


Alejandro López Martínez

Exámen

Parte 1: Creación de una VPC y configuración de red (20 puntos)

Para crear la VPC clicamos en  y buscamos VPC, una vez dentro clicamos en Crear VPC.

En etiqueta de nombre ponemos, VPC-Examen y en CIDR IPv4 192.168.0.0/16

Crear VPC Información

Una VPC es una parte aislada de la nube de AWS que contiene objetos de AWS, como instancias de Amazon EC2.

Configuración de la VPC

Recursos que se van a crear Información
Cree únicamente el recurso de VPC o la VPC y otros recursos de red.

☒ Solo la VPC ☐ VPC y más

Etiqueta de nombre - *opcional*
Crea una etiqueta con una clave de "Nombre" y el valor que usted especifique.

my-vpc-01

Bloque de CIDR IPv4 Información
☒ Entrada manual de CIDR IPv4
☐ Bloque de CIDR IPv4 asignado por IPAM

CIDR IPv4
10.0.0.0/24
El tamaño del bloque CIDR debe estar entre /16 y /28.

Bloque de CIDR IPv6 Información
☒ Sin bloque de CIDR IPv6
☐ Bloque de CIDR IPv6 asignado por IPAM
☐ Bloque de CIDR IPv6 proporcionado por Amazon
☐ CIDR IPv6 de mi propiedad

Tenencia Información
Predeterminado ▼

CloudShell Comentarios Privacidad Términos Preferencias d

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

 14:11
25/03/2025

Ahora accedemos a subredes y le damos a crear subred.

En ID de la VPC elegimos la nuestra y en nombre de subred le damos un nombre y en subred ipv4 la ip 192.168.1.0/24

VPC > Subredes > Crear subred

Crear subred Información

VPC

ID de la VPC
Cree subredes en esta VPC.

vpc-0352dc44eaf67d8aa (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.

my-subnet-01

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.

CloudShell Comentarios Privacidad Términos Preferencias de

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

14:16
25/03/2025

Nombre de la subred

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

my-subnet-01

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

192.168.0.0/20

< > ^ v

▼ Etiquetas: *opcional*

No hay ninguna etiqueta asociada a este recurso.

Agregar nueva etiqueta

Puede agregar 50 más etiquetas.

Quitar

Agregar nueva subred

Cancelar

Crear subred

Shell Comentarios

Privacidad

Términos

Preferencias de cookies

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



14:29
25/03/2025



Creamos el gateway y le ponemos un nombre en mi caso será PuertaEnlaceExamen y pulsamos crear gateway de internet

Crear gateway de Internet Información

Una gateway de Internet es un router virtual que conecta una VPC a Internet. Para crear una nueva gateway de Internet, especifique el nombre de la gateway a continuación.

Configuración de gateway de Internet

Etiqueta de nombre
Crea una etiqueta con una clave de "Nombre" y el valor que usted especifique.

PuertaEnlaceExamen

Etiquetas: *opcional*
Una etiqueta es una marca que se asigna a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizar las etiquetas para buscar y filtrar sus recursos o hacer un seguimiento de los costos de AWS.

Clave	Valor - <i>opcional</i>
<div><div>Q</div><div>Name</div><div>X</div></div>	<div><div>Q</div><div>PuertaEnlaceExamen</div><div>X</div></div>

Quitar

Agregar nueva etiqueta

Puede agregar 49 más etiquetas.

Cancelar

Crear gateway de Internet

CloudShell

Comentarios

Privacidad

Términos

Preferencias de cookies

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

14:26

25/03/2025

2

Conectamos nuestra VPC a la gateway de internet

Conectar a la VPC (igw-0a27a9cf3f6171218)

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.

Q

vpc-0352dc44eaf67d8aa

X

► Comando de la interfaz de línea de comandos de AWS

Cancelar

Conectar gateway de Internet

CloudShell

Comentarios

Privacidad

Términos

Preferencias de cookies

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

^

14:36

25/03/2025

2

Creamos la tabla de enrutamiento, le damos un nombre TablaEnrutamientoExamen y asociamos nuestra VPC llamada VPC-Examen y pulsamos en Crear tabla de enrutamiento.

Editar rutas

Ruta 1

Destino

192.168.0.0/16

Destino

local

local

Estado

Activo

Propagada

No

Ruta 2

Destino

0.0.0.0/0

Destino

Puerta de enlace de Internet

igw-0a27a9cf3f6171218

Estado

Activo

Propagada

No

Quitar

Agregar ruta

Cancelar

Vista previa

Guardar cambios

CloudShell

Comentarios

Privacidad

Términos

Preferencias de cookies

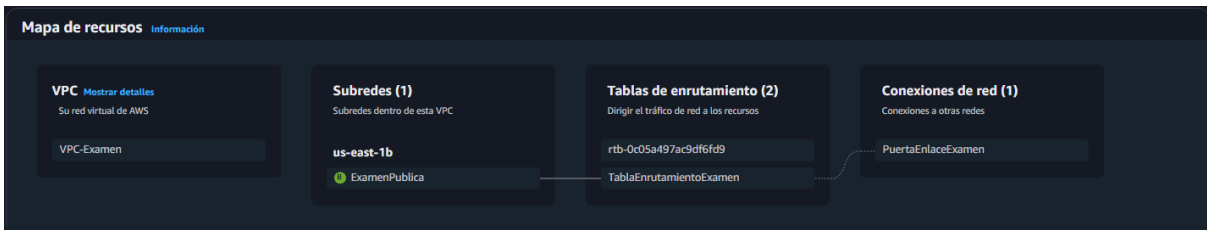
© 2025, Amazon Web Services, Inc. o sus filiales.

14:38

25/03/2025

2

Finalmente comprobamos que nuestra vpc tiene conexión a internet.



Parte 2: Creación y configuración de una instancia EC2 (20 puntos)

Buscamos en la barra del buscador EC2 y lanzamos una instancia que vamos a crear, le ponemos un nombre y seleccionamos Amazon Linux

Nombre y etiquetas Información

Nombre

InstanciaAL2Examen

[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.

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

Recientes

Inicio rápido

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE Linux

Debian

debian

Buscar más AMI

Inclusión de AMI de AWS, Marketplace y la comunidad

Imágenes de máquina de Amazon (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type
ami-04aa00acb1165b32a (64 bits (x86)) / ami-0a90799d0400252c7 (64 bits (Arm))
Virtualización: hvm Activado para ENA: true Tipo de dispositivo raíz: ebs

Apto para la capa gratuita

Descripción

Amazon Linux 2 incluye cinco años de soporte. Proporciona el kernel de Linux 5.10 adaptado para un rendimiento óptimo en Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1 y en los últimos paquetes de software a través de complementos.

Amazon Linux 2 Kernel 5.10 AMI 2.0.20250305.0 x86_64 HVM gp2

Arquitectura	ID de AMI	Fecha de	Nombre de usuario
--------------	-----------	----------	-------------------

[CloudShell](#) [Comentarios](#) [Privacidad](#) [Términos](#) [Preferencias de cookies](#)

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

16:23
25/03/2025

Dejamos todo por defecto excepto el par de claves que elegiremos Vockey y en la configuración de red le damos a editar y elegimos nuestra VPC, habilitamos la IP pública

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

Tipo de instancia

t2.micro

Apto para la capa gratuita

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

Bajo demanda Windows base precios: 0.0162 USD por hora

Bajo demanda Ubuntu Pro base precios: 0.0134 USD por hora

Bajo demanda SUSE base precios: 0.0116 USD por hora

Bajo demanda RHEL base precios: 0.026 USD por hora

▼

☐ Todas las generaciones

[Comparar tipos de instancias](#)

Se aplican costos adicionales a las AMI con software preinstalado

▼ Par de claves (inicio de sesión) [Información](#)

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

Nombre del par de claves - obligatorio

vockey

▼

[Crear un nuevo par de claves](#)

▼ Configuraciones de red [Información](#)

VPC: obligatorio [Información](#)

vpc-0352dc44eaf67d8aa (VPC-Examen)

192.168.0.0/16

▼

[Crear nueva VPC](#)

Subred [Información](#)

subnet-00907e93a8cf24578

ExamenPublica

VPC: vpc-0352dc44eaf67d8aa Propietario: 385796270358 Zona de disponibilidad: us-east-1b

Tipo de zona: Zona de disponibilidad Direcciones IP disponibles: 251 CIDR: 192.168.1.0/24

▼

[Crear nueva subred](#)

Asignar automáticamente la IP pública [Información](#)

Desactivar

▼

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

Habilitamos el acceso SSH, agregamos la regla HTTP en el grupo de seguridad, bajamos del todo y pulsamos Lanzar instancia

Nombre del grupo de seguridad - obligatorio

launch-wizard-1

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

Descripción - obligatorio

Información

launch-wizard-1 created 2025-03-25T14:54:38.122Z

Reglas de grupos de seguridad de entrada

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

Eliminar

Tipo

Información

ssh

Protocolo

Información

TCP

Intervalo de puertos

Información

22

Tipo de origen

Información

Cualquier lugar

Origen

Información

Q

Agregue CIDR, lista de prefijos o grupo de

0.0.0.0/0

X

Descripción - opcional

Información

por ejemplo, SSH para Admin Desktop

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

Eliminar

Tipo

Información

HTTP

Protocolo

Información

TCP

Intervalo de puertos

Información

80

Tipo de origen

Información

Cualquier lugar

Origen

Información

Q

Agregue CIDR, lista de prefijos o grupo de

0.0.0.0/0

X

Descripción - opcional

Información

por ejemplo, SSH para Admin Desktop

Conectamos por SSH usando putty

18.234.31.43 - PuTTY

login as:

< Detalles Estado y alarmas Monitoreo Seguridad Redes Almacén


▼ Resumen de instancia Información

ID de la instancia i-07ea6708b146af3fb	Dirección IPv4 pública 18.234.31.43 dirección abierta	Direcciones IPv4 privadas 192.168.1.82
Dirección IPv6 -	Estado de la instancia En ejecución	DNS de IPv4 pública -
Tipo de nombre de anfitrión Nombre de IP: ip-192-168-1-82.ec2.internal	Nombre DNS de IP privada (solo IPv4) ip-192-168-1-82.ec2.internal	

Accedemos por putty a la instancia y actualizamos el sistema con **sudo yum update -y**

```
ec2-user@ip-192-168-1-109:~  
login as: ec2-user  
Authenticating with public key "imported-openssh-key"  
Last login: Tue Mar 25 15:27:58 2025 from 189.red-81-38-172.dynamicip.rima-tde.n  
et  
  
#_#_  
##### Amazon Linux 2  
~~~~\#####\  
~~~\###| AL2 End of Life is 2026-06-30.  
~~~ \#/ \  
~~~ V~' '->  
~~~~ / A newer version of Amazon Linux is available!  
~~~~.-./ /  
___/_/ / Amazon Linux 2023, GA and supported until 2028-03-15.  
_/m/' https://aws.amazon.com/linux/amazon-linux-2023/  
  
[ec2-user@ip-192-168-1-109 ~]$ sudo dnf update -y  
sudo: dnf: command not found  
[ec2-user@ip-192-168-1-109 ~]$ sudo yum update -y  
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd  
amzn2-core | 3.6 kB 00:00  
No packages marked for update  
[ec2-user@ip-192-168-1-109 ~]$
```

Instalamos el servido web Apache



```
ec2-user@ip-192-168-1-109:~  
[ec2-user@ip-192-168-1-109 ~]$ sudo yum install -y httpd
```

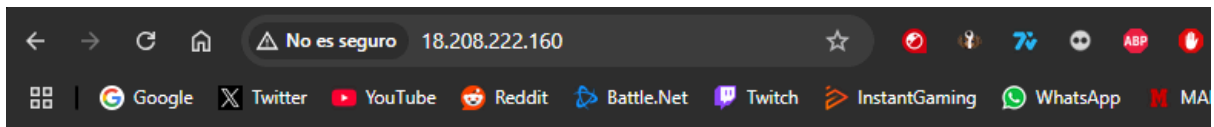
Habilitamos e iniciamos el apache

```
[ec2-user@ip-192-168-1-109 ~]$ sudo systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[ec2-user@ip-192-168-1-109 ~]$
```

```
[ec2-user@ip-192-168-1-109 ~]$ sudo systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[ec2-user@ip-192-168-1-109 ~]$ sudo systemct status httpd
sudo: systemct: command not found
[ec2-user@ip-192-168-1-109 ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd.service(8)
[ec2-user@ip-192-168-1-109 ~]$ sudo systemctl start httpd
[ec2-user@ip-192-168-1-109 ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2025-03-25 15:38:11 UTC; 2s ago
     Docs: man:httpd.service(8)
  Main PID: 3532 (httpd)
    Status: "Processing requests..."
    CGroup: /system.slice/httpd.service
            └─3532 /usr/sbin/httpd -DFOREGROUND
              └─3533 /usr/sbin/httpd -DFOREGROUND
                └─3534 /usr/sbin/httpd -DFOREGROUND
                  └─3535 /usr/sbin/httpd -DFOREGROUND
                    └─3536 /usr/sbin/httpd -DFOREGROUND
                      └─3537 /usr/sbin/httpd -DFOREGROUND

Mar 25 15:38:11 ip-192-168-1-109.ec2.internal systemd[1]: Starting The Apache...
Mar 25 15:38:11 ip-192-168-1-109.ec2.internal systemd[1]: Started The Apache ...
Hint: Some lines were ellipsized, use -l to show in full.
[ec2-user@ip-192-168-1-109 ~]$
```

Accedemos a /var/www/html y creamos index.html si no lo hay para ello hay que entrar como super usuario con **sudo su -**, creamos el html y comprobamos que funciona accediendo a la ip desde navegador



Hola Jesus, esto merece un 10

```
root@ip-192-168-1-109:/var/www/html
GNU nano 2.9.8 index.html
<html>
<body>
<h1>Hola Jesus, esto merece un 10</h1>
</body>
</html>
```

[Read 5 lines]

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Spell ^_ Go To Line

Parte 3: Creación de un Bucket S3 y Página Web Estática (20 puntos)

Creamos un bucket y le ponemos nuestro nombre a examen-web-estatica

Crear bucket Información

Los buckets son contenedores de datos almacenados en S3.

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

examen-web-estatica-alm

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/prefijo

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.

Propiedad del objeto
Aplicada al propietario del bucket

Desbloqueamos el acceso publico para que se pueda ver lo que hayamos subido al bucket

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.

Accedemos a propiedades del bucket y bajamos a abajo del todo editamos el alojamiento de sitios web estáticos y habilitamos.

Editar alojamiento de sitios web estáticos [Información](#)

Alojamiento de sitios web estáticos

Utilice este bucket para alojar un sitio web o redireccionar solicitudes. [Más información](#)

Alojamiento de sitios web estáticos

☐ Desactivar

☒ **Habilitar**

Tipo de alojamiento

☒ **Alojar un sitio web estático**
Utilice el punto de enlace del bucket como dirección web. [Más información](#)

☐ Redirigir las solicitudes de un objeto
Redirija las solicitudes a otro bucket o dominio. [Más información](#)

Le ponemos nombre a el documento de index y al de error

Documento de índice
Especifique la página predeterminada o de inicio del sitio web.

index.html

Documento de error - *opcional*
Esto se devuelve cuando se produce un error.

error.html

Reglas de redireccionamiento: *opcionales*
Redirija las reglas, escritas en JSON, para redirigir automáticamente las solicitudes de páginas web de contenido específico. [Más información](#)

1

JSON Ln 1, Col 1 ✖ Errores: 0 ⚠ Advertencias: 0 ⚙

Editamos los permisos y para que el contenido sea accesible para el público

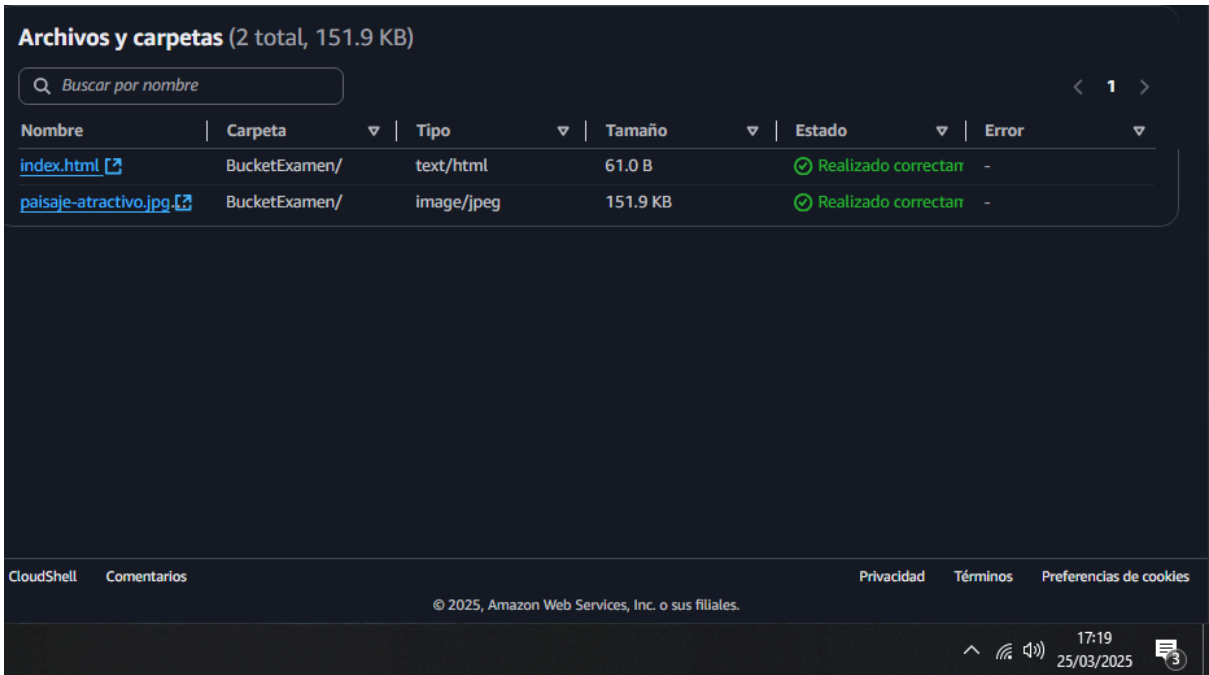
Política de bucket Editar Eliminar

La política del bucket, escrita en JSON, proporciona acceso a los objetos almacenados en el bucket. Las políticas de bucket no se aplican a los objetos que pertenecen a otras cuentas. [Más información](#)

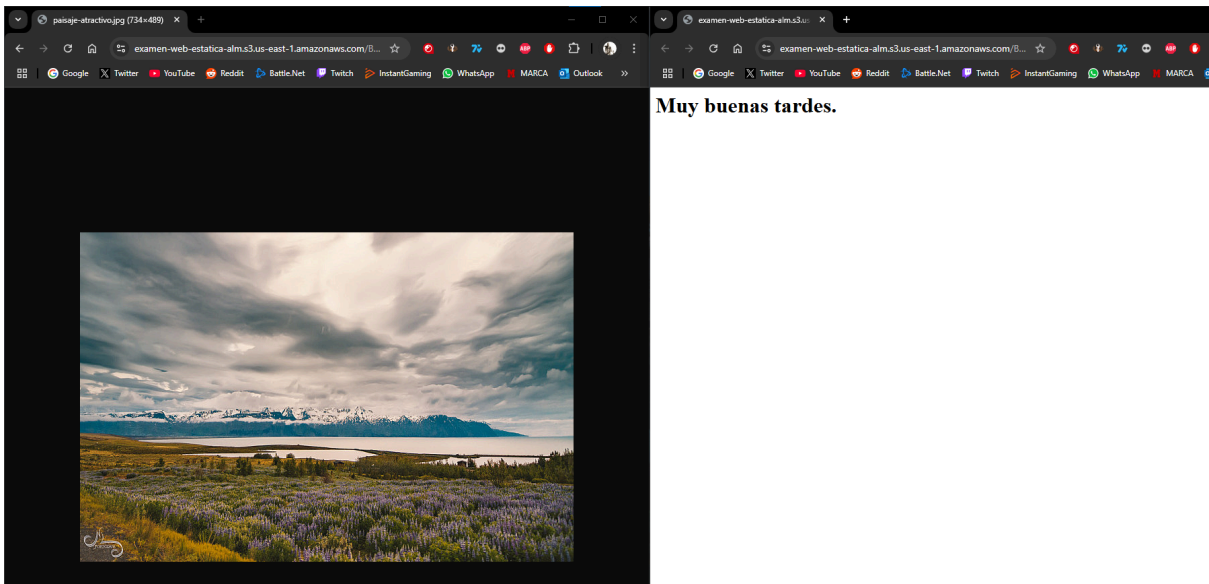
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examen-web-estatica-alm/*"
    }
  ]
}
```

Copiar

Subimos en mi caso una carpeta con un index.html sencillo y una imagen y pulsamos en cargar.



Accedemos a nuestros objetos y pulsamos en la url
url-index:<https://examen-web-estatica-alm.s3.us-east-1.amazonaws.com/BucketExamen/index.html>
url-imagen:<https://examen-web-estatica-alm.s3.us-east-1.amazonaws.com/BucketExamen/paisaje-atractivo.jpg>



Parte 4: Creación de una base de datos en RDS (20 puntos)

Buscamos en la barra de búsqueda RDS y clicamos, le damos a crear base de datos y seleccionamos MySQL

Crear base de datos Información

Elegir un método de creación de base de datos

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

☐ Creación sencilla
Utilice las configuraciones recomendadas. Algunas opciones de configuración se pueden cambiar después de crear la base de datos.

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 TiB.
- 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.

En plantilla seleccionamos Capa gratuita

Plantillas

Elija una plantilla de ejemplo para adaptarla a su caso de uso.

☐ **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](#)

En configuración ponemos el nombre la base de datos y nombre de usuario maestro admin, le damos a autoadministrado y le ponemos de contraseña maestra ExamenAWS2025

Configuración

Identificador del clúster de base de datos

Información

Ingrese un nombre para el clúster de base de datos. El nombre debe ser único entre todos los clústeres de base de datos de la cuenta de AWS de la región de AWS actual.

examen-db

El identificador del clúster de base de datos no distingue entre mayúsculas y minúsculas, pero se almacena todo en minúsculas (por ejemplo, "mydbcluster"). Restricciones: de 1 a 63 caracteres alfanuméricos o guiones. El primer carácter debe ser una letra. No puede contener dos guiones consecutivos. No puede terminar con un guion.

▼ Configuración de credenciales

Nombre de usuario maestro

Información

Escriba un ID de inicio de sesión para el usuario maestro del clúster de la base de datos.

admin

1 a 16 caracteres alfanuméricos. El primer carácter debe ser una letra.

Administración de credenciales

Puede usar AWS Secrets Manager o administrar sus credenciales de usuario maestro.

☐ Administrado en AWS Secrets Manager - más seguro

RDS genera una contraseña y la administra durante todo su ciclo de vida mediante AWS Secrets Manager.

☒ Autoadministrado

Cree su propia contraseña o pida a RDS que cree una contraseña para que pueda administrarla.

☐ Generar contraseña automáticamente

Amazon RDS puede generar una contraseña en su nombre, o bien puede especificar su propia contraseña.

Contraseña maestra

Información

Password strength

Very strong

Restricciones mínimas: al menos 8 caracteres ASCII imprimibles. No puede contener ninguno de los siguientes símbolos: / ' * @

Confirmar la contraseña maestra

Información

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 TiB.

• 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.

CloudShell

Comentarios

Privacidad

Términos

Preferencias de cookies

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

17:37

25/03/2025

3

En conectividad ponemos nuestra VPC

Conectividad Información

Recurso de computación

Seleccione si desea configurar una conexión a un recurso de computación para esta base de datos. Al establecer una conexión, se cambiará automáticamente la configuración de conectividad para que el recurso de computación se pueda conectar a esta base de datos.

☒ **No se conecte a un recurso informático EC2**
No configure una conexión a un recurso informático para esta base de datos. Puede configurar manualmente una conexión a un recurso informático más adelante.

☐ **Conectarse a un recurso informático de EC2**
Configure una conexión a un recurso informático EC2 para esta base de datos.

Nube privada virtual (VPC) Información

Elija la VPC. La VPC define el entorno de red virtual para este clúster de DB.

VPC-Examen (vpc-0352dc44eaf67d8aa)
1 Subredes, 1 Zonas de disponibilidad

Solo se muestran las VPC con grupos de subredes de base de datos correspondientes.

Ahora clicamos en Sí y elegimos un grupo de Seguridad de VPC existente que será la que creamos cuando hicimos la VPC

Grupo de subredes de la base de datos Información

Elija el grupo de subred de DB. El grupo de subred de DB que define las subredes e intervalos de IP que puede usar el clúster de base de datos en la VPC seleccionada.

Crear un nuevo grupo de subredes de base de datos.

Acceso público Información

☒ **Sí**
RDS asigna una dirección IP pública al clúster. Las instancias de Amazon EC2 y otros recursos fuera de la VPC pueden conectarse al clúster. Los recursos dentro de la VPC también pueden conectarse al clúster. Elija uno o varios grupos de seguridad de VPC que especifiquen qué recursos pueden conectarse al clúster.

☐ **No**
RDS no asigna una dirección IP pública al clúster. Solo las instancias de Amazon EC2 y otros recursos dentro de la VPC pueden conectarse al clúster. Elija uno o varios grupos de seguridad de VPC que especifiquen qué recursos pueden conectarse al clúster.

Grupo de seguridad de VPC (firewall) Información

Elija uno o varios grupos de seguridad de VPC para permitir el acceso a su base de datos. Asegúrese de que las reglas del grupo de seguridad permitan el tráfico entrante adecuado.

☒ **Elegir existente**
Elegir grupos de seguridad de VPC existentes

☐ **Crear nuevo**
Crear un grupo de seguridad nuevo de VPC

Grupos de seguridad de VPC existentes

Elegir una o más opciones

launch-wizard-2 ✕

Una vez creada entramos a Base de datos elegimos nuestra base de datos copiamos el punto de enlace y dentro de putty accedemos a mysql de esta manera **mysql -h examen-db.cj4prb4hmvho.us-east-1.rds.amazonaws.com -u admin -p** damos intro y nos pedirá la contraseña que antes habíamos puesto, ExamenAWS2025 y ya entramos a nuestra base de datos.

```
[root@ip-192-168-1-109 ~]# mysql -h examen-db.cj4prb4hmvho.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 32
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       |
| mysql                    |
| performance_schema       |
| sys                      |
+-----+
4 rows in set (0.01 sec)

MySQL [(none)]> █
```