Below the table, another 'Upload' button is also highlighted with a red circle. On the right, a modal window titled 'Create folder' is open, showing a form to enter a 'Folder name' (with 'archivos' typed in) and a note about bucket policy restrictions.

Objects (0) Info

Actions ▾

Upload

No objects

You don't have any objects in this bucket.

Files and folders (1 Total, 1.9 KB)

All files and folders in this table will be uploaded.

Create folder Info

Your bucket policy might block folder creation

Folder name: archivos /

Find by name

Name	Type	Folder	Type
index.html	-		text/html

4. ALMACENAMIENTO S3

4.1 Creación de Bucket S3 y Subida de Archivos

Subir algún archivo al nuevo bucket creado (botón Upload). Crear alguna carpeta para organizar los archivos (es posible usar Cut / Paste para mover los archivos entre las carpetas). Estudiar las propiedades de los archivos subidos al bucket (pulsando sobre la casilla de selección del archivo). ¿Qué ocurre si intentamos descargar el archivo pulsando sobre su URL?

The screenshot shows the AWS S3 console interface. On the left, there is a list of objects in a bucket named 'archivos'. One object, 'index.html', is selected. A context menu is open over this file, with the 'Move' option highlighted. On the right, there is a 'Create folder' dialog box where a new folder named 'archivos/' has been created.

Objects (2) Info

- Upload
- Copy S3 URI
- Copy URL
- Download
- Open
- Delete
- Actions ▲
- Create folder

Download as
Share with a presigned URL
Calculate total size
Copy
Move
Initiate restore
Query with S3 Select
Edit actions
Rename object

Name	Type	Last modified	Size
archivos/	Folder	-	
<input checked="" type="checkbox"/> index.html	html	April 16, 2024, 19:33:44 (UTC+02:00)	

Files and folders (1 Total, 1.9 KB)

All files and folders in this table will be uploaded.

Name	Folder	Type
index.html	-	text/html

Create folder

Your bucket policy might block folder creation
If your bucket policy prevents uploading objects without specific tags, metadata, or access grantees, you will not be able to create a folder using this configuration. Instead, you can configuration to upload an empty folder and specify the appropriate settings.

Folder name: archivos/

Folder names can't contain "/". See rules for naming.

4. ALMACENAMIENTO S3

4.1 Creación de Bucket S3 y Subida de Archivos

Subir algún archivo al nuevo bucket creado (botón Upload). Crear alguna carpeta para organizar los archivos (es posible usar Cut / Paste para mover los archivos entre las carpetas). Estudiar las propiedades de los archivos subidos al bucket (pulsando sobre la casilla de selección del archivo). ¿Qué ocurre si intentamos descargar el archivo pulsando sobre su URL?

index.html [Info](#)

Copy S3 URI Download Open Object actions

Properties Permissions Versions

Object overview

Owner awslabsc0w4199845t1653611581

AWS Region US East (N. Virginia) us-east-1

Last modified April 16, 2024, 19:35:46 (UTC+02:00)

Size 1.9 KB

Type html

Key [archivos/index.html](#)

S3 URI s3://palomapmlbucket/archivos/index.html

Amazon Resource Name (ARN) arn:aws:s3:::palomapmlbucket/archivos/index.html

Entity tag (Etag) 7f50202904c5bef6acfe983471385ad2

Object URL <https://palomapmlbucket.s3.amazonaws.com/archivos/index.html>

No podemos acceder a el por qué no tenemos permisos

https://palomapmlbucket.s3.amazonaws.com/archivos/index.html

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>84XSMFS5ZNR9DKA</RequestId>
  <HostId>afm0JXgc8UrmPqZRjwqqpzthh/2Yb241zAg1Q+5EnGyYG0qh8Tc1ZSjebG3ST4+PUY07p7yHwVKgpcvJ5DpmCA==</HostId>
</Error>
```

4. ALMACENAMIENTO S3

4.2 Configuración para Hosting Web Estático

Vamos a usar el bucket para alojar contenidos web estáticos de acceso público a través de un URL. Para ello seleccionamos el bucket y editamos su configuración. Habrá que deshabilitar la **configuración de bloqueo de acceso público** y **escribir una política de bucket**. En Permisos, desactivar la opción Bloquear acceso público. En Propiedades, editar la sección Static website hosting, y activar esta opción, indicando en las propiedades las páginas index.html y error.html propuestas.

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access
View analyzer for us-east-1

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Block all public access

► Individual Block Public Access settings for this bucket

- Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
- Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Block all public access

⚠ Off

► Individual Block Public Access settings for this bucket

4. ALMACENAMIENTO S3

4.2 Configuración para Hosting Web Estático

Vamos a usar el bucket para alojar contenidos web estáticos de acceso público a través de un URL. Para ello seleccionamos el bucket y editamos su configuración. Habrá que deshabilitar la **configuración de bloqueo de acceso público** y **escribir una política de bucket**. En Permisos, desactivar la opción Bloquear acceso público. En Propiedades, editar la sección Static website hosting, y activar esta opción, indicando en las propiedades las páginas index.html y error.html propuestas.

The screenshot shows the AWS S3 console interface for configuring a static website host. On the left, there's a navigation bar with tabs for 'Objects', 'Properties' (which is selected), and 'Permissions'. Below this, under 'Static website hosting', it says 'Enabled' and 'Bucket hosting'. A red arrow points from the 'Enabled' text to the 'Enable' radio button in the right-hand configuration pane. Another red arrow points from the 'Disabled' text to the 'Hosting type' section in the right-hand pane. The right-hand pane contains sections for 'Static website hosting' (with a link to learn more), 'Static website hosting' configuration (radio buttons for 'Disable' or 'Enable', currently 'Enable' is selected), 'Hosting type' (radio buttons for 'Host a static website' or 'Redirect requests for an object', currently 'Host a static website' is selected), a note about making objects readable for public access (link to 'Using Amazon S3 Block Public Access'), 'Index document' (set to 'index.html'), and 'Error document - optional' (set to 'error.html').

4. ALMACENAMIENTO S3

4.3 Pruebas de Acceso y Descarga de Archivos

Añadir una página de inicio (index.html) en la raíz del bucket con un texto significativo. Si queremos acceder vía web a todos los contenidos del bucket será necesario establecer una política de acceso adecuada (en la misma pestaña de Permisos, añadir una Bucket policy). Podría ser algo similar a esto (sustituir el nombre del bucket por el que corresponda):

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "PublicReadGetObject",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "s3:GetObject",  
      "Resource": "arn:aws:s3:::nombre-del-bucket/*"  
    }  
  ]  
}
```

The screenshot shows the 'Files and folders' section of the AWS S3 console. It displays two uploaded files: 'error.html' and 'index.html'. Both files are of type 'text/html'. There are buttons for 'Remove', 'Add files', and 'Add folder' at the top right. A search bar labeled 'Find by name' is present. The table has columns for Name, Folder, and Type.

Name	Folder	Type
error.html	-	text/html
index.html	-	text/html

Subimos un
Index.html y
un error.html

The screenshot shows the 'Edit bucket policy' page. It includes sections for 'Bucket policy', 'Bucket ARN' (set to 'arn:aws:s3:::palomapmlbucket'), and 'Policy'. The policy JSON is identical to the one shown in the code block above, granting public read access to all objects in the bucket.

```
1 ▾ {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "PublicReadGetObject",  
6       "Effect": "Allow",  
7       "Principal": "*",  
8       "Action": "s3:GetObject",  
9       "Resource": "arn:aws:s3:::palomapmlbucket/*"  
10      }  
11    ]  
12 }
```

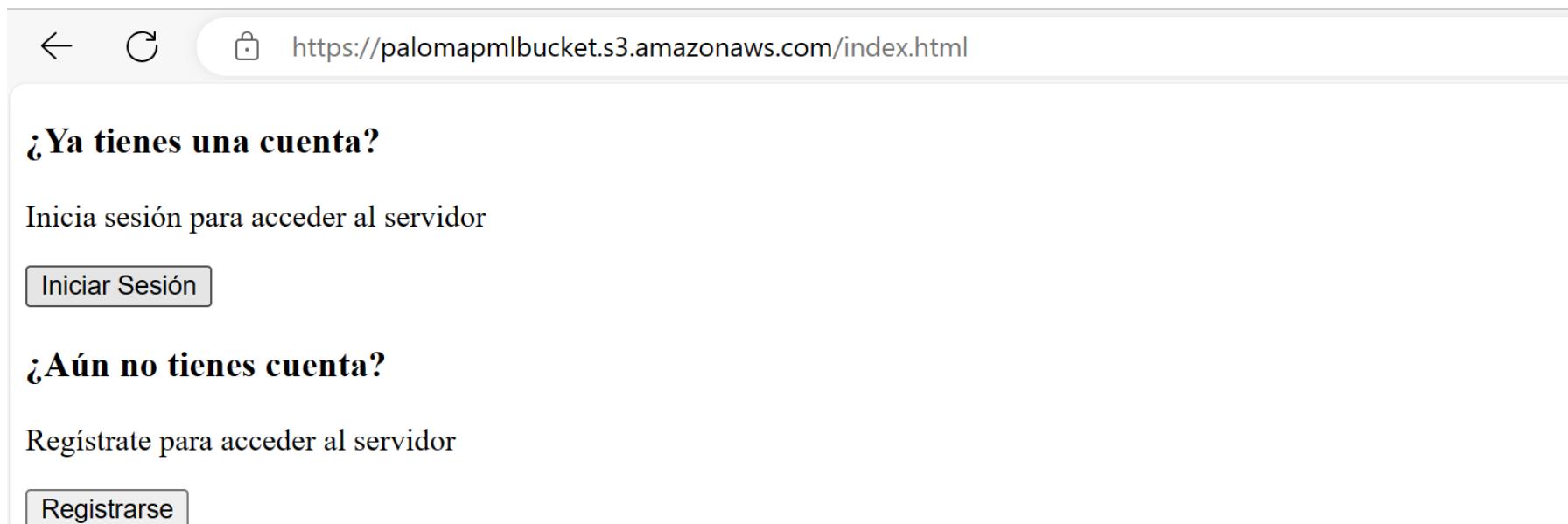
4. ALMACENAMIENTO S3

4.3 Pruebas de Acceso y Descarga de Archivos

Añadir una página de inicio (index.html) en la raíz del bucket con un texto significativo. Si queremos acceder vía web a todos los contenidos del bucket será necesario establecer una política de acceso adecuada (en la misma pestaña de Permisos, añadir una Bucket policy). Podría ser algo similar a esto (sustituir el nombre del bucket por el que corresponda):

Acceder a la URL de un objeto:

Objects >> index.html >><https://palomapmlbucket.s3.amazonaws.com/index.html>



4. ALMACENAMIENTO S3

4.4 Eliminación del Bucket

Desde el panel de control de S3 eliminar el bucket de pruebas

The screenshot illustrates the process of deleting an S3 bucket named "palomapmlbucket".

Step 1: Delete bucket
A message box states: "This bucket is not empty. Buckets must be empty before they can be deleted." A "Empty bucket" button is present.

Step 2: Empty bucket
A warning box lists: "Emptying the bucket deletes all objects in the bucket and cannot be undone.", "Objects added to the bucket while the empty bucket action is in progress might be deleted.", and "To prevent new objects from being added to this bucket while the empty bucket action is in progress, you might need to update your bucket policy to stop objects from being added to the bucket." A "Learn more" link is provided. Below, a note says: "If your bucket contains a large number of objects, creating a lifecycle rule to delete all objects in the bucket might be a more efficient way of emptying your bucket." A "Go to lifecycle rule configuration" link is available.

Step 3: Permanently delete all objects in bucket "palomapmlbucket"?
A confirmation message asks: "To confirm deletion, type *permanently delete* in the text input field." A text input field contains the text "permanently delete".

Step 4: Summary
The summary shows the source as "s3://palomapmlbucket" and indicates "Successfully deleted 6 objects, 7.1 KB".

ÍNDICE

1. Ejecución de Instancias EC2

- 1.1 Acceso a la Consola y Creación de Claves
- 1.2 Creación de Grupo de Seguridad
- 1.3 Comprobación de VPC y Subredes
- 1.4 Lanzamiento de Instancia PruebasWeb
- 1.5 Configuración de la Instancia y Tareas de Mantenimiento
- 1.6 Efecto de Reinicio y Detención de la Instancia
- 1.7 Generación de Imagen de la Instancia
- 1.8 Terminación de la Instancia

2. Balanceador de Carga ELB (Elastic Load Balancer)

- 2.1 Lanzamiento de Instancias y Creación de Grupo de Seguridad
- 2.2 Creación de Grupo de Destinatarios
- 2.3 Creación de Balanceador de Carga
- 2.4 Pruebas de Acceso y Balanceo
- 2.5 Acceso por SSH a Instancias Internas
- 2.6 Terminación de Instancias y Recursos Asociados

3. Subredes Públicas/Privadas y NAT Gateway

- 3.1 Creación de Subredes y Lanzamiento de Instancias
- 3.2 Configuración de NAT Gateway y Tablas de Rutas
- 3.3 Configuración de Network ACLs
- 3.4 Terminación de Instancias, NAT Gateway y Recursos Asociados

4. Almacenamiento S3

- 4.1 Creación de Bucket S3 y Subida de Archivos
- 4.2 Configuración para Hosting Web Estático
- 4.3 Pruebas de Acceso y Descarga de Archivos
- 4.4 Eliminación del Bucket

5. Autoescalado para Aplicaciones Web

- 5.1 Creación de Grupo de Destinatarios y Balanceador
- 5.2 Creación de Plantilla de Lanzamiento y Grupo de Autoescalado
- 5.3 Configuración de Escalado Automático
- 5.4 Pruebas de Funcionamiento del Escalado
- 5.5 Eliminación de Recursos de Autoescalado

5. AUTOESCALADO PARA APLICACIONES WEB

5.1 Creación de Grupo de Destinatarios y Balanceador

Vamos a definir un grupo de auto escalado horizontal para un servicio web. Estará formado por un balanceador ELB y entre 2 y 5 instancias EC2 que ejecutarán la imagen ServidorWeb creada en el apartado 2 y que tiene instalado el servidor Apache. Las instancias se irán levantando o deteniendo en función de la demanda del servicio. La configuración del auto escalado requiere definir el balanceador al que se asociarán las instancias, la imagen AMI y el tipo de máquina que usaremos (en la sección Launch Templates) y las características del escalado (en la sección Auto Scaling Group): número inicial y máximo de instancias, zona(s) en las que se lanzarán y condiciones de arranque/detención.

Creamos un grupo de destinatarios (ServicioWeb-tg) de tipo Instancia, con protocolo y check HTTP, e inicialmente sin destinatarios. A continuación, creamos un balanceador de carga de aplicación (ServicioWeb-elb), de tipo Internet-facing HTTP para IPv4. Trabajará en las zonas a y b, donde se lanzarán las instancias, con el grupo de seguridad SSH_HTTP_Any y el grupo de destinatarios creado (ServicioWeb-tg).

Protocol : Port
Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some anomaly detection for the targets and you can set mitigation options once your target group is created. This choice after creation

HTTP ▾ 80
1-65535

IP address type
Only targets with the indicated IP address type can be registered to this target group.

- IPv4**
Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.
- IPv6**
Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#) ▾

VPC
Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected in the previous step are available in this list.

vpc-00a5dfc0664ac615a
IPv4 VPC CIDR: 172.31.0.0/16

Protocol version
 HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or

ServicioWeb-tg

Details

arn:aws:elasticloadbalancing:us-east-1:1958486390477:targetgroup/ServicioWeb-tg/83d8df5873c61723

Target type
Instance

Protocol : Port
HTTP: 80

Protocol version
HTTP1

5. AUTOESCALADO PARA APLICACIONES WEB

5.1 Creación de Grupo de Destinatarios y Balanceador

Creamos un grupo de destinatarios (ServicioWeb-tg) de tipo Instancia, con protocolo y check HTTP, e inicialmente sin destinatarios. A continuación, creamos un balanceador de carga de aplicación (ServicioWeb-elb), de tipo Internet-facing HTTP para IPv4. Trabajará en las zonas a y b, donde se lanzarán las instancias, con el grupo de seguridad SSH_HTTP_Any y el grupo de destinatarios creado (ServicioWeb-tg).

Basic configuration	
Load balancer name Name must be unique within your AWS account and can't be changed. ServicioWeb-elb A maximum of 32 alphanumeric characters including hyphens are allowed.	Network mapping <small>Info</small> The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.
Scheme <small>Info</small> Scheme can't be changed after the load balancer is created. <input checked="" type="radio"/> Internet-facing An internet-facing load balancer routes requests from clients <input type="radio"/> Internal An internal load balancer routes requests from clients to targets.	VPC <small>Info</small> Select the virtual private cloud (VPC) for your targets or you can create a new VPC . Only VPCs with an internet gateway are listed. To confirm the VPC for your targets, view your target groups . - vpc-00a5dfc0664ac615a IPv4 VPC CIDR: 172.31.0.0/16
IP address type <small>Info</small> Select the type of IP addresses that your subnets use. <input checked="" type="radio"/> IPv4 Includes only IPv4 addresses. <input type="radio"/> Dualstack Includes IPv4 and IPv6 addresses.	Mappings <small>Info</small> Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones. If the target or the VPC are not available for selection. <input checked="" type="checkbox"/> us-east-1a (use1-az1) Subnet subnet-0096e44e33f1d04e8 IPv4 address Assigned by AWS <input checked="" type="checkbox"/> us-east-1b (use1-az2) Subnet subnet-0d183fe04df17c9dd IPv4 address Assigned by AWS

Protocol:Port	Default action
HTTP:80	Forward to target group <ul style="list-style-type: none">ServicioWeb-tg: 1 (100%)Group-level stickiness: Off

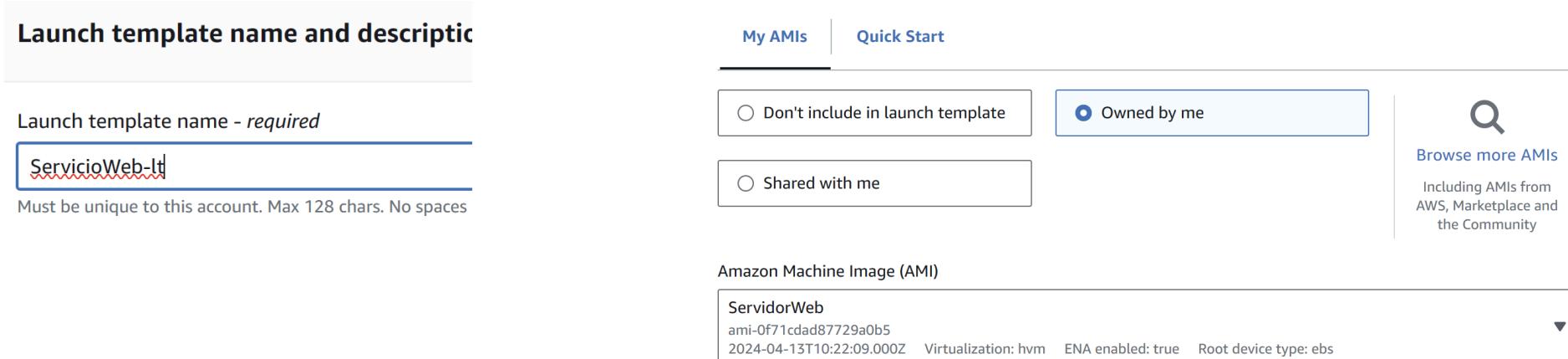
Security groups	
<small>A security group is a set of firewall rules that control the traffic to and from your instances.</small>	
Security groups <small>Select up to 5 security groups</small>	PR6_SecurityGroup <small>X</small> sg-0720b0ae0ed758ea5 VPC: vpc-00a5dfc0664ac615a

5. AUTOESCALADO PARA APLICACIONES WEB

5.2 Creación de Plantilla de Lanzamiento y Grupo de Autoescalado

Creamos una Plantilla de Lanzamiento (ServicioWeb-It). Nota: Anteriormente se usaban Configuraciones de Lanzamiento, pero se recomienda migrar a las nuevas Plantillas de Lanzamiento.

Seleccionamos Launch Templates (en la sección Instances) y a continuación Create Launch Instance. Damos el nombre a la plantilla (ServicioWeb-It). Usaremos nuestra AMI (ServidorWeb) con tipo de instancia t2.micro, y nuestra pareja de claves SSH. No incluimos la subred en la plantilla, y sí el grupo de seguridad (SSH_HTTP_Any: usamos este para poder conectarnos a las instancias también desde el exterior por SSH, aunque realmente no sería necesario, sería suficiente con el servicio HTTP accesible sólo desde la VPC). Salvamos la plantilla. En este punto podemos seleccionar la creación del grupo de autoescalamiento, o no activar la opción y hacerlo a continuación en un nuevo paso.



- ▼ Instances
- Instances
- Instance Types

5. AUTOESCALADO PARA APLICACIONES WEB

5.2 Creación de Plantilla de Lanzamiento y Grupo de Autoescalado

Creamos una Plantilla de Lanzamiento (ServicioWeb-It). Nota: Anteriormente se usaban Configuraciones de Lanzamiento, pero se recomienda migrar a las nuevas Plantillas de Lanzamiento.

Seleccionamos Launch Templates (en la sección Instances) y a continuación Create Launch Instance. Damos el nombre a la plantilla (ServicioWeb-It). Usaremos nuestra AMI (ServidorWeb) con tipo de instancia t2.micro, y nuestra pareja de claves SSH. No incluimos la subred en la plantilla, y sí el grupo de seguridad (SSH_HTTP_Any: usamos este para poder conectarnos a las instancias también desde el exterior por SSH, aunque realmente no sería necesario, sería suficiente con el servicio HTTP accesible sólo desde la VPC). Salvamos la plantilla. En este punto podemos seleccionar la creación del grupo de autoescalado, o no activar la opción y hacerlo a continuación en un nuevo paso.

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro	Free tier eligible		
Family: t2	1 vCPU	1 GiB Memory	Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour			
On-Demand SUSE base pricing: 0.0116 USD per Hour			
On-Demand RHEL base pricing: 0.0716 USD per Hour			
On-Demand Linux base pricing: 0.0116 USD per Hour			

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access before you launch the instance.

Key pair name

▼ Network settings [Info](#)

Subnet [Info](#)

Don't include in launch template

When you specify a subnet, a network interface is automatically added to your template.

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to your instance.

Select existing security group

Create security group

Security groups [Info](#)

Select security groups

PR6_SecurityGroup sg-0720b0ae0ed758ea5 X
VPC: vpc-00a5dfc0664ac615a

► Advanced network configuration

Launch Template ID	Launch Template Name
lt-0fe01a0e3ddb9c69d	ServicioWeb-It

5. AUTOESCALADO PARA APLICACIONES WEB

5.2 Creación de Plantilla de Lanzamiento y Grupo de Autoescalamiento

Creamos una Plantilla de Lanzamiento (ServicioWeb-It). Nota: Anteriormente se usaban Configuraciones de Lanzamiento, pero se recomienda migrar a las nuevas Plantillas de Lanzamiento.

Seleccionamos Launch Templates (en la sección Instances) y a continuación Create Launch Instance. Damos el nombre a la plantilla (ServicioWeb-It). Usaremos nuestra AMI (ServidorWeb) con tipo de instancia t2.micro, y nuestra pareja de claves SSH. No incluimos la subred en la plantilla, y sí el grupo de seguridad (SSH_HTTP_Any: usamos este para poder conectarnos a las instancias también desde el exterior por SSH, aunque realmente no sería necesario, sería suficiente con el servicio HTTP accesible sólo desde la VPC). Salvamos la plantilla. En este punto podemos seleccionar la creación del grupo de autoescalado, o no activar la opción y hacerlo a continuación en un nuevo paso.

Launch Template ID	Launch Template Name	Default Version	Latest Ver	
lt-0fe01a0e3ddb9c69d	ServicioWeb-It	1	1	<ul style="list-style-type: none">Delete templateDelete template versionSet default versionManage tagsCreate Spot FleetCreate Auto Scaling group

5. AUTOESCALADO PARA APLICACIONES WEB

5.2 Creación de Plantilla de Lanzamiento y Grupo de Autoescalado

Creamos un nuevo grupo de Auto Scaling (ServicioWeb-as). Seleccionamos la plantilla de lanzamiento creada previamente (ServicioWeb-It). En la sección de Network, establecemos la VPC y las subredes donde se crearán todas las instancias (subredes públicas de las zonas a y b). A continuación, asociamos el balanceador de carga ya definido, a través del Target Group. En el chequeo dejamos seleccionado el tipo de comprobación de estado EC2, y el periodo de comprobación de gracia de 300 segundos (no hace falta activar la monitorización por parte del balanceador). Activamos la monitorización de CloudWatch. En cuanto al tamaño del grupo, establecemos inicialmente las capacidades deseada, mínima y máxima en 2, y NO activamos la política de escalado. No añadimos notificaciones ni etiquetas. Aparecerá un resumen de configuración. Creamos el grupo de autoescalado y se inicia.

The screenshot shows the AWS Auto Scaling Create Auto Scaling Group wizard with three main steps:

- Name**: Set the Auto Scaling group name to "ServicioWeb-as".
- Network**: Set the VPC to "vpc-00a5dfc0664ac615a" and choose "us-east-1a | subnet-0096e44e33f1d04e8" and "us-east-1b | subnet-0d183fe04df17c9dd" as Availability Zones and subnets.
- Load balancing**: Select "Attach to an existing load balancer" and choose "ServicioWeb-tg | HTTP" as the target group.

Summary: The summary table includes:

Setting	Value
Auto Scaling group name	ServicioWeb-as
VPC	vpc-00a5dfc0664ac615a
Launch template	ServicioWeb-It
Subnets	us-east-1a subnet-0096e44e33f1d04e8, us-east-1b subnet-0d183fe04df17c9dd
Load balancer	ServicioWeb-tg HTTP
Min. instances	1
Max. instances	2
Health check type	EC2
Health check period	300
CloudWatch Metrics	Enabled

5. AUTOESCALADO PARA APLICACIONES WEB

5.2 Creación de Plantilla de Lanzamiento y Grupo de Autoescalado

Creamos un nuevo grupo de Auto Scaling (ServicioWeb-as). Seleccionamos la plantilla de lanzamiento creada previamente (ServicioWeb-It). En la sección de Network, establecemos la VPC y las subredes donde se crearán todas las instancias (subredes públicas de las zonas a y b). A continuación, asociamos el balanceador de carga ya definido, a través del Target Group. En el chequeo dejamos seleccionado el tipo de comprobación de estado EC2, y el periodo de comprobación de gracia de 300 segundos (no hace falta activar la monitorización por parte del balanceador). Activamos la monitorización de CloudWatch. En cuanto al tamaño del grupo, establecemos inicialmente las capacidades deseada, mínima y máxima en 2, y NO activamos la política de escalado. No añadimos notificaciones ni etiquetas. Aparecerá un resumen de configuración. Creamos el grupo de autoescalado y se inicia.

The screenshot shows the configuration of a launch template for an Auto Scaling group. It includes sections for Health checks, Additional settings, Automatic scaling - optional, and Scaling limits.

Health checks
Health checks increase availability by replacing unhealthy instances. When one fails, instance replacement occurs.

EC2 health checks
 Always enabled

Additional health check types - optional
 Turn on Elastic Load Balancing health checks (Recommended)
Elastic Load Balancing monitors whether instances are available to handle requests and can replace it on its next periodic check.
 Turn on VPC Lattice health checks
VPC Lattice can monitor whether instances are available to handle requests and replaces it after its next periodic check.

Health check grace period | Info
This time period delays the first health check until your instances finish initializing and are placed into a non-running state.
300 seconds

Additional settings

Monitoring | Info
 Enable group metrics collection within CloudWatch

Automatic scaling - optional

Choose whether to use a target tracking policy | Info
You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

No scaling policies
Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

Target tracking scaling
Choose a CloudWatch metric and CloudWatch Metrics Insights scaling policy to automatically adjust the capacity based on the metric's value.

Group size | Info
Set the initial size of the Auto Scaling group. After creating the group, you can change the size using the Set desired capacity button or the CloudWatch Metrics Insights scaling policy.
Desired capacity type: Units (number of instances)

Desired capacity
Specify your group size.
2

Scaling | Info
You can resize your Auto Scaling group manually or automatically to meet changing demands.

Scaling limits
Set limits on how much your desired capacity can be increased or decreased.
Min desired capacity: 2
Max desired capacity: 2
Equal or less than desired capacity
Equal or greater than desired capacity

5. AUTOESCALADO PARA APLICACIONES WEB

5.2 Creación de Plantilla de Lanzamiento y Grupo de Autoescalado

Creamos un nuevo grupo de Auto Scaling (ServicioWeb-as). Seleccionamos la plantilla de lanzamiento creada previamente (ServicioWeb-It). En la sección de Network, establecemos la VPC y las subredes donde se crearán todas las instancias (subredes públicas de las zonas a y b). A continuación, asociamos el balanceador de carga ya definido, a través del Target Group. En el chequeo dejamos seleccionado el tipo de comprobación de estado EC2, y el periodo de comprobación de gracia de 300 segundos (no hace falta activar la monitorización por parte del balanceador). Activamos la monitorización de CloudWatch. En cuanto al tamaño del grupo, establecemos inicialmente las capacidades deseada, mínima y máxima en 2, y NO activamos la política de escalado. No añadimos notificaciones ni etiquetas. Aparecerá un resumen de configuración. Creamos el grupo de autoescalado y se inicia.

The screenshot shows the AWS Auto Scaling Groups page. At the top, there is a sidebar for 'Instance maintenance policy' which includes sections for 'Control your Auto Scaling group's availability during instance lifetime features and events that happen automatically' and 'Choose a replacement behavior depending on your needs'. It lists two options: 'Mixed behavior' (selected) and 'Prioritize availability'. The 'Mixed behavior' section describes that for rebalancing events, new instances will launch before terminating others, while for all other events, instances terminate and launch at the same time. The 'Prioritize availability' section describes launching new instances and waiting for them to be ready before terminating others, allowing you to scale above your desired capacity by a percentage and temporarily incur costs.

The main area displays the 'Auto Scaling groups (1)' table. The table has columns for Name, Launch template/configuration, Instances, Status, Desired capacity, Min, and Max. One row is shown for 'ServicioWeb-as', which uses the 'ServicioWeb-It' launch template, has 0 instances, and is in an 'Updating capacity...' status with a desired capacity of 2, min of 2, and max of 2. There are buttons for 'Launch configurations', 'Launch templates', 'Actions', and a 'Create Auto Scaling group' button.

5. AUTOESCALADO PARA APLICACIONES WEB

5.3 Configuración de Escalado Automático

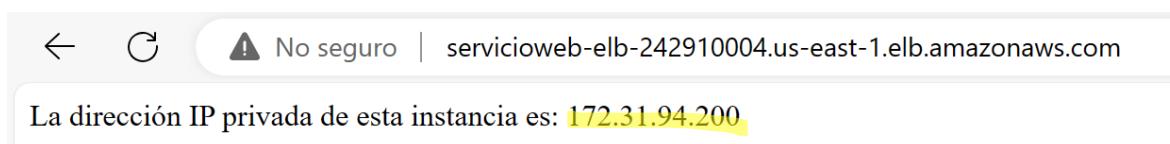
Comprobamos que se lanzan automáticamente las dos primeras instancias (las únicas que arrancarán). También podemos comprobar que las instancias se han registrado en el balanceador y que se reparte el tráfico web entre las mismas (accedemos al servicio a través del nombre de DNS del Balanceador ServicioWeb-elb). Todavía no hay escalado y sólo se lanzarán nuevas instancias si dejan de funcionar las actuales (podemos comprobarlo si terminamos alguna de ellas o detenemos su servicio HTTP; la pestaña de Activity nos informa del comportamiento del grupo de AutoEscalado).

<input checked="" type="checkbox"/>	Name	Launch template/configuration	Instances	Status	Desired capacity	
<input checked="" type="checkbox"/>	ServicioWeb-as	ServicioWeb-It Version Default	2	-	2	
<input type="text"/> Find Instance by attribute or tag (case-sensitive)				All states	< 1 >	
<input type="checkbox"/>	Name 	Instance ID	Instance state	Instance type	Status check	
<input type="checkbox"/>		i-004b72df56d423676	 Running  	t2.micro	 2/2 checks passed View alarms 	us-east-1a
<input type="checkbox"/>		i-05c466090f3bcffa1	 Running  	t2.micro	 Initializing View alarms 	us-east-1b

5. AUTOESCALADO PARA APLICACIONES WEB

5.3 Configuración de Escalado Automático

Comprobamos que se lanzan automáticamente las dos primeras instancias (las únicas que arrancarán). También podemos comprobar que las instancias se han registrado en el balanceador y que se reparte el tráfico web entre las mismas (accedemos al servicio a través del nombre de DNS del Balanceador ServicioWeb-elb). Todavía no hay escalado y sólo se lanzarán nuevas instancias si dejan de funcionar las actuales (podemos comprobarlo si terminamos alguna de ellas o detenemos su servicio HTTP; la pestaña de Activity nos informa del comportamiento del grupo de AutoEscalado).

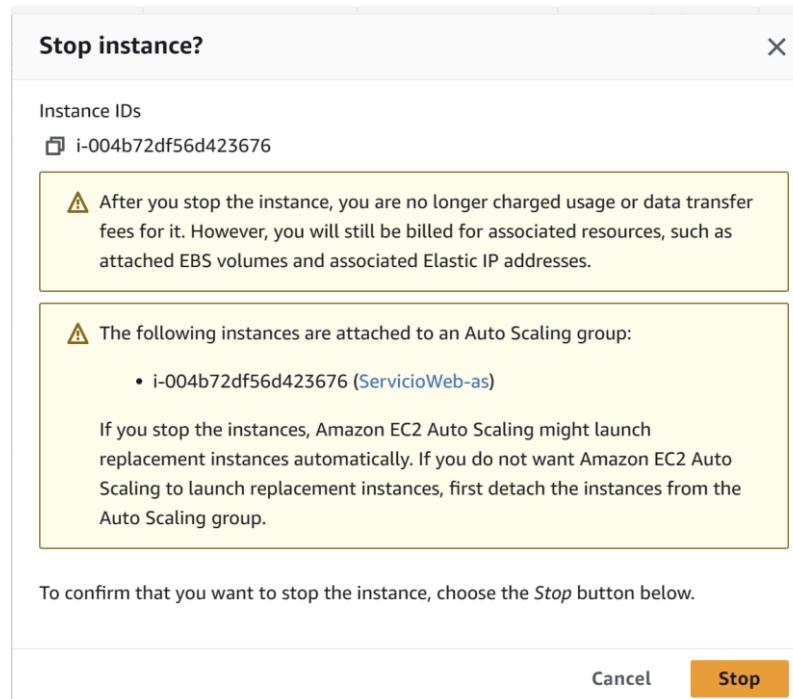


Two screenshots of the AWS Lambda console showing the details of two Lambda functions. The first function, "Instance: i-004b72df56d423676", has a Public IPv4 address **52.54.68.248** and a Private IPv4 address **172.31.12.88**. The second function, "Instance: i-05c466090f3bcffa1", has a Public IPv4 address **44.212.39.145** and a Private IPv4 address **172.31.94.200**.

5. AUTOESCALADO PARA APLICACIONES WEB

5.4 Pruebas de Funcionamiento del Escalado

Comprobamos que se lanzan automáticamente las dos primeras instancias (las únicas que arrancarán). También podemos comprobar que las instancias se han registrado en el balanceador y que se reparte el tráfico web entre las mismas (accedemos al servicio a través del nombre de DNS del Balanceador ServicioWeb-elb). Todavía no hay escalado y sólo se lanzarán nuevas instancias si dejan de funcionar las actuales (podemos comprobarlo si terminamos alguna de ellas o detenemos su servicio HTTP; la pestaña de Activity nos informa del comportamiento del grupo de AutoEscalado).



	Name	Instance ID	Instance state
		i-004b72df56d423676	Stopped
		i-05c466090f3bcffa1	Running
		i-02828bbc27b325e85	Pending

Se crea una nueva instancia

Auto Scaling group: ServicioWeb-as		
Successf ul	Launching a new EC2 instance: i-02828bbc27b325e85	At 2024-04-17T14:27:11Z an instance was launched in response to an unhealthy instance needing to be replaced.
Connecti on draining i n progress	Terminating EC2 instance: i-004b72df56d423676 - Waiting For ELB Connection Draining.	At 2024-04-17T14:27:11Z an instance was taken out of service in response to an EC2 health check indicating it has been terminated or stopped.
Successf ul	Launching a new EC2 instance: i-004b72df56d423676	At 2024-04-17T14:13:03Z a user request created an AutoScalingGroup changing the desired capacity from 0 to 2. At 2024-04-17T14:13:14Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 0 to 2.
Successf ul	Launching a new EC2 instance: i-05c466090f3bcffa1	At 2024-04-17T14:13:03Z a user request created an AutoScalingGroup changing the desired capacity from 0 to 2. At 2024-04-17T14:13:14Z an instance was started in response to a difference between desired and actual capacity, increasing the capacity from 0 to 2.

5. AUTOESCALADO PARA APLICACIONES WEB

5.4 Pruebas de Funcionamiento del Escalado

Vamos a modificar el grupo de auto escalado creado (ServicioWeb-as). Editamos los Group Details y mantenemos la capacidad mínima y deseada a 2 instancias, y aumentamos a 5 su capacidad máxima. Salvamos con Update. En la pestaña Automatic Scaling creamos una política dinámica de escalado. Seleccionamos su tipo en Target tracking scaling, le damos el nombre PoliticaEscalado, métrica de CPU y umbral de 50 (se activará cuando el consumo total de todas las instancias pase del 50%).

Auto Scaling group: ServicioWeb-as

Group details			
Auto Scaling group name ServicioWeb-as	Desired capacity 2	Desired capacity type Units (number of instances)	Amazon Resource Name (ARN) <code>arn:aws:autoscaling:us-east-1:958486390477:autoScalingGroup:ade074f8-f834-4e03-9184-b514a44915e6:autoScalingGroupName/ServicioWeb-as</code>
Date created Wed Apr 17 2024 16:13:03 GMT+0200 (hora de verano de Europa central)	Minimum capacity 2	Status -	
	Maximum capacity 2		

Edit (button circled in red)

Group size
Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum scaling limits.

Desired capacity type
Choose the unit of measurement for the desired capacity value. vCPUs and Memory(GiB) are only supported for mixed instances groups configured with a set of instance attributes.

Units (number of instances) ▾

Desired capacity
Specify your group size.

Scaling limits
Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity

Equal or less than desired capacity

Max desired capacity

Equal or greater than desired capacity

Cancel **Update**

5. AUTOESCALADO PARA APLICACIONES WEB

5.4 Pruebas de Funcionamiento del Escalado

Vamos a modificar el grupo de auto escalado creado (ServicioWeb-as). Editamos los Group Details y mantenemos la capacidad mínima y deseada a 2 instancias, y aumentamos a 5 su capacidad máxima. Salvamos con Update. En la pestaña Automatic Scaling creamos una política dinámica de escalado. Seleccionamos su tipo en Target tracking scaling, le damos el nombre PoliticaEscalado, métrica de CPU y umbral de 50 (se activará cuando el consumo total de todas las instancias pase del 50%).

The screenshot shows the 'Create dynamic scaling policy' wizard in the AWS Management Console. The steps are:

- Step 1: Policy type**
Selected: Target tracking scaling.
- Step 2: Scaling policy name**
Name: PoliticaEscalado.
- Step 3: Metric type**
Selected: Average CPU utilization.
Info: Monitored metric that determines if resource utilization is too low or high. If using EC2 better scaling performance.
- Step 4: Target value**
Value: 50.
- Step 5: Instance warmup**
Value: 300 seconds.
- Step 6: Disable scale in to create only a scale-out policy**
 (unchecked).

5. AUTOESCALADO PARA APLICACIONES WEB

5.4 Pruebas de Funcionamiento del Escalado

Podemos comprobar el funcionamiento del escalado abriendo una sesión SSH en las dos instancias iniciales y forzando un uso intensivo de la CPU con el programa stress, instalado previamente (ej: `stress --cpu 1 --timeout 60m`). Al aumentar el consumo de CPU el número de instancias debería aumentar a 4 o 5 (hay que esperar unos minutos: consultar el historial de actividad). Posteriormente, si desactivamos el programa de stress el número de instancias debería volver a bajar a 2 (pacienza, tarda bastante...).

```
[ec2-user@ip-172-31-94-200 ~]$ stress --cpu 1 --timeout 60m
stress: info: [4123] dispatching hogs: 1 cpu, 0 io, 0 vm, 0 hdd
```

Instances (5) Info						
<input type="checkbox"/>	Name ✎	Instance ID	Instance state	Instance type	Status check	Alarm status
<input type="checkbox"/>		i-0a46b1c457467efae	Running ? Q	t2.micro	Initializing ?	View alarms +
<input type="checkbox"/>	✎	i-004b72df56d423676	Terminated ? Q	t2.micro	-	View alarms +
<input type="checkbox"/>		i-09c150b77fb276974	Running ? Q	t2.micro	Initializing ?	View alarms +
<input type="checkbox"/>		i-05c466090f3bcffa1	Running ? Q	t2.micro	2/2 checks passed ?	View alarms +
<input type="checkbox"/>		i-02828bbc27b325e85	Running ? Q	t2.micro	2/2 checks passed ?	View alarms +

5. AUTOESCALADO PARA APLICACIONES WEB

5.4 Pruebas de Funcionamiento del Escalado

Podemos comprobar el funcionamiento del escalado abriendo una sesión SSH en las dos instancias iniciales y forzando un uso intensivo de la CPU con el programa stress, instalado previamente (ej: stress --cpu 1 --timeout 60m). Al aumentar el consumo de CPU el número de instancias debería aumentar a 4 o 5 (hay que esperar unos minutos: consultar el historial de actividad). Posteriormente, si desactivamos el programa de stress el número de instancias debería volver a bajar a 2 (pacienza, tarda bastante...).

Desactivamos stress:

Grupo Autoescalado >> Monitoring>> Instance Management

Instance ID	Lifecycle	Instance Type	Weight	Launch Configuration	Availability Zone	Health Status	Pro
i-02828bbc27b325e85	Terminating	t2.micro	-	ServicioWeb-lt	us-east-1a	Healthy	
i-05c466090f3bcffa1	InService	t2.micro	-	ServicioWeb-lt	us-east-1b	Healthy	
i-09c150b77fb276974	Terminating	t2.micro	-	ServicioWeb-lt	us-east-1b	Healthy	
i-0a46b1c457467efae	InService	t2.micro	-	ServicioWeb-lt	us-east-1a	Healthy	

5. AUTOESCALADO PARA APLICACIONES WEB

5.5 Eliminación de Recursos de Autoescalado

Una vez completado el apartado eliminar el Grupo de auto escalado creado (se terminarán todas las instancias del grupo, aunque el proceso es lento). Eliminar también el balanceador, el grupo de destinatarios, y la plantilla de lanzamiento.

The image contains four screenshots of the AWS Management Console:

- Auto Scaling groups (1/1) Info**: Shows a single group named "ServicioWeb-as". The "Actions" menu is open, with the "Delete" option highlighted.
- Load balancers (1/1)**: Shows one load balancer named "ServicioWeb-elb". The "Actions" menu is open, with the "Delete load balancer" option highlighted.
- Target groups (1/1) Info**: Shows one target group named "ServicioWeb-tg". The "Actions" menu is open, with the "Delete" option highlighted.
- Launch Templates (1/1) Info**: Shows one launch template named "ServicioWeb-lt". The "Actions" menu is open, with the "Delete template" option highlighted.