

[Home](#)

[About](#)

AWS
AWS
AWS

Diana Alejandra Radu Giju

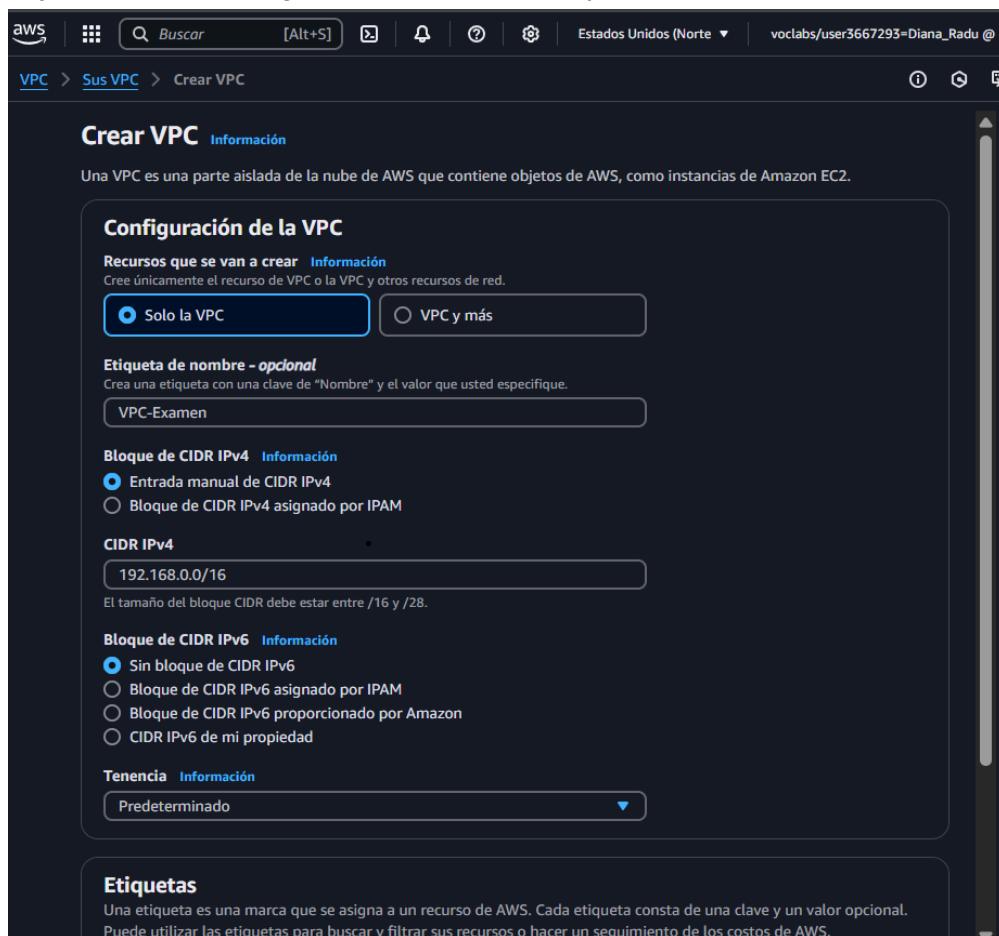
PARTE 1: AWS Y RED

1. Acceder a AWS y Navegar hasta el Servicio VPC

1. Inicia sesión en la Consola de AWS.
2. En el buscador de servicios, escribe **VPC** y selecciona **VPC (Virtual Private Cloud)**.
3. Dentro del servicio de VPC, haz clic en **Crear VPC**.

2. Crear una VPC Personalizada

1. En la sección de "Crear VPC", selecciona la opción **VPC con una sola subred**.
2. Asigna el nombre **VPC-Examen**.
3. En el campo de "Bloque CIDR IPv4", ingresa **192.168.0.0/16**.
4. Deja el resto de configuraciones por defecto y haz clic en **Crear VPC**.



3. Crear una Subred Pública

1. En el panel izquierdo, selecciona **Subredes** y haz clic en **Crear subred**.
2. Selecciona la **VPC-Examen**.
3. Asigna el nombre **SubredPublica**.
4. Elige una zona de disponibilidad (por ejemplo: us-east-1a) o déjala predeterminada.
5. Ingresa el bloque CIDR **192.168.1.0/24**.

6. Haz clic en **Crear subred**.

Crear subred [Información](#)

VPC

ID de la VPC
Cree subredes en esta VPC.

vpc-03c4ba4ac066b1515 (VPC-Examen) ▾

CIDR de VPC asociados

CIDR IPv4
192.168.0.0/16

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

Subred 1 de 1

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

subredPublica

El nombre puede tener un máximo de 256 caracteres.

Zona de disponibilidad [Información](#)
Elija la zona en la que residirá la subred o deje que Amazon elija una por usted.

Sin preferencia ▾

Bloque de CIDR de VPC IPv4 [Información](#)
Elija el bloque CIDR IPv4 de la VPC para la subred. El CIDR IPv4 de la subred debe estar dentro de este bloque.

192.168.0.0/16 ▾

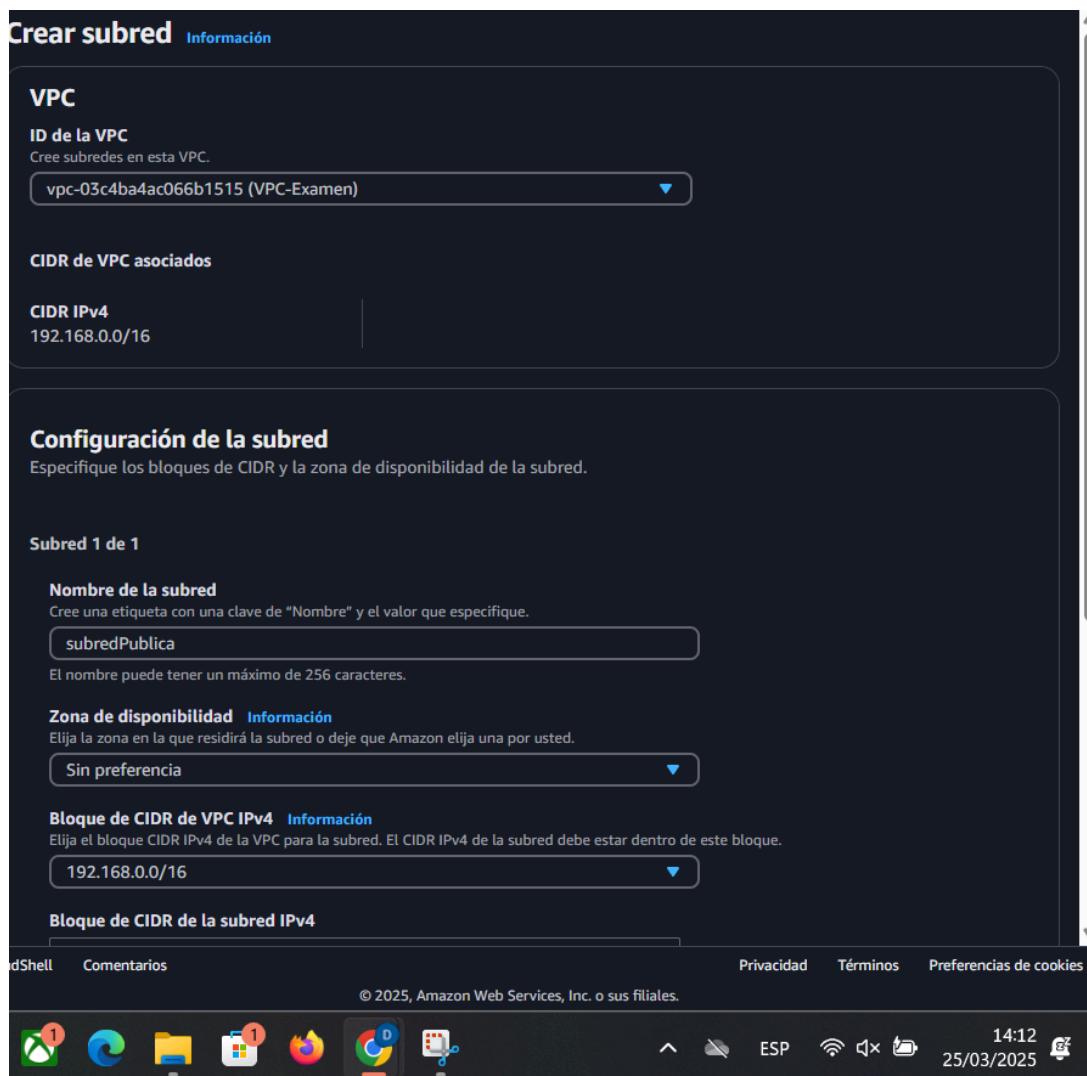
Bloque de CIDR de la subred IPv4

cmdShell Comentarios

Privacidad Términos Preferencias de cookies

© 2025, Amazon Web Services, Inc. o sus filiales.

14:12 25/03/2025



VPC > Subredes > Crear subred

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

Subred 1 de 1

Nombre de la subred
Cree una etiqueta con una clave de "Nombre" y el valor que especifique.
El nombre puede tener un máximo de 256 caracteres.

Zona de disponibilidad [Información](#)
Elija la zona en la que residirá la subred o deje que Amazon elija una por usted.

Bloque de CIDR de VPC IPv4 [Información](#)
Elija el bloque CIDR IPv4 de la VPC para la subred. El CIDR IPv4 de la subred debe estar dentro de este bloque.

Bloque de CIDR de la subred IPv4
 256 IPs
[Ajustar](#)

Etiquetas: opcional

Clave	Valor - opcional
<input type="text" value="Name"/> X	<input type="text" value="subredPublica"/> X Quitar

[Agregar nueva etiqueta](#)
Puede agregar 49 más etiquetas.
[Quitar](#)

[Agregar nueva subred](#)

[Cancelar](#) [Crear subred](#)

CloudShell Comentarios Privacidad Términos Preferencias de cookies

4. Configurar una Internet Gateway y Asociarla a la VPC

1. En el panel izquierdo, selecciona **Gateways de Internet** y haz clic en **Crear Internet Gateway**.
2. Asigna el nombre **gatewayExamen** y haz clic en **Crear Internet Gateway**.
3. Luego de la creación, selecciona la **gatewayExamen**, haz clic en **Acciones > Conecta a la VPC**.

4. Selecciona **VPC-Examen** y haz clic en **Conejar Gateway de Internet**.

The screenshot shows the 'Crear gateway de Internet' (Create Internet Gateway) wizard. The current step is 'Configuración de gateway de Internet' (Internet Gateway Configuration). In the 'Etiquetas: opcional' (Optional Tags) section, a tag 'Name' is added with the value 'gatewayExamen'. The 'Cancelar' (Cancel) and 'Crear gateway de Internet' (Create Internet Gateway) buttons are at the bottom.

CloudShell Comentarios © 2025, Amazon Web Services, Inc. o sus filiales. Privacidad Términos Preferencias de cookies

aws Buscar [Alt+S] Estados Unidos (Norte de Virginia) vocabs/user3667293=Diana_Radu @ 0126-2968-3249

VPC > Gateways de Internet > Conectar a la VPC (igw-09c2ae4bdcc095921)

Conectar a la VPC (igw-09c2ae4bdcc095921) Información

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

VPC disponibles Conecte la gateway de Internet a esta VPC.

vpc-05c4ba4ac066b1515

Comando de la interfaz de línea de comandos de AWS

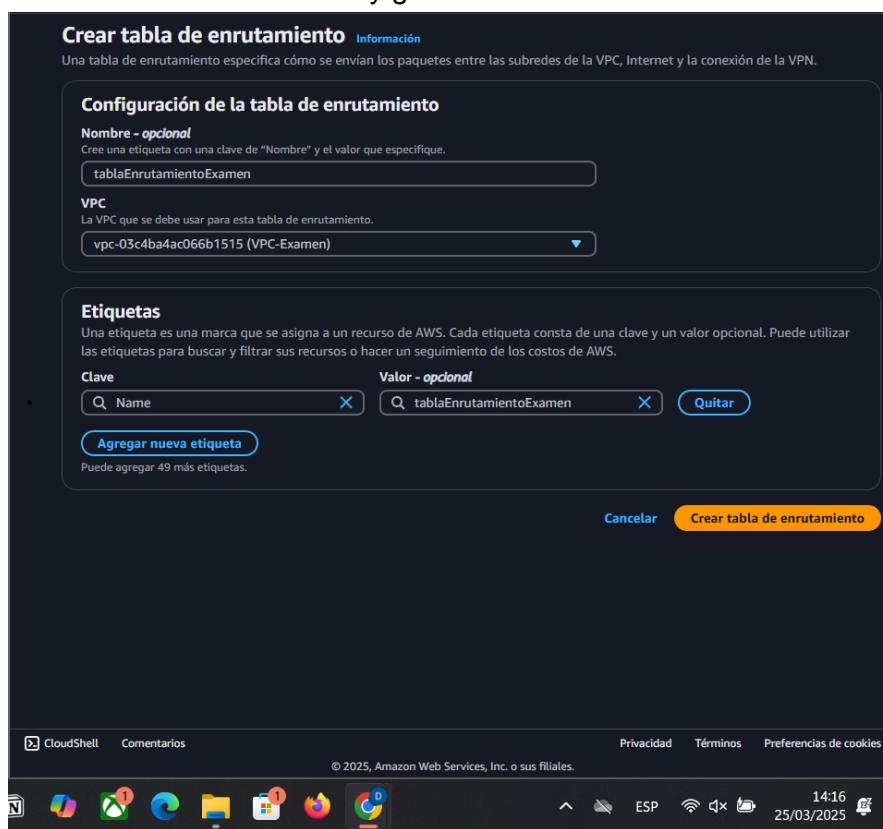
Cancelar Conejar gateway de Internet

CloudShell Comentarios © 2025, Amazon Web Services, Inc. o sus filiales. Privacidad Términos Preferencias de cookies

Búsqueda 14:22 25/03/2025

5. Crear una Tabla de Enrutamiento y Asociarla a la Subred Pública

1. En el panel izquierdo, selecciona **Tablas de enrutamiento** y haz clic en **Crear tabla de enrutamiento**.
2. Ingresa el nombre **tablaEnrutamientoExamen** y selecciona la **VPC-Examen**.
3. Una vez creada, selecciona la tabla y ve a la pestaña **Rutas**.
4. Agrega una nueva ruta:
 - Destino: **0.0.0.0/0**
 - Destino: **gatewayExamen** (seleccionar el Internet Gateway creado).
5. Guarda los cambios.
6. Luego, ve a la pestaña **Asociaciones de subred** y haz clic en **Editar asociaciones de subred**.
7. Selecciona **SubredPublica** y guarda los cambios.



VPC > Tablas de enrutamiento > rtb-04b71e0bdd6402d19 > Editar rutas

Editar rutas

Destino	Destino	Estado	Propagada
192.168.0.0/16	local	Activo	No
Q 0.0.0.0/0	X		
Q local	X		
Q Puerta de enlace de Internet	X	Activo	No
Q igw-09c2ae4bdcc095921	X		

[Agregar ruta](#) [Cancelar](#) [Vista previa](#) [Guardar cambios](#) [Quitar](#)

CloudShell Comentarios © 2025, Amazon Web Services, Inc. o sus filiales. Privacidad Términos Preferencias de cookies 14:22 25/03/2025

VPC > Tablas de enrutamiento > rtb-04b71e0bdd6402d19 > Editar asociaciones de subredes

Editar asociaciones de subredes

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

Subredes disponibles (1/1)

Nombre	ID de subred	CIDR IPv4	CIDR IPv6
subredPublica	subnet-057e2dfa7087bd199	192.168.1.0/24	-

Subredes seleccionadas

subnet-057e2dfa7087bd199 / subredPublica X

[Cancelar](#) [Guardar asociaciones](#)

CloudShell Comentarios © 2025, Amazon Web Services, Inc. o sus filiales. Privacidad Términos Preferencias de cookies 14:19 25/03/2025

6. Captura de Pantalla

The screenshot shows the AWS VPC console for a VPC named "VPC-Examen". The top navigation bar includes "Actions", "Mapa de recursos", "CIDR", "Registros de flujo", "Etiquetas", and "Integraciones". The main section displays the following details:

Detalles		Estado		Bloquear el acceso público		Nombres de host de DNS	
ID de la VPC	vpc-03c4ba4ac066b1515	Tenencia	Available	Desactivado	Desactivado	Table de enrutamiento principal	rtb-0a4d5973db9c33033
Resolución de DNS	Habilitado	VPC predeterminada	default	Conjunto de opciones de DHCP	dopt-0c99b426aafb5473a	Grupo IPv6	-
ACL de red principal	acl-0b2fcf7189e487890	Métricas de uso de direcciones de red	Desactivado	CIDR IPv4	192.168.0.0/16	ID de propietario	012629683249
CIDR IPv6 (grupo de bordes de red)	-	Resolver	-	Grupos de reglas del firewall de DNS de Route 53	No se pudieron cargar los grupos de reglas		

Below the details, there is a "Mapa de recursos" section with four cards:

- VPC**: Mostrar detalles. Su red virtual de AWS. VPC-Examen.
- Subredes (1)**: Subredes dentro de esta VPC. us-east-1c. subredPublica.
- Tablas de enrutamiento (2)**: Dirigir el tráfico de red a los recursos. tablaEnrutamientoExamen. rtb-0a4d5973db9c33033.
- Conexiones de red (1)**: Conexiones a otras redes. gatewayExamen.

The bottom of the screen shows the AWS navigation bar with links for "Búsqueda", "Privacidad", "Términos", and "Preferencias de cookies". It also displays the time as 14:23 and the date as 25/03/2025.

PARTE 2: INSTANCIA EC2

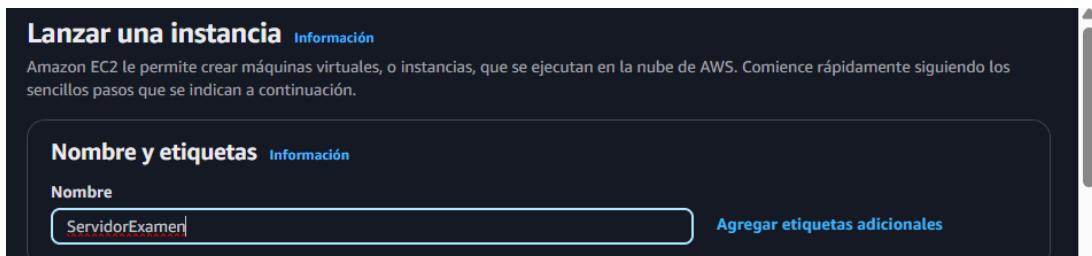
1. Acceder al Servicio EC2 y Lanzar una Nueva Instancia

1. En la consola de AWS, busca **EC2** y accede al servicio.
2. Haz clic en **Instancias** y luego en **Lanzar instancia**.
3. Asigna el nombre **ServidorExamen**.

2. Seleccionar la Imagen del Sistema Operativo

1. En la sección "Amazon Machine Image (AMI)", elige **Amazon Linux** (apto para capa gratuita).

2. Haz clic en **Seleccionar**.



Lanzar una instancia [Información](#)
Amazon EC2 le permite crear máquinas virtuales, o instancias, que se ejecutan en la nube de AWS. Comience rápidamente siguiendo los sencillos pasos que se indican a continuación.

Nombre y etiquetas [Información](#)

Nombre Agregar etiquetas adicionales

▼ **Imágenes de aplicaciones y sistemas operativos (Imagen de máquina de Amazon)** [Información](#)
Una AMI es una plantilla que contiene la configuración de software (sistema operativo, servidor de aplicaciones y aplicaciones) necesaria para lanzar la instancia. Busque o examine las AMI si no ve lo que busca a continuación.

Mis AMI **Inicio rápido**

Amazon Linux macOS Ubuntu Windows Red Hat SUSE Linux Debian [Buscar más AMI](#)
Inclusión de AMI de AWS, Marketplace y la comunidad

Imágenes de máquina de Amazon (AMI)
AMI de Amazon Linux 2023
ami-08b5b3a93ed654d19 (64 bits (x86), uefi-preferred) / ami-0eae2a0fc13b15fce (64 bits (Arm), uefi)
Virtualización: hvm Activado para ENA: true Tipo de dispositivo raíz: ebs Apto para la capa gratuita ▾

Descripción
Amazon Linux 2023 es un sistema operativo moderno y de uso general basado en Linux que incluye 5 años de soporte a largo plazo.

CloudShell Comentarios © 2025, Amazon Web Services, Inc. o sus filiales. Privacidad Términos Preferencias de cookies

14:30 25/03/2025

3. Configurar la Instancia en la Subred Pública

1. En "Par de claves", selecciona un par de claves existentes (vockey) o crea uno nuevo para conectarte por SSH.
2. En "Configuraciones de Red":
 - Selecciona **VPC-Examen**.
 - En "Subred", elige **SubredPublica**.

- Habilita la asignación de una IP pública.

The screenshot shows the AWS EC2 'Launch Instance' wizard. The first step, 'Tipo de instancia', is selected. It shows the 't2.nano' instance type with its details: Family: t2, 1 vCPU, 0.5 GiB Memory, Generation actual: true. It also lists base prices for Linux, SUSE, Windows, and Ubuntu Pro. A note at the bottom states: 'Se aplican costos adicionales a las AMI con software preinstalado'. To the right, there are links for 'Todas las generaciones' and 'Comparar tipos de instancias'.

The second step, 'Par de claves (inicio de sesión)', is shown below. It asks for a key pair name, with 'vokey' selected. There is a link to 'Crear un nuevo par de claves'.

The third step, 'Configuraciones de red', is the current active step. It includes sections for 'VPC' (set to 'vpc-03c4ba4ac066b1515 (VPC-Examen)') and 'Subred' (set to 'subnet-057e2dfa7087bd199'). Both sections have 'Create new' buttons. Below these, there is a section for 'Asignar automáticamente la IP pública'.

The bottom of the screen shows the AWS navigation bar with CloudShell, Comentarios, Privacidad, Términos, Preferencias de cookies, and a timestamp of 14:31 on 25/03/2025.

4. Configurar el Grupo de Seguridad (Permitir SSH y HTTP)

1. En "Grupo de Seguridad", selecciona "Crear un nuevo grupo de seguridad". Ponle un nombre y una descripción (por defecto).
2. Agrega las siguientes reglas:
 - **SSH (TCP 22)**: Fuente **0.0.0.0/0** (o tu IP para mayor seguridad). Tipo cualquier lugar.
 - **HTTP (TCP 80)**: Fuente **0.0.0.0/0**. Tipo cualquier lugar.
3. Todos los demás valores dejalos por defecto o modificalos según necesidad. Almacenamiento, etc.

4. Lanza la instancia y espera a que el estado sea "Corriendo".

Asignar automáticamente la IP pública | **Información**

Habilitar

Se aplican cargos adicionales cuando no se cumplen los límites del [nivel gratuito](#)

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

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

[Crear grupo de seguridad](#)

[Seleccionar un grupo de seguridad existente](#)

Nombre del grupo de seguridad - *obligatorio*

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

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

Reglas de grupos de seguridad de entrada

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

Tipo | [Información](#)

Protocolo | [Información](#)

Intervalo de puertos | [Información](#)

Tipo de origen | [Información](#)

Origen | [Información](#)

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

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

Tipo | [Información](#)

Protocolo | [Información](#)

Intervalo de puertos | [Información](#)

CloudShell Comentarios

© 2025, Amazon Web Services, Inc. o sus filiales.

Privacidad Términos Preferencias de cookies

N CloudShell Comentarios

ESP 14:31 25/03/2025

The screenshot shows the AWS CloudFormation console interface. At the top, there is a navigation bar with links for Home, Services, and Support. Below the navigation bar, the main content area displays two sections:

- Regla del grupo de seguridad 2 (TCP, 80, 0.0.0.0/0)**: This section shows a security group rule configuration. It includes fields for Type (HTTP), Protocol (TCP), Port Range (80), Source Type (Anywhere), and Source IP (0.0.0.0/0). A note below states: "Las reglas con origen 0.0.0.0/0 permiten que todas las direcciones IP tengan acceso a la instancia. Le recomendamos que configure las reglas del grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas." An "Agregar regla del grupo de seguridad" button is also present.
- Configurar almacenamiento**: This section shows storage volume configuration. It indicates 1x 8 GiB gp3 volume for the root volume, labeled as "Volumen raíz, 3000 IOPS, No cifrado". A note below says: "Los clientes que cumplen los requisitos de la capa gratuita pueden obtener hasta 30 GB de almacenamiento magnético o de uso general (SSD) de EBS". An "Agregar un nuevo volumen" button is available. Another note below says: "Haga clic en actualizar para ver la información de la copia de seguridad. Las etiquetas que asigne determinan si alguna política de Data Lifecycle Manager realizará una copia de seguridad de la instancia." A "C" icon is next to this note.

At the bottom of the page, there are links for CloudShell, Comentarios, Privacidad, Términos, and Preferencias de cookies. The footer also includes copyright information: © 2025, Amazon Web Services, Inc. o sus filiales. On the right side of the footer, there are icons for browser tabs, refresh, search, and other navigation controls, along with the date and time: 25/03/2025, 14:31.

5. Conectarse a la Instancia Vía SSH y Actualizar el Sistema

1. Copia la IP pública de la instancia desde la consola de AWS.
2. Conéctate usando SSH:
 - a. Descarga el .ppk que es la clave de seguridad.
 - b. Accede a través de PuTTY accede pon en HostName la IP pública.
 - c. Y en Connections>SSH>Auth>Credentials y en el primer campo seleccionar el archivo .ppk que hemos descargado antes.

The screenshot shows two side-by-side browser windows. Both windows are displaying the AWS CloudWatch Metrics interface for a specific metric named 'CPU Utilization' over a time range from 'Last hour'. The left window shows a single data series for 'CPU Utilization' with a value of approximately 10%. The right window shows the same metric with a value of approximately 15%.

Left Window (CPU Utilization):

- Y-axis: CPU Utilization (0.00 - 1.00)
- X-axis: Last hour
- Data series: CPU Utilization (approx. 0.10)

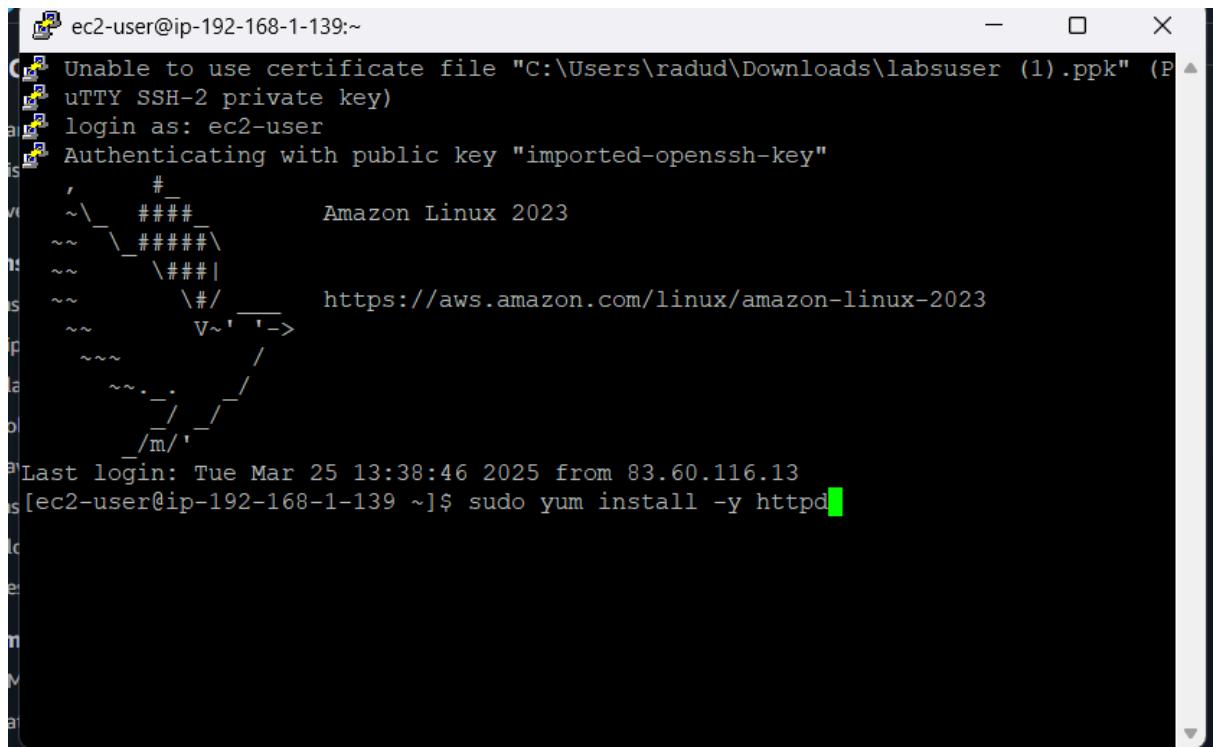
Right Window (CPU Utilization):

- Y-axis: CPU Utilization (0.00 - 1.00)
- X-axis: Last hour
- Data series: CPU Utilization (approx. 0.15)

6. Instalar y Configurar un Servidor Apache

1. Instala Apache:

```
sudo yum install -y httpd
```

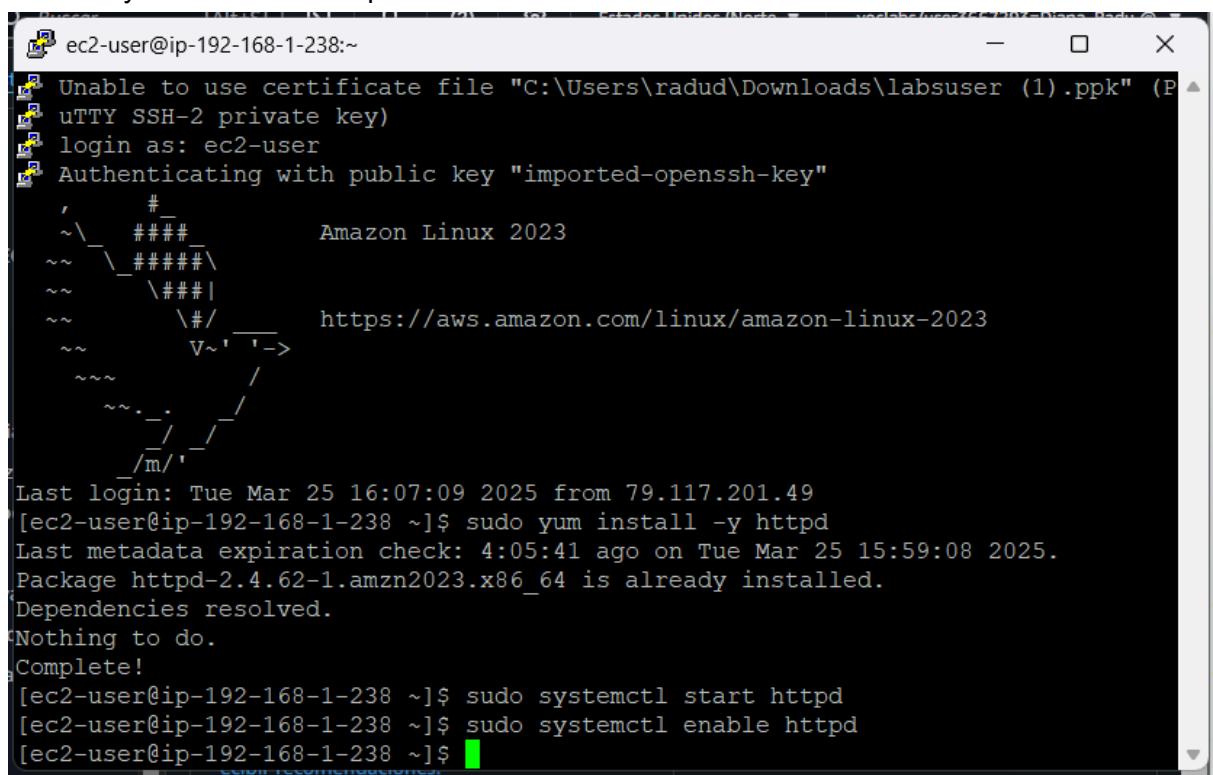


```
[ec2-user@ip-192-168-1-139:~] Unable to use certificate file "C:\Users\radud\Downloads\labsuser (1).ppk" (P
[ec2-user@ip-192-168-1-139:~] uTTY SSH-2 private key)
[ec2-user@ip-192-168-1-139:~] login as: ec2-user
[ec2-user@ip-192-168-1-139:~] Authenticating with public key "imported-openssh-key"
[ec2-user@ip-192-168-1-139:~] 
[ec2-user@ip-192-168-1-139:~] Amazon Linux 2023
[ec2-user@ip-192-168-1-139:~] https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-192-168-1-139:~] 
[ec2-user@ip-192-168-1-139:~] 
[ec2-user@ip-192-168-1-139:~] Last login: Tue Mar 25 13:38:46 2025 from 83.60.116.13
[ec2-user@ip-192-168-1-139:~] $ sudo yum install -y httpd
```

2. Inicia y habilita Apache:

```
sudo systemctl start httpd
```

3. sudo systemctl enable httpd



```
[ec2-user@ip-192-168-1-238:~] Unable to use certificate file "C:\Users\radud\Downloads\labsuser (1).ppk" (P
[ec2-user@ip-192-168-1-238:~] uTTY SSH-2 private key)
[ec2-user@ip-192-168-1-238:~] login as: ec2-user
[ec2-user@ip-192-168-1-238:~] Authenticating with public key "imported-openssh-key"
[ec2-user@ip-192-168-1-238:~] 
[ec2-user@ip-192-168-1-238:~] Amazon Linux 2023
[ec2-user@ip-192-168-1-238:~] https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@ip-192-168-1-238:~] 
[ec2-user@ip-192-168-1-238:~] 
[ec2-user@ip-192-168-1-238:~] Last login: Tue Mar 25 16:07:09 2025 from 79.117.201.49
[ec2-user@ip-192-168-1-238:~] $ sudo yum install -y httpd
[ec2-user@ip-192-168-1-238:~] Last metadata expiration check: 4:05:41 ago on Tue Mar 25 15:59:08 2025.
[ec2-user@ip-192-168-1-238:~] Package httpd-2.4.62-1.amzn2023.x86_64 is already installed.
[ec2-user@ip-192-168-1-238:~] Dependencies resolved.
[ec2-user@ip-192-168-1-238:~] Nothing to do.
[ec2-user@ip-192-168-1-238:~] Complete!
[ec2-user@ip-192-168-1-238:~] $ sudo systemctl start httpd
[ec2-user@ip-192-168-1-238:~] $ sudo systemctl enable httpd
[ec2-user@ip-192-168-1-238:~] $
```

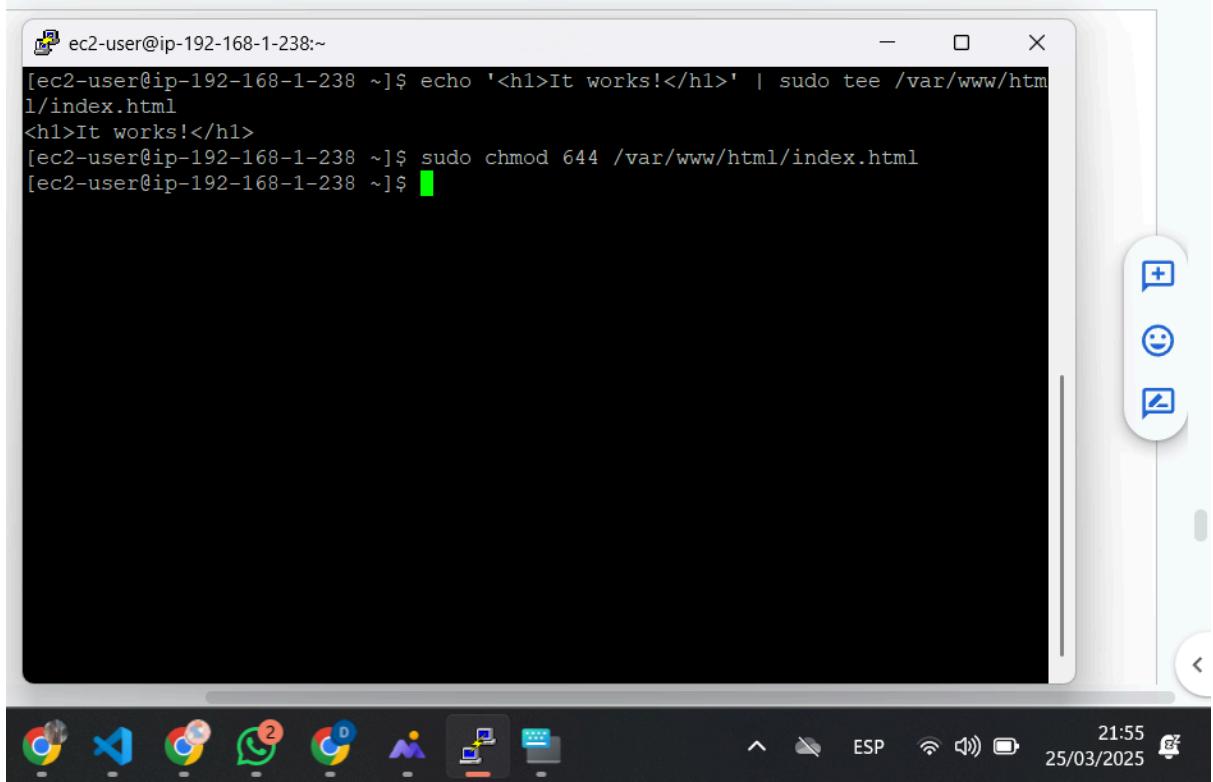
7. Subir un Archivo HTML a /var/www/html/

Crea un archivo HTML básico:

```
echo '<h1>It works!</h1>' | sudo tee /var/www/html/index.html
```

Asegúrate de que Apache pueda leer el archivo:

```
sudo chmod 644 /var/www/html/index.html
```

A screenshot of a terminal window titled "ec2-user@ip-192-168-1-238:~". The window contains the following text:

```
[ec2-user@ip-192-168-1-238 ~]$ echo '<h1>It works!</h1>' | sudo tee /var/www/html/index.html
<h1>It works!</h1>
[ec2-user@ip-192-168-1-238 ~]$ sudo chmod 644 /var/www/html/index.html
[ec2-user@ip-192-168-1-238 ~]$
```

The terminal has a light gray background and black text. The prompt is "[ec2-user@ip-192-168-1-238 ~]\$. The command "echo" is followed by an HTML header "<h1>It works!</h1>". This output is piped ("|") to the command "sudo tee", which writes it to the file "/var/www/html/index.html". Below this, another "sudo chmod 644" command is run on the same file. The bottom right corner of the terminal shows the date and time: "21:55 25/03/2025".

The terminal window is part of a desktop environment, as evidenced by the taskbar at the bottom. The taskbar includes icons for various applications like a browser, code editor, and messaging. On the far right of the taskbar, there are system status icons for battery, signal strength, and volume, along with the current date and time.

8. Captura de Pantalla del Sitio Web

1. Abre un navegador y accede a http://IP_PUBLICA.
2. Si todo está correcto, deberías ver el mensaje "It works!".



It works!

PARTE 3: BUQUET S3

1. Acceder al Servicio S3 y Crear un Bucket

1. Inicia sesión en la Consola de AWS.
2. En el buscador de servicios, escribe **S3** y selecciona **Amazon S3**.
3. Haz clic en **Crear bucket**.
4. Asigna el nombre **examen1daw**.
5. Desmarca la opción de **Bloquear todo el acceso público**.
6. Haz clic en **Crear bucket**.
7. Todo lo demás lo dejamos por defecto.

<https://examen1daw.s3.us-east-1.amazonaws.com/TKD/HTML/home.css>

The screenshot shows the AWS S3 'Crear bucket' (Create Bucket) configuration page. At the top, the navigation bar includes the AWS logo, a search bar, and links for 'Buscar' and '[Alt+S]'. On the right, it shows 'Estados Unidos (Nort)' and the user 'voclabs/user3667293=Diana_Radu'. Below the navigation, the breadcrumb trail reads 'Amazon S3 > Buckets > Crear bucket'. The main title 'Crear bucket' has an 'Información' link. A sub-section 'Configuración general' is displayed. Under 'Región de AWS', it shows 'EE.UU. Este (Norte de Virginia) us-east-1'. The 'Tipo de bucket' section shows 'Uso general' selected, with a description: 'Recomendado para la mayoría de los casos de uso y patrones de acceso. Los buckets de uso general son del tipo de bucket de S3 original. Permiten una combinación de clases de almacenamiento que almacenan objetos de forma redundante en múltiples zonas de disponibilidad.' Another option, 'Directorio', is also listed with its description: 'Recomendado para casos de uso de baja latencia. Estos buckets utilizan únicamente la clase de almacenamiento S3 Express One Zone, que proporciona un procesamiento más rápido de los datos dentro de una única zona de disponibilidad.' The 'Nombre del bucket' field contains 'exam1daw'. Below it, a note states: 'Los nombres de los buckets deben tener entre 3 y 63 caracteres y ser únicos dentro del espacio de nombres global. Los nombres de los buckets también deben empezar y terminar con una letra o un número. Los caracteres válidos son a-z, 0-9, puntos (.) y guiones (-). [Más información](#)'.

Configuración general

Región de AWS
EE.UU. Este (Norte de Virginia) us-east-1

Tipo de bucket | [Información](#)

Uso general
Recomendado para la mayoría de los casos de uso y patrones de acceso. Los buckets de uso general son del tipo de bucket de S3 original. Permiten una combinación de clases de almacenamiento que almacenan objetos de forma redundante en múltiples zonas de disponibilidad.

Directorio
Recomendado para casos de uso de baja latencia. Estos buckets utilizan únicamente la clase de almacenamiento S3 Express One Zone, que proporciona un procesamiento más rápido de los datos dentro de una única zona de disponibilidad.

Nombre del bucket | [Información](#)
exam1daw

Los nombres de los buckets deben tener entre 3 y 63 caracteres y ser únicos dentro del espacio de nombres global. Los nombres de los buckets también deben empezar y terminar con una letra o un número. Los caracteres válidos son a-z, 0-9, puntos (.) y guiones (-). [Más información](#)

Copiar la configuración del bucket existente: *opcional*
Solo se copia la configuración del bucket en los siguientes ajustes.

Elegir el bucket
Formato: s3://bucket/prefixo

Propiedad de objetos | [Información](#)

Controle la propiedad de los objetos escritos en este bucket desde otras cuentas de AWS y el uso de listas de control de acceso (ACL). La propiedad de los objetos determina quién puede especificar el acceso a los objetos.

ACL deshabilitadas (recomendado)
Todos los objetos de este bucket son propiedad de esta cuenta. El acceso a este bucket y sus objetos se especifica solo mediante políticas.

ACL habilitadas
Los objetos de este bucket pueden ser propiedad de otras cuentas de AWS. El acceso a este bucket y sus objetos se puede especificar mediante ACL.

8.

Configuración de bloqueo de acceso público para este bucket

Se concede acceso público a los buckets y objetos a través de listas de control de acceso (ACL), políticas de bucket, políticas de puntos de acceso o todas las anteriores. A fin de garantizar que se bloquee el acceso público a todos sus buckets y objetos, active Bloquear todo el acceso público. Esta configuración se aplica exclusivamente a este bucket y a sus puntos de acceso. AWS recomienda activar Bloquear todo el acceso público, pero, antes de aplicar cualquiera de estos ajustes, asegúrese de que las aplicaciones funcionarán correctamente sin acceso público. Si necesita cierto nivel de acceso público a los buckets u objetos, puede personalizar la configuración individual a continuación para adaptarla a sus casos de uso de almacenamiento específicos. [Más información](#)

Bloquear todo el acceso público

Activar esta configuración equivale a activar las cuatro opciones que aparecen a continuación. Cada uno de los siguientes ajustes son independientes entre sí.

- Bloquear el acceso público a buckets y objetos concedido a través de nuevas listas de control de acceso (ACL)**
S3 bloqueará los permisos de acceso público aplicados a objetos o buckets agregados recientemente, y evitará la creación de nuevas ACL de acceso público para buckets y objetos existentes. Esta configuración no cambia los permisos existentes que permiten acceso público a los recursos de S3 mediante ACL.
- Bloquear el acceso público a buckets y objetos concedido a través de cualquier lista de control de acceso (ACL)**
S3 ignorará todas las ACL que conceden acceso público a buckets y objetos.
- Bloquear el acceso público a buckets y objetos concedido a través de políticas de bucket y puntos de acceso públicas nuevas**
S3 bloqueará las nuevas políticas de buckets y puntos de acceso que concedan acceso público a buckets y objetos. Esta configuración no afecta a las políticas ya existentes que permiten acceso público a los recursos de S3.
- Bloquear el acceso público y entre cuentas a buckets y objetos concedido a través de cualquier política de bucket y puntos de acceso pública**
S3 ignorará el acceso público y entre cuentas en el caso de buckets o puntos de acceso que tengan políticas que concedan acceso público a buckets y objetos.

⚠ Desactivar el bloqueo de todo acceso público puede provocar que este bucket y los objetos que contiene se vuelvan públicos

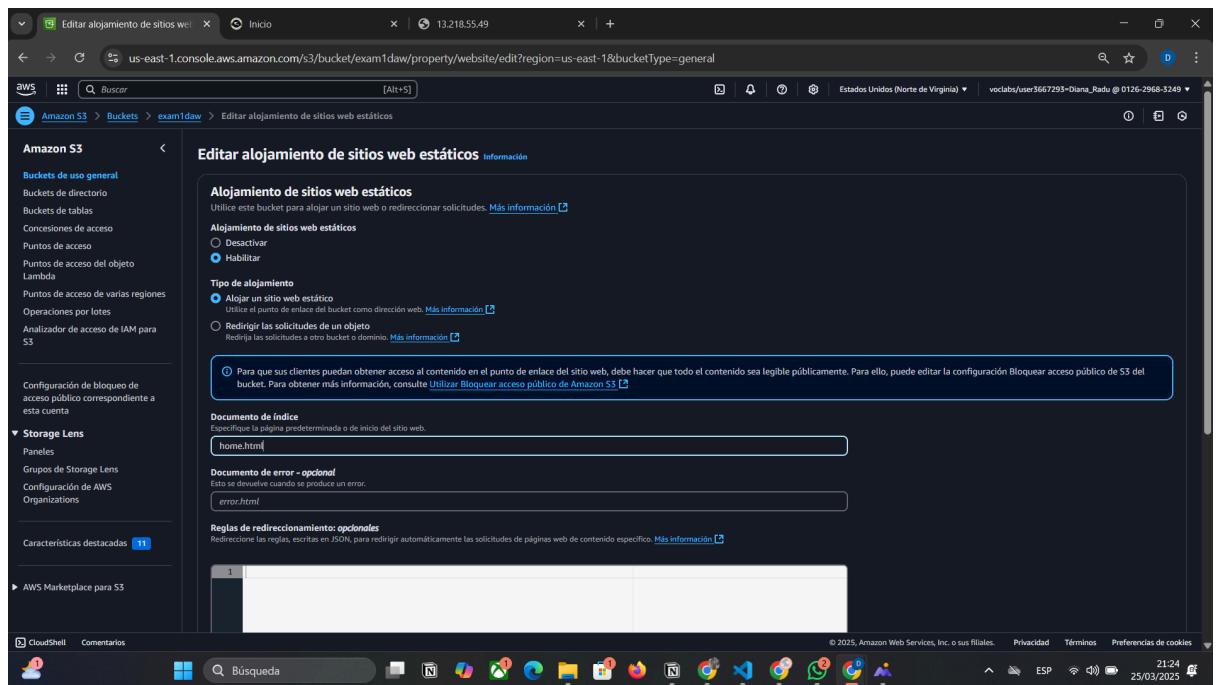
AWS recomienda que active la opción para bloquear todo el acceso público, a menos que se requiera acceso público para [casos de uso específicos y verificados, como el alojamiento de sitios web estáticos](#).

Reconozco que la configuración actual puede provocar que este bucket y los objetos que contiene se vuelvan públicos.

2. Configurar el Bucket para Alojar un Sitio Web Estático

1. Abre el bucket y ve a la pestaña **Propiedades**.
2. Busca la sección **Alojamiento de sitio web estático** y haz clic en **Editar**.
3. Activa la opción **Usar este bucket para alojar un sitio web**.
4. En **Documento de índice**, escribe [index.html](#).

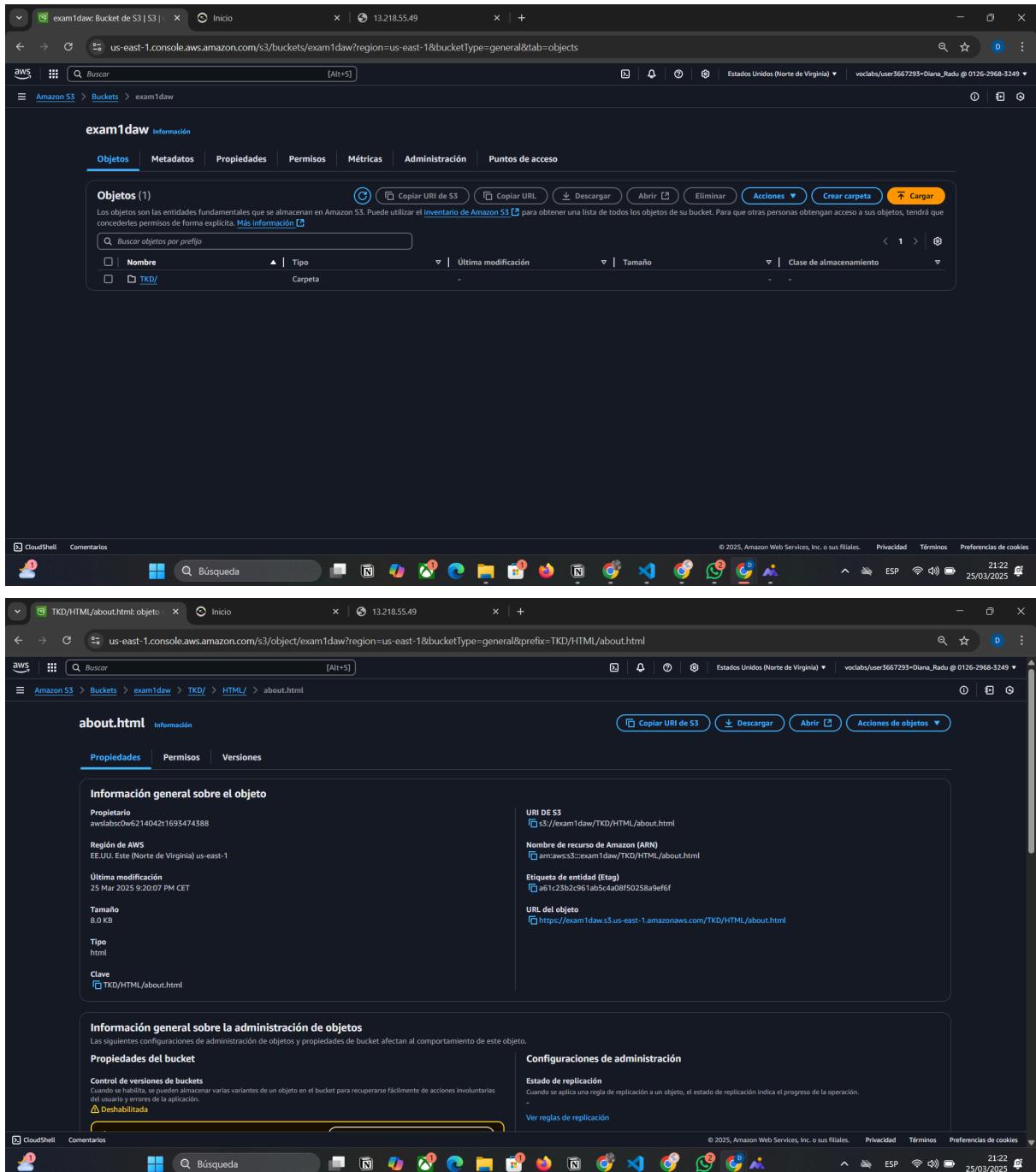
5. Guarda los cambios.



3. Subir Archivos HTML y una Imagen al Bucket

1. Ve a la pestaña **Objetos** y haz clic en **Cargar**.

2. Haz clic en "Cargar" y añade los archivos necesarios.



The screenshots show the AWS S3 console interface. The top window displays the 'exam1daw' bucket with one item, 'TKD/'. The bottom window shows the properties for the 'about.html' object within the 'TKD/' folder, with the 'Actions' menu open, specifically highlighting the 'Cargar' (Upload) option.

4. Modificar Permisos para Acceso Público

1. Ve a la pestaña **Permisos** del bucket.
2. En **Política de bucket**, haz clic en **Editar**.

Agrega la siguiente política para permitir acceso público:

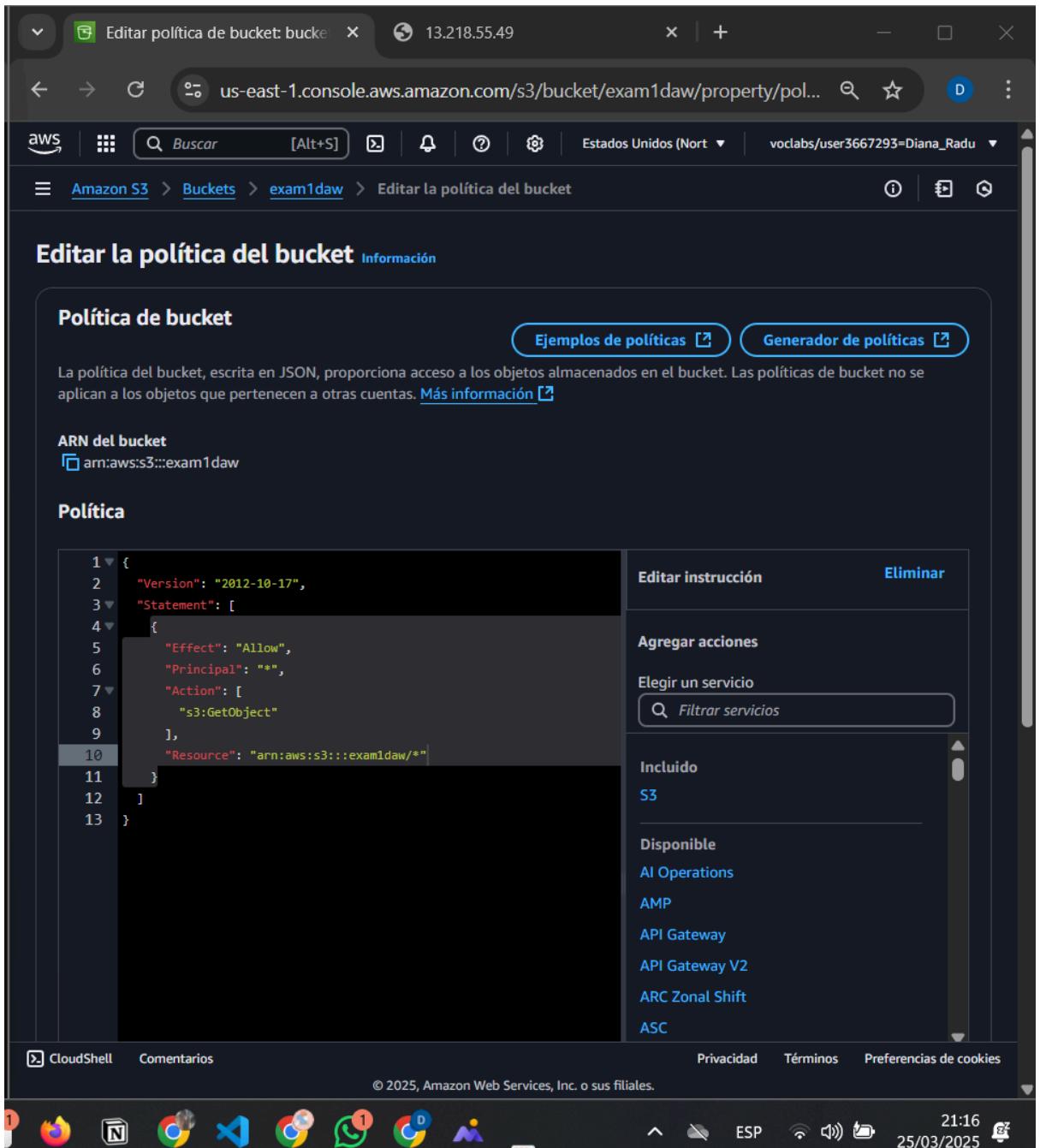
```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {
```

```

        "Effect": "Allow",
        "Principal": "*",
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::examen1daw/*"
    }
]

```

3. }
4. Guarda los cambios.



The screenshot shows the AWS S3 Bucket Policy Editor interface. The URL in the browser is `us-east-1.console.aws.amazon.com/s3/bucket/exam1daw/property/pol...`. The page title is "Editar la política del bucket". The main content area displays the following JSON policy:

```

1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Principal": "*",
7              "Action": [
8                  "s3:GetObject"
9              ],
10             "Resource": "arn:aws:s3:::examen1daw/*"
11         }
12     ]
13 }

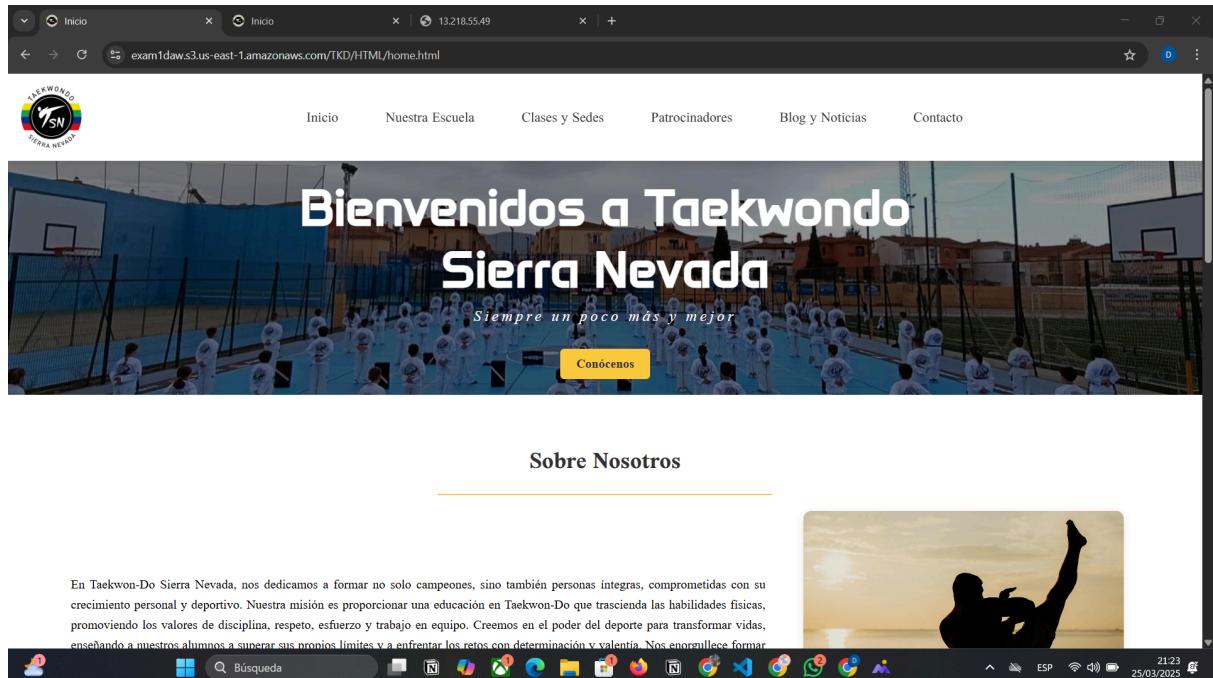
```

The "Resource" field is highlighted with a cursor. To the right of the editor, there are two buttons: "Ejemplos de políticas" and "Generador de políticas". Below the editor, there are sections for "Agregar acciones" (with a search bar for "Filtrar servicios") and "Incluido" (listing "S3"). At the bottom, there are links for "CloudShell", "Comentarios", "Privacidad", "Términos", and "Preferencias de cookies". The footer includes the copyright notice "© 2025, Amazon Web Services, Inc. o sus filiales." and the system status bar showing "21:16 25/03/2025".

5. Captura la URL del Sitio Web

1. Ve a la pestaña Propiedades.

- Copia la URL de **Alojamiento de sitio web estático** en el buscador.



PARTE 4: BASE DE DATOS RDS

1. Acceder al Servicio RDS y Crear una Instancia

- En la consola de AWS, busca **RDS** y accede al servicio.
- Haz clic en **Crear base de datos**.
- Selecciona **MySQL**.
- Elige la opción de **Capa gratuita de AWS**.

Elegir un método de creación de base de datos

- Creación estándar
- Creación sencilla

Puede definir todas las opciones de configuración, incluidas las de disponibilidad, seguridad, copias de seguridad y mantenimiento.

Opciones del motor

Tipo de motor: [Información](#)

- Aurora (MySQL Compatible)
- Aurora (PostgreSQL Compatible)
- MySQL
- PostgreSQL
- MariaDB
- Oracle
- Microsoft SQL Server
- IBM Db2

MySQL

MySQL es la base de datos de código abierto más popular del mundo. MySQL en RDS ofrece las completas características de la edición comunitaria de MySQL con la flexibilidad necesaria para escalar fácilmente los recursos de computación o la capacidad de almacenamiento de la base de datos.

- Admite un tamaño de base de datos máximo de 64 TB.
- Admite las clases de instancias de uso general, optimizadas para memoria y de rendimiento ampliable.
- Admite las copias de seguridad automatizadas y la recuperación a un momento dado.
- Admite hasta 15 réplicas de lectura por instancia, dentro de una única región, o 5 réplicas de lectura entre regiones.

Producción

Utilice los valores predeterminados para disfrutar de una alta disponibilidad y de un rendimiento rápido y constante.

Desarrollo y pruebas

Esta instancia se ha diseñado para su uso en desarrollo, fuera de un entorno de producción.

Capa gratuita

Utilice el nivel gratuito de RDS para desarrollar nuevas aplicaciones, probar aplicaciones existentes o adquirir experiencia práctica con Amazon RDS. [Información](#)

Disponibilidad y durabilidad

Opciones de implementación: [Información](#)

Diga la manera de implementación que proporciona la disponibilidad y durabilidad necesarias en función del caso de uso. AWS se compromete a un determinado nivel de tiempo de actividad según la opción de implementación que elija. Obtenga más información en el [Acuerdo de nivel de servicios \(SLA\) de Amazon RDS](#).

- Implementación de clúster de base de datos multi-AZ (3 instancias)
- Implementación de una instancia de base de datos principal con dos en espera legibles en zonas de disponibilidad separadas. Esta configuración proporciona:
 - Tiempo de actividad del 99,5 %
 - Independencia entre zonas de disponibilidad
 - Mínima latencia de escritura
 - Menor latencia de escritura
- Punto de conexión de escritura/lectura/Puntos de conexión del lector
- Implementación de una instancia de base de datos de zona de disponibilidad única (1 instancia)
- Implementación de una instancia de base de datos sin instancias en espera. Esta configuración proporciona:
 - Tiempo de actividad del 99,5 %
 - Independencia entre zonas de disponibilidad

Configuración

Identificador de Instancias de bases de datos: [Información](#)

Escriba un nombre para la instancia de base de datos. El nombre debe ser único en relación con todas las instancias de base de datos pertenecientes a su cuenta de AWS en la región de AWS actual.

MySQL

MySQL es la base de datos de código abierto más popular del mundo. MySQL en RDS ofrece las completas características de la edición comunitaria de MySQL con la flexibilidad necesaria para escalar fácilmente los recursos de computación o la capacidad de almacenamiento de la base de datos.

- Admite un tamaño de base de datos máximo de 64 TB.
- Admite las clases de instancias de uso general, optimizadas para memoria y de rendimiento ampliable.
- Admite las copias de seguridad automatizadas y la recuperación a un momento dado.
- Admite hasta 15 réplicas de lectura por instancia, dentro de una única región, o 5 réplicas de lectura entre regiones.

2. Configurar la Base de Datos

- Asigna los siguientes valores:
 - Nombre de la base de datos:** examen_db
 - Nombre de usuario:** admin

- **Contraseña: lab-password**

The screenshot shows the 'Create database' wizard for MySQL. The 'Configuration' step is selected. In the 'Identifier of instances of bases de datos' field, 'examen-db' is entered. Under 'Configuración de credenciales', the 'Nombre de usuario maestro' is set to 'admin'. The 'Administración de credenciales' section shows 'Autoadministrado' is selected. Below it, 'Generar contraseña automáticamente' is checked. The 'Contraseña maestra' field contains a strong password, and 'Confirmar la contraseña maestra' is also present. The 'Configuración de la instancia' section is at the bottom, with a note about instance configuration being limited by the chosen engine. On the right, a sidebar for MySQL provides general information and links to documentation.

2. En Configuraciones de red y seguridad:

- Selecciona **VPC-Examen**.
- Asegúrate de que la base de datos **SI tenga acceso público**.
- Configura el grupo de seguridad para permitir conexiones desde la EC2.

3. Haz clic en **Crear base de datos**.

The screenshot shows the 'Create database' configuration page for MySQL. The left panel contains several configuration sections:

- Configuración adicional:** Includes options for data encryption, security copy, point-in-time recovery, maintenance, CloudWatch logs, and deletion protection.
- Opciones de base de datos:** Set the initial database name to 'lab'. A note states: "Si no especifica un nombre de base de datos, Amazon RDS no crea una base de datos."
- Grupo de parámetros de base de datos:** Set to 'default.mysql8.0'.
- Grupo de opciones:** Set to 'default:mysql-8-0'.
- Copia de seguridad:** Unchecked checkbox for 'Habilitar las copias de seguridad automatizadas'. A note says: "Crea una instantánea de un momento dado de su base de datos".
- Cifrado:** Unchecked checkbox for 'Habilitar el cifrado'. A note says: "Elija cifrar la instancia proporcionada. Los ID y alias de la clave maestra aparecen en la lista después de haberse creado mediante la consola de AWS Key Management Service.".
- Mantenimiento:** Checked checkbox for 'Habilitar actualización automática de versiones secundarias'. A note says: "La habilitación de la actualización automática de versión secundaria se actualizará automáticamente a nuevas versiones secundarias a medida que se vayan publicando. Las actualizaciones automáticas se realizan durante el periodo de mantenimiento de la base de datos".
- Periodo de mantenimiento:** A note: "Seleccione el periodo en el que desea que Amazon RDS realice las modificaciones en su base de datos".

The right panel displays information about MySQL:

- MySQL:** MySQL is described as the most popular open-source database. It offers full MySQL functionality with the flexibility to scale resources or storage capacity.
- A bulleted list highlights MySQL's features:
 - Admits a maximum database size of 64 TiB.
 - Supports general-purpose instances optimized for memory and performance.
 - Allows automated backups and recovery at any moment.
 - Supports up to 15 read replicas per instance within a single region, or 5 read replicas across regions.

At the bottom of the page are links for CloudShell, Comentarios, Privacidad, Términos, and Preferencias de cookies, along with a footer for © 2025, Amazon Web Services, Inc. o sus filiales, and system status icons.

4. Ingresamos en VPC>VPC-Examen>Acciones>Editar la configuración de la VPC y habilitamos ambas opciones de configuración de DNS.

5. Lo guardamos.

The screenshot shows the 'Editar la configuración de VPC' (Edit VPC Configuration) page in the AWS Management Console. The VPC ID is vpc-03c4ba4ac066b1515, and the name is VPC-Examen. Under 'Configuración de DNS', two options are checked: 'Habilitar la resolución de DNS' and 'Habilitar nombres de host DNS'. At the bottom right, there are 'Cancelar' (Cancel) and 'Guardar' (Save) buttons. The browser status bar at the bottom indicates it's 23:12 on 25/03/2025.

Detalles de la VPC

ID de la VPC
vpc-03c4ba4ac066b1515

Nombre
VPC-Examen

Configuración de DHCP

Conjunto de opciones de DHCP [Información](#)

dopt-0c99b426aafb5473a

Configuración de DNS

Habilitar la resolución de DNS [Información](#)

Habilitar nombres de host DNS [Información](#)

Configuración de las métricas de uso de las direcciones de red

Habilitar las métricas de uso de las direcciones de red [Información](#)

Botones

Cancelar Guardar

Barras y pie de página

CloudShell Comentarios Privacidad Términos Preferencias de cookies
© 2025, Amazon Web Services, Inc. o sus filiales.
23:12 25/03/2025

3. Conectarse a la Base

The screenshot shows the 'Editar reglas de salida' (Edit Outbound Rules) page in the AWS VPC console. A single rule is listed:

ID de la regla del grupo de seguridad	Tipo	Protocolo
sgr-0de09a5b6c07a6a2e	MySQL/Aurora	TCP

Details for the rule:

- Intervalo de puertos:** 3306
- Tipo de destino:** Personalizada
- Destino:** sg-019166d273b82989e

Buttons at the bottom include: Cancelar, Previsualizar los cambios (Preview changes), and Guardar reglas (Save rules).

de Datos desde MySQL Workbench o SSH

Opción 1: Conexión desde la Instancia EC2

1. Conéctate a la instancia EC2 vía SSH como en EC2 a través de PuTTY

2. Instala el cliente MySQL si no está instalado:

```
sudo dnf install mariadb105-server -y
```

The screenshot shows a terminal window titled "ec2-user@ip-192-168-1-238:~". It displays the following output:

```
login as: ec2-user
Authenticating with public key "imported-openssh-key"
,      #
~\_ #####
~~ \##### Amazon Linux 2023
~~ \###|
~~   \#/  https://aws.amazon.com/linux/amazon-linux-2023
~~   V~' '-->
~~   / 
~~ .-/
~/m/ ' 

Last login: Tue Mar 25 20:39:22 2025 from 79.117.201.49
[ec2-user@ip-192-168-1-238 ~]$ sudo dnf install mariadb105-server -y
Last metadata expiration check: 17:56:45 ago on Tue Mar 25 15:59:08 2025.
Dependencies resolved.
=====
 Package           Arch    Version            Repository  Size
=====
Installing:
 mariadb105-server        x86_64  3:10.5.25-1.amzn2023.0.1  amazonlinux 11 M
Installing dependencies:
 mariadb-connector-c        x86_64  3.1.13-1.amzn2023.0.3    amazonlinux 196 k
 mariadb-connector-c-config noarch  3.1.13-1.amzn2023.0.3    amazonlinux 9.2 k
```

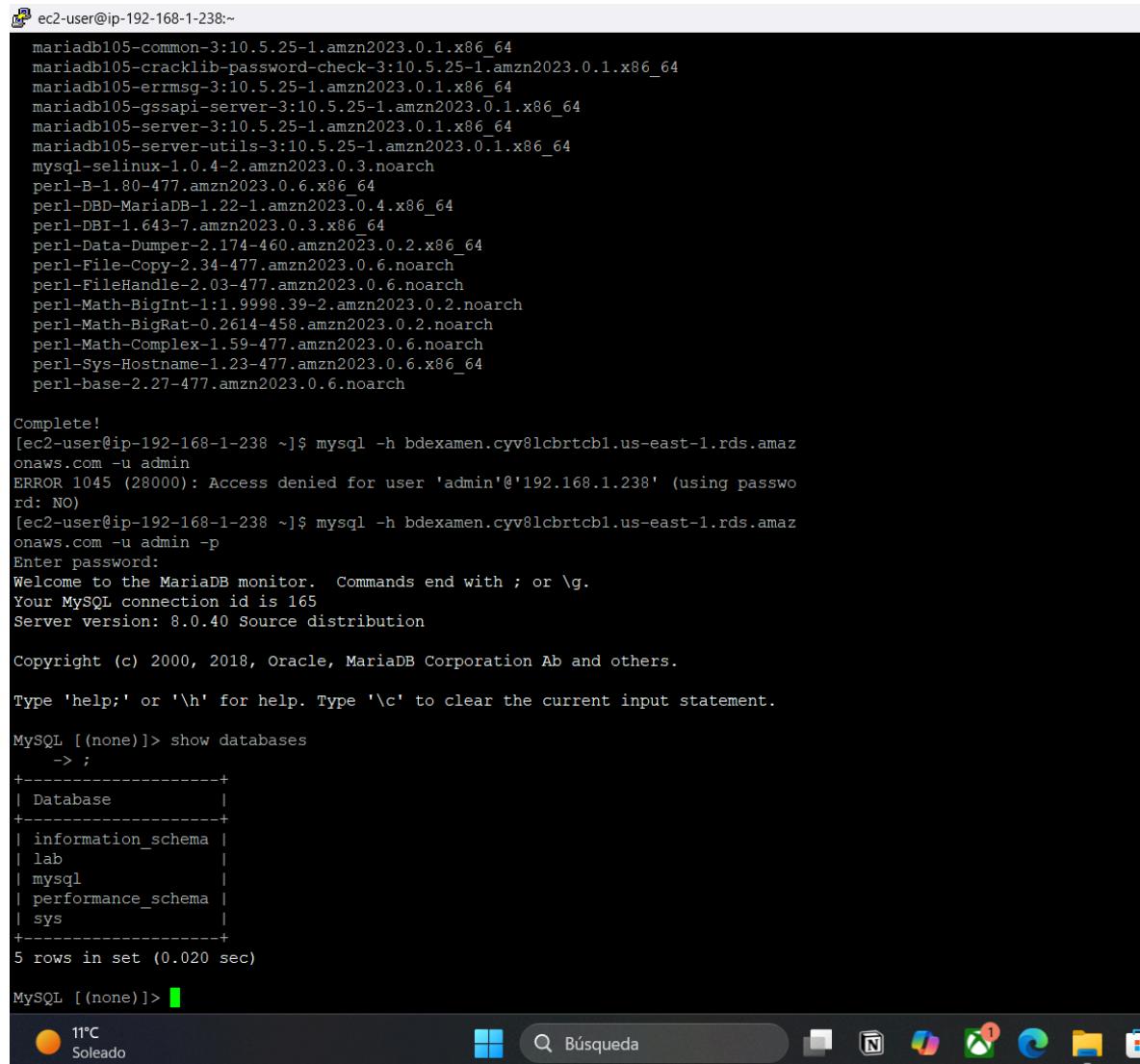
3. Conéctate a la base de datos:

```
mysql -h endpoint-de-rds -u admin -p
```

4. Ingresa la contraseña **lab-password** y verifica la conexión con:

```
SHOW DATABASES;
```

4. Captura de Pantalla de la Conexión



ec2-user@ip-192-168-1-238:~

```
mariadb105-common-3:10.5.25-1.amzn2023.0.1.x86_64
mariadb105-cracklib-password-check-3:10.5.25-1.amzn2023.0.1.x86_64
mariadb105-errormsg-3:10.5.25-1.amzn2023.0.1.x86_64
mariadb105-gssapi-server-3:10.5.25-1.amzn2023.0.1.x86_64
mariadb105-server-3:10.5.25-1.amzn2023.0.1.x86_64
mariadb105-server-utils-3:10.5.25-1.amzn2023.0.1.x86_64
mysql-selinux-1.0.4-2.amzn2023.0.3.noarch
perl-B-1.80-477.amzn2023.0.6.x86_64
perl-DBD-MariaDB-1.22-1.amzn2023.0.4.x86_64
perl-DBI-1.643-7.amzn2023.0.3.x86_64
perl-Data-Dumper-2.174-460.amzn2023.0.2.x86_64
perl-File-Copy-2.34-477.amzn2023.0.6.noarch
perl-FileHandle-2.03-477.amzn2023.0.6.noarch
perl-Math-BigInt-1:1.9998.39-2.amzn2023.0.2.noarch
perl-Math-BigRat-0.2614-458.amzn2023.0.2.noarch
perl-Math-Complex-1.59-477.amzn2023.0.6.noarch
perl-Sys-Hostname-1.23-477.amzn2023.0.6.x86_64
perl-base-2.27-477.amzn2023.0.6.noarch

Complete!
[ec2-user@ip-192-168-1-238 ~]$ mysql -h bdexamens.cyv8lcbrcb1.us-east-1.rds.amazonaws.com -u admin
ERROR 1045 (28000): Access denied for user 'admin'@'192.168.1.238' (using password: NO)
[ec2-user@ip-192-168-1-238 ~]$ mysql -h bdexamens.cyv8lcbrcb1.us-east-1.rds.amazonaws.com -u admin -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 165
Server version: 8.0.40 Source distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help,' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases
-> ;
+-----+
| Database      |
+-----+
| information_schema |
| lab           |
| mysql          |
| performance_schema |
| sys            |
+-----+
5 rows in set (0.020 sec)

MySQL [(none)]>
```

The screenshot shows a terminal window with a black background and white text. It displays a MySQL session where the user connects to a remote database instance and lists the available databases. Below the terminal is a system tray with various icons, including a weather widget showing "11°C Soleado".