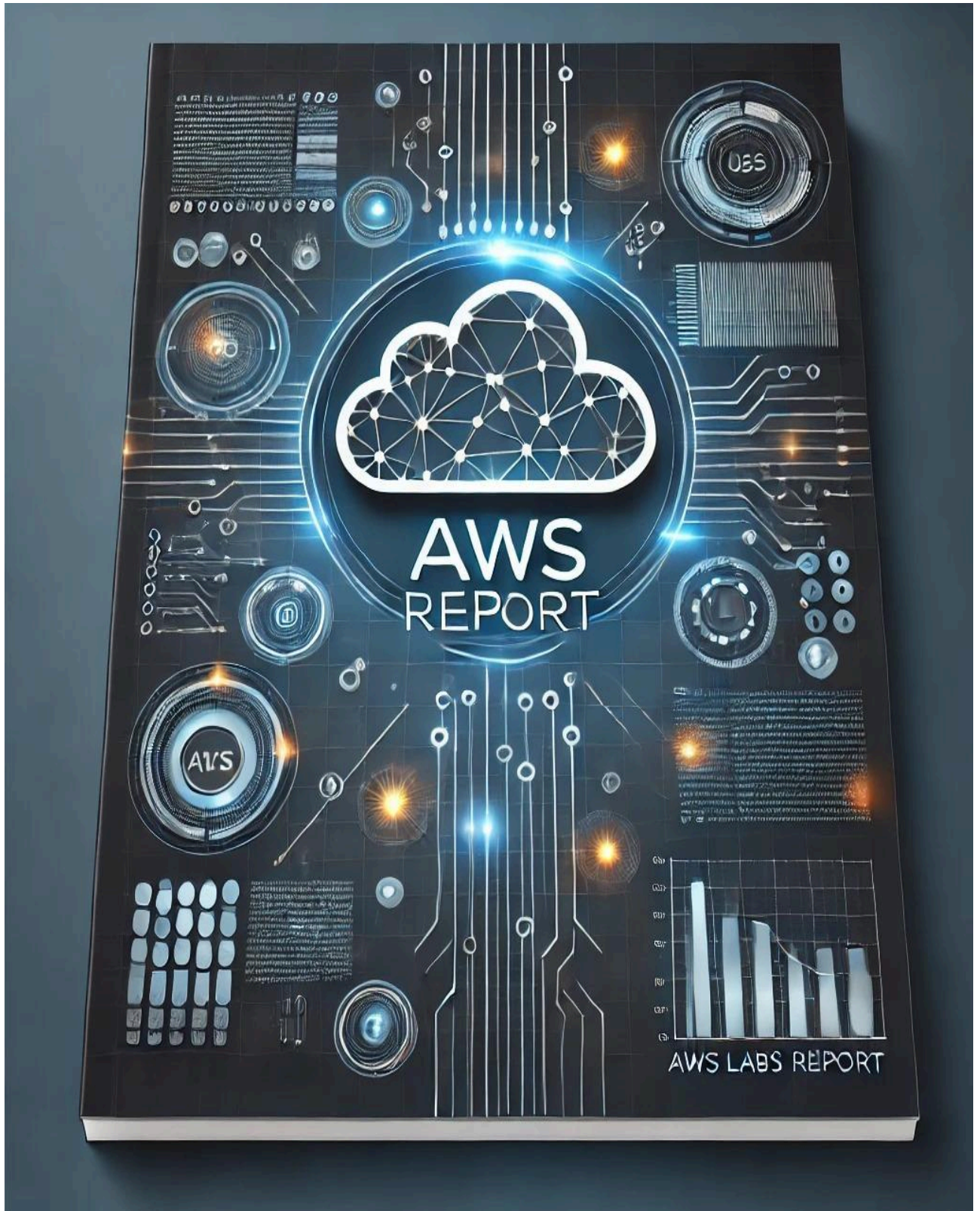
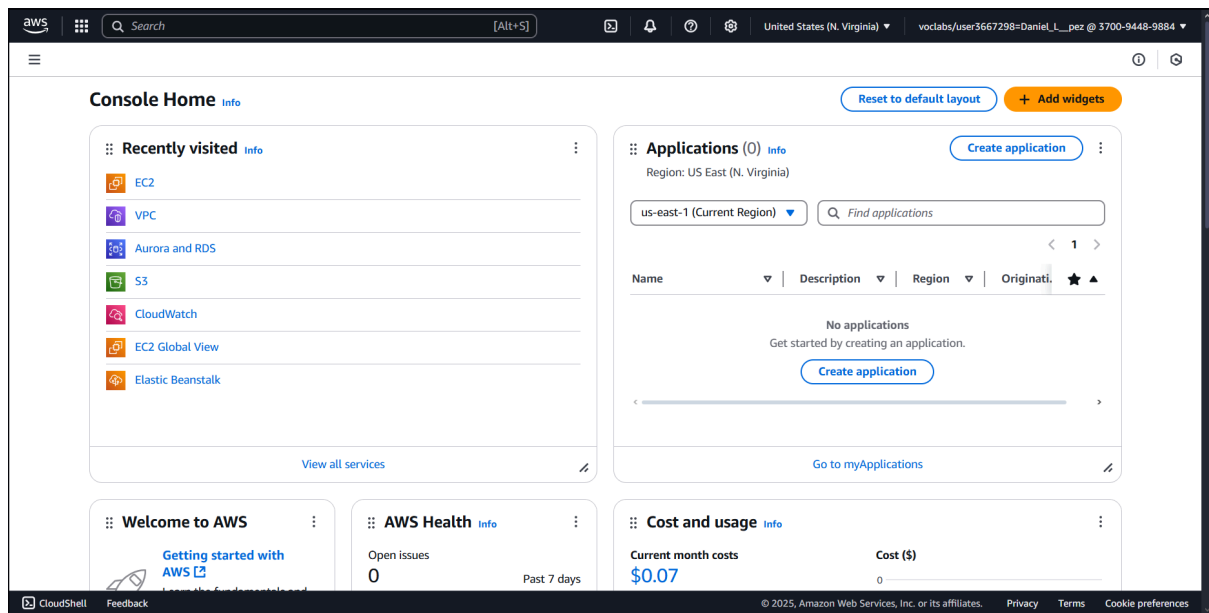


El fin de este documento es aprender a configurar varios servicios en AWS - Desde la VPC hasta la RDS.

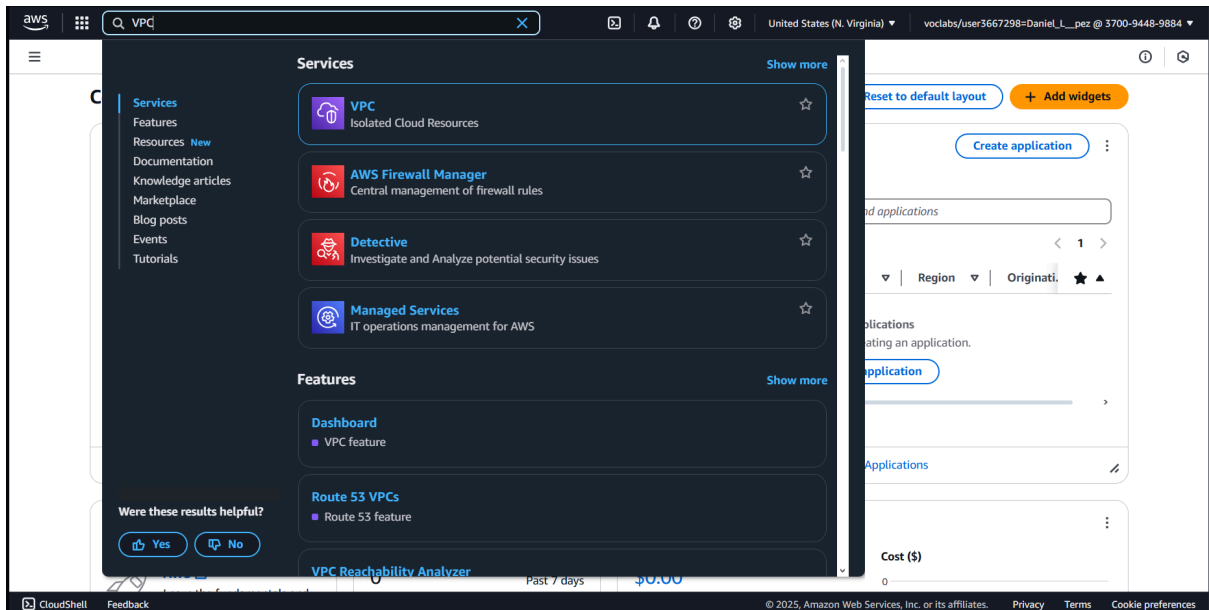


Punto 1 - Creaciones de VPC y configuraciones de R&D.

Para empezar a configurar la VPC vamos a tener que entrar al laboratorio y encontrar el menú de Home:



Una vez aquí vamos al buscador Search, y vamos a meter VPC y seleccionamos VPC la que tiene el borde en azul.



Cuando hemos entrado al sitio de VPC se nos abrirá la consola y vamos a pulsar el botón:

Crear VPC

Una vez aquí tendremos el configurable de:

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

☒ VPC only ☐ VPC and more

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

VPC-Examen

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input ☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

192.168.0.0/16

CIDR block size must be between /16 and /28.

En recursos marcamos VPC only, en Nametag le ponemos el nombre que estimemos y en el IPv4 CIDR introducimos el rango de IPs de la VPC.

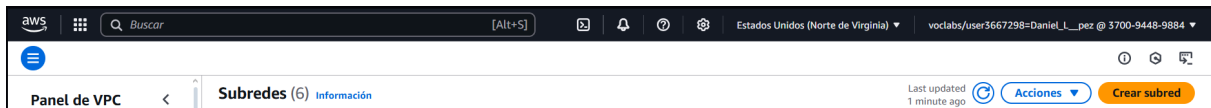
Y ahora podemos pulsar el botón:

Crear VPC

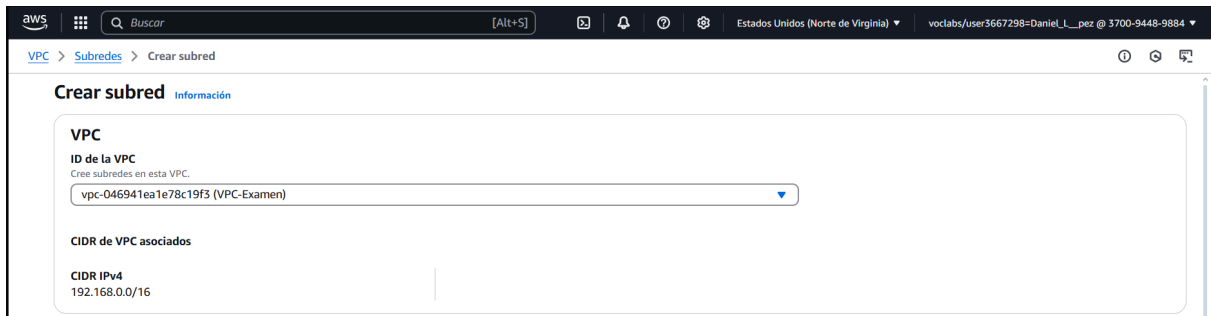
Para poder crearla,

Una vez creada miramos el menú de la izquierda y elegimos Subredes.

Tendremos un panel parecido en la parte superior de la pantalla y le damos al botón de Crear Subred.



Dentro de la configuración para crear la subred seleccionamos la VPC creada anteriormente donde está el desplegable de la ID de la VPC.



Bajamos hasta encontrar esto y le podemos poner el nombre a la Subred, elegimos la zona de disponibilidad de la misma mediante un desplegable, en mi caso us-east-1a, elegimos el rango y ponemos el rango de IPs en la parte de Bloque de CIDR de la subred IPv4.

Y si seguimos bajando encontraremos el botón de:

Crear subred

Apretamos y ya tenemos la subred creada.

En el menú de la izquierda elegimos Puertas de Enlace de Internet y le damos al botón:

Crear gateway de Internet

Una vez aquí le podemos poner el nombre de nuestra puerta de enlace y después le damos al botón de la derecha.

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.

Puerta de Enlace 1

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

Q. Name

Valor - *opcional*

Q. Puerta de Enlace 1

Quitar

Agregar nueva etiqueta

Puede agregar 49 más etiquetas.

Cancelar

Crear gateway de Internet

Una vez creada le damos a Acciones y Conectar a la VPC

The screenshot shows the AWS Management Console interface for an Internet Gateway. The main content area displays the details for 'igw-0244159868cb59ded / Puerta de Enlace 1'. The 'Detalles' section shows the gateway's ID, state (Detached), and VPC ID. The 'Etiquetas' section shows a table with one tag: 'Puerta de Enlace 1'. On the right, the 'Acciones' dropdown menu is open, showing options like 'Conectar a la VPC', 'Desconectar de la VPC', 'Administrar etiquetas', and 'Eliminar'. The 'Conectar a la VPC' option is highlighted. The left sidebar shows the 'Panel de VPC' with various navigation options. The bottom of the console shows the footer with copyright information and links to privacy and terms.

Seleccionamos en VPC disponibles la que creamos antes y le damos a Conectar gateway de Internet.

Conectar a la VPC (igw-0244159868cb59ded) 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-046941ea1e78c19f3

Utilizar: "vpc-046941ea1e78c19f3"

vpc-046941ea1e78c19f3 - VPC-Examen

Cancelar

Conectar gateway de Internet

Una vez terminada la conexión a la VPC, en el menú de la izquierda elegimos Tablas de enrutamiento.
Y la creamos.

Crear tabla de enrutamiento

Crear tabla de enrutamiento [Información](#)

Una tabla de enrutamiento especifica cómo se envían los paquetes entre las subredes de la VPC, Internet y la conexión de la VPN.

Configuración de la tabla de enrutamiento

Nombre - *opcional*

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

Tabla1

VPC

La VPC que se debe usar para esta tabla de enrutamiento.

vpc-046941ea1e78c19f3 (VPC-Examen)

Etiquetas

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

Q Name

Valor - *opcional*

Q Tabla1

Quitar

Agregar nueva etiqueta

Puede agregar 49 más etiquetas.

Cancelar

Crear tabla de enrutamiento

Aquí le damos Nombre a la tabla y ponemos la VPC creada y le damos a Crear tabla de enrutamiento.

Una vez creada veremos esto y le damos a Editar Rutas.

Panel de VPC <

Vista global de EC2

Filtrar por VPC

▼ Nube virtual privada

- Sus VPC
- Subredes
- Tablas de enrutamiento
- Puertas de enlace de Internet
- Puerta de enlace de Internet de solo salida
- Gateways de operador
- Conjuntos de opciones de DHCP
- Direcciones IP elásticas
- Listas de prefijos administradas
- Gateways NAT
- Interconexiones

▼ Seguridad

- ACL de red
- Grupos de seguridad

rtb-0bb6ea51c474130d2 / Tabla1 Acciones

Detalles [Información](#)

ID de tabla de enrutamiento rtb-0bb6ea51c474130d2

Principal No

Asociaciones de subredes explícitas -

Asociaciones de borde -

VPC vpc-046941ea1e78c19f3 | VPC-Examen

ID de propietario 370094489884

Rutas [Asociaciones de subredes](#) [Asociaciones de borde](#) [Propagación de rutas](#) [Etiquetas](#)

Rutas (1) Ambos Editar rutas

Destino	Destino	Estado	Propagada
192.168.0.0/16	local	Activo	No

Nos aparecerá esto con solo la ruta local, le damos a Agregar y le ponemos Destino 0.0.0.0/0 , y en el de la derecha seleccionamos Puerta de enlace de internet, y abajo seleccionamos la Puerta de Enlace creada por nosotros.
Y le damos a Guardar Cambios.

VPC > Tablas de enrutamiento > rtb-0bb6ea51c474130d2 > Editar rutas

Editar rutas

Destino	Destino	Estado	Propagada
192.168.0.0/16	local	Activo	No
Q 0.0.0.0/0	Q local		No
	Puerta de enlace de Internet		
	Q igw-0244159868cb59ded		

[Agregar ruta](#)

[Cancelar](#) [Vista previa](#) [Guardar cambios](#)

Si hemos hecho bien los pasos:

Iremos a Sus VPC, seleccionamos la VPC creada y le damos a Mapa de Recursos y se tendría que ver algo parecido a esto:



Como se puede ver tenemos otra subred hazla con ola zona us-east-1b

Punto 2 - Creaciones y Configuración de Instancias EC2.

En el buscador buscamos EC2 y lo seleccionamos y le damos a Lanzar Instancia:

aws | Buscar [Alt+S] | Estados Unidos (Norte de Virginia) | voclabs/user3667298=Daniel_L_pez @ 3700-9448-9884

EC2

Panel

Vista global de EC2

Eventos

▼ **Instancias**

- Instancias
- Tipos de instancia
- Plantillas de lanzamiento
- Solicitudes de spot
- Savings Plans
- Instancias reservadas
- Alojamientos dedicados
- Reservas de capacidad

▼ **Imágenes**

- AMI
- Catálogo de AMI

▼ **Elastic Block Store**

- Volúmenes
- Instantáneas
- Administrador del ciclo de vida

Puede cambiar la página de inicio predeterminada para EC2. [Descartar permanentemente](#) [Cambiar la página de inicio](#)

Recursos

Actualmente, utiliza los siguientes recursos de Amazon EC2 en la región Estados Unidos (Norte de Virginia):

Instancias (en ejecución)	0	Balanceadores de carga	0	Capacity Reservations	0
Direcciones IP elásticas	0	Grupos de escalamiento automático	0	Grupos de seguridad	2
Grupos de ubicación	0	Hosts dedicados	0	Instancias	0
Instantáneas	0	Pares de claves	1	Volúmenes	0

Lanzar la instancia

Para comenzar, lance una instancia de Amazon EC2, que es un servidor virtual en la nube.

[Lanzar la instancia](#)

[Migrar un servidor](#)

Nota: Sus instancias se lanzarán en la región Estados Unidos (Norte de Virginia)

Estado del servicio

[Panel de AWS Health](#)

Región: Estados Unidos (Norte de Virginia)

Estado: Este servicio funciona con normalidad.

Atributos de la cuenta

VPC predeterminada: vpc-0caa5775027f64e5e

Configuración

- Protección y seguridad de datos
- Allowed AMIs
- Zonas
- Consola de serie de EC2
- Especificación de crédito predeterminada
- Preferencias de la consola de EC2

Información adicional

- Instrucciones para comenzar
- Guía de introducción
- Documentación
- Todos los recursos de EC2
- Foros
- Precios
- Póngase en contacto con nosotros

© 2025, Amazon Web Services, Inc. o sus filiales. [Privacidad](#) [Términos](#) [Preferencias de cookies](#)

Le ponemos el nombre a nuestra Instancia y seleccionamos Amazon Linux

EC2 > Instancias > Lanzar una instancia

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

Linux

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

Inicio rápido

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE

Debian

debian

Q

Buscar más AMI

Inclusión de AMI de AWS, Marketplace y la comunidad

Imágenes de máquina de Amazon (AMI)

Si bajamos un poco encontramos un desplegable con AMI (Imágenes de máquina de Amazon), y seleccionamos Amazon Linux 2.

Imágenes de máquina de Amazon (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type

Apto para la capa gratuita

ami-04aa00acb1165b32a (64 bits (x86)) / ami-0a90799d0400252c7 (64 bits (Arm))

Virtualización: hvm Activado para ENA: true Tipo de dispositivo raíz: ebs

Si bajamos hasta encontrar Configuraciones de Red, le damos a editar.

▼ Configuraciones de red

Información

Editar

Red

Información

vpc-0caa5775027f64e5e

Subred

Información

Sin preferencias (subred predeterminada en cualquier zona de disponibilidad)

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

Si miramos la opciones vemos el Par de Claves dale a vockey, y en las configuraciones de red elige la VPC creada y la subred creada justo debajo habilitamos la Asignación automática de la IP pública.

▼ 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-046941ea1e78c19f3 (VPC-Examen) 192.168.0.0/16 ▼

↻

Subred | [Información](#)

subnet-0ea44cf05def83eeb Pública1 ▼

VPC: vpc-046941ea1e78c19f3 Propietario: 370094489884
Zona de disponibilidad: us-east-1a 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](#)

Habilitar ▼

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

Encontramos esto y mantenemos el ssh pero le damos a Añadir regla de grupo. Y seleccionamos HTTP y en origen 0.0.0.0/0.

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](#)

🔍 [Agregue CIDR, lista de prefijos o grupo](#)

0.0.0.0/0 ✕

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

por ejemplo, SSH para Admin Desktop

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

Tipo | [Información](#)

HTTP ▼

Protocolo | [Información](#)

TCP

Intervalo de puertos | [Información](#)

80

Tipo de origen | [Información](#)

Cualquier lugar ▼

Origen | [Información](#)

🔍 [Agregue CIDR, lista de prefijos o grupo](#)

0.0.0.0/0 ✕

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

por ejemplo, SSH para Admin Desktop

Y ahora podemos darle a

Lanzar instancia

Una vez creada seleccionamos la instancia y buscamos esto y copiamos la IPv4:

▼ Resumen de instancia [Información](#)

ID de la instancia
i-0677acc8053882529

Dirección IPv6
-

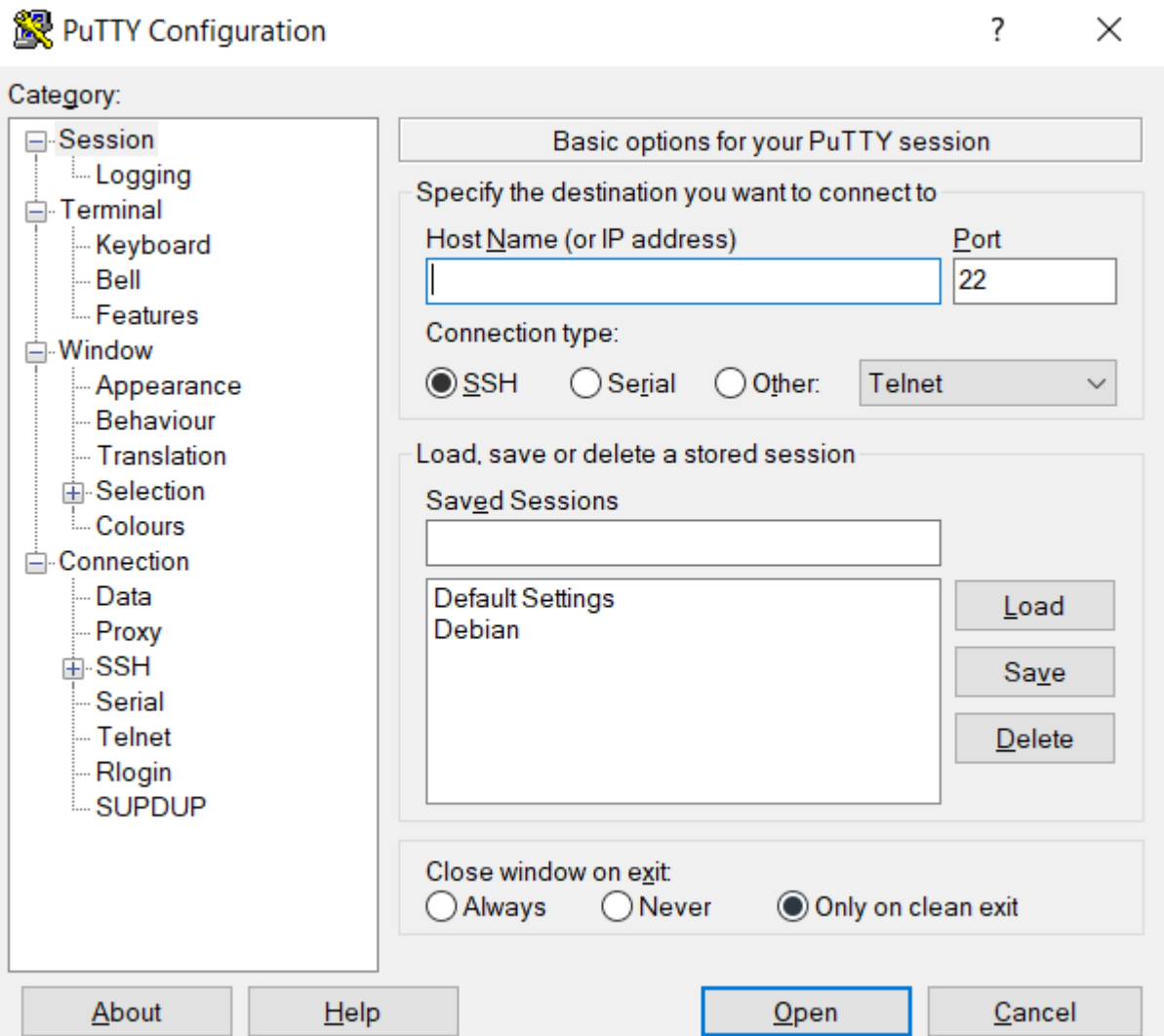
Dirección IPv4 pública
44.222.84.181 | [dirección abierta](#)

Estado de la instancia
En ejecución

Direcciones IPv4 privadas
192.168.1.203

DNS de IPv4 pública
-

Vamos a abrir el Putty y en HostName pegamos la IP



Para conseguir la llave vamos a la pantalla de lanzamiento del Laboratorio y le damos a AWS details, y le damos a download PPK

ALLv2ES-E... > Contenidos > Laboratori...
> Lanzamiento del Laboratorio para el alumnado de AWS Academy

Página de inicio

Contenidos

Foros de discusión

Notas

Lucid (pizarra)

AWS ● Used \$0.1 of \$50 02:25 ▶ Start Lab ■ End Lab ⓘ AWS Details ⓘ Readme ↺ Reset ✕

```
eee_M_4317047@runweb166339:~$
```

Cloud Access Close

AWS CLI: Show

Cloud Labs

Remaining session time: 02:24:10(145 minutes)
Session started at: 2025-03-26T02:26:26-0700
Session to end at: 2025-03-26T06:26:26-0700

Accumulated lab time: 05:26:00 (326 minutes)

No running instance

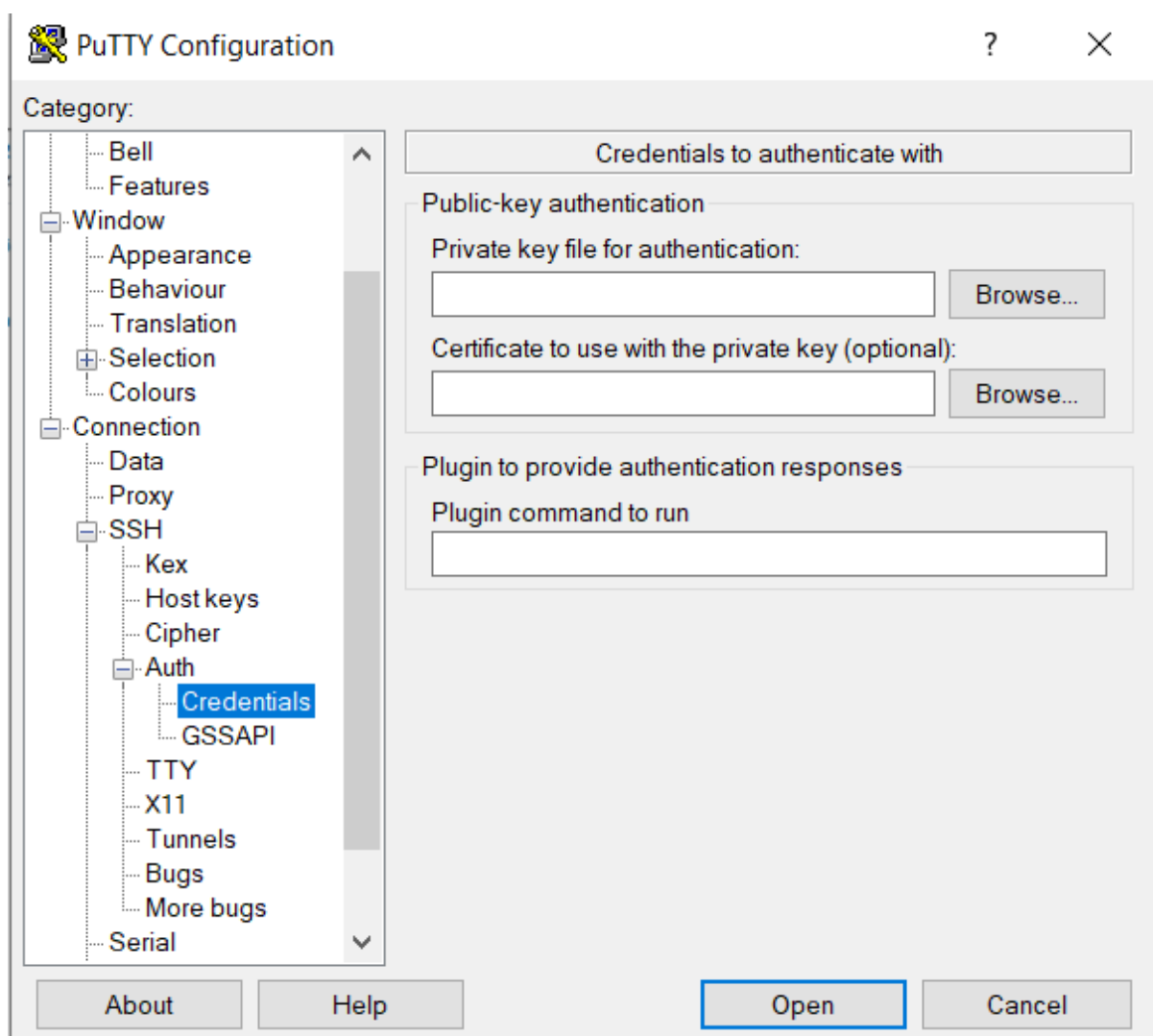
SSH key Show Download PEM

Download PPK

AWS SSO Download URL

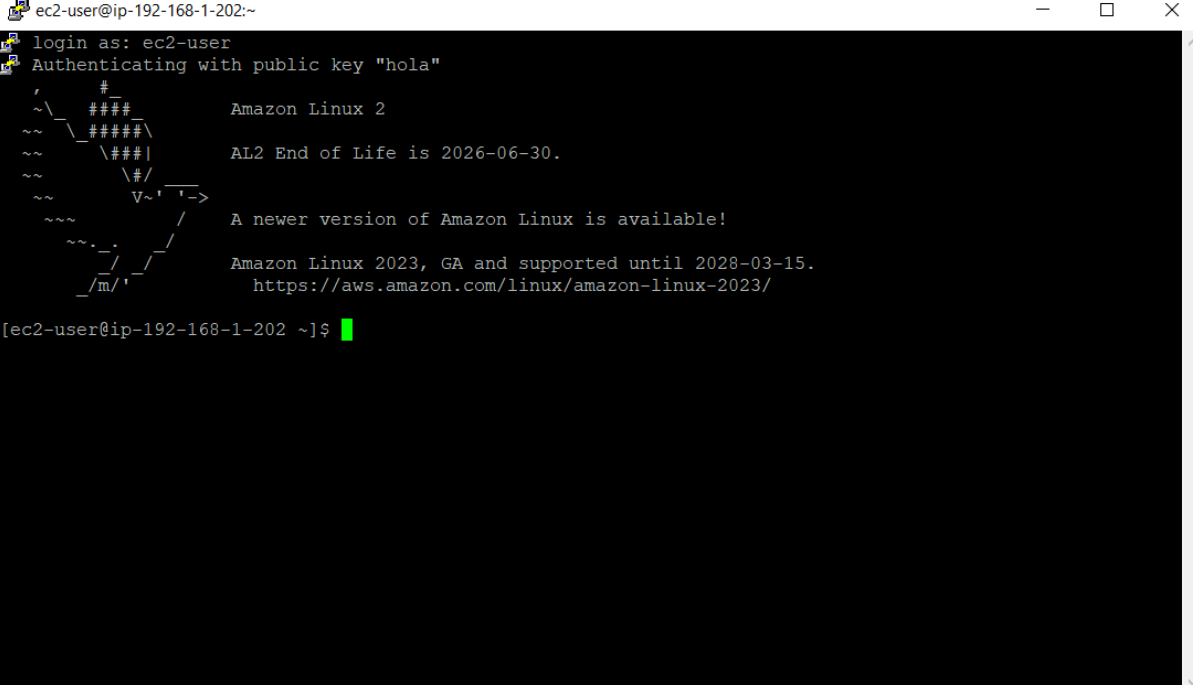
AWSAccountid	370094489884
Region	us-east-1

Abriendo la ruta SSH, Auth, Credentials seleccionamos Browse en Private key file... y le damos a Open



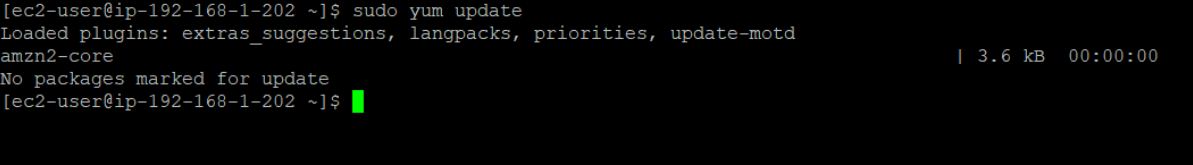
Dentro de la máquina nos pedirá el usuario y ponemos ec2-user como usuario y le damos a enter.

Saliendo:



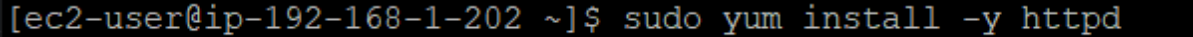
```
ec2-user@ip-192-168-1-202:~  
login as: ec2-user  
Authenticating with public key "hola"  
#####  
Amazon Linux 2  
#####  
AL2 End of Life is 2026-06-30.  
#####  
A newer version of Amazon Linux is available!  
#####  
Amazon Linux 2023, GA and supported until 2028-03-15.  
https://aws.amazon.com/linux/amazon-linux-2023/  
[ec2-user@ip-192-168-1-202 ~]$
```

Hacemos el `sudo yum update`, para actualizar la máquina.



```
[ec2-user@ip-192-168-1-202 ~]$ sudo yum update  
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd  
amzn2-core | 3.6 kB 00:00:00  
No packages marked for update  
[ec2-user@ip-192-168-1-202 ~]$
```

Para instalar el servidor apache hacemos el comando de abajo `sudo yum install -y httpd` y después la actualizamos con el `sudo systemctl restart httpd`

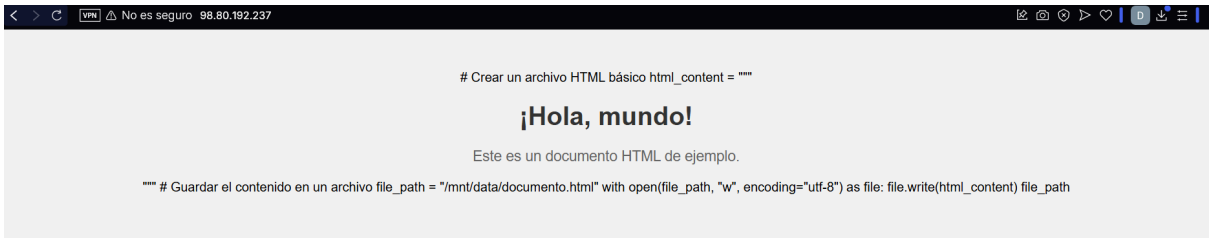


```
[ec2-user@ip-192-168-1-202 ~]$ sudo yum install -y httpd
```

Creamos una página HTML en `/var/www/html/index.html` para eso usamos el nano `/var/www/html/index.html`, ten en cuenta que si no te deja abrirlo usa el `sudo` delante.

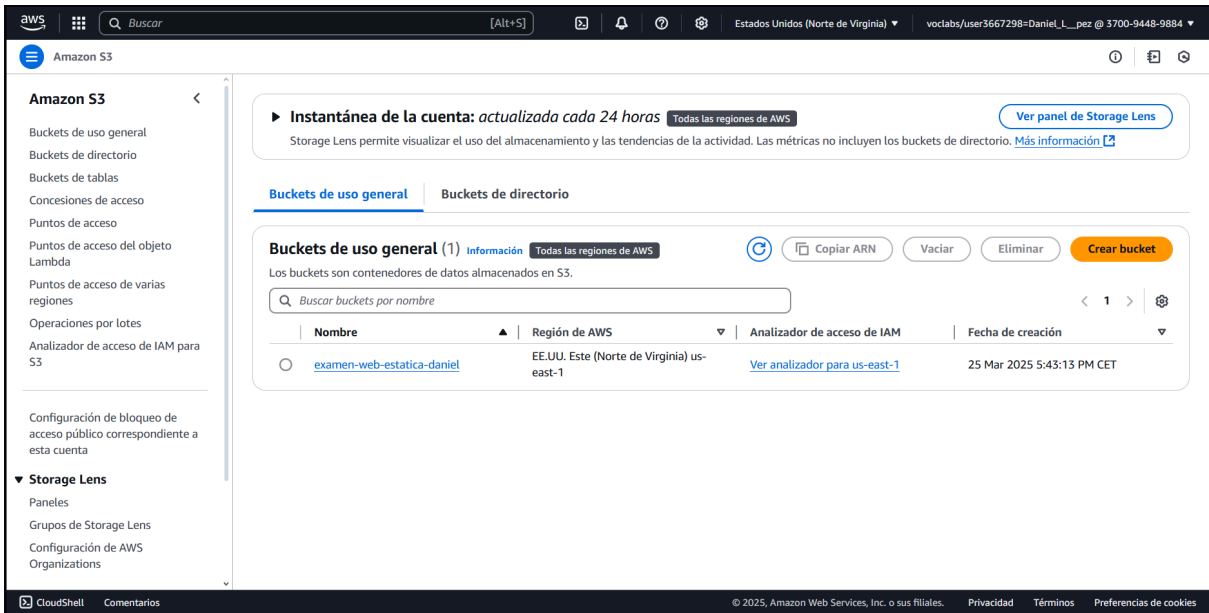
Una vez creada la página copiamos la IP y la metemos en nuestro navegador

Enseñándonos esta página de ejemplo.



Punto 3 - Creaciones de Páginas Estáticas y Buckets S3.

En el buscador buscamos S3 y lo seleccionamos y le damos a Crear Bucket



En configuración mantenemos uso general y le ponemos el nombre



Si bajamos encontramos todo esto activado y desactivamos Bloquear todo el acceso público, lo que desactivaría todo

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.

Una vez hecho todo esto bajamos y le damos a crear el Bucket.

Cuando la tenemos podemos entrar en Permisos y le damos a Política de Bucket y le damos a editar.

examen-web-estatica-daniel [Información](#)

Objetos Metadatos Propiedades **Permisos** Métricas Administración Puntos de acceso

Información general sobre los permisos

Búsqueda de acceso

Los analizadores de acceso externos de IAM proporcionan los hallazgos de acceso. Obtenga más información sobre [cómo funcionan los hallazgos del analizador de IAM](#)

[Ver analizador para us-east-1](#)

Bloquear acceso público (configuración del bucket) [Editar](#)

Se concede acceso público a 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 de S3, active Bloquear todo acceso público. Esta configuración se aplica en exclusiva a este bucket y a sus puntos de acceso. AWS recomienda activar Bloquear todo acceso público pero, antes de aplicar cualquiera de estos ajustes, asegúrese de que sus aplicaciones funcionarán correctamente sin acceso público. Si necesita cierto nivel de acceso público a sus buckets u objetos, puede personalizar los valores de configuración individuales a continuación para que se ajusten mejor a sus necesidades específicas de almacenamiento. [Más información](#)

Bloquear todo el acceso público

 Desactivado

► Configuración de bloqueo de acceso público individual para este bucket

Política de bucket [Editar](#) [Eliminar](#)

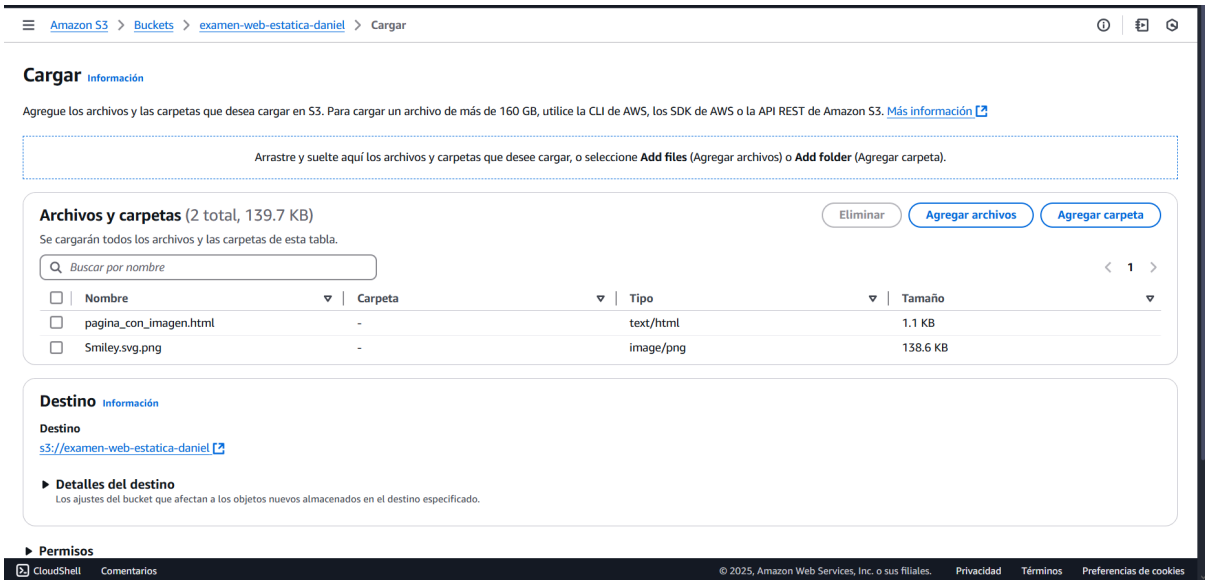
La política del bucket, escrita en JSON, proporciona acceso a los objetos almacenados en el bucket. Las políticas de bucket no se aplican a los objetos que pertenecen a otras cuentas. [Más información](#)

Una vez dentro pegamos esto y sustituimos una cosa:

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

Sustituye YOUR_BUCKET_NAME por el nombre de tu Bucket y prestar extrema atención a los * en Principal y delante de la barra en Resource.

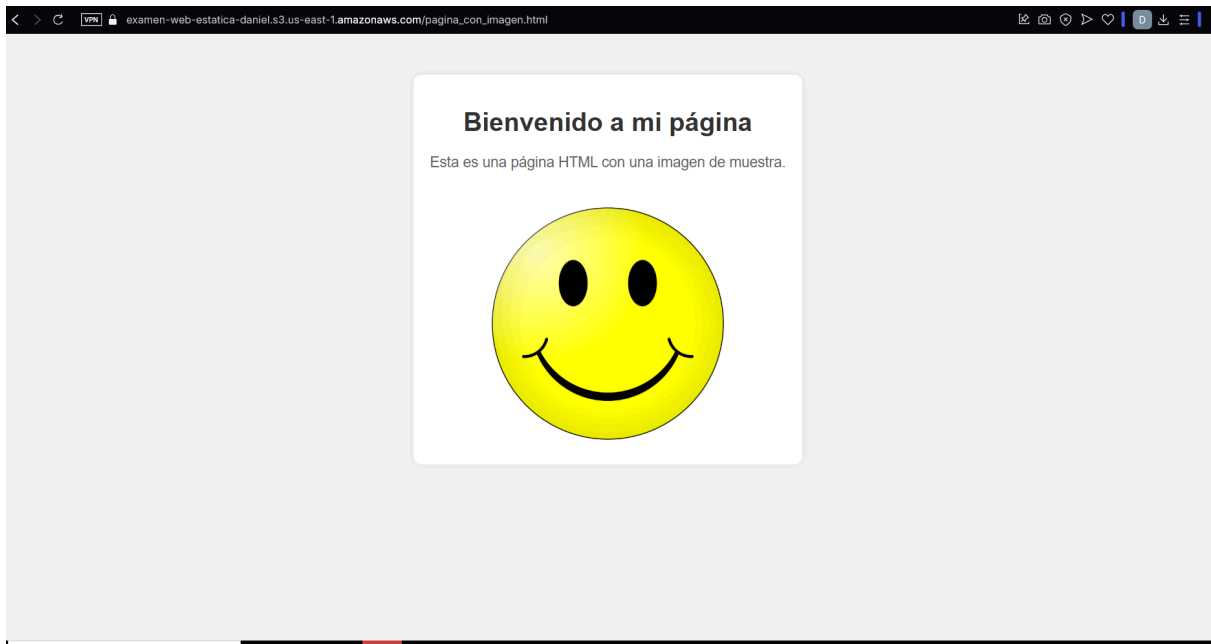
Salimos a hay y seleccionamos nuestro bucket y le podemos dar a cargar una página para hacer una página estática dale a cargar y agregar archivos, mete lo que quieras. html, imágenes, css , javascript



Luego le damos a propiedades y copiamos el Nombre de recurso.



Lo pegamos en el buscador y nos enseñará la página.



Punto 4 - Creación de una BD con RDS y Aurora.

Cuando hemos terminado el bucket seleccionamos el buscador y buscamos “Aurora and RDS”.

Una vez dentro en el menú de la izquierda selecciona bases de datos y creamos la Base de Datos.

Lo primero en seleccionar es MySQL que se ve así:



Seguimos bajando y encontramos Capa gratuita deseleccionada, la seleccionamos. Con esto se habrán seleccionado Implementación.

● Capa gratuita

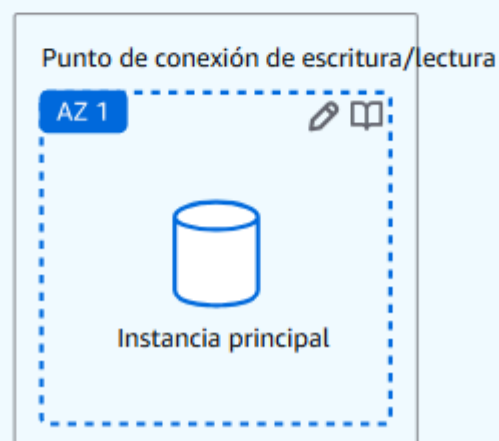
Utilice el nivel gratuito de RDS para desarrollar nuevas aplicaciones, probar aplicaciones existentes o adquirir experiencia práctica con Amazon RDS. [Información](#)

Comete a un determinado nivel de tiempo de actividad según la

● Implementación de una instancia de base de datos de zona de disponibilidad única (1 instancia)

Crea una única instancia de base de datos sin instancias en espera. Esta configuración proporciona:

- 99.5% uptime
- Sin redundancia de datos



Bajamos hasta configuración y le ponemos el nombre a la base de datos

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.

database-1

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.

Justo debajo rellena el usuario maestro, en Autoadministrado seleccionamos la contraseña y debajo hay que confirmarla

▼ Configuración de credenciales

Nombre de usuario maestro [Información](#)

Escriba un ID de inicio de sesión para el usuario maestro de la instancia de 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: / ' * @

Seleccionamos la VPC bajando bastante.

Nube privada virtual (VPC) [Información](#)

Elija la VPC. La VPC define el entorno de red virtual para esta instancia de DB.

VPC-Examen (vpc-046941ea1e78c19f3)

1 Subredes, 1 Zonas de disponibilidad

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

Y ya la podemos crear.