

# DOCUMENTACIÓN TÉCNICA DEL PROCESO DE INSTALACIÓN, SOLICITUD DE LOS SERVICIOS DE TERCEROS Y PRODUCCIÓN

Por:

- Yhoan Alejandro Guzmán García
- Juan Sebastián Pérez Salazar
- Daniel Felipe Gómez Martínez

Profesor:

Edwin Nelson Montoya Munera

17/05/2021

Universidad EAFIT

Imagen 1 – VPC creada y configurada .....	3
Imagen 2 – Subredes públicas y privadas creadas para la zona A (recuadro verde) y la zona B (recuadro naranja).....	4
Imagen 3 – Conexión del internet Gateway con la VPC del proyecto .....	4
Imagen 4 – Puertos de acceso y comunicación con el internet Gateway.....	5
Imagen 5 – Conexión de la instancia NAT de la zona A con la VPC y la subred publica de la zona A .....	5
Imagen 6 - Conexión de la instancia NAT de la zona B con la VPC y la subred publica de la zona B .....	6
Imagen 7 – Tabla de rutas para cada subred en la zona A (recuadro verde) y zona B (recuadro naranja) .....	6
Imagen 8 – Conexión de la tabla de rutas publica en la zona A con la subred publica en la zona A .....	7
Imagen 9 – conexión de la subred publica en la zona A con el internet Gateway .....	7
Imagen 10 – Internet Gateway del sistema .....	7
Imagen 11 - Conexión de la tabla de rutas publica en la zona B con la subred publica en la zona B.....	8
Imagen 12 - conexión de la subred publica en la zona B con el internet Gateway .....	8
Imagen 13 – Internet Gateway del sistema .....	9
Imagen 14 - Conexión de la tabla de rutas privada en la zona A con la subred privada en la zona A.....	9
Imagen 15 – Conexión de la subred privada A con la instancia NAT de la zona A.....	10
Imagen 16 – Instancia NAT de la zona A .....	10
Imagen 17 - Conexión de la tabla de rutas privada en la zona B con la subred privada en la zona B.....	11
Imagen 18 - Conexión de la subred privada B con la instancia NAT de la zona B .....	11
Imagen 19 - Instancia NAT de la zona A .....	11
Imagen 20 – Grupo de seguridad del Bastion Host en la instancia creada para la zona A .....	12
Imagen 21- Grupo de seguridad del Bastion Host en la instancia creada para la zona A .....	12
Imagen 22 - Grupo de seguridad para las instancias del Bastion Host.....	13
Imagen 23 - Puertos de entrada y salida del grupo de seguridad para la instancia de la web .....	13
Imagen 24 – Grupo de seguridad de la base de datos.....	14
Imagen 25 – Subredes que tienen acceso al servicio de RDS creado .....	14
Imagen 26 – Grupo de seguridad de la base de datos.....	15
Imagen 27 – Nombre de la base de datos.....	15
Imagen 28 – Subredes privadas de cada zona que tiene acceso al EFS.....	16
Imagen 29 – Grupo de seguridad de las instancias web.....	17
Imagen 30 – Creación de la imagen AMI para replicar las instancias.....	17
Imagen 31 – Imagen AMI creada y lista par ser utilizada en el auto scaling goup .....	18
Imagen 32 – Subredes públicas de cada zona.....	19
Imagen 33 – Listener por el puerto 80 .....	19
Imagen 34 – Configuración del auto scaling .....	20
Imagen 35 – Grupo de auto scaling desplegado .....	20
Imagen 36 - Cantidad de instancias mínimas y máximas que puede desplegar al auto scaling group .....	21
Imagen 37 - Nombre del dominio .....	21
Imagen 38 - Delegando el dominio a Cloudflare .....	22
Imagen 39 - Añadiendo registros en Cloudflare.....	22
Imagen 40 - Generación del certificado SSL .....	23
Imagen 41 - Asociando el certificado SSL a un listener en el LoadBalancer .....	23
Imagen 42 - Cambiando los atributos para ponerles el nombre del dominio.....	24
Imagen 43 - Añadiendo lineas al archivo wp-settings.php para registrar el dominio .....	24
Imagen 44 - Certificado generado y asociado de manera exitosa para el aplicativo web.....	25

## VPC

Para el alojamiento de nuestro proyecto se creó una VPC con una dirección privada personalizada (172.24.0.0/16). Con esta VPC además de tener todos los recursos y herramientas concentradas en una sola parte nos brinda seguridad, privacidad y control.

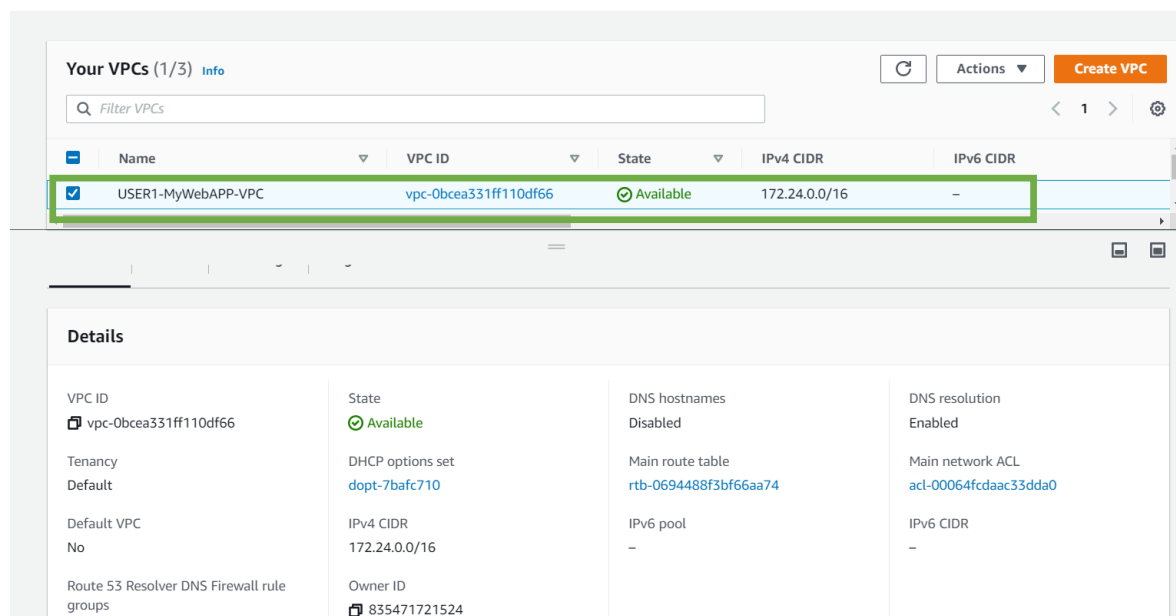


Imagen 1 – VPC creada y configurada

## Subnets

En estas 2 subredes que se ven en la siguiente imagen se dividen en dos zonas una en (us-east-2a y us-east-2b) y en cada una de estas zonas se creó una subred privada y una pública.

Para la primera zona us-east-2a (Ohio) se utilizaron las direcciones 172.24.1.0/24 (para la subred privada) y 172.24.2.0/24 (para la subred publica).

Para la primera zona us-east-2b (Ohio) se utilizaron las direcciones 172.24.3.0/24 (para la subred privada) y 172.24.4.0/24 (para la subred publica).

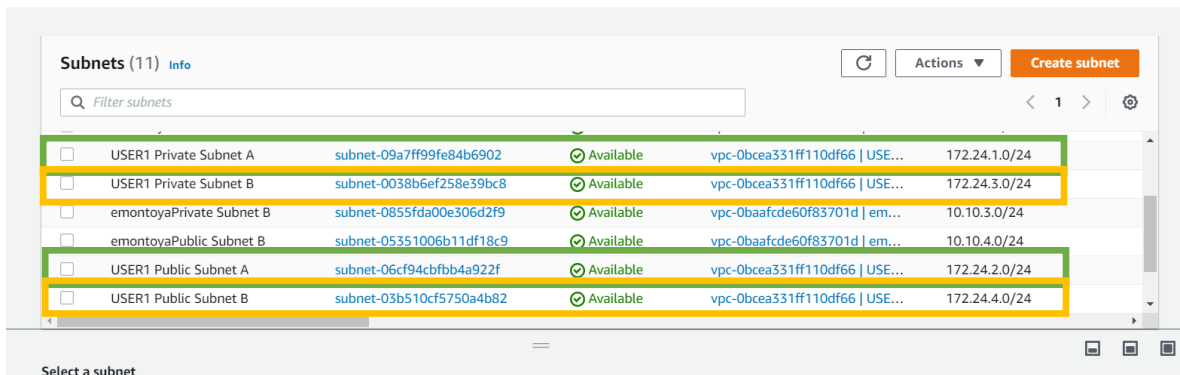


Imagen 2 – Subredes públicas y privadas creadas para la zona A (recuadro verde) y la zona B (recuadro naranja)

## Internet Gateway

Para tener la entrada internet solo necesita que se le asigne a nuestra VPC creada, la cual va a ser utilizada para comunicarse y tener acceso a la web, por ende, hace que las instancias puedan desplegar el WordPress.

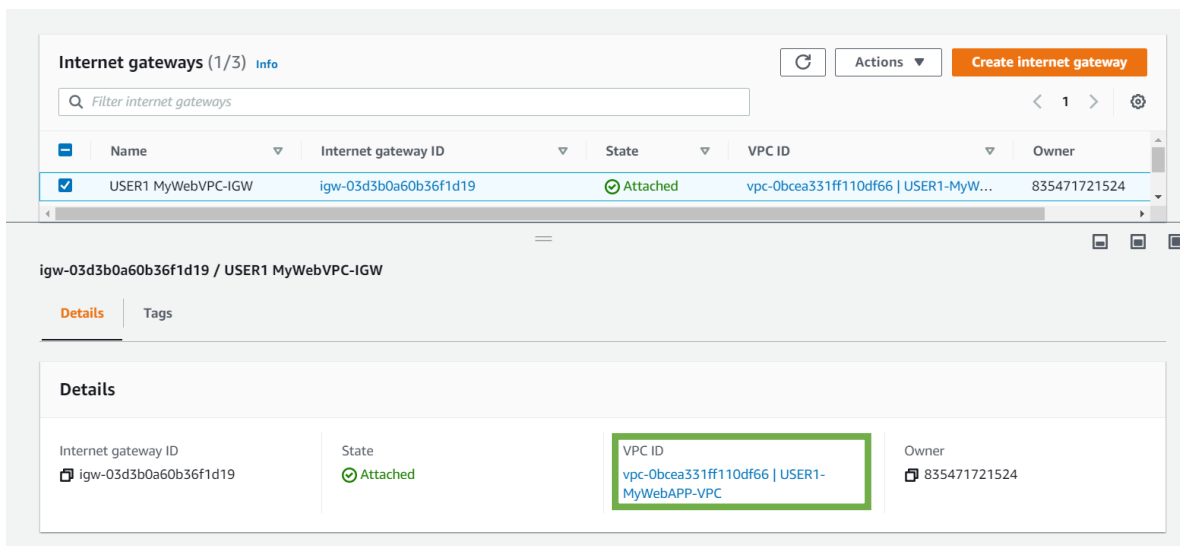


Imagen 3 – Conexión del internet Gateway con la VPC del proyecto

Además de solo crear la entrada a internet, tambien le creamos un grupo de seguridad donde se van a habilitar los puertos de entrada y salida.

Security Groups (1/11) Info						
Filter security groups						
	Name	Security group ID	Security group name	VPC ID	Description	Owner
<input checked="" type="checkbox"/>	USER1 SG-NAT-Instance	sg-0944cad750e12ff98	USER1 SG-NAT-Instance	vpc-0bcea331ff110df66	Enable outgoing traffic...	8354717

Inbound rules (8)				
Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	172.24.1.0/24	Allow inbound HTTP traffic from servers in the private subnet.
HTTP	TCP	80	172.24.3.0/24	Allow inbound HTTP traffic from servers in the private subnet
SSH	TCP	22	0.0.0.0/0	Allow inbound SSH access to the NAT instance from your home network (over the internet gateway)
SSH	TCP	22	::/0	Allow inbound SSH access to the NAT instance from your home network (over the internet gateway)
HTTPS	TCP	443	172.24.1.0/24	Allow inbound HTTPS traffic from servers in the private subnet
HTTPS	TCP	443	172.24.3.0/24	Allow inbound HTTPS traffic from servers in the private subnet
All ICMP - IPv4	ICMP	All	172.24.1.0/24	-
All ICMP - IPv4	ICMP	All	172.24.3.0/24	-

Imagen 4 – Puertos de acceso y comunicación con el internet Gateway

## Instancias NAT

A través de las dos instancias NAT una por cada zona (porque estas solo se van a conectar a las subredes públicas), se les va a dar salida a las redes privadas de nuestro proyecto a la web.

Instancias (1/11) Información							
Filtrar instancias							
	Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación ...	Estado de la...	Zona de dispon...
<input checked="" type="checkbox"/>	USER1 NAT-Instance A	i-0a22a14a83d956c46	En ejecución	t2.micro	2/2 comprobación	Sin alarmas	us-east-2a

Resumen de instancia Información		
ID de la instancia i-0a22a14a83d956c46 (USER1 NAT-Instance A)	Dirección IPv4 pública 3.129.216.122   <a href="#">dirección abierta</a>	Direcciones IPv4 privadas 172.24.2.58
Estado de la instancia En ejecución	DNS de IPv4 pública -	DNS IPv4 privado ip-172-24-2-58.us-east-2.compute.internal
Tipo de instancia t2.micro	Direcciones IP elásticas -	ID de VPC vpc-0bcea331ff110df66 (USER1-MyWebAPP-VPC)
Hallazgo de AWS Compute Optimizer User: arn:aws:iam:835471721524:user/st0263user1 is not authorized to perform: compute-	Rol de IAM -	ID de subred subnet-06cf94cbfb4a922f (USER1 Public Subnet A)

Imagen 5 – Conexión de la instancia NAT de la zona A con la VPC y la subred publica de la zona A

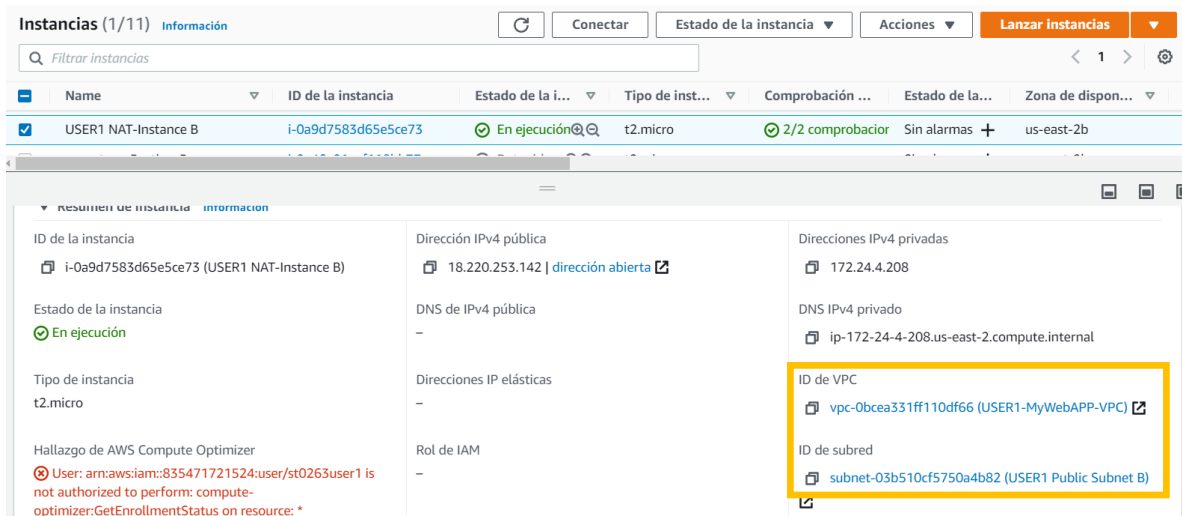


Imagen 6 - Conexión de la instancia NAT de la zona B con la VPC y la subred publica de la zona B

## Tablas de ruta

A través de esta configuración de las tablas de rutas se van a asignar los flujos de acceso y respuesta de las subredes públicas y privadas a la web.

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
emontoyaPrivate Route Table B	rtb-0ddbb42366a76ad26	subnet-0855fda00e306d2f9	-	No	vpc-0baafcd60f83701d   ...
USER1 Private Route Table A	rtb-0c8f0bc69080b6718	subnet-09a7ff99fe84b6902	-	No	vpc-0bcea331ff110df66   ...
emontoyaPublic Route Table B	rtb-0baa49d6a8ff1d62a	subnet-05351006b11df18c9	-	No	vpc-0baafcd60f83701d   ...
emontoyaPublic Route Table A	rtb-07b054896ae27018d	subnet-0e1aa5818b5eb3db5	-	No	vpc-0baafcd60f83701d   ...
USER1 Public Route Table A	rtb-03afa55c7eaaa382c	subnet-06cf94cbfb4a922f	-	No	vpc-0bcea331ff110df66   ...
USER1 Public Route Table B	rtb-01c0071d071d7463c	subnet-03b510cf5750a4b82	-	No	vpc-0bcea331ff110df66   ...
USER1 Private Route Table B	rtb-00a046fb6f539ad39	subnet-0038b6ef258e39bc8	-	No	vpc-0bcea331ff110df66   ...
emontoyaPrivate Route Table A	rtb-0059a3937212a84e9	subnet-0f35ac4e9e9c41984	-	No	vpc-0baafcd60f83701d   ...

Imagen 7 – Tabla de rutas para cada subred en la zona A (recuadro verde) y zona B (recuadro naranja)

- Para la tabla de rutas públicas de la zona A y de la zona B, deben ser conectadas a sus respectivas subredes, las cuales apuntan directamente al internet Gateway.
  - Para el caso de la tabla de rutas publica de la zona A:

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
USER1 Public Route Table A	rtb-0694488f3bf66aa74	-	-	Yes	vpc-0bcea331ff110df66   ...	8354717
USER1 Public Route Table B	rtb-03afa55c7eaaa382c	subnet-06cf94cbfbb4a922f	-	No	vpc-0bcea331ff110df66   ...	8354717
USER1 Public Route Table C	rtb-01c0071d071d7463c	subnet-03b510cf5750a4b82	-	No	vpc-0bcea331ff110df66   ...	8354717

Route Table: rtb-03afa55c7eaaa382c

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit subnet associations

Subnet ID IPv4 CIDR IPv6 CIDR

subnet-06cf94cbfbb4a922f 172.24.2.0/24 -

Imagen 8 – Conexión de la tabla de rutas publica en la zona A con la subred publica en la zona A

Subnets (1/1) Info

search: subnet-06cf94cbfbb4a922f X Clear filters

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6
USER1 Public Subnet A	subnet-06cf94cbfbb4a922f	Available	vpc-0bcea331ff110df66   USE...	172.24.2.0/24	-

Details Flow logs Route table Network ACL Sharing Tags

Route table: rtb-03afa55c7eaaa382c / USER1 Public Route Table A

Edit route table association

Routes (2)

Filter routes

Destination	Target
172.24.0.0/16	local
0.0.0.0/0	igw-03d3b0a60b36f1d19

Imagen 9 – conexión de la subred publica en la zona A con el internet Gateway

Internet gateways (1/1) Info

Filter internet gateways

Internet gateway ID: igw-03d3b0a60b36f1d19 X Clear filters

Name	Internet gateway ID	State	VPC ID	Owner
USER1 MyWebVPC-...	igw-03d3b0a60b36f1d19	Attached	vpc-0bcea331ff110df66   USER1-MyW...	835471721524

igw-03d3b0a60b36f1d19 / USER1 MyWebVPC-IGW

Details Tags

Details

Internet gateway ID igw-03d3b0a60b36f1d19	State Attached	VPC ID vpc-0bcea331ff110df66   USER1-MyWebAPP-VPC	Owner 835471721524
--	-------------------	--	-----------------------

Imagen 10 – Internet Gateway del sistema

- Para el caso de la tabla de rutas publica de la zona B:

Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
USER1 Public Route Table A	rtb-03afa55c7eaaa382c	subnet-06cf94cbfbb4a922f	-	No	vpc-0bcea331ff110df66   ...	83547172
USER1 Public Route Table B	rtb-01c0071d071d7463c	subnet-03b510cf5750a4b82	-	No	vpc-0bcea331ff110df66   ...	83547172
USER1 Private Route Table B	rtb-00a046fb6f539ad39	subnet-0038b6ef258e39bc8	-	No	vpc-0bcea331ff110df66   ...	83547172

Route Table: rtb-01c0071d071d7463c

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit subnet associations

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-03b510cf5750a4b...	172.24.4.0/24	-

Imagen 11 - Conexión de la tabla de rutas publica en la zona B con la subred publica en la zona B

Subnets (1/1) Info

Filter subnets

search: subnet-03b510cf5750a4b82 X Clear filters

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
USER1 Public Subn...	subnet-03b510cf5750a4b82	Available	vpc-0bcea331ff110df66   USE...	172.24.4.0/24	-

Details Flow logs Route table Network ACL Sharing Tags

Route table: rtb-01c0071d071d7463c / USER1 Public Route Table B

Edit route table association

Routes (2)

Filter routes

Destination	Target
172.24.0.0/16	local
0.0.0.0/0	igw-03d3b0a60b36f1d19

Imagen 12 - conexión de la subred publica en la zona B con el internet Gateway



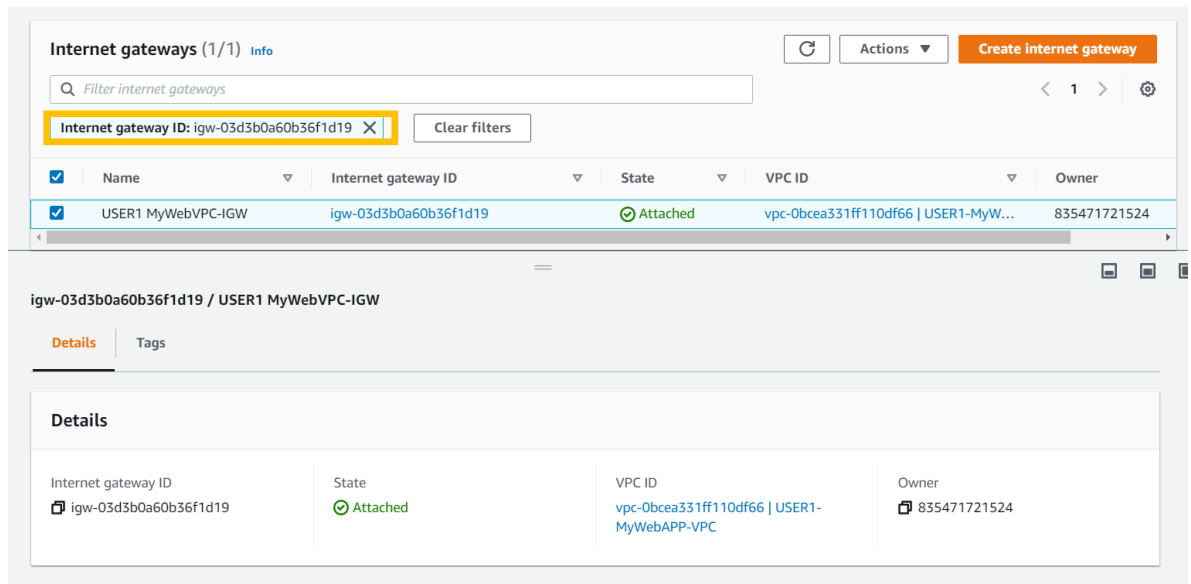


Imagen 13 – Internet Gateway del sistema

Nota: Mire que ambas subredes apuntan directamente al internet Gateway del sistema.

- Para la tabla de rutas privadas de la zona A y zona B, la conexión es distinta porque esta no va directamente conectada al internet Gateway, sino que estas deben apuntar a las respectivas instancias NAT creadas en el punto anterior.
  - Para el caso de la tabla de ruta privada A:

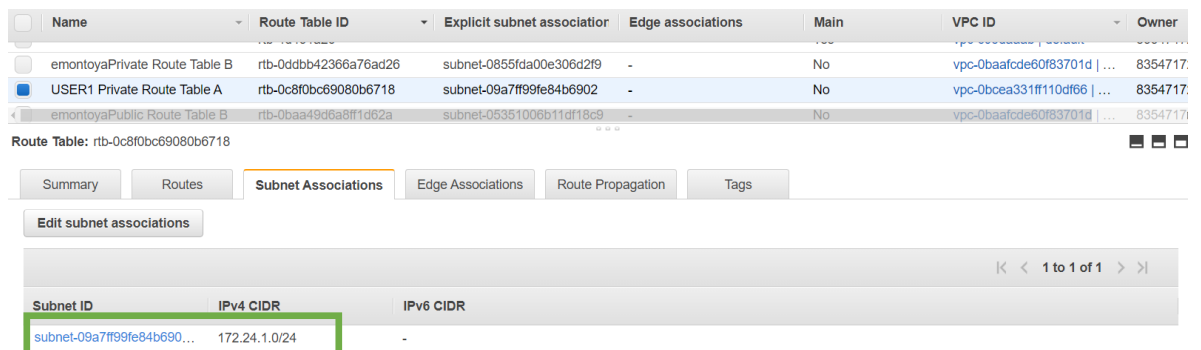


Imagen 14 - Conexión de la tabla de rutas privada en la zona A con la subred privada en la zona A

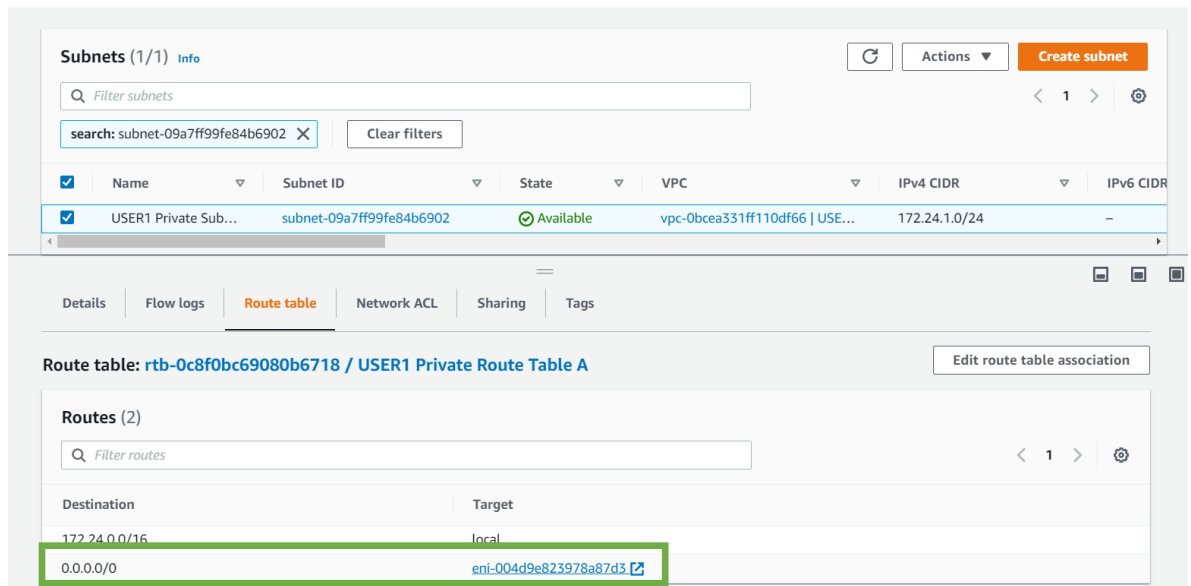


Imagen 15 – Conexión de la subred privada A con la instancia NAT de la zona A

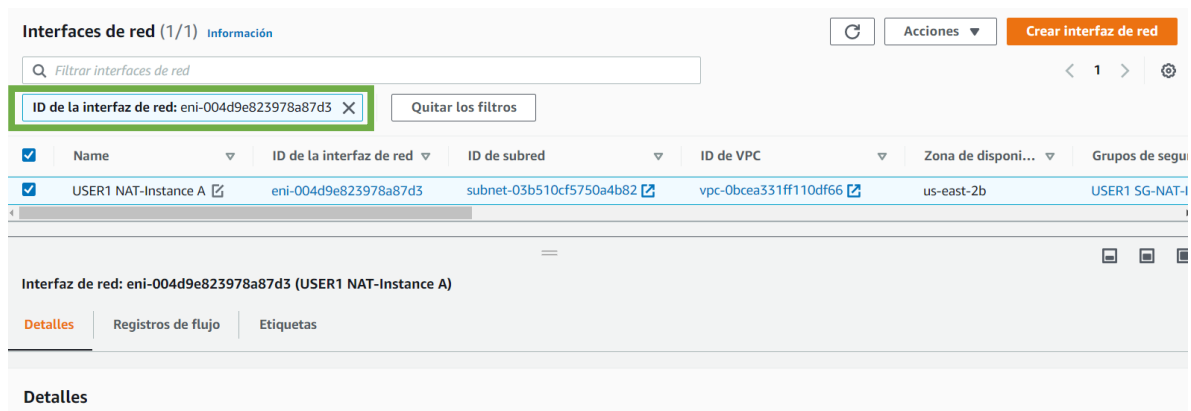


Imagen 16 – Instancia NAT de la zona A

- Para el caso de la tabla de ruta privada B:

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
<input checked="" type="checkbox"/>	USER1 Private Route Table B	rtb-00a046fb6f539ad39	subnet-0038b6ef258e39bc8	-	No	vpc-0bcea331ff110df66   ...	83547172
<input type="checkbox"/>	emontoyaPrivate Route Table A	rtb-0059a3937212a84e9	subnet-0f35ac4e9e9c41984	-	No	vpc-0baafcd60f83701d   ...	83547172
<input type="checkbox"/>		rtb-001f3b8b916373bf3	-	-	Yes	vpc-0baafcd60f83701d   ...	83547172

Route Table: rtb-00a046fb6f539ad39

Summary Routes Subnet Associations Edge Associations Route Propagation Tags

Edit subnet associations

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-0038b6ef258e39bc8	172.24.3.0/24	-

Imagen 17 - Conexión de la tabla de rutas privada en la zona B con la subred privada en la zona B

Subnets (1/1) Info

Filter subnets

search: subnet-0038b6ef258e39bc8 X Clear filters

<input checked="" type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
<input checked="" type="checkbox"/>	USER1 Private Sub...	subnet-0038b6ef258e39bc8	Available	vpc-0bcea331ff110df66   USE...	172.24.3.0/24	-

Details Flow logs Route table Network ACL Sharing Tags

Route table: rtb-00a046fb6f539ad39 / USER1 Private Route Table B

Edit route table association

Routes (2)

Filter routes

Destination	Target
172.24.0.0/16	local
0.0.0.0/0	eni-03b40525124cf4dd6

Imagen 18 - Conexión de la subred privada B con la instancia NAT de la zona B

Interfaces de red (1/1) Información

Filter interfaces de red

ID de la interfaz de red: eni-03b40525124cf4dd6 X Quitar los filtros

<input checked="" type="checkbox"/>	Name	ID de la interfaz de red	ID de subred	ID de VPC	Zona de disponi...	Grupos de segur
<input checked="" type="checkbox"/>	USER1 NAT-Instance B	eni-03b40525124cf4dd6	subnet-06cf94cbfbb4a922f	vpc-0bcea331ff110df66	us-east-2a	USER1 SG-NAT-I

Interfaz de red: eni-03b40525124cf4dd6 (USER1 NAT-Instance B)

Detalles Registros de flujo Etiquetas

Imagen 19 - Instancia NAT de la zona A

## Bastion host

El Bastion Host nos proporciona acceso seguro a las instancias ubicadas tanto en las subredes públicas como privadas, por lo que se van a crear dos instancias EC2 para configurar el Bastion Host una en de cada zona (A y B).

- Instancia Bastion host para la zona A:

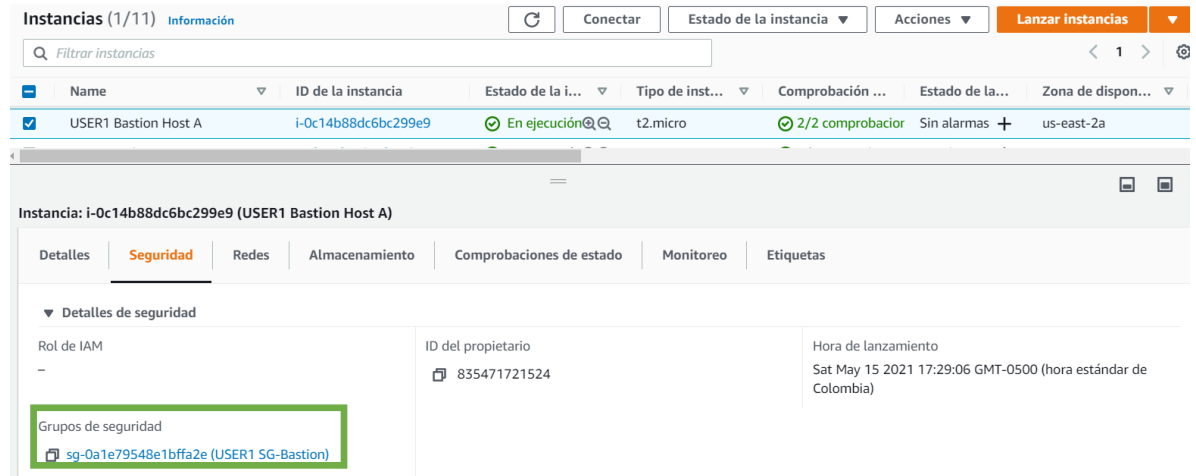


Imagen 20 – Grupo de seguridad del Bastion Host en la instancia creada para la zona A

- Instancia Bastion host para la zona B:

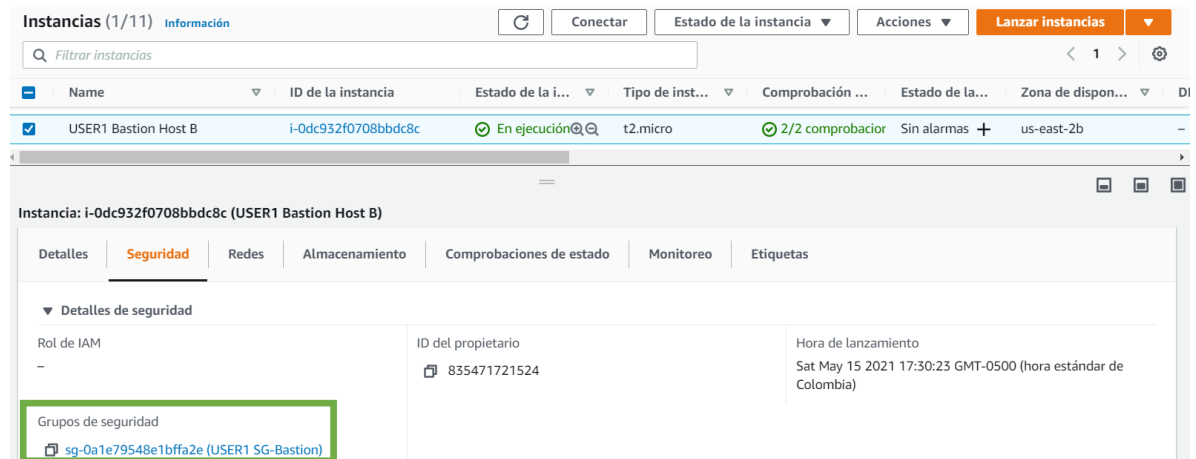


Imagen 21- Grupo de seguridad del Bastion Host en la instancia creada para la zona A

Nota: Ambas instancias tiene el mismo grupo de seguridad (USER1 SG-Bastion). El grupo de seguridad del Bastion Host solo tiene abierto el puerto 22 (SSH):

EC2 > Grupos de seguridad > sg-0a1e79548e1bffa2e - USER1 SG-Bastion

### sg-0a1e79548e1bffa2e - USER1 SG-Bastion

Acciones ▾

**Detalles**

Nombre del grupo de seguridad USER1 SG-Bastion	ID del grupo de seguridad sg-0a1e79548e1bffa2e	Descripción Enable SSH Access	ID de la VPC vpc-0bcea331ff110df66 <a href="#">↗</a>
Propietario 835471721524	Número de reglas de entrada 2 Entradas de permisos	Número de reglas de salida 1 Entrada de permiso	

Reglas de entrada | Reglas de salida | Etiquetas

**Reglas de entrada (2)**

Editar reglas de entrada

Tipo	Protocolo	Intervalo de puertos	Origen	Descripción: opcional
SSH	TCP	22	0.0.0.0/0	Allow ssh traffic
SSH	TCP	22	::/0	Allow ssh traffic

Imagen 22 - Grupo de seguridad para las instancias del Bastion Host

## Grupo de seguridad de la página web

Antes de crear las instancias en las cuales se van a desplegar los WordPress se deben configurar los puertos de entrada y salida de las instancias, sin duda alguna uno de los puertos más importantes son el HTTP y el HTTPS ya que en estos dos puertos se van a recibir peticiones del WordPress y en el caso del HTTPS se tendrá el certificado SSL.

Grupos de seguridad (1/11) Información

🔄 Acciones ▾ **Crear grupo de seguridad**

🔍 Filtrar grupos de seguridad

< 1 > ⚙️

<input checked="" type="checkbox"/>	Name	ID del grupo de segu...	Nombre del grupo ...	ID de la VPC	Descripción	Propietario	Número de reglas d...	Númer...
<input checked="" type="checkbox"/>	USER1 SG-Web	sg-07ab5506a4fa0f1fb	USER1 SG-Web	vpc-0bcea331ff110df66 <a href="#">↗</a>	Enable HTTP Access	835471721524	10 Entradas de permisos	1 Entrac
<input type="checkbox"/>	-	sg-0880c198dbf3b4425	emontoya-SG-Web	vpc-0baafcd60f83701e <a href="#">↗</a>	Enable HTTP Access	835471721524	8 Entradas de permisos	1 Entrac
<input type="checkbox"/>	USER1 SG-NAT-Inst...	sg-0944cad750e12ff98	USER1 SG-NAT-Instance	vpc-0bcea331ff110df66 <a href="#">↗</a>	Enable outgoing traffic...	835471721524	8 Entradas de permisos	1 Entrac

Detalles | **Reglas de entrada** | Reglas de salida | Etiquetas

**Reglas de entrada (10)**

Editar reglas de entrada

Tipo	Protocolo	Intervalo de puertos	Origen	Descripción: opcional
HTTP	TCP	80	0.0.0.0/0	Permit Web Requests
HTTP	TCP	80	::/0	Permit Web Requests
SSH	TCP	22	0.0.0.0/0	Permit SSH Requests
SSH	TCP	22	::/0	Permit SSH Requests
HTTPS	TCP	443	0.0.0.0/0	Permit HTTPS Requests
HTTPS	TCP	443	::/0	Permit HTTPS Requests
Todos los ICMP IPv4	ICMP	Todo	0.0.0.0/0	-
Todos los ICMP IPv4	ICMP	Todo	::/0	-
NFS	TCP	2049	0.0.0.0/0	Permit NFS Requests for EFS
NFS	TCP	2049	::/0	Permit NFS Requests for EFS

Imagen 23 - Puertos de entrada y salida del grupo de seguridad para la instancia de la web

## Grupo de seguridad de la base de datos

En este grupo de seguridad solo se abrirá el puerto 3306 el cual es el predefinido para la base de datos MYSQL/Aurora.

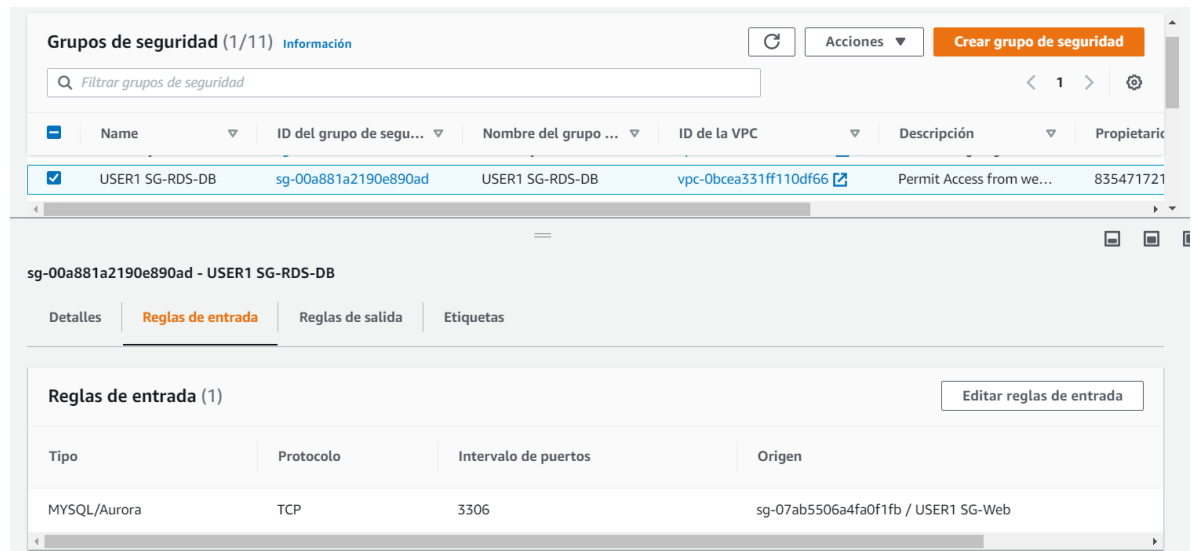


Imagen 24 – Grupo de seguridad de la base de datos

## Grupo de seguridad del RDS

Este grupo de seguridad se crea con el fin de indicarle al servicio RDS las subredes que tienen acceso a esta. En nuestro caso solo las subredes privadas de cada zona (A y B) van a tener acceso a este servicio.

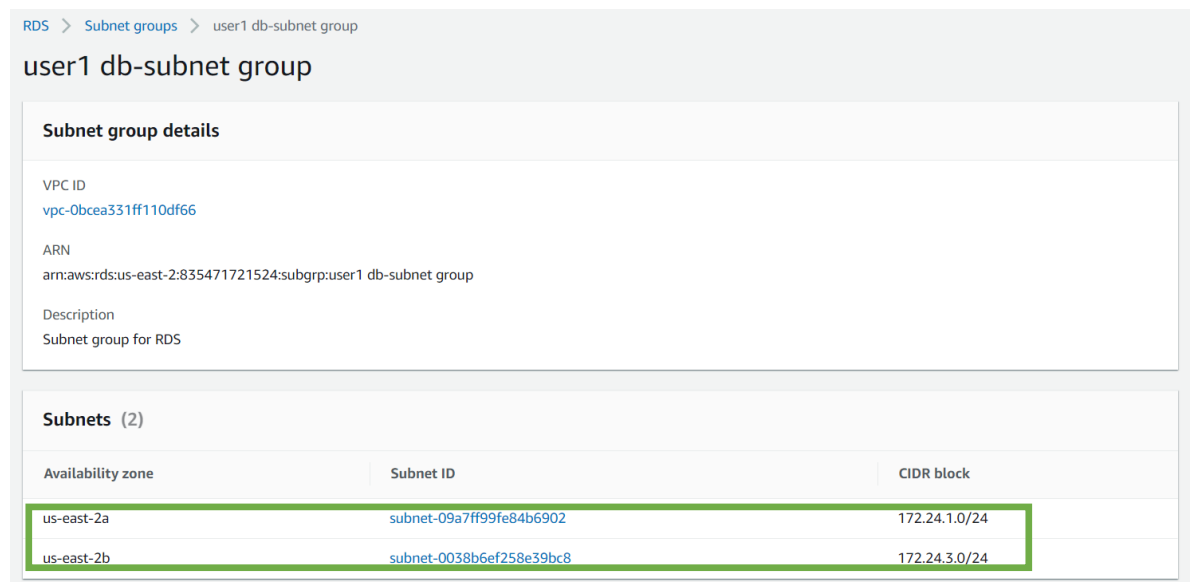


Imagen 25 – Subredes que tienen acceso al servicio de RDS creado

## Base de datos RDS

Para la creación de la base de datos se deben de tener en cuenta dos aspectos importantes, uno de ellos es agregar el grupo de seguridad creado en el punto anterior (rectángulo negro). Y el otro punto es ser muy conscientes del nombre de la base de datos (rectángulo azul), porque este nombre será utilizado en el despliegue del WordPress.

**user1-exampledgb** Modify Actions ▼

**Summary**

DB identifier user1-exampledgb	CPU 2.54%	Status Available	Class db.t2.micro
Role Instance	Current activity 0 Connections	Engine MySQL Community	Region & AZ us-east-2a

**Connectivity & security** | Monitoring | Logs & events | Configuration | Maintenance & backups | Tags

**Connectivity & security**

<b>Endpoint &amp; port</b> Endpoint user1-exampledgb.c3jz07w8xkd.us-east-2.rds.amazonaws.com Port 3306	<b>Networking</b> Availability zone us-east-2a VPC USER1-MyWebAPP-VPC (vpc-0bcea331ff110df66) Subnet group	<b>Security</b> VPC security groups USER1 SG-RDS-DB (sg-00a881a2190e890ad) (active) Public accessibility No
--	---	---

Imagen 26 – Grupo de seguridad de la base de datos

**user1-exampledgb** Modify Actions ▼

**Configuration** | Monitoring | Logs & events | Maintenance & backups | Tags

**Instance**

<b>Configuration</b> DB instance ID user1-exampledgb Engine version 8.0.20 <b>DB name</b> wordpress License model General Public License Option groups default:mysql-8-0 Amazon Resource Name (ARN) arn:aws:rds:us-east-2:835471721524:db:user1-exampledgb Resource ID db-6POEIDY6HVCUC37YTR6WCGTPD4	<b>Instance class</b> Instance class db.t2.micro vCPU 1 RAM 1 GB <b>Availability</b> Master username exampleuser IAM DB authentication Not enabled Multi-AZ No Secondary Zone	<b>Storage</b> Encryption Not enabled Storage type General Purpose (SSD) IOPS - Storage 20 GiB Storage autoscaling Enabled Maximum storage threshold 1000 GiB	<b>Performance Insights</b> Performance Insights enabled No
--	---	---	---

Imagen 27 – Nombre de la base de datos

## EFS

Se crea una EFS (Elastic file system) con el fin de tener un sistema elástico y sencillo para compartir datos de archivos. Lo que nos va a permitir compartir todos los archivos de la aplicación WordPress y archivos estáticos como los que gestiona el servicio CMS (sistema de gestión de contenidos) entre las instancias creadas.

En esta imagen se ven las dos subredes privadas de cada zona:

USER1 WP-EFS (fs-e160909a)

Eliminar Asociar

### General

Editar

Modo de rendimiento  
Uso general

Modo de desempeño  
Transmisión por ráfagas

Política del ciclo de vida  
30 días desde el último acceso

Zona de disponibilidad  
Regional

Copias de seguridad automáticas  
Activado

Cifrado  
e572af4a-ec20-4a69-bee3-f63904265956 (aws/elasticfilesystem)

Estado del sistema de archivos  
Disponible

Tamaño medido | Monitoreo | Etiquetas | Política del sistema de archivos | Puntos de acceso | Red

### Red

Administrar

Zona de disponibilidad	ID del destino de montaje	ID de la subred	Estado de destino de montaje	Dirección IP	ID de la interfaz de red	Grupos de seguridad
us-east-2a	fsmt-931d08ea	subnet-09a7ff99fe84b6907	Disponible	172.24.1.184	eni-0fe75dc662308c629	sg-07ab5506a4fa0f1fb (USER1 SG-Web)
us-east-2b	fsmt-171d086e	subnet-0038b6ef258	Disponible	172.24.3.128	eni-0d533795e54bb18e	sg-07ab5506a4fa0f1fb (USER1 SG-Web)

Imagen 28 – Subredes privadas de cada zona que tiene acceso al EFS

## Instancia de la página Web

Para la instancia de la página web es importante abrir los puertos de 80 (HTTP), 443 (HTTPS) y 22 (SSH), los cuales van a servir para el despliegue y el montaje del WordPress.



Instancias (1/11) Información

Conectar Estado de la instancia Acciones Lanzar instancias

Filtrar instancias

Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación ...	Estado de la ...	Zona de dispon...	DNS de IPv4 pública	Dirección IP...	IP elá
<input checked="" type="checkbox"/> USER1 Web Server	i-0f4c9f20d01fe61b1	En ejecución	t2.micro	2/2 comprobador	Sin alarmas	us-east-2a	-	-	-
<input type="checkbox"/> WebInstance16-05	i-0fcb9977d02b521f9	En ejecución	t2.micro	2/2 comprobador	Sin alarmas	us-east-2a	-	-	-
<input type="checkbox"/> emontoyaNAT-Instance B	i-05f0bce5d6cb1eb97	Detenida	t2.micro	-	Sin alarmas	us-east-2b	-	-	-

Filtrar reglas

Intervalo de p...	Protocolo	Origen	Grupos de seguridad
80	TCP	0.0.0.0/0	USER1 SG-Web
80	TCP	::/0	USER1 SG-Web
22	TCP	0.0.0.0/0	USER1 SG-Web
22	TCP	::/0	USER1 SG-Web
443	TCP	0.0.0.0/0	USER1 SG-Web

Reglas de salida

Filtrar reglas

Intervalo de p...	Protocolo	Destino	Grupos de seguridad
Todo	Todo	0.0.0.0/0	USER1 SG-Web

Imagen 29 – Grupo de seguridad de las instancias web

Nota: Una vez que tenga la instancia lanzada se puede crear el Docker compouser para la instalación de WordPress y la base de datos.

## Imagen en la instancia web

Una vez creada la instancia de la página web para poder implementar el servicio de auto scaling group, se debe crear una imagen (AMI) la cual va a ser la plantilla con la cual se crearán las nuevas instancias las cuales se van a desplegar con un contenido idéntico.

Instancias (1/11) Información

Conectar Estado de la instancia Acciones Lanzar instancias

Filtrar instancias

Name	ID de la instancia	Estado de la i...	Tipo de inst...	Comprobación ...	Estado de la ...	Zona de dispon...	DNS
<input type="checkbox"/> emontoyaNAT-Instance A	i-0f2e472ce9035447d	Detenida	t2.micro	-	Sin alarmas	us-east-2a	-
<input type="checkbox"/> emontoya-Bastion-A	i-02cbf217283d981e6	Detenida	t2.micro	-	Sin alarmas	us-east-2a	-
<input type="checkbox"/> USER1 NAT-Instance A	i-0a22a14a83d956c46	En ejecución	t2.micro	2/2 comprobador	Sin alarmas	us-east-2a	-
<input type="checkbox"/> USER1 Bastion Host A	i-0c14b88dc6bc299e9	En ejecución	t2.micro	2/2 comprobador	Sin alarmas	us-east-2a	-
<input checked="" type="checkbox"/> USER1 Web Server	i-0f4c9f20d01fe61b1	En ejecución	t2.micro	2/2 comprobador	Sin alarmas	us-east-2a	-
<input type="checkbox"/> WebInstance16-05	i-0fcb9977d02b521f9	En ejecución	t2.micro	2/2 comprobador	Sin alarmas	us-east-2a	-
<input type="checkbox"/> emontoyaNAT-Instance B	i-05f0bce5d6cb1eb97	Detenida	t2.micro	-	Sin alarmas	us-east-2b	-
<input type="checkbox"/> USER1 NAT-Instance B	i-0a9d7583d65e5ce73	En ejecución	t2.micro	2/2 comprobador	Sin alarmas	us-east-2b	-
<input type="checkbox"/> emontoya-Bastion-B	i-0a46e91eaf118bb77	Detenida	t2.micro	-	Sin alarmas	us-east-2b	-
<input type="checkbox"/> USER1 Bastion Host B	i-0dc932f0708bbdc8c	En ejecución	t2.micro	2/2 comprobador	Sin alarmas	us-east-2b	-
<input type="checkbox"/> WebInstance16-05	i-03cabd37817083781	En ejecución	t2.micro	2/2 comprobador	Sin alarmas	us-east-2b	-

Crear imagen

Crear plantilla a partir de una instancia

Lanzar más como esta

Ver detalles

Administrar el estado de la instancia

Configuración de la instancia

Redes

Seguridad

Imagen y plantillas

Monitoreo y solución de problemas

Imagen 30 – Creación de la imagen AMI para replicar las instancias

Lanzar
EC2 Image Builder
Acciones

De mi propiedad
Filtrar por etiquetas y atributos o buscar por palabra clave

Name	Nombre de AMI	ID de AMI	Origen	Propietario	Visibilidad	Estado	Fecha de creación	Plataforma	Tipo de dispositivo
	USER1 Web Server AMI 16-05	ami-0028582cf737da50d	835471721524/...	835471721524	Privado	available	16 de mayo de 2021, 10:56:...	Other Linux	ebs

Imagen: ami-0028582cf737da50d

Detalles
Permisos
Etiquetas

ID de AMI	ami-0028582cf737da50d	Nombre de AMI	USER1 Web Server AMI 16-05
Propietario	835471721524	Origen	835471721524/USER1 Web Server AMI 16-05
Estado	available	Motivo del estado	-
Fecha de creación	16 de mayo de 2021, 10:56:28 UTC-5	Platform details	Linux/UNIX
Arquitectura	x86_64	Usage operation	RunInstances
Tipo de imagen	machine	Tipo de virtualización	hvm
Descripción	AMI for Web Server	Nombre del dispositivo raíz	/dev/xvda
Tipo de dispositivo raíz	ebs	ID de disco de RAM	-
ID de kernel	-	Códigos de productos	-
Dispositivos de bloques	/dev/xvda=snap-03f379c1bcab51469.8:true:gp2	Boot mode	-

Imagen 31 – Imagen AMI creada y lista par ser utilizada en el auto scaling goup

Load Balancer

Para crear el balanceador de carga se utilizará el servicio administrado de AWS, en el momento de la configuración se deben de tener dos aspectos fundamentales para su configuración. El primero de ellos es la selección de las subredes ya que estas deben ser las subredes públicas de cada zona (recuadro rojo); y el segundo aspecto es configurar un listener el cual apunte al puerto 80 (recuadro amarillo) porque este va a ser el puerto por el cual va a escuchar las peticiones que se le hagan a la página web.

Crear balanceador de carga Acciones

Filtrar por etiquetas y atributos o buscar por palabra clave

Nombre	Nombre de DNS	Estado	ID de VPC	Zonas de disponibilidad	Tipo	Creado el	Monitoriz
USER1-ELB-MyWebApp	USER1-ELB-MyWebApp-91...	active	vpc-0bcea331ff110df66	us-east-2b, us-east-2a	application	16 de mayo de 2021, 10:10...	

Balanceador de carga: USER1-ELB-MyWebApp

Descripción Agentes de escucha Monitorización Servicios integrados Etiquetas

Configuración básica

Nombre USER1-ELB-MyWebApp

ARN arn:aws:elasticloadbalancing:us-east-2:835471721524:loadbalancer/app/USER1-ELB-MyWebApp/3d5a7345a1aa712b

Nombre de DNS USER1-ELB-MyWebApp-915799436.us-east-2.elb.amazonaws.com (Registro A)

Estado active

Tipo application

Esquema Internet-facing

Tipo de dirección IP ipv4

VPC vpc-0bcea331ff110df66

Zonas de disponibilidad

- subnet-03b510cf5750a4b82 - us-east-2b Dirección IPv4. Asignado por AWS
- subnet-06cf94cbb4a922f - us-east-2a Dirección IPv4. Asignado por AWS

Editar las subredes

Imagen 32 – Subredes públicas de cada zona

Crear balanceador de carga Acciones

Filtrar por etiquetas y atributos o buscar por palabra clave

Nombre	Nombre de DNS	Estado	ID de VPC	Zonas de disponibilidad	Tipo
USER1-ELB-MyWebApp	USER1-ELB-MyWebApp-91...	active	vpc-0bcea331ff110df66	us-east-2b, us-east-2a	application

Balanceador de carga: USER1-ELB-MyWebApp

Descripción Agentes de escucha Monitorización Servicios integrados Etiquetas

Un agente de escucha busca las solicitudes de conexión mediante su protocolo y puerto configurados, y el balanceador de carga usa las reglas del agente de escucha para dirigir el tráfico.

Agregar agente de escucha Editar Eliminar

ID de agente de escucha	Política de seguridad	Certificado SSL	Reglas
<input type="checkbox"/> HTTP : 80 arn:...e82ecbd7c57348f7	n/a	n/a	Predeterminada: reenviando a USER1-TG-MyWebApp2 <a href="#">Ver/editar las reglas</a>

Imagen 33 – Listener por el puerto 80

## Auto scaling group

Por ultimo se utilizó otro servicio administrado de AWS el cual es el Auto scaling group, el cual se encarga de aumentar o disminuir la cantidad de instancias en el sistema a medida que disminuye o aumenta las solicitudes de la pagina web, este nos permite conservar unos tiempos de respuesta estándar para nuestra página web.

Para configurar este servicio se necesita configurar dos cosas de suma importancia, una de estas es configurar el lugar donde se van a crear las nuevas instancias por lo que es fundamental alojarlas en las subredes privadas de cada zona (recuadro morado); y por ultimo se deben especificar la cantidad máxima y mínima de instancias a desplegar.

EC2 > Configuraciones de lanzamiento

Configuraciones de lanzamiento (1/1) Información

Buscar configuraciones de lanzamiento

Acciones Copiar en la plantilla de lanzamiento Crear configuración de lanzamiento

Nombre	ID de AMI	Tipo de instancia	Precio de spot	Hora de creación
USER1-MyWebb...	ami-0028582cf7...	t2.micro	-	Sun May 16 2021 10:58:02 GMT-0500 (hora estándar de Colombia)

Optimizada para EBS: false

Horas de creación: Sun May 16 2021 10:58:02 GMT-0500 (hora estándar de Colombia)

Datos de usuario: -

Grupos de seguridad: sg-07ab5506a4fa0f1fb

ID de disco de RAM: -

Precio de spot: -

Tipo de dirección IP: Predeterminado

Almacenamiento (volúmenes)

Buscar dispositivos de bloques

Dispositivo de bloques	Tamaño (GiB)	Tipo	IOPS	Eliminar al terminar	Cifrado
/dev/xvda	8	gp2	-	true	false

Imagen 34 – Configuración del auto scaling

EC2 > Grupos de Auto Scaling:

Grupos de Auto Scaling: (1/1)

Buscar sus grupos de Auto Scaling

Editar Eliminar Crear grupo de Auto Scaling

Nombre	Plantilla de lanzamiento/config...	Instanc...	Estado	Capacidad des...	M...	M...	Zonas de disponibilidad
USER1 MyWebApp-Auto Sc	USER1-MyWebbApp-16-05	2	-	2	2	3	us-east-2a, us-east-2b

Detalles Actividad Escalado automático Administración de instancias Monitoreo Actualización de instancias

Instancias (2)

Filtrar las instancias

Acciones

ID de instancia	Ciclo de vida	Tipo de instancia	Capacidad ponderada	Plantilla de lanzamiento/configuración	Zona de disponibilidad	Estado	Protegi...
i-03cabd37817083781	InService	t2.micro	-	USER1-MyWebbApp-16-05	us-east-2b	Healthy	
i-0fcb9977d02b521f9	InService	t2.micro	-	USER1-MyWebbApp-16-05	us-east-2a	Healthy	

Imagen 35 – Grupo de auto scaling desplegado

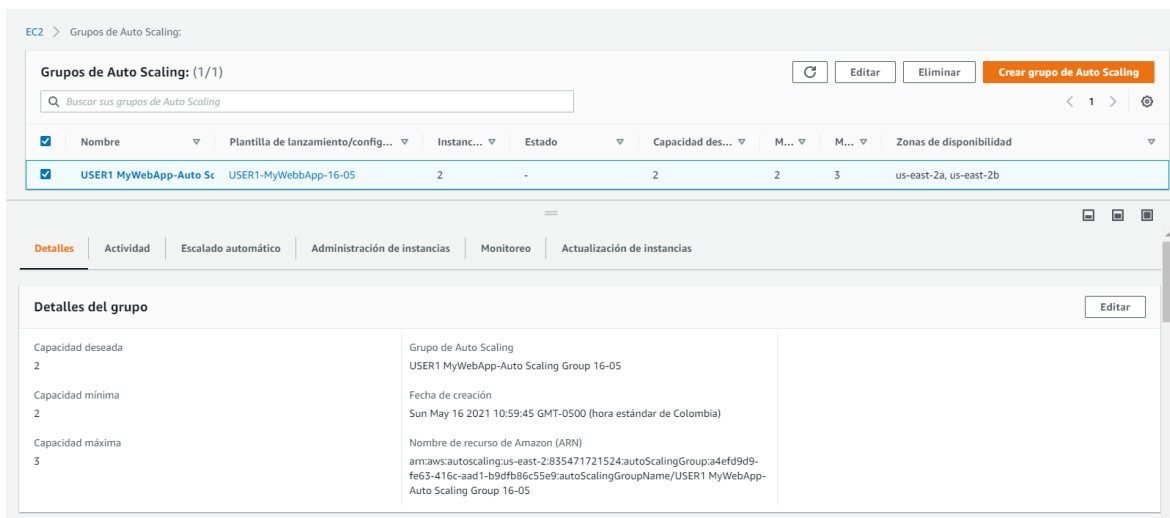


Imagen 36 - Cantidad de instancias mínimas y máximas que puede desplegar al auto scaling group

## Generación del certificado SSL

El certificado SSL se genera al nombre del dominio para garantizar al usuario final que su conexión a dicha pagina es segura. Lo primero que se realiza es la reserva de un nombre para el dominio en freenom. En este caso el elegido fue sadteamproyecto2.tk.

Dominio	Fecha de Registro	Fecha de caducidad	Estado	Tipo	
sadteamproyecto2.tk	2021-05-18	2022-05-18	ACTIVE	Gratis	Manage Domain
sadteam2.tk	2021-05-17	2022-05-17	ACTIVE	Gratis	Manage Domain
sadgroup.ml	2021-04-23	2022-04-23	ACTIVE	Gratis	Manage Domain
sadaanalytics.tk	2020-11-23	2022-02-23	ACTIVE	Gratis	Manage Domain
aqualife.tk	2020-11-09	2022-02-09	ACTIVE	Gratis	Manage Domain

Resultados Por Página: 10 5 Registros encontrados, Página 1 de 1

Imagen 37 - Nombre del dominio

Posteriormente se delega el manejo del dominio a Cloudflare para desde esta plataforma generar el certificado SSL, para hacer esto se cambian los nombres de servidores en freenom y se ponen los DNS de Cloudflare para delegarle el dominio.



Imagen 38 - Delegando el dominio a Cloudflare

Luego en Cloudflare se añaden los registros necesarios para que el certificado se asocie de manera correcta.

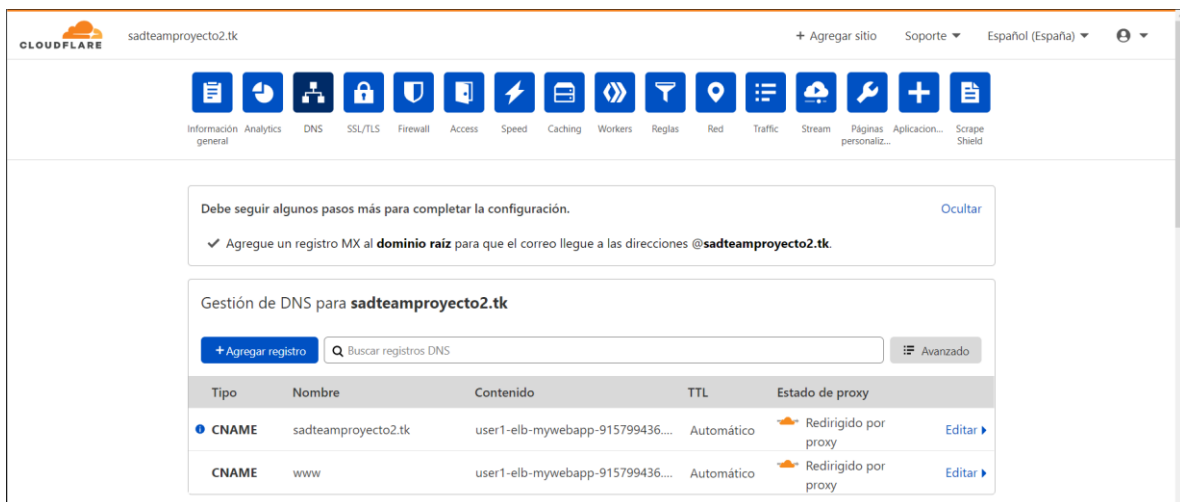


Imagen 39 - Añadiendo registros en Cloudflare

Una vez se haya realizado esto procederemos a generar el certificado desde Cloudflare, para posteriormente asociar la key y el cuerpo que este nos genere a un listener en el load balancer.

### Certificados de cliente

Proteja y autentique sus API y aplicaciones web con los certificados de cliente.  
Bloquee el tráfico de dispositivos que no tengan un certificado SSL/TLS de cliente válido con reglas mTLS.

**Servidores**  
Elija qué servidor(es) desea habilitar mTLS

Ninguno [Editar](#)

Crear certificado

Crear una regla mTLS

Asunto del certificado	Autoridad	Expira el	Estado	
> CN=Cloudflare, C=US	CA administrado de Cloudflare para jsperezsalar2001@gmail.com	16 de may. de 2031	Activo	Revocar

Imagen 40 - Generación del certificado SSL

Crear balanceador de carga

Acciones

Filtrar por etiquetas y atributos o buscar por palabra clave

1 a 1 de 1

Nombre	Nombre de DNS	Estado	ID de VPC	Zonas de disponibilidad	Tipo	Cr
USER1-ELB-MyWebApp	USER1-ELB-MyWebApp-91...	active	vpc-0bcea331ff110df66	us-east-2b, us-east-2a	application	16

Balanceador de carga: USER1-ELB-MyWebApp

Descripción Agentes de escucha Monitorización Servicios integrados Etiquetas

Un agente de escucha busca las solicitudes de conexión mediante su protocolo y puerto configurados, y el balanceador de carga usa las reglas del agente de escucha para direccionar las solicitudes a los destinos. Puede agregar, quitar o actualizar los agentes de escucha y las reglas de agente de escucha.

Agregar agente de escucha Editar Eliminar

ID de agente de escucha	Política de seguridad	Certificado SSL	Reglas
<input type="checkbox"/> HTTP : 80 arn...e82ecbd7c57348f7	n/a	n/a	Predeterminada: reenviando a USER1-TG-MyWebApp2 <a href="#">Ver/editar las reglas</a>
<input type="checkbox"/> HTTPS : 443 arn...24428d7a534df14e	ELBSecurityPolicy-2016-08	Predeterminada: Sadteam (IAM) <a href="#">Ver/editar los certificados</a>	Predeterminada: reenviando a USER1-TG-MyWebApp2 <a href="#">Ver/editar las reglas</a>

Imagen 41 - Asociando el certificado SSL a un listener en el LoadBalancer

Como se puede ver en la imagen anterior, el certificado que se generó desde Cloudflare se ha asociado mediante https a el load balancer por el puerto 443. Sin embargo, en este momento la pagina carga sin estilos, puesto que aún falta realizar configuraciones en la instancia del wordpress. Por lo tanto, lo primero que se debe realizar es ingresar al wordpress como administrador y en la pestaña settings, cambiar los atributos Wordpress Address (URL) y Site Address (URL) que contienen el DNS del loadbalancer por nuestro dominio “sadteamproyecto2.tk”.

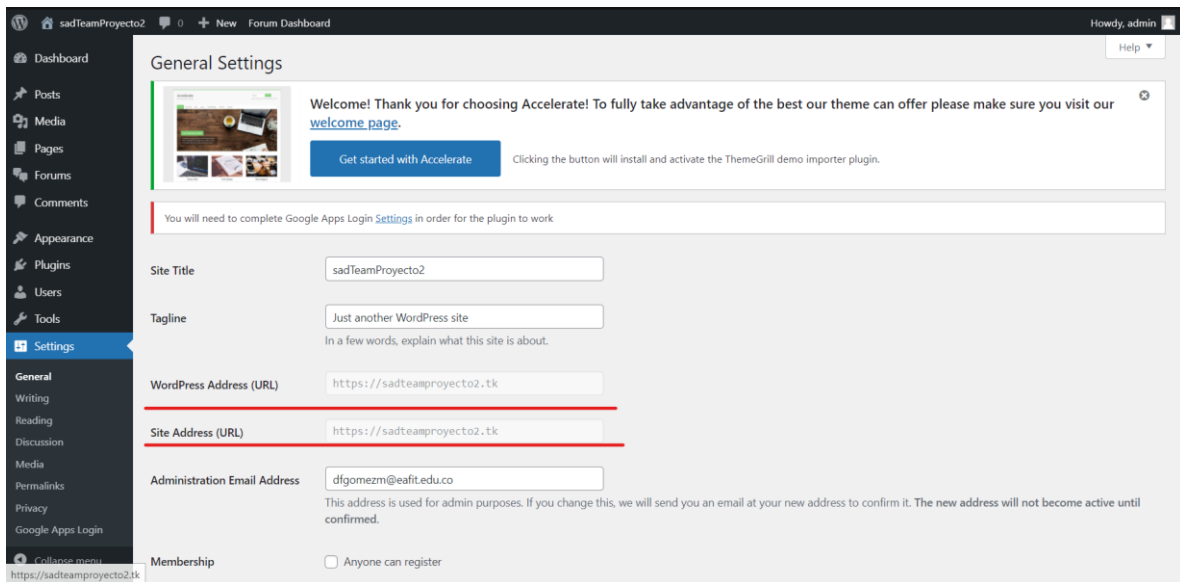


Imagen 42 - Cambiando los atributos para ponerles el nombre del dominio

Posterior a esto, se debe cambiar el archivo `/mnt/efs/wordpress/wp-settings.php` para inscribir allí los atributos que se cambian en la interfaz gráfica, para ellos agregamos las siguientes líneas en el archivo.

```

define( 'WPINC', 'wp-includes' );
define( 'WP_HOME', 'https://sadteamproyecto2.tk' );
define( 'WP_SITEURL', 'https://sadteamproyecto2.tk' );
$_SERVER['HTTPS'] = 'on';

```

Imagen 43 - Añadiendo líneas al archivo wp-settings.php para registrar el dominio

Una vez realizado todo este proceso ya se tiene un certificado para el dominio de forma tal que se garantice que la conexión a nuestro aplicativo web es segura.



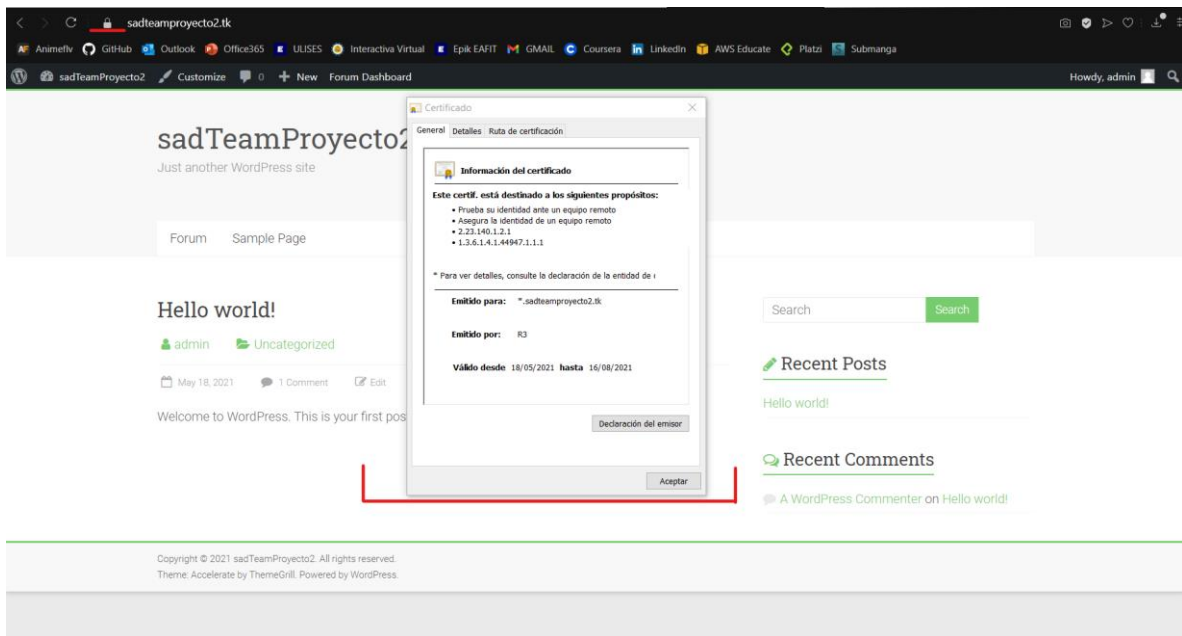


Imagen 44 - Certificado generado y asociado de manera exitosa para el aplicativo web