

# Despliegue de entorno cloud Wordpress en alta disponibilidad en diferentes VPC's

---

## Práctica 2 - GIRC

### Autor

Aarón Escolano Candela

### Tutor/es

Víctor Adsuar Abaldea



Grado en Ingeniería Informática



Escuela  
Politécnica  
Superior



Universitat d'Alacant  
Universidad de Alicante

ALICANTE, Mayo 2023



# Índice general

<b>1</b>	<b>Introducción</b>	<b>1</b>
1.1	Enunciado de la práctica . . . . .	1
1.2	Servicios que utilizaremos . . . . .	1
1.2.1	Virtual Private Network (VPC) . . . . .	1
1.2.1.1	Subnets . . . . .	1
1.2.2	EC2 (Elastic Compute Cloud) . . . . .	2
1.2.3	EFS (Elastic File System) . . . . .	2
1.2.4	RDS (Relational Database System) . . . . .	3
<b>2</b>	<b>Implementación</b>	<b>5</b>
2.1	Creación de las VPC's . . . . .	5
2.1.1	Peering Connection . . . . .	5
2.2	Creación EFS . . . . .	5
2.3	Creación RDS . . . . .	5
2.4	Creación Instancias . . . . .	9
2.5	Balanceador de carga . . . . .	13
2.5.1	Target Group . . . . .	13
2.6	Configuración de las instancias . . . . .	13
2.6.1	Instalación del host bastión . . . . .	13
2.6.2	Instalación de servidor web . . . . .	17
2.6.3	Conexión del EFS con las instancias . . . . .	17
2.6.4	Instalación de Wordpress . . . . .	18
2.6.4.1	Configuración base de datos de Wordpress . . . . .	18
	<b>Bibliografía</b>	<b>21</b>



# Índice de figuras

1.1	Esquema Arquitectura . . . . .	2
2.1	Creación de la VPC principal . . . . .	6
2.2	Esquema VPC principal . . . . .	7
2.3	Esquema VPC secundaria . . . . .	7
2.4	Creación EFS . . . . .	7
2.7	Comprobación origen y destino . . . . .	15
2.8	Admin UI . . . . .	15
2.9	Concesión de acceso a las subredes privadas desde la VPN . . . . .	16
2.10	Aplicación OpenVPN Connect . . . . .	16
2.11	Configuración Base de datos Wordpress . . . . .	18



# Índice de Códigos

2.1	Establecer conexión SSH . . . . .	13
2.2	Instalación OpenVPN . . . . .	13
2.3	Instalación servidor Apache . . . . .	17
2.4	Configuración servidor web . . . . .	17
2.5	Auto-Montaje del EFS . . . . .	17
2.6	Instalación Wordpress . . . . .	18
2.7	Creación Base de datos . . . . .	19





# 1 Introducción

El objetivo de la práctica es familiarizarnos con el entorno cloud. Para ello, utilizaremos diversos servicios de AWS que nos permitirán implementar un servidor web en alta disponibilidad Wordpress en diferentes VPC's, utilizando además EFS y RDS.

## 1.1 Enunciado de la práctica

Se nos pide implementar los siguientes elementos:

- Host bastión para la administración remota
- Arquitectura red basada en redes privadas y públicas en alta disponibilidad
- Base de datos instalada en una VPC diferente conectada mediante una conexión peering a la VPC principal
- Despliegue de Wordpress con almacenamiento EFS

El esquema de la arquitectura completa que debemos implementar en esta práctica se muestra en la figura 1.1.

## 1.2 Servicios que utilizaremos

Para entender para qué sirve cada servicio realizaremos una breve descripción de cada uno de ellos.

### 1.2.1 Virtual Private Network (VPC)

Una nube privada virtual (VPC) es una red virtual dedicada a su cuenta de AWS. Está lógicamente aislada de otras redes virtuales en la nube de AWS. Puede especificar un rango de direcciones IP para la VPC, añadir subredes, añadir gateways y asociar grupos de seguridad.

#### 1.2.1.1 Subnets

Una subred es un rango de direcciones IP en su VPC. Puede lanzar recursos de AWS, como instancias de Amazon EC2, en sus subredes. Puede conectar una subred a Internet, a otras VPC y a sus propios centros de datos, y enrutar el tráfico hacia y desde sus subredes mediante tablas de rutas.

Utilizaremos dos tipos de subnets:

- **Private Network** La subred no tiene una ruta directa a una pasarela de Internet. Los recursos de una subred privada necesitan un dispositivo NAT para acceder a la Internet pública.

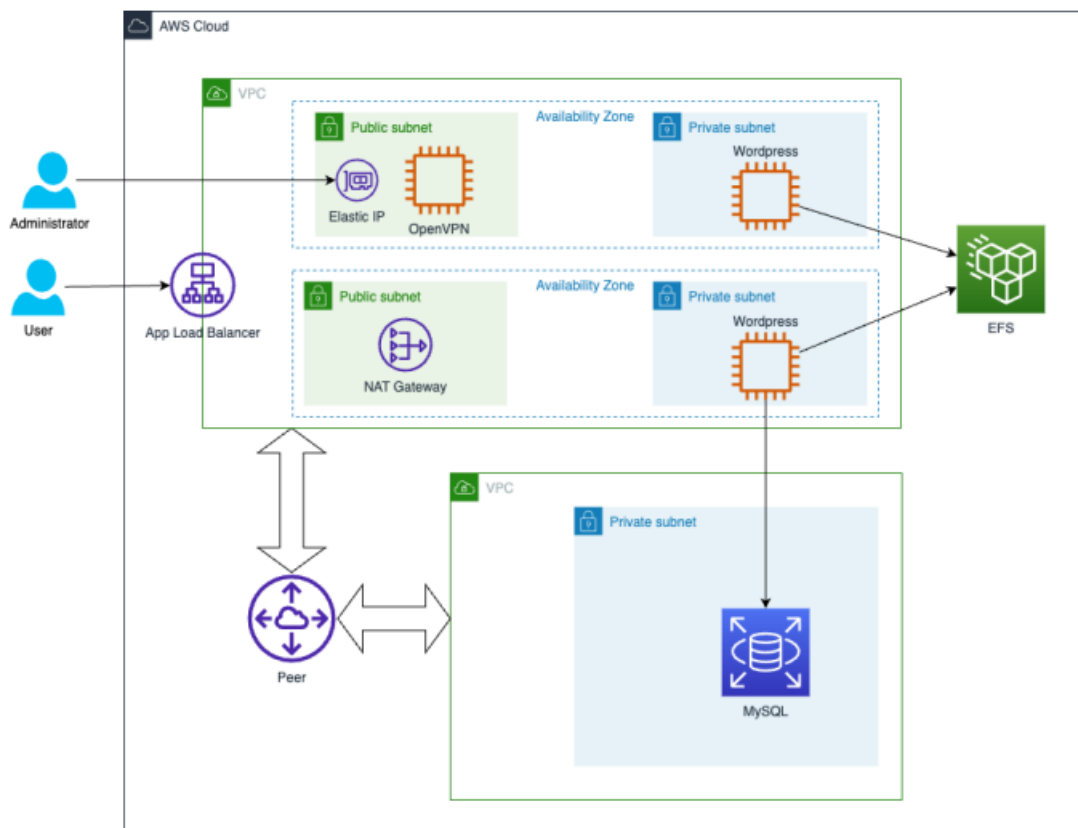


Figura 1.1: Esquema Arquitectura

- **Public Network** La subred tiene una ruta directa a una pasarela de Internet. Los recursos de una subred pública pueden acceder a la Internet pública.

### 1.2.2 EC2 (Elastic Compute Cloud)

Este servicio proporciona capacidad informática escalable en la nube de Amazon Web Services (AWS). Mediante las instancias podemos crear servidores de diferente capacidad computacional que se adapte a la demanda de los usuarios.

En la creación de las instancias podemos determinar el sistema operativo, el grupo de seguridad asociado, la potencia computacional, las credenciales SSH, la VPC y subnet a la que estará asociado entre otros.

### 1.2.3 EFS (Elastic File System)

Este servicio proporciona un sistema de archivo en la nube que nos permitirá tener el mismo wordpress instalado en todas las instancias. De esta forma es mucho más sencilla la administración de actualizaciones de wordpress ya que todas las instancias utilizarán la misma versión.

#### **1.2.4 RDS (Relational Database System)**

Este servicio cumple una función similar al anterior servicio con la diferencia que en este caso se trata de una base de datos en red. Será necesaria para la instalación de Wordpress.



## 2 Implementación

### 2.1 Creación de las VPC's

El primer paso para el desarrollo de la arquitectura es implementar las VPC de nuestro proyecto. Existen dos VPC's, la principal y la secundaria.

La VPC principal contendrá dos subredes públicas y dos subredes privadas. Esta VPC deberá estar en dos zonas de disponibilidad para cumplir con el requisito de alta disponibilidad. Tendremos una red privada y una pública en cada zona de disponibilidad.

La VPC secundaria sólo tendrá una subred privada en una única zona de disponibilidad. El esquema 2.3 muestra dos subredes privadas porque será necesario añadirla para la creación de la base de datos.

#### 2.1.1 Peering Connection

Una conexión VPC peering es una conexión de red entre dos VPCs que permite enrutar el tráfico entre ellas de forma privada. Las instancias de cualquiera de las dos VPC pueden comunicarse entre sí como si estuvieran dentro de la misma red. Crearemos una peering connection entre la VPC principal y la VPC secundaria.

### 2.2 Creación EFS

La figura 2.4 muestra la ventana de creación. Crearemos el EFS en la misma VPC que las instancias que accederán a este, es decir, la VPC principal. Es importante seleccionaremos el tipo de almacenamiento Standard para poder acceder al EFS desde las dos zonas de disponibilidad desde las dos instancias privadas.

A continuación deberemos modificar el grupo de seguridad asociado al EFS. Crearemos un grupo de seguridad específico para el EFS con la regla de entrada que permita todo el tráfico de las redes privadas de la VPC principal.

### 2.3 Creación RDS

Para la creación de la base de datos seleccionaremos el tipo Aurora (MySQL Compatible) porque más adelante nos permitirá elegir un tipo de base de datos muy barata. En la figura 2.5b seleccionaremos Dev/Test porque esta práctica no está pensada para un entorno de producción y además queremos reducir los costes al mínimo. En la figura 2.5c le daremos un nombre a la base de datos y proporcionaremos un usuario y contraseña que nos servirá para conectarnos a ella más adelante desde las instancias privadas. Como indica la figura 2.5d, seleccionaremos el tipo de instancia DB Burstable porque son más baratas y nos permiten

### 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 auto-generation [Info](#)  
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☒ Auto-generate

project1

IPv4 CIDR block [Info](#)  
Determine the starting IP and the size of your VPC using CIDR notation.

10.1.0.0/1665.536 IPs

(a) Selección nombre, CIDR

Number of Availability Zones (AZs) [Info](#)  
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1

2

3

► Customize AZs

Number of public subnets [Info](#)  
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0

2

Number of private subnets [Info](#)  
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0

2

4

(b) Selección subredes

NAT gateways (\$) [Info](#)  
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None

In 1 AZ

1 per AZ

VPC endpoints [Info](#)  
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None

S3 Gateway

DNS options [Info](#)

☒ Enable DNS hostnames

☒ Enable DNS resolution

(c) Selección NAT Gateway y Endpoint

Figura 2.1: Creación de la VPC principal

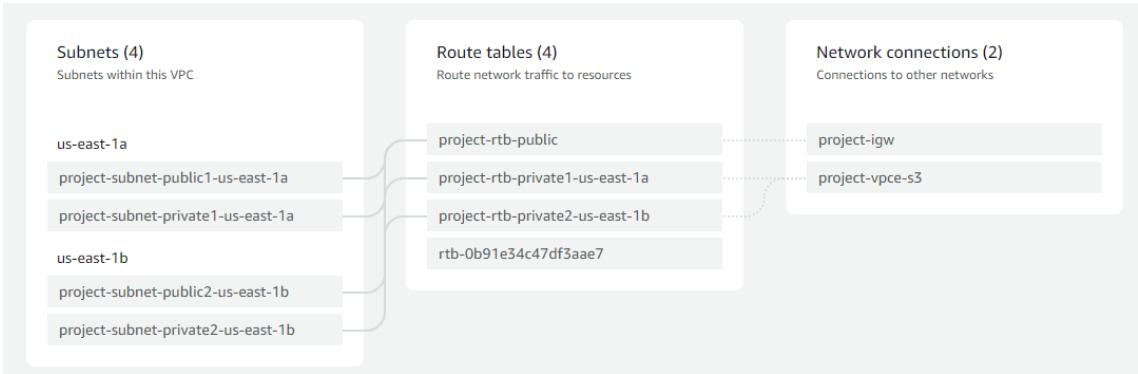


Figura 2.2: Esquema VPC principal

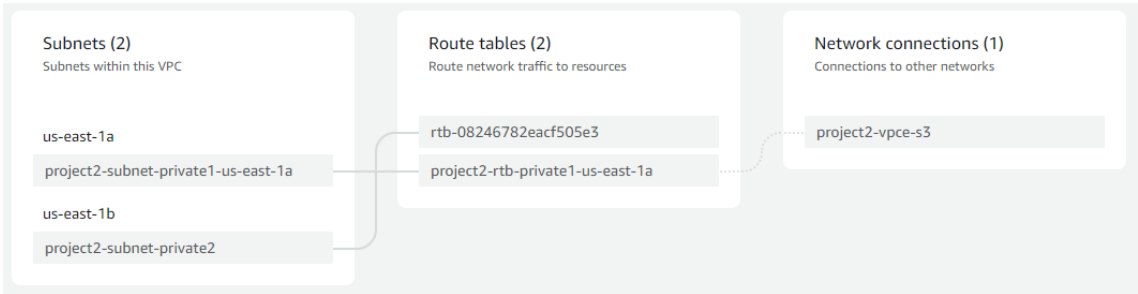


Figura 2.3: Esquema VPC secundaria

Create file system

Create an EFS file system with service recommended settings. [Learn more](#)

Name - optional

Name your file system.

MyFS

Name can include letters, numbers, and +,=,\_,/ symbols, up to 256 characters.

Virtual Private Cloud (VPC)

Choose the VPC where you want EC2 instances to connect to your file system.

vpc-3c39ef57  
default

Storage class [Learn more](#)

☒ Standard

Stores data redundantly across multiple AZs

☐ One Zone

Stores data redundantly within a single AZ

Cancel


Customize


Create


Figura 2.4: Creación EFS


**Engine options**


Engine type [Info](#)


☒ Aurora (MySQL Compatible) 


☐ Aurora (PostgreSQL Compatible) 

☐ MySQL 

☐ MariaDB 

☐ PostgreSQL 

☐ Oracle 

☐ Microsoft SQL Server 

Engine version [Info](#)  
View the engine versions that support the following database features.

► [Show filters](#)

Available versions (37/38) [Info](#)

Aurora (MySQL 5.7) 2.11.1 ▼

(a) Tipo de motor

**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.

(b) Tipo de plantilla

seleccionar instancias más pequeñas y adecuadas a esta práctica. En las figuras 2.5e y 2.5f configuramos la conectividad de la base de datos. Debemos instalar la base de datos en la VPC secundaria para cumplir con las especificaciones.

Es importante recordar que la base de datos debe estar en la misma VPC que las instancias que se conectarán a ella. Por eso debemos crear una peering connection que permita la conectividad entre las instancias de la VPC principal y la base de datos en la VPC secundaria. La opción public access la dejamos en NO porque no queremos que puedan acceder individuos externos a nuestras redes privadas.

Dejamos todas las demás opciones cómo vienen por defecto.



## 2.4 Creación Instancias

Crearemos una instancia en cada subred de la VPC principal. Cada una de ellas desempeñará una función.

- La instancia en la subred pública uno será dónde instalaremos el host bastión (VPN) para poder acceder a las subredes privadas desde el exterior.
- Las instancia en la otra subred pública funcionará cómo NAT Gateway para proporcionar conectividad a internet a las instancias de las redes privadas.
- Las instancias de las redes privadas serán las que ejecutarán el servidor web. Estas instancias accederán al EFS y a la base de datos para poder instalar wordpress.

En la figura 2.6a seleccionaremos Amazon linux cómo el sistema operativo de las instancias porque es el más barato. Para la creación de la instancia que funcionará cómo NAT Gateway debemos buscar *NAT* y seleccionar de entre los AMIs de la comunidad el que queramos.

En la figura 2.6c seleccionaremos una clave. La primera vez que lo hagamos deberemos crearla en el botón azul que aparece a la derecha. En la figura 2.6d podemos ver la ventana de creación de claves. Dejaremos todo por defecto y le daremos un nombre. Esta clave tendremos que descargarla en nuestro ordenador y configurar SSH para poder hacer login en las instancias. En cuanto a las redes, deberemos seleccionar la que corresponda para cada instancia. La figura 2.6e muestra la ventana de configuración de este aspecto. La opción Auto-assign public IP lo dejaremos abilitado para las instancias en las subredes públicas.

Es importante que cuando creemos la instancia NAT Gateway seleccionemos la opción de detener la comprobación de origen y destino como muestra la figura 2.7.

### Settings

**DB cluster identifier** [Info](#)  
Enter a name for your DB cluster. The name must be unique across all DB clusters owned by your AWS account in the current AWS Region.

The DB cluster identifier is case-insensitive, but is stored as all lowercase (as in "mydbcluster"). Constraints: 1 to 60 alphanumeric characters or hyphens. 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 32 alphanumeric characters. First character must be a letter.

☐ **Manage master credentials in AWS Secrets Manager**  
Manage master user credentials in Secrets Manager. RDS can generate a password for you and manage it throughout its lifecycle.

**?** If you manage the master user credentials in Secrets Manager, some RDS features aren't supported.  
[Learn more](#)

☐ **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), ' (single quote), " (double quote) and @ (at sign).

**Confirm master password** [Info](#)

(c) Credenciales e ID de la BD

### Instance configuration

The DB instance configuration options below are limited to those supported by the engine that you selected above.

**DB instance class** [Info](#)

☐ Memory optimized classes (includes r classes)

☒ Burstable classes (includes t classes)

db.t3.medium

2 vCPUs 4 GiB RAM Network: 2085 Mbps

▼

☒ Include previous generation classes

(d) Tipo de instancia

Connectivity [Info](#)

Compute resource

Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

Don't connect to an EC2 compute resource

Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

Connect to an EC2 compute resource

Set up a connection to an EC2 compute resource for this database.

Network type

[Info](#)

To use dual-stack mode, make sure that you associate an IPv6 CIDR block with a subnet in the VPC you specify.

IPv4

Your resources can communicate only over the IPv4 addressing protocol.

Dual-stack mode

Your resources can communicate over IPv4, IPv6, or both.

(e) Creación EFS

Virtual private cloud (VPC) [Info](#)

Choose the VPC. The VPC defines the virtual networking environment for this DB cluster.

project2-vpc (vpc-03793c1c40e1f323e)

Only VPCs with a corresponding DB subnet group are listed.

After a database is created, you can't change its VPC.

DB subnet group

[Info](#)

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

default-vpc-03793c1c40e1f323e

Public access

[Info](#)

Yes

RDS assigns a public IP address to the cluster. Amazon EC2 instances and other resources outside of the VPC can connect to your cluster. Resources inside the VPC can also connect to the cluster. Choose one or more VPC security groups that specify which resources can connect to the cluster.

No

RDS doesn't assign a public IP address to the cluster. Only Amazon EC2 instances and other resources inside the VPC can connect to your cluster. Choose one or more VPC security groups that specify which resources can connect to the cluster.

(f) Creación EFS

▼ **Application and OS Images (Amazon Machine Image)** [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

**Quick Start**

Amazon Linux macOS Ubuntu Windows Red Hat

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type  
ami-005f9685cb30f234b (64-bit (x86)) / ami-05a56dc4a507a82cc (64-bit (Arm))  
Virtualization: hvm ENA enabled: true Root device type: ebs Free tier eligible

Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20230307.0 x86\_64 HVM gp2

Architecture AMI ID

64-bit (x86) ami-005f9685cb30f234b **Verified provider**

(a) Tipo de motor

▼ **Instance type** [Info](#)

Instance type

t2.micro Free tier eligible

Family: t2 1 vCPU 1 GiB Memory  
On-Demand Windows pricing: 0.0162 USD per Hour  
On-Demand SUSE pricing: 0.0116 USD per Hour  
On-Demand RHEL pricing: 0.0716 USD per Hour  
On-Demand Linux pricing: 0.0116 USD per Hour

[Compare instance types](#)

(b) Tipo de plantilla

▼ **Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

Practica2VPCs [Create new key pair](#)

(c) Credenciales e ID de la BD

## 2.5 Balanceador de carga

El balanceador de carga permite alta disponibilidad de nuestra aplicación en la capa de instancias. Si una instancia cae o tiene mucha carga computacional, el balanceador de carga puede redirigir el tráfico hacia otra instancia para mantener activo el servicio. En nuestra práctica implementaremos un balanceador de carga de aplicación porque sólo tendremos tráfico HTTP y HTTPS.

El balanceador deberemos configurarlo como internet-facing porque enrutará las peticiones de los clientes desde internet hacia nuestra aplicación.

En la opción listeners dejaremos configurado el puerto 80 y seleccionaremos el target group que configuremos.

### 2.5.1 Target Group

El target group es el grupo de instancias en nuestro caso que el balanceador tendrá en cuenta para balancear las peticiones HTTP y HTTPS de nuestra aplicación. Nosotros tenemos dos instancias que se encargarán de procesar las peticiones al servidor web, por lo tanto estas instancias serán las que formen parte del target group.

## 2.6 Configuración de las instancias

En esta sección explicaré todos los pasos y comandos necesarios para la instalación.

### 2.6.1 Instalación del host bastión

El host bastión o VPN permite que podamos configurar de forma remota las instancias establecidas en las redes privadas. Primero tenemos que conectarnos a la instancia uno en la red publica utilizando SSH. Para ello debemos tener descargada la clave que hayamos configurado en esa instancia en nuestro ordenador. En el caso de Windows, la clave debe estar en la carpeta C:\Users\<user name>\.ssh. Ejecutamos el siguiente comando en esa carpeta.

Código 2.1: Establecer conexión SSH

```
1#!/bin/bash
2$ ssh -i "Practica2VPCs.pem" ec2-user@ec2-3-226-176-193.compute-1.amazonaws.com ↵
  ↵ com
```

Una vez estamos dentro de la máquina instalamos la VPN de la siguiente forma:

Código 2.2: Instalación OpenVPN

```
1#!/bin/bash
2$ yum -y remove openvpn-as-yum
3$ yum -y install https://as-repository.openvpn.net/as-repo-amzn2.rpm
4$ yum -y install openvpn-as
5
6#####
7#Access Server 2.11.3 has been successfully installed in /usr/local/openvpn_as
8#Configuration log file has been written to /usr/local/openvpn_as/init.log
9
```

Create key pair

×

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Key pair name

Enter key pair name

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA  
RSA encrypted private and public key pair

☐ ED25519  
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

☒ .pem  
For use with OpenSSH

☐ .ppk  
For use with PuTTY

Cancel

Create key pair

#### (d) Creación claves SSH

▼ Network settings Info

VPC - required Info

vpc-06477ffebf4e728bd (project-vpc)  
10.1.0.0/16

Subnet Info

subnet-05d505bc47b630405 project-subnet-public1-us-east-1a  
VPC: vpc-06477ffebf4e728bd Owner: 245352032843 Availability Zone: us-east-1a  
IP addresses available: 4089 CIDR: 10.1.0.0/20

Auto-assign public IP Info

Enable

#### (e) Selección de redes

Change Source / destination check

The source / destination check ensures that the instance is the source or destination of all the traffic it sends and receives. Each EC2 instance performs source and destination checks by default. [Learn more](#)

Instance ID  
i-0ee4d34c2ed6d0cac (VPC1Public2 - NAT Interface)

Network interface  
eni-00a18e5a5f08a0f27


Source / destination checking  
Stop to allow your instance to send and receive traffic when the source or destination is not itself.

☒ Stop

Cancel

Save

Figura 2.7: Comprobación origen y destino



Admin Login

Username

Password

Sign In

Figura 2.8: Admin UI

```

10 #Access Server Web UIs are available here:
11 #Admin UI: https://192.168.102.130:943/admin
12 #Client UI: https://192.168.102.130.943
13 #Login as "openvpn" with "RR4ImyhwbFFq" to continue
14 #(password can be changed on Admin UI)
15 #+++++
16
17 $ passwd openvpn #For changing the password

```

Ahora ya podemos acceder a la página web de configuración de OpenVPN para configurar el acceso a las subredes privadas. Para ello accederemos a la Admin UI<sup>2.8</sup> mediante la IP pública de la instancia. Una vez dentro, en la sección de configuración buscaremos la opción VPN Settings. En esa ventana, buscaremos la sección Routing y añadiremos las subredes privadas<sup>2.9</sup>.

Ya tenemos configurada la VPN. Ahora sólo queda instalarnos la aplicación OpenVPN Connect para realizar la conexión. Debemos descargar desde la Admin UI un archivo .ovpn que deberemos importar el perfil a la aplicación. Una vez importado, modificaremos el campo *Server Override*<sup>2.10</sup> y escribiremos la ip pública de la instancia.

### Routing

Should VPN clients have access to private subnets (non-public networks on the server side)?

No Yes, using NAT Yes, using Routing

Specify the private subnets to which all clients should be given access (one per line):

10.10.0/20  
10.1128.0/20  
10.1144.0/20

Should client Internet traffic be routed through the VPN?

Yes

Should clients be allowed to access network services on the VPN gateway IP address?

Yes

**Figura 2.9:** Concesión de acceso a las subredes privadas desde la VPN

OpenVPN Connect

< Edit Profile Save

Profile Name  
openvpn

Server Hostname (locked)  
10.1.11.149

Server Override (optional)  
3.226.176.193

Username (locked)  
openvpn

☒ Save password

Password  
.....

**Figura 2.10:** Aplicación OpenVPN Connect







Below you should enter your database connection details. If you're not sure about these, contact your host.

Database Name	<input type="text" value="wordpress"/>	The name of the database you want to use with WordPress.
Username	<input type="text" value="username"/>	Your database username.
Password	<input type="password" value="password"/>	Your database password.
Database Host	<input type="text" value="localhost"/>	You should be able to get this info from your web host, if localhost doesn't work.
Table Prefix	<input type="text" value="wp_"/>	If you want to run multiple WordPress installations in a single database, change this.

**Figura 2.11:** Configuración Base de datos Wordpress

```
6
7 #TO CHECK FILE SYNTAX
8 $ sudo mount -fav
9
10 #TO CHECK THAT EFS IS MOUNTED
11 $df -h
```

## 2.6.4 Instalación de Wordpress

Para la instalación de Wordpress necesitaremos descargarnos y guardar en el efs Wordpress. Para ello utilizaremos los siguientes comandos:

### Código 2.6: Instalación Wordpress

```
1 #!/bin/bash
2 $ sudo cd /var/www/html/efs
3 $ sudo wget https://wordpress.org/latest.tar.gz
4 $ sudo tar -xvzf latest.tar.gz
5 $ sudo rm latest.tar.gz
6 $ sudo systemctl restart httpd
```

Con esto, ya tenemos instalado Wordpress. Para comprobar si la instalación ha sido correcta, accederemos al dns del balanceador de carga y comprobaremos que aparece la pantalla de configuración de la base de datos.

### 2.6.4.1 Configuración base de datos de Wordpress

Uno de los archivos más importantes de la instalación de WordPress es el archivo wp-config.php. Este archivo se encuentra en la raíz del directorio de archivos de WordPress y contiene los detalles de configuración básicos del sitio web, como la información de conexión a la base de datos.

Cuando descargas WordPress por primera vez, el archivo wp-config.php no está incluido. Puede crear y editar el archivo wp-config.php usted mismo, o puede omitir este paso y dejar que WordPress intente hacerlo por sí mismo cuando ejecute el script de instalación. (Aún así, tendrá que indicar a WordPress la información de su base de datos).

Antes de realizar la instalación deberemos asegurarnos de tener una base de datos creada. La opción más rápida es inicializar el RDS con una base de datos ya creada. Si no es el caso, deberemos crearla manualmente. Para ello podemos utilizar diferentes herramientas como phpMyAdmin, Plesk, cPanel o MySQL Client from the shell.

A continuación mostraré cómo realizarlo desde el cliente MySQL.

Código 2.7: Creación Base de datos

```
1#!/bin/bash
2# INSTALLATION (Install the one available)
3$ sudo yum install mysql
4$ sudo yum install mariadb-client
5$ mysql --version
6# CONNECTION
7# mysql -u database_user -p -h host_name or Ip-address or Endpoint -P port
8$ sudo mysql -h -mysqlinstance1.123456789012.us-east-1.rds.amazonaws.com -P ↵
   ↵ 3306 -u mymasteruser -p
9
10Welcome to the MySQL monitor. Commands end with ; or \g.
11Your MySQL connection id is 9738
12Server version: 8.0.23 Source distribution
13
14Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
15
16mysql>
17mysql> CREATE DATABASE db;
18mysql> GRANT ALL PRIVILEGES ON db.* TO "wordpressusername"@"endpoint"
19-> IDENTIFIED BY "password";
20mysql> FLUSH PRIVILEGES;
21mysql> exit
```

Para poder realizar la conexión a la base de datos necesitaremos comprobar las rutas de las subredes privadas hacia la VPC de la base de datos pasando por la peering conexión y viceversa. Por otro lado, debemos permitir en el grupo de seguridad de la base de datos conexiones desde las subredes privadas.

A continuación seguiremos con la configuración de la figura 2.11. En el campo Host introduciremos el dns de la instancia de la base de datos. Concretamente el dns de la instancia writer. En el campo database name deberemos introducir el nombre de una base de datos existente.

Una vez establecida la conexión, nos pedirá crear el archivo wp-config.php. Deberemos crearlo en la dentro de la carpeta wordpress copiando la configuración que aparece en la pantalla de configuración de wordpress.



## Bibliografía

Amazon web services documentation [Manual de software informático]. (s.f.). Descargado de <https://docs.aws.amazon.com/index.html>

Openvpn documentation [Manual de software informático]. (s.f.). Descargado de <https://as-portal.openvpn.com/get-access-server/amazon-linux>