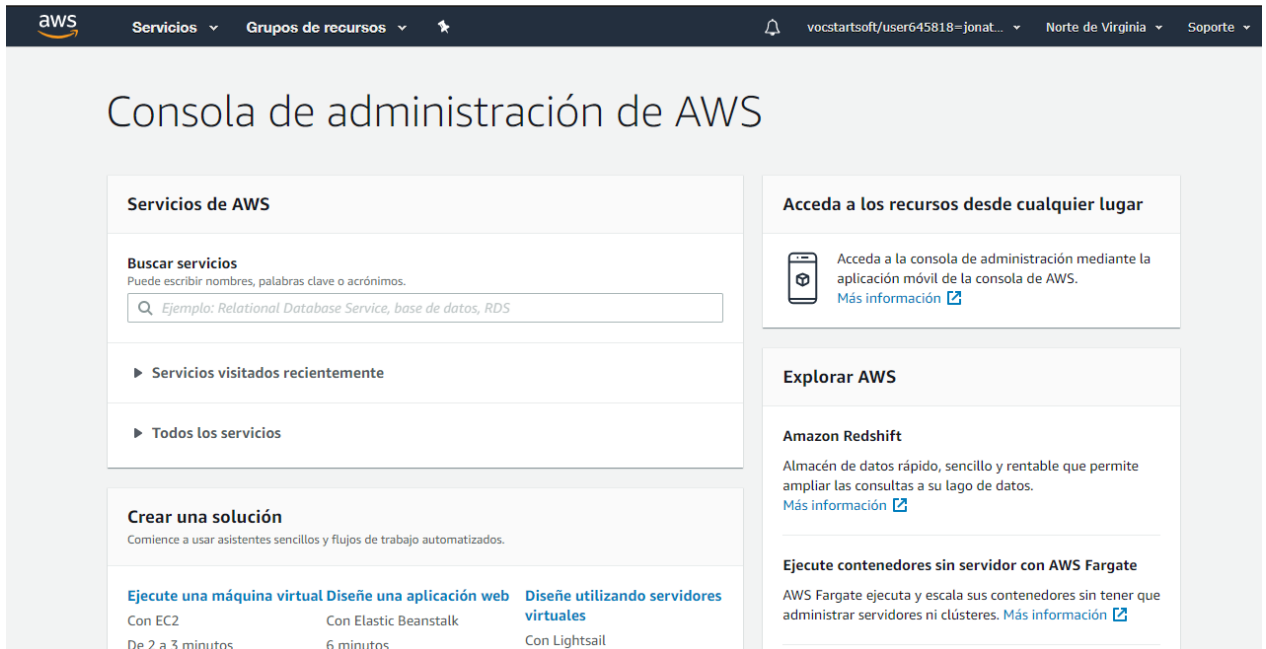


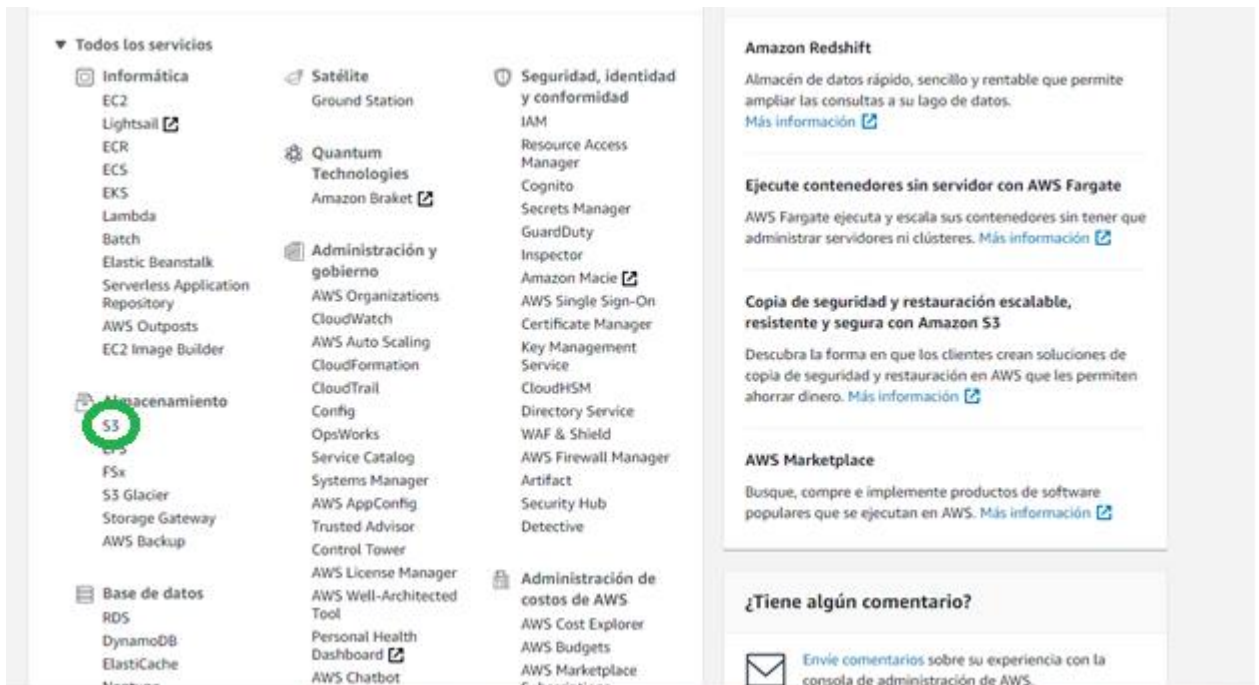
Desplegar un sitio estático usando S3

Para esto debemos tener cuenta en AWSEducate o AWS

1. Lo primero que hacemos es abrir la consola de Administración de AWS.



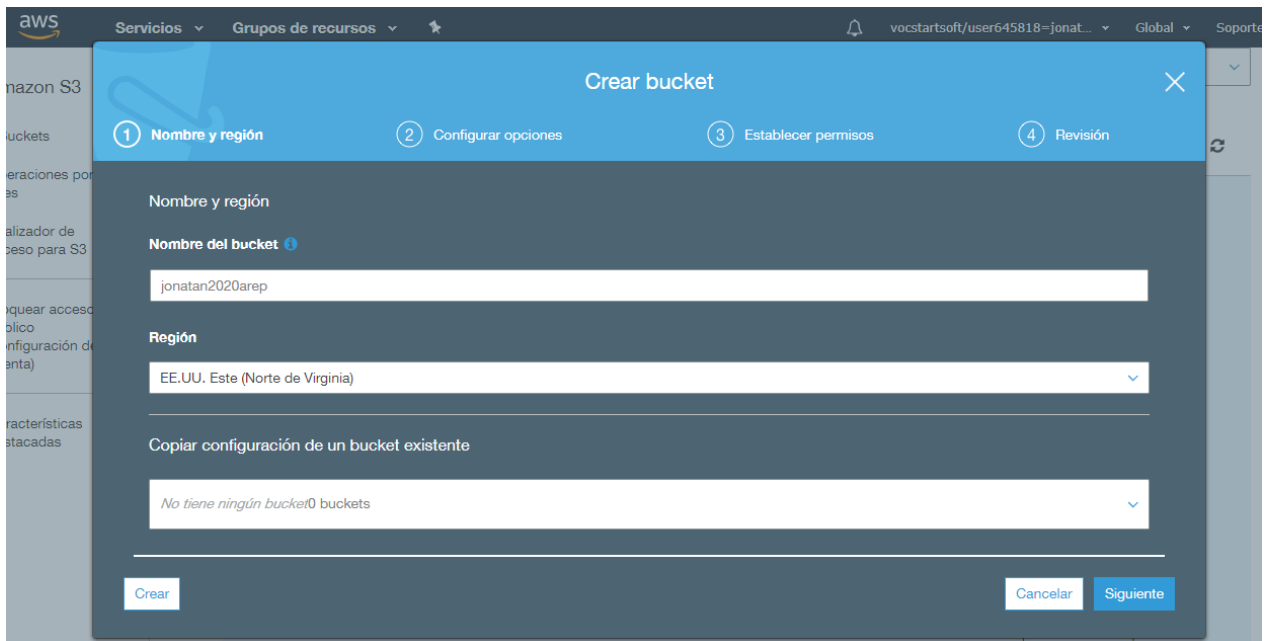
2. Nos dirigimos a la parte de Todos los servicios y seleccionamos S3 en la sección 'Almacenamiento'.



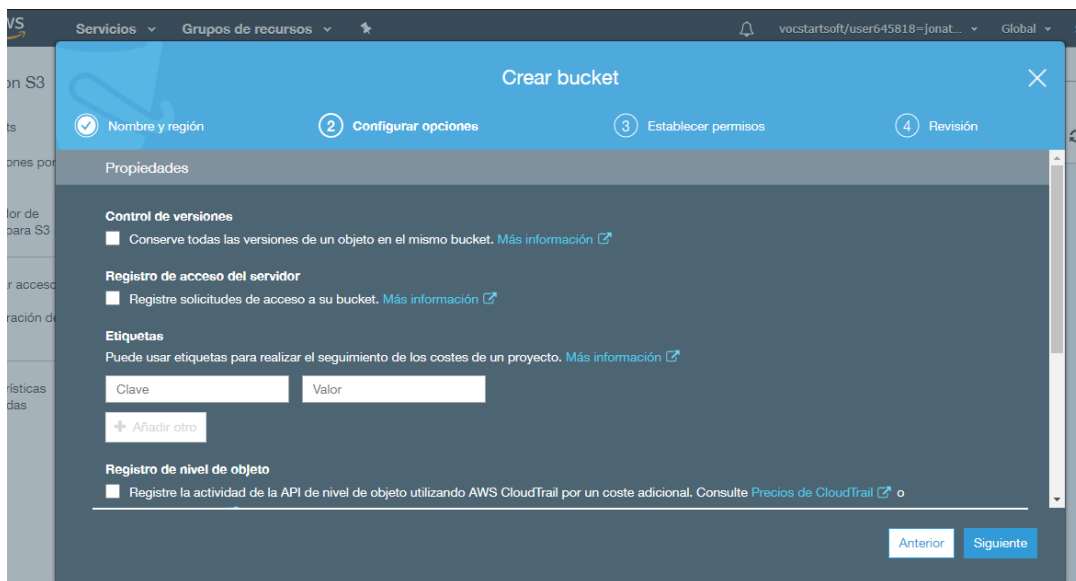
3. Damos click en el botón 'Creat Buket'



4. Le asignamos un nombre al bucket, en mi caso le pondré 'jonatan2020arep', también le asignamos la región donde se desplegará el recurso estático, en mi caso la dejare en EE.UU. Este (Norte de Virginia) y luego damos clic en Siguiente.

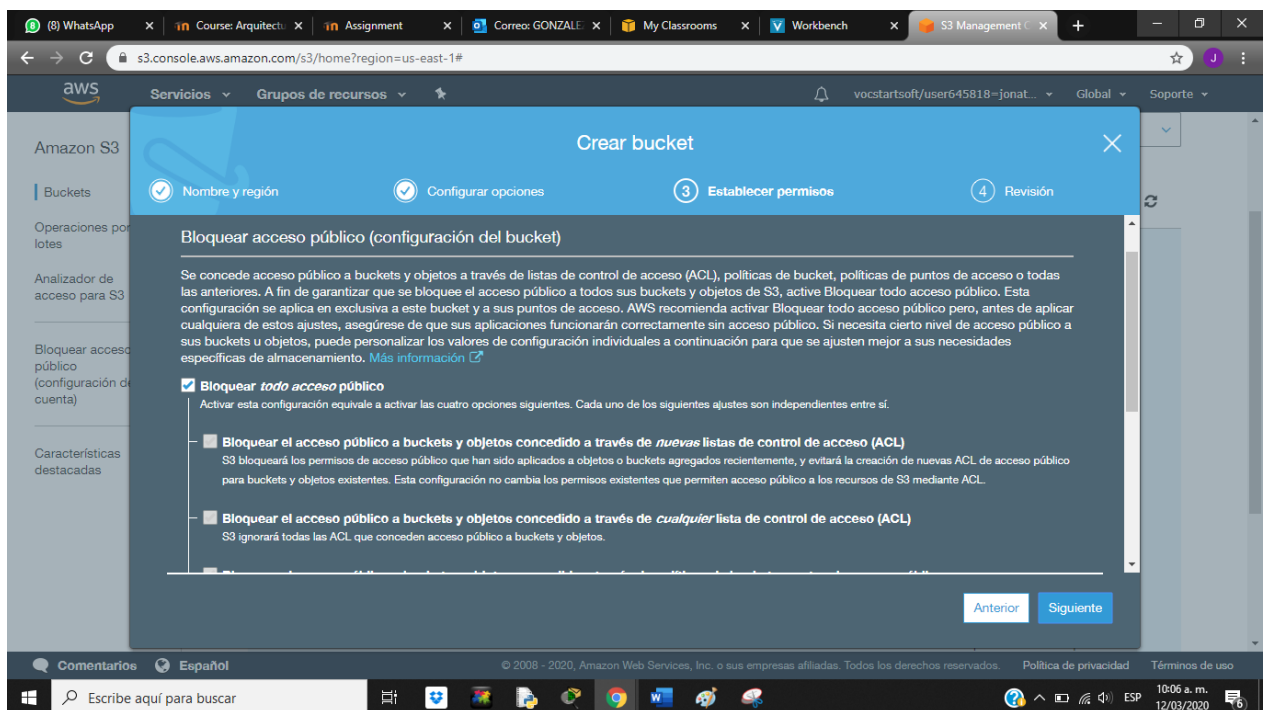


5. Para el caso de Configurar las opciones, no es necesario modificar los valores que vienen por defecto, simplemente damos clic en Siguiente.

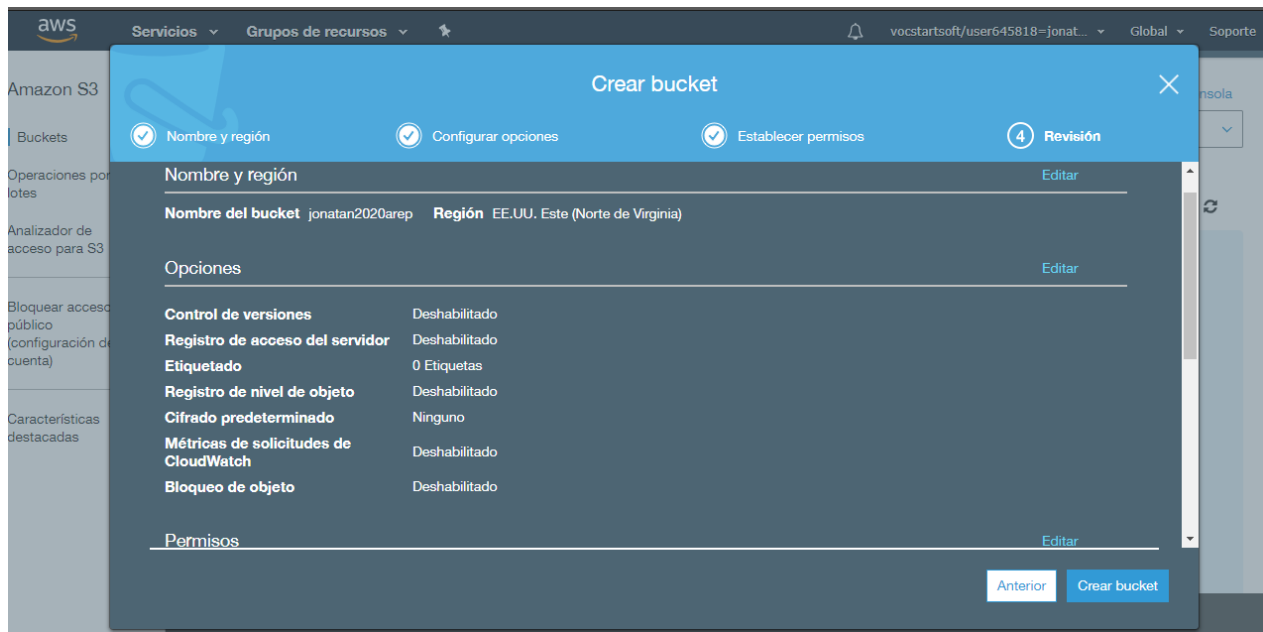


6. Desactivamos la opción de 'Bloquear todo acceso público' para poder dar acceso público y damos clic en Siguiente.

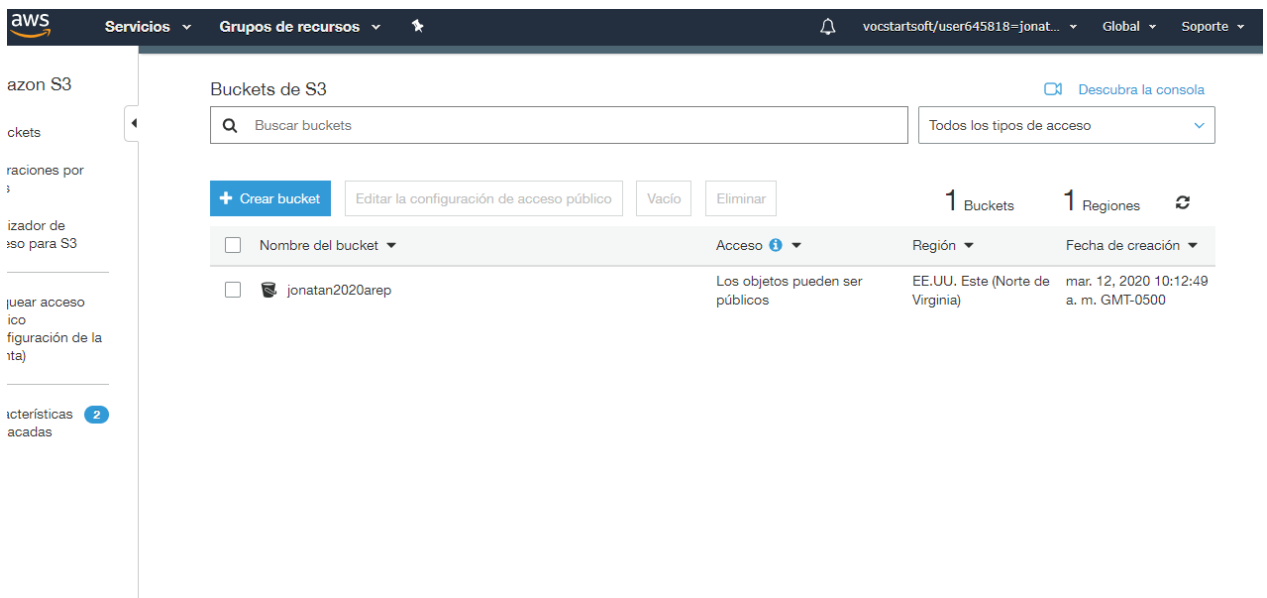
Nota: Al desactivar la opción de Bloquear todo acceso público se despliega una ventana y damos click en donde dice Reconozco que la configuración actual puede hacer que este bucket y los objetos que contiene se vuelvan públicos.



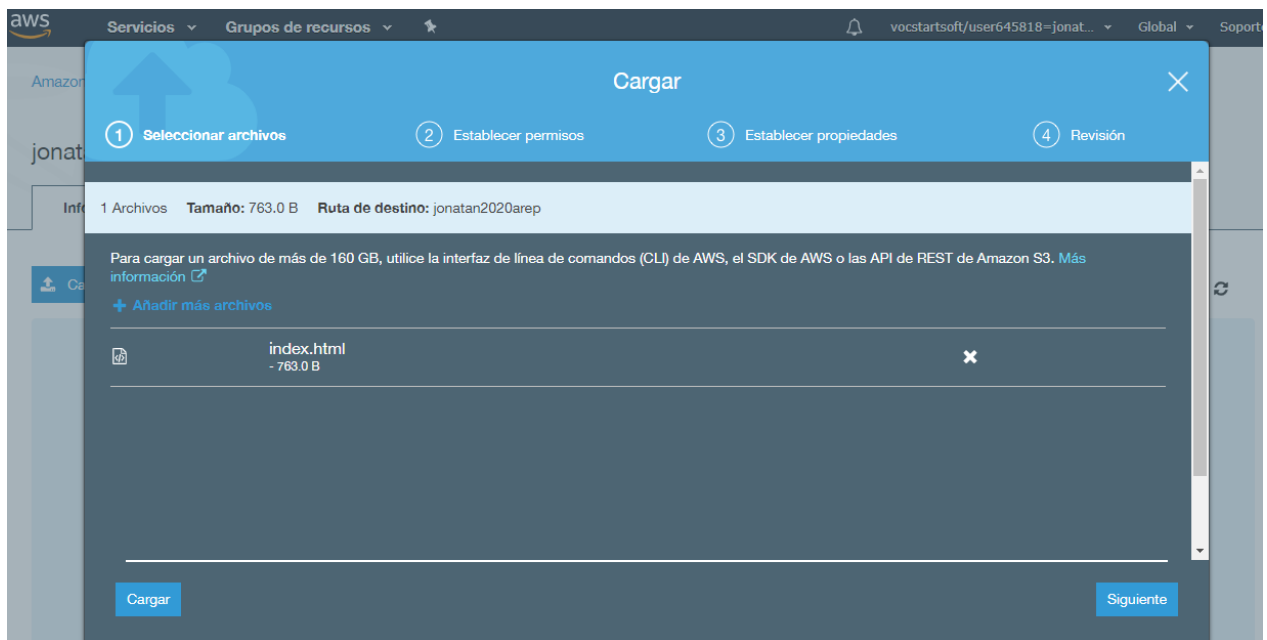
7. Revisamos que todo este configurado como nosotros queremos y damos click en 'Crear bucket'



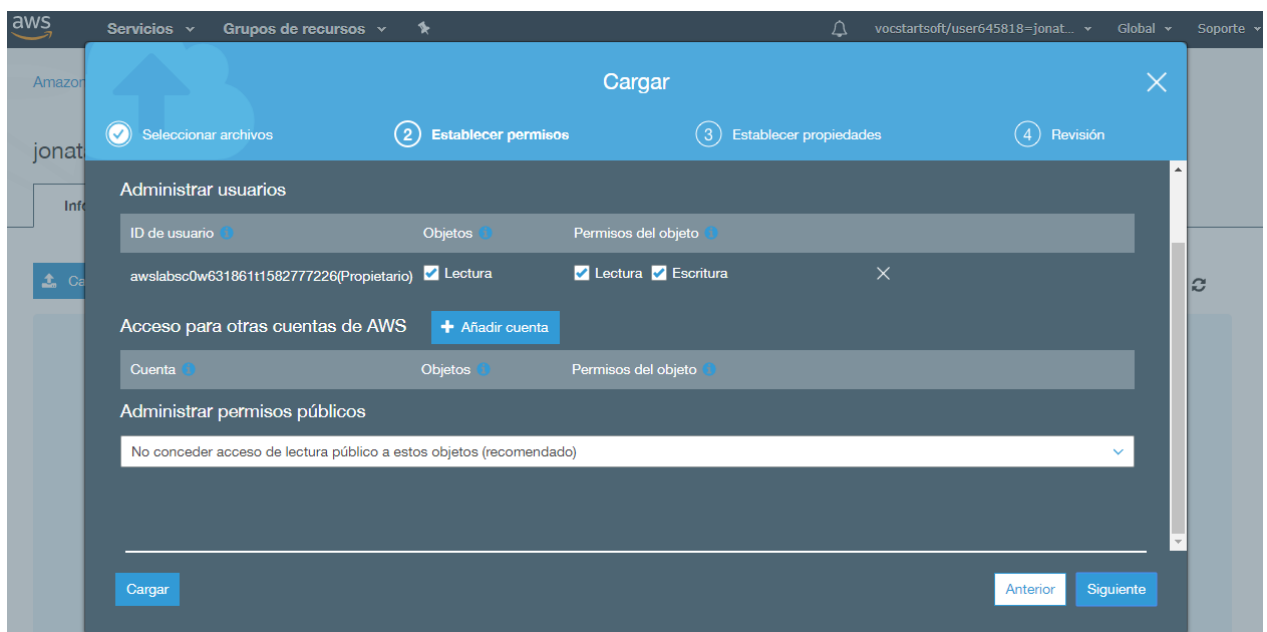
8. Una vez creado el bucket nos debe aparecer en la zona de buckets de S3



9. Entramos al bucket creado dando clic encima de él y damos clic en '**Cargar**' para subir nuestro archivo estático, en este caso yo subiré un archivo index.html de un laboratorio pasado, después damos click en Siguiente cuando tengamos el archivo seleccionado.



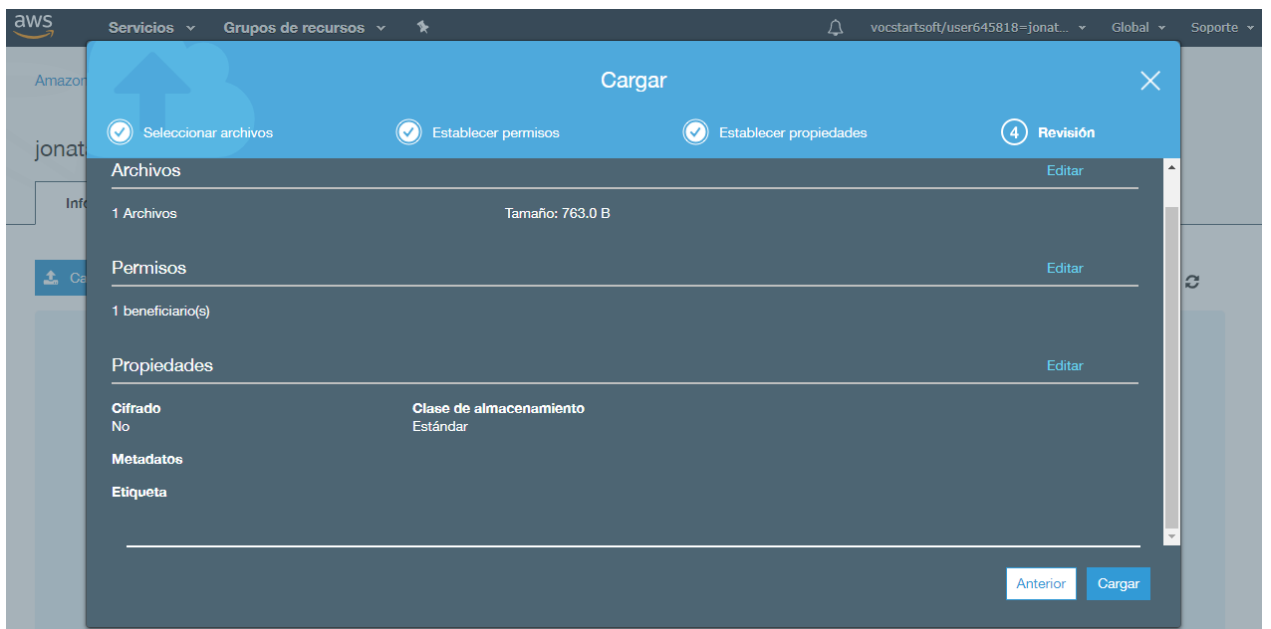
10. En la pestaña de cargar no debemos cambiar nada, solo damos clic en Siguiente.



11. En la siguiente ventana de Cargar seleccionamos la opción '**Estándar**' y damos click en siguiente.



12. Revisamos que las configuraciones estén como queremos y después damos click en Cargar.



13. Una vez subido el archivo, debe mostrarlo en la información general de mi bucket creado anteriormente, damos clic sobre él para poder verlo.

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with the AWS logo, 'Servicios', 'Grupos de recursos', and a user profile 'vocstartsoft/user645818=jonat...'. Below this, the breadcrumb 'index.html' is followed by a 'Última versión' dropdown. A tabbed interface shows 'Información general' (selected), 'Propiedades', 'Permisos', and 'Seleccionar desde'. Below the tabs are buttons: 'Abrir', 'Descargar', 'Descargar como', 'Hacer público', and 'Copiar ruta'. The main content area displays the following information:

- Propietario:** awslabsc0w631861t1582777226
- Última modificación:** mar. 12, 2020 10:26:26 a. m. GMT-0500
- ETag:** 4dfd037e0be6dbde0d0e01684e1f598a
- Clase de almacenamiento:** Estándar
- Cifrado del lado del servidor:** Ninguno
- Tamaño:** 763.0 B
- Clave:** index.html
- URL del objeto:** <https://jonatan2020arep.s3.amazonaws.com/index.html>

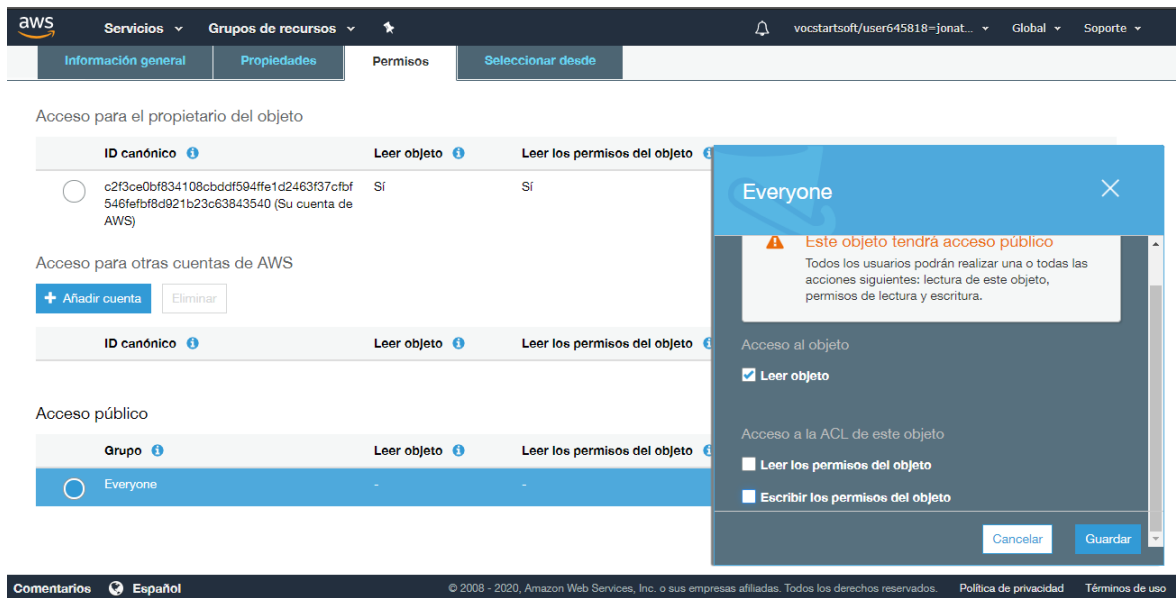
At the bottom, there's a 'Comentarios' section with a language selector set to 'Español', and a footer with copyright information and links to 'Política de privacidad' and 'Términos de'.

14. Al seleccionar la URL nos redirige a la siguiente página.

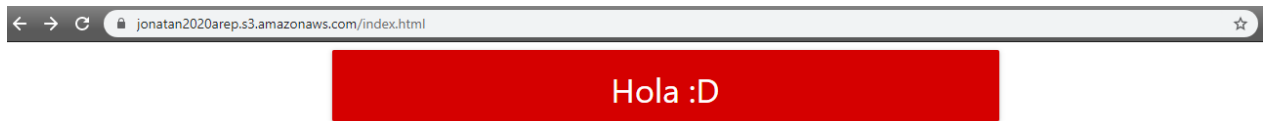
The screenshot shows a web browser window with the address bar displaying 'jonatan2020arep.s3.amazonaws.com/index.html'. The page content shows an error message: 'This XML file does not appear to have any style information associated with it. The document tree is shown below.' Below this message is an XML document tree:

```
<?xml version="1.0" encoding="UTF-8" ?>
<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>C1275F65524E28FB</RequestId>
  <HostId>
    PMI532H1oE97f7WfajP3CyBqdZXWdRsh9ye8U5rwQZpBytJRGtpNdcQxL/jfWn48ZA7XETuT/qM=
  </HostId>
</Error>
```

15. Para corregir lo anterior vamos a la pestaña de '**Permisos**', y en la sección de Acceso Público seleccionamos la opción de '**Everyone**', después se nos despliega un recuadro al lado derecho de la pantalla y damos click en Leer objeto y damos click en guardar.

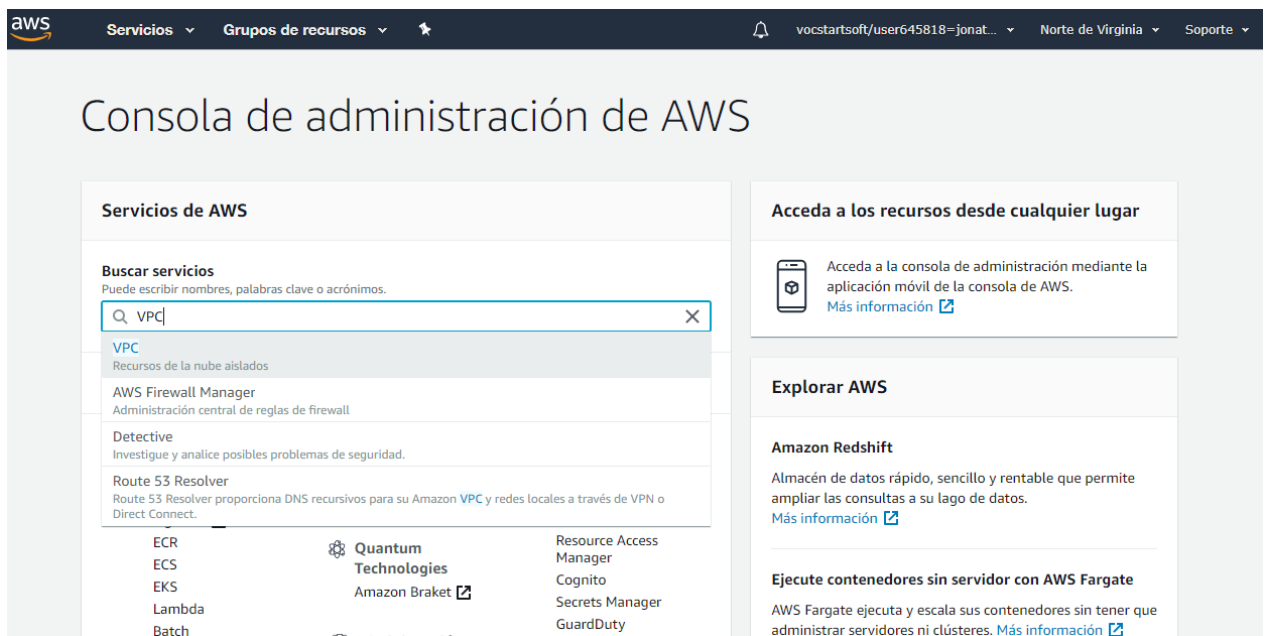


16. Volvemos y presionamos el link y nos sale la información correcta, en este caso sale mi index.htm con un botón que redirecciona a una imagen estática.

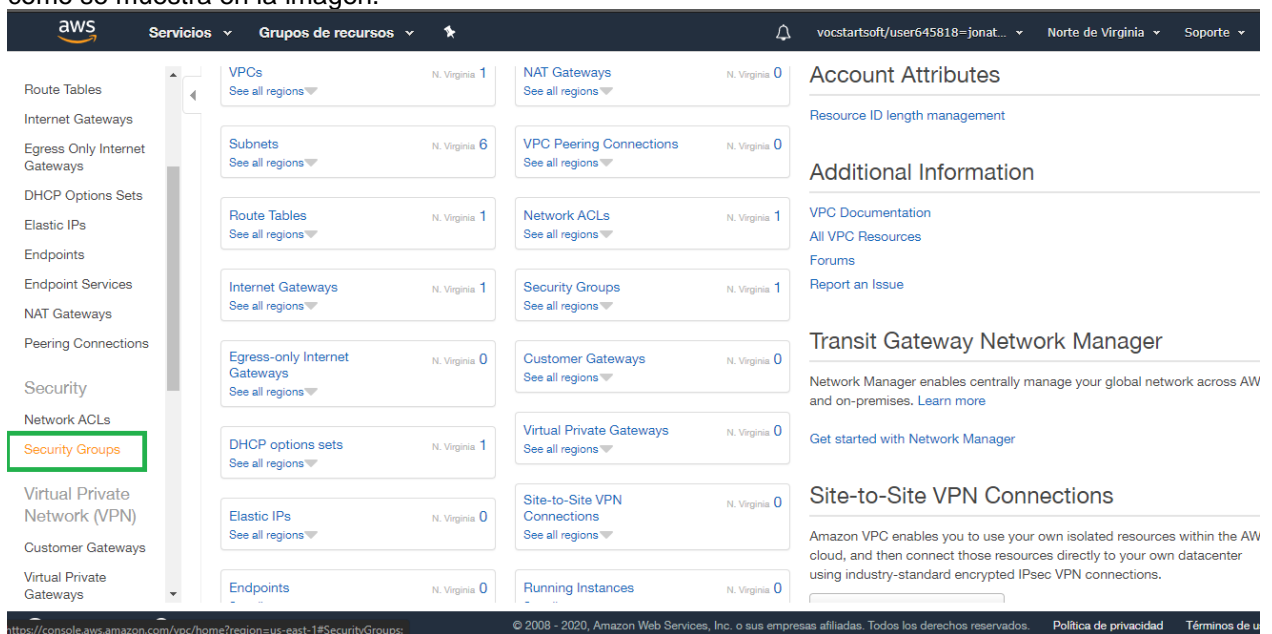


Desplegar un formulario dinámico usando EC2 enlazado con una base de datos y configurado con un VPC (Cloud Privado virtual)

1. Una vez dentro de la consola, buscamos VPC, el cual nos ayudará a abrir los puertos para poder conectarnos a la base de datos.



- Nos dirigimos en la parte izquierda a la sección de **Security** y damos clic en **Security Groups**, como se muestra en la imagen.



- Creamos un grupo de seguridad, para esto damos clic en **Create security group** en la parte superior

aws Servicios Grupos de recursos

Filter by tags and attributes or search by keyword

Name	Group ID	Group Name	VPC ID	Type	Description	Owner
sg-bdd77590	sg-bdd77590	default	vpc-38704e42	EC2-VPC	default VPC securi...	702789732216

Security Group: sg-bdd77590

Description Inbound Rules Outbound Rules Tags

Group ID sg-bdd77590
VPC ID vpc-38704e42
Owner 702789732216

Group Name default
Description default VPC security group
Inbound rule count 1

- Configuramos los valores que piden, que es un nombre para el grupo, una descripción y la VPC, en este caso le asignamos la que aparece por defecto, luego presionamos el botón Create.

aws Servicios Grupos de recursos

Security Groups > Create security group

Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group fill in the fields below.

Security group name* jonatanSecurityGroup

Description* SeguridadParaDB

VPC vpc-38704e42

* Required

Cancel Create

- Una vez creado el grupo de seguridad, se puede observar en la sección de Grupos de Recursos.

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

Endpoint Services

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

Virtual Private Network (VPN)

Customer Gateways

Virtual Private Gateways

Create security group Actions

Filter by tags and attributes or search by keyword

Name	Group ID	Group Name	VPC ID	Type	Description	Owner
	sg-0cb38fe21c337...	jonatanSecurityGr...	vpc-38704e42	EC2-VPC	SeguridadParaDB	702789732216
<input checked="" type="checkbox"/>	sg-bdd77590	default	vpc-38704e42	EC2-VPC	default VPC securi...	702789732216

Security Group: sg-bdd77590

Description Inbound Rules Outbound Rules Tags

Group ID sg-bdd77590

VPC ID vpc-38704e42

Owner 702789732216

Group Name default

Description default VPC security group

Inbound rule count 1

- Después seleccionamos el grupo de Seguridad que creamos, y nos dirigimos en la parte inferior a la sección de **'Inbound Rules'** y luego en la parte de **'Edit Rules'**.

<input type="checkbox"/>	Name	Group ID	Group Name	VPC ID	Type	Description	Owner
<input checked="" type="checkbox"/>		sg-0cb38fe21c337...	jonatanSecurityGr...	vpc-38704e42	EC2-VPC	SeguridadParaDB	702789732216
<input type="checkbox"/>		sg-bdd77590	default	vpc-38704e42	EC2-VPC	default VPC securi...	702789732216

Security Group: sg-0cb38fe21c3371a68

Description Inbound Rules Outbound Rules Tags

Edit rules

Type Protocol Port Range Source Description

- Después vamos a el botón de Add Rule y Creamos una regla con Type: MYSQL/Aurora, Protocol: TCP, Port Range: 3306, **Source: Anywhere** y una descripción si queremos, luego damos click en Save rules.

Nota: Debemos configurar la sección de Source como Anywhere ya que esto es lo que nos deja que cualquiera ingrese a la página.

Edit inbound rules

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

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
MySQL/Aurora ▼	TCP	3306	Anywhere ▼	0.0.0.0/0, ::/0
e.g. SSH for Admin Desktop				

Add Rule

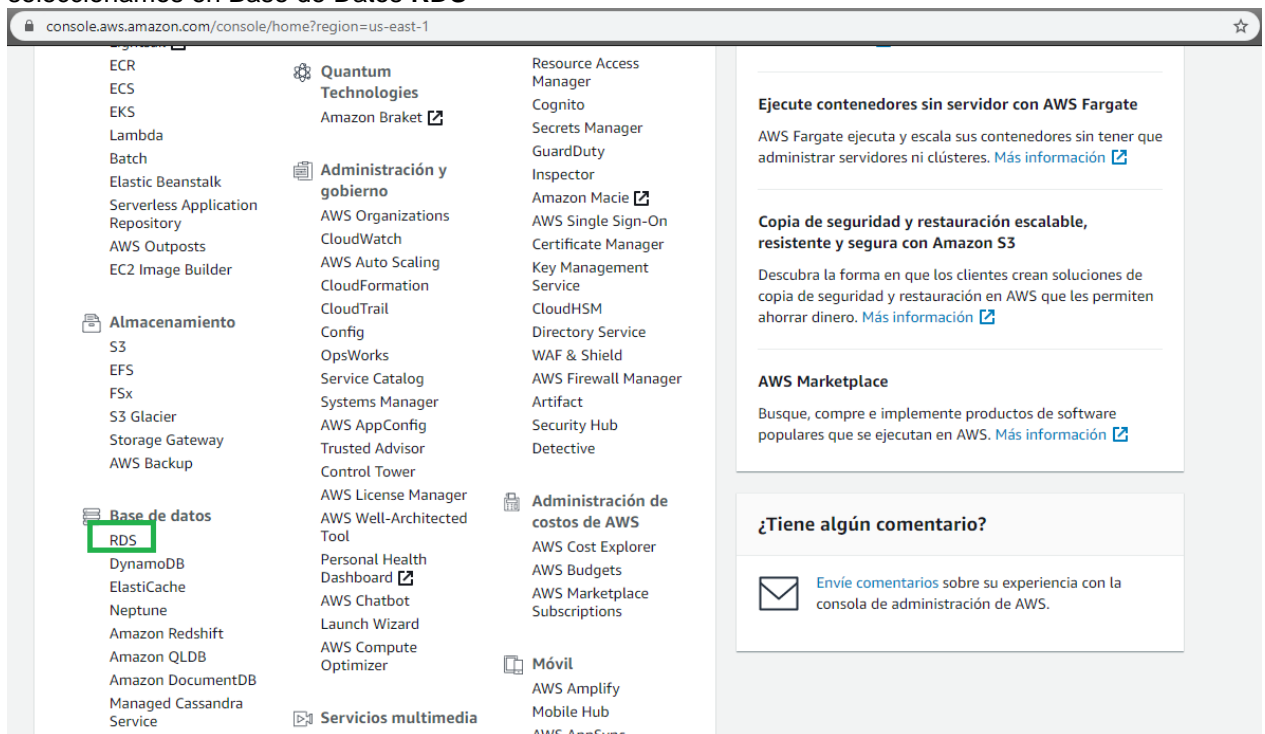
NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

* Required

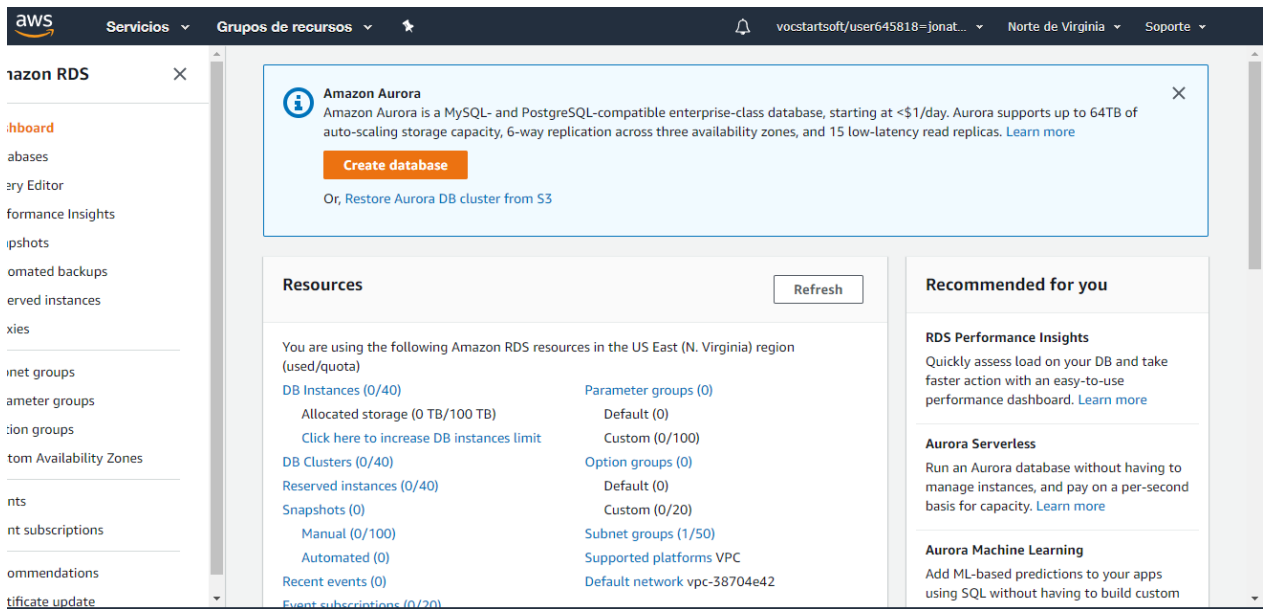
Cancel

Save rules

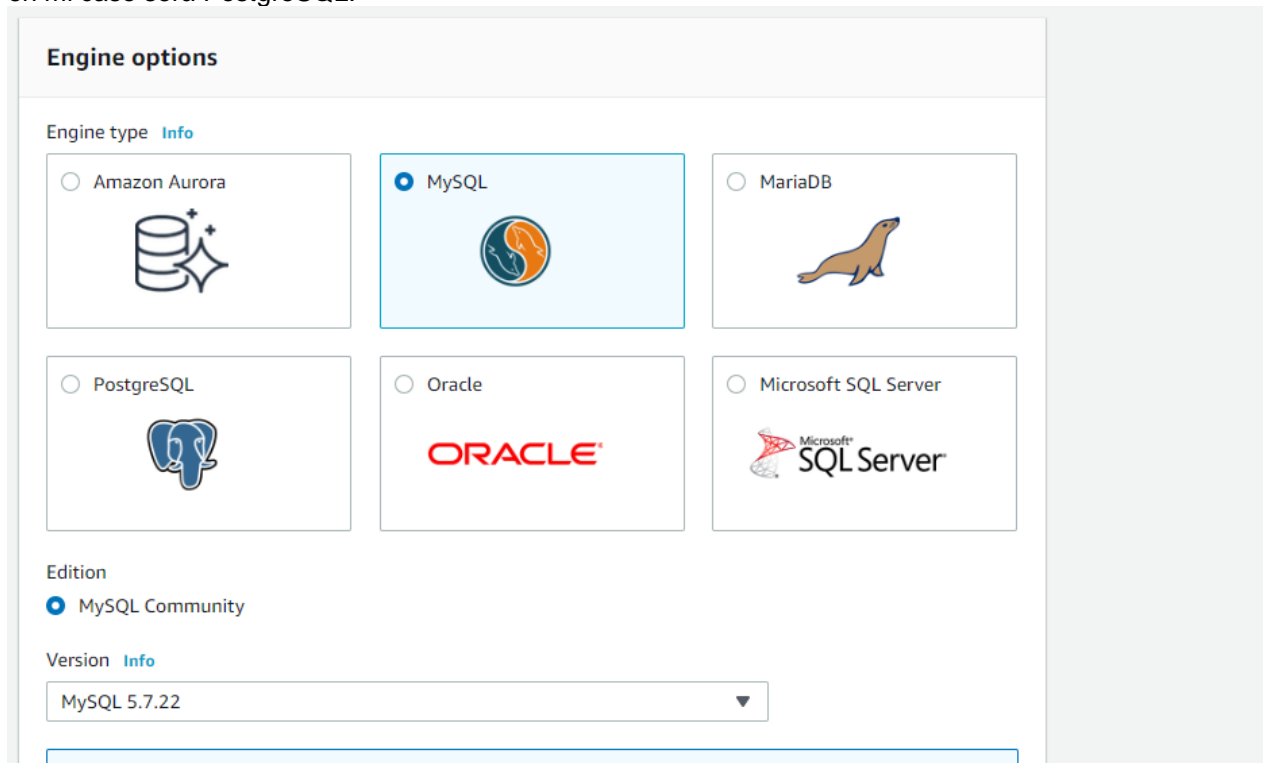
- Volvemos a la consola de Administración de AWS, nos dirigimos a Todos los servicios y seleccionamos en Base de Datos **RDS**



- Damos click en Create Database



10. Aquí seleccionamos Standard create y PostgreSQL, que es con el motor que queremos trabajar, en mi caso será PostgreSQL.



11. En la sección 'Templates' seleccionamos Free tier.

Templates

Choose a sample template to meet your use case.

☐ **Production**
 Use defaults for high availability and fast, consistent performance.

☐ **Dev/Test**
 This instance is intended for development use outside of a production environment.

☒ **Free tier**
 Use RDS Free Tier to develop new applications, test existing applications, or gain hands-on experience with Amazon RDS. [Info](#)

12. Debemos configurarle los nombres y password a la base de datos.

Settings

DB instance identifier [Info](#)

Type a name for your DB instance. The name must be unique cross all DB instances owned by your AWS account in the current AWS Region.

The DB instance identifier is case-insensitive, but is stored as all lowercase (as in "mydbinstance"). Constraints: 1 to 60 alphanumeric characters or hyphens (1 to 15 for SQL Server). First character must be a letter. Can't contain two consecutive hyphens. Can't end with a hyphen.

▼ **Credentials Settings**

Master username [Info](#)

Type a login ID for the master user of your DB instance.

1 to 16 alphanumeric characters. First character must be a letter

☐ **Auto generate a password**
 Amazon RDS can generate a password for you, or you can specify your own password

Master password [Info](#)

Constraints: At least 8 printable ASCII characters. Can't contain any of the following: / (slash), "(double quote) and @ (at sign).

Confirm password [Info](#)

13. En la sección Connectivity, dejaremos que sea de acceso público, así que en 'Publicly accessible' cambiamos a **Yes**. En VPC Security group seleccionamos creada anteriormente.

aws Servicios Grupos de recursos

DB subnet group that defines which subnets and IP ranges the DB instance can use in the VPC you selected.

default-vpc-38704e42

Publicly accessible [Info](#)

☒ Yes
Amazon EC2 instances and devices outside the VPC can connect to your database. Choose one or more VPC security groups that specify which EC2 instances and devices inside the VPC can connect to the database.

☐ No
RDS will not assign a public IP address to the database. Only Amazon EC2 instances and devices inside the VPC can connect to your database.

VPC security group
Choose one or more RDS security groups to allow access to your database. Ensure that the security group rules allow incoming traffic from EC2 instances and devices outside your VPC. (Security groups are required for publicly accessible databases.)

☒ Choose existing
Choose existing VPC security groups

☐ Create new
Create new VPC security group

Existing VPC security groups

Choose VPC security groups

jonatanSecurityGroup X default X

Availability zone [Info](#)

No preference

Database port [Info](#)
TCP/IP port the database will use for application connections.

14. Finalmente asignamos un nombre a la base de datos, y damos en la parte final **'Create database'**

▼ **Additional configuration**
Database options, backup enabled, backtrack disabled, Enhanced Monitoring disabled, maintenance, CloudWatch Logs, delete protection disabled

Database options

Initial database name [Info](#)

dataBaseMySQL

If you do not specify a database name, Amazon RDS does not create a database.

DB parameter group [Info](#)

default.mysql5.7

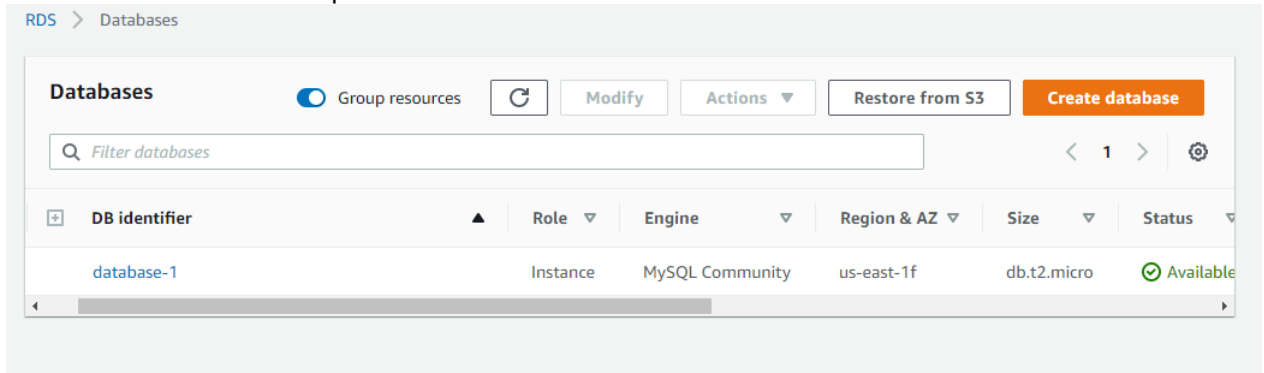
Option group [Info](#)

default:mysql-5-7

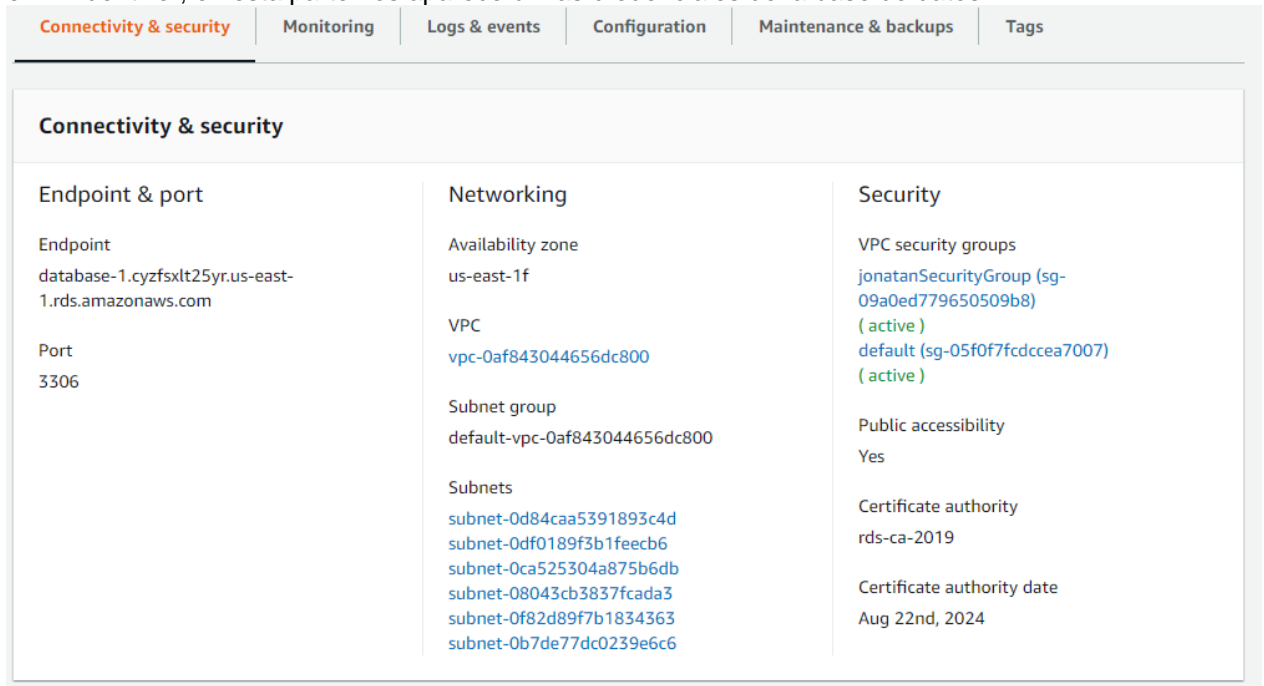
Backup
Creates a point in time snapshot of your database

☒ **Enable automatic backups**
Enabling backups will automatically create backups of your database during a certain time window.

15. En la sección de Database podemos observar la nueva base de datos creada



16. Cuando la sección de Status aparezca Available entramos a la base de datos dando click sobre el DB identifier, en esta parte nos aparecerán las credenciales de la base de datos.



17. Ahora, abrimos DBeaver para conectarnos a la base de datos creada anteriormente, anotamos el host que es el que aparece en el Endpoint & port y el usuario y contraseña que dimos anteriormente, hacemos un test de conexión y observamos que está conectada correctamente.

Connect to database

Connection Settings

MySQL 8+ connection settings

General Driver properties SSH Proxy SSL

Server Host: database-1.cyzfsxlt25yr.us-east-1.rds.amazonaws.com

Port: 3306

Database: dataBaseMySQL

User name: dataBaseMySQL

Password: ☒ Save password locally

Server Time Zone: Auto-detect

Local Client: MySQL Binaries

Advanced settings:

Driver name: MySQL

name, type, ...)

Driver Settings

Connection Test

Connected (2735 ms)

Server: MySQL 5.7.22-log

Driver: MySQL Connector/J mysql-connector-java-8.0.17
(Revision: 16a712ddb3f826a1933ab42b0039f7fb9eebc6ec)

OK

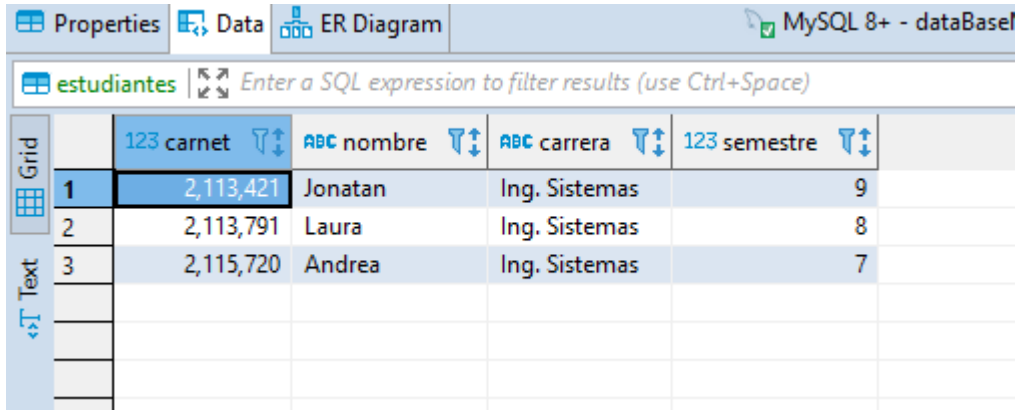
< Back Next > Finish Close Test Connection ...

18. Una vez conectados a la base de datos, creamos un SQLEditor para crear tablas para utilizarlas en la API.

```
CREATE TABLE dataBaseMySQL.estudiantes(
  carnet INT NOT NULL,
  nombre VARCHAR(100) NOT NULL,
  carrera VARCHAR(100) NOT NULL,
  semestre INT NOT NULL
);

INSERT INTO dataBaseMySQL.estudiantes VALUES (2113421, "Jonatan", "Ing. Sistemas", 9);
INSERT INTO dataBaseMySQL.estudiantes VALUES (2113791, "Laura", "Ing. Sistemas", 8);
INSERT INTO dataBaseMySQL.estudiantes VALUES (2115720, "Andrea", "Ing. Sistemas", 7);
```

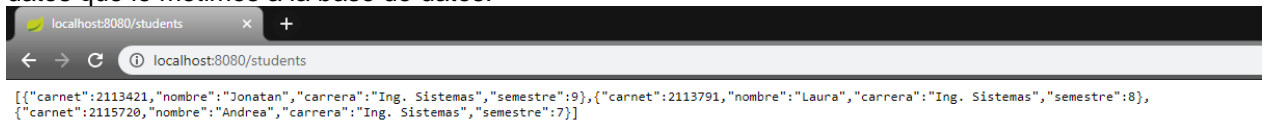
19. Podemos observar los datos en la base de datos



The screenshot shows the MySQL 8+ - dataBase1 interface. The 'Data' tab is selected, displaying the 'estudiantes' table. The table has columns: carnet, nombre, carrera, and semestre. The data is as follows:

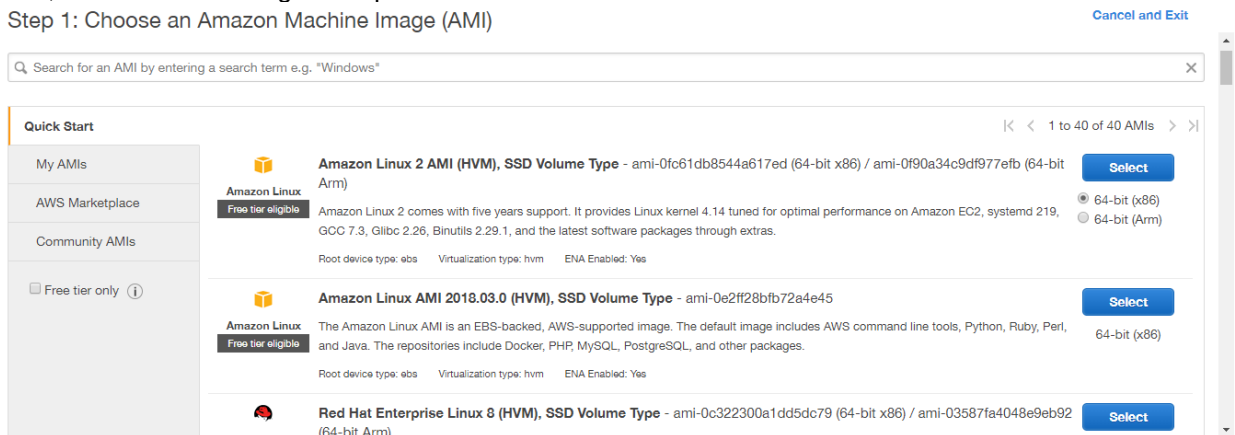
	carnet	nombre	carrera	semestre
1	2,113,421	Jonatan	Ing. Sistemas	9
2	2,113,791	Laura	Ing. Sistemas	8
3	2,115,720	Andrea	Ing. Sistemas	7

20. Ahora lo que hacemos es correr nuestra API localmente y debería aparecernos algo así, con los datos que le metimos a la base de datos.



21. Ahora procedemos a desplegar la API con EC2. Para esto, en la consola de AWS seleccionamos el servicio EC2 en la sección 'Compute', y seleccionamos la maquina virtual que tenga instalado Java, en este caso la segunda opción.

Step 1: Choose an Amazon Machine Image (AMI)



22. Dejamos la opción Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type y damos clic en Next.

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

23. En el paso 6 damos clic en 'Add rule'. En la pestaña Type seleccionamos Custom TCP, en el puerto ponemos 8080 y en Source ponemos Anywhere. Damos clic en Review and Launch.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
Custom TCP	TCP	8080	Anywhere 0.0.0.0/0, ::/0	e.g. SSH for Admin Desktop

Add Rule

24. Después de presionar el botón Review and Launch, presionamos Launch.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details Edit AMI

Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-0e2ff28bfb72a4e45

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

Root Device Type: ebs Virtualization type: hvm

Instance Type Edit instance type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

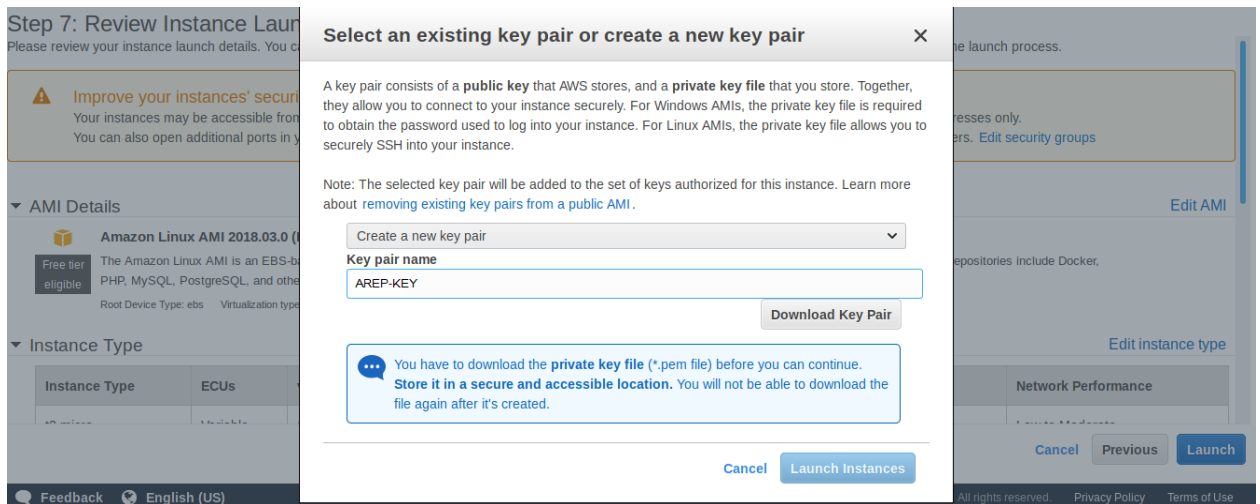
Security Groups Edit security groups

Security group name: launch-wizard-1

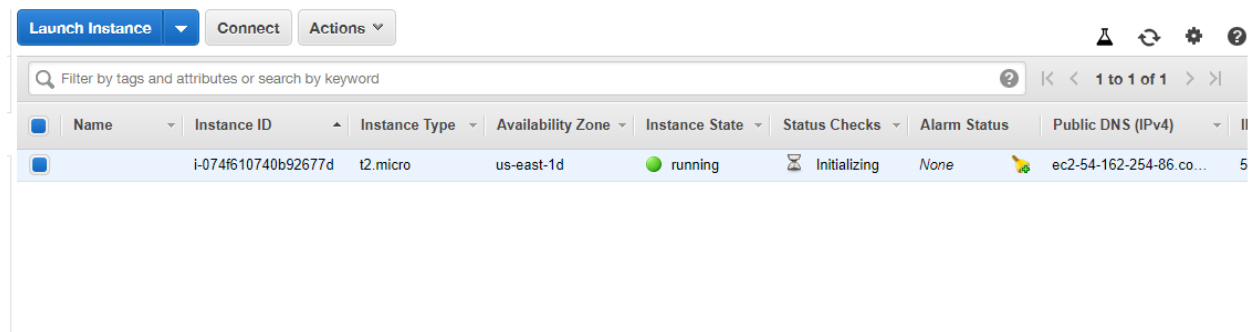
Description: launch-wizard-1 created 2020-03-14T21:39:33.705-05:00

Cancel Previous Launch

25. Creamos una key pair, así que le damos en Create a new key pair, ponemos el nombre que queramos a la llave, luego la descargamos y la guardamos en nuestro proyecto.



26. Finalmente podemos observar la instancia de la base de datos creada.



27. Luego damos click en Connect para observar como conectarnos mediante ssh desde la maquina creada

Connect to your instance

Connection method

☒ A standalone SSH client ⓘ

☐ Session Manager ⓘ

☐ EC2 Instance Connect (browser-based SSH connection) ⓘ

To access your instance:

1. Open an SSH client. (find out how to [connect using PuTTY](#))

2. Locate your private key file (AREP-KEY.pem). The wizard automatically detects the key you used to launch the instance.

3. Your key must not be publicly viewable for SSH to work. Use this command if needed:


```
chmod 400 AREP-KEY.pem
```

4. Connect to your instance using its Public DNS:


```
ec2-54-162-254-86.compute-1.amazonaws.com
```

Example:

```
ssh -i "AREP-KEY.pem" ec2-user@ec2-54-162-254-86.compute-1.amazonaws.com
```

Please note that in most cases the username above will be correct, however please ensure that you read your AMI usage instructions to ensure that the AMI owner has not changed the default AMI username.

If you need any assistance connecting to your instance, please see our [connection documentation](#).

Close

28. Después nos conectamos mediante ssh al recurso EC2

```
ec2-user@ip-172-31-84-75:~  
File Edit View Search Terminal Help  
jonatan@ubuntu:~/Downloads$ ssh -i "AREP-KEY.pem" ec2-user@ec2-54-162-254-86.com  
pute-1.amazonaws.com  
Last login: Sun Mar 15 04:57:10 2020 from dynamic-190-27-79-83.dynamic.etb.net.c  
o  
  
  _ |  _ | _ )  
  _ | (    /  Amazon Linux AMI  
  __| \___|___|  
  
https://aws.amazon.com/amazon-linux-ami/2018.03-release-notes/  
7 package(s) needed for security, out of 11 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-172-31-84-75 ~]$
```

29. Instalamos Maven, Git y actualizamos el java a la versión 1.8

```
ec2-user@ip-172-31-84-75:~  
File Edit View Search Terminal Help  
[ec2-user@ip-172-31-84-75 ~]$ mvn --version  
Apache Maven 3.5.2 (138ed61fd100ec658bfa2d307c43b76940a5d7d; 2017-10-18T07:58:13Z)  
Maven home: /usr/share/apache-maven  
Java version: 1.8.0_242, vendor: Oracle Corporation  
Java home: /usr/lib/jvm/java-1.8.0-openjdk-1.8.0.242.b08-0.50.amzn1.x86_64/jre  
Default locale: en_US, platform encoding: UTF-8  
OS name: "linux", version: "4.14.165-102.185.amzn1.x86_64", arch: "amd64", family: "unix"  
[ec2-user@ip-172-31-84-75 ~]$ java -version  
openjdk version "1.8.0_242"  
OpenJDK Runtime Environment (build 1.8.0_242-b08)  
OpenJDK 64-Bit Server VM (build 25.242-b08, mixed mode)  
[ec2-user@ip-172-31-84-75 ~]$ git version  
git version 2.14.5  
[ec2-user@ip-172-31-84-75 ~]$
```

30. Clonamos el repositorio el cual tiene la API, en nuestra maquina EC2.

```
ec2-user@ip-172-31-84-75:~  
File Edit View Search Terminal Help  
[ec2-user@ip-172-31-84-75 ~]$ ls  
AREP-Patrones  
[ec2-user@ip-172-31-84-75 ~]$
```

31. Luego ejecutamos la clase edu.escuelaing.arep.students.StudentApplication

```
ec2-user@ip-172-31-84-75:~/AREP-Patrones  
File Edit View Search Terminal Help  
/COMMONS-EXEC/1.1/COMMONS-EXEC-1.1.jar (33 KB at 333 KB/s)  
Downloaded from central: https://repo.maven.apache.org/maven2/org/codehaus/plexus/  
s/plexus-container-default/1.0-alpha-9/plexus-container-default-1.0-alpha-9.jar  
(195 kB at 1.3 MB/s)  
  
:: Spring Boot :: (v1.5.1.RELEASE)  
  
2020-03-15 05:32:33.184 INFO 29603 --- [lication.main()] e.e.arep.students.Stud  
entApplication : Starting StudentApplication on ip-172-31-84-75 with PID 296  
03 (/home/ec2-user/AREP-Patrones/target/classes started by ec2-user in /home/ec2  
-user/AREP-Patrones)  
2020-03-15 05:32:33.195 INFO 29603 --- [lication.main()] e.e.arep.students.Stud  
entApplication : No active profile set, falling back to default profiles: de  
fault  
2020-03-15 05:32:33.333 INFO 29603 --- [lication.main()] ationConfigEmbeddedWeb  
ApplicationContext : Refreshing org.springframework.boot.context.embedded.Annota  
tionConfigEmbeddedWebApplicationContext@69e3ba9d: startup date [Sun Mar 15 05:32  
:33 UTC 2020]; root of context hierarchy
```

32. En la pagina de AWS Educate podemos ver el link de la EC2 . Con ese link es con el que podemos conectarnos a la máquina virtual, lo ponemos y le agregamos ':8080/students', donde students es el nombre que le hayamos puesto en nuestra API para conectarnos.

```
ec2-54-162-254-86.compute-1.amazonaws.com:8080/students  
Not secure | ec2-54-162-254-86.compute-1.amazonaws.com:8080/students  
[{"carnet":2113421,"nombre":"Jonatan","carrera":"Ing. Sistemas","semestre":9}, {"carnet":2113791,"nombre":"Laura","carrera":"Ing. Sistemas","semestre":8}, {"carnet":2115720,"nombre":"Andrea","carrera":"Ing. Sistemas","semestre":7}]
```