

Instalar WordPress en una arquitectura de tres niveles

José Fco. Mejías Bendala

Nombre: José Fco. Mejías Bendala
Módulo: Implantación de Aplicaciones Web

Ciclo: Administración de Sistemas Informáticos en Red
Fecha: 18/01/23

Índice

1.- Objetivo.....	3
2.- Desarrollo.....	3

1.- Objetivo

El objetivo de la práctica es realizar una instalación de WordPress sobre máquinas virtuales en AWS. Se crearán cuatro máquinas virtuales del tipo EC2: una de ellas tendrá el rol de balanceador de carga, repartiendo las peticiones que reciba a las otras máquinas EC2, donde estará instalado WordPress.

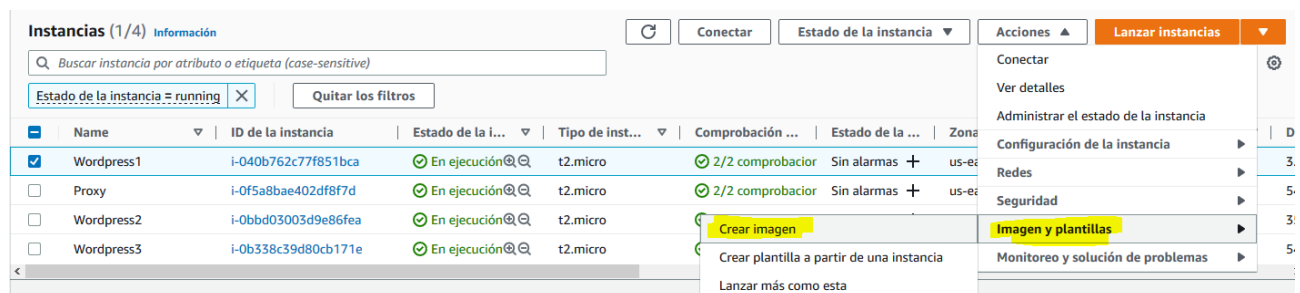
Una quinta instancia de AWS, en este caso del tipo RDS, almacenará la base de datos de WordPress, aceptando las peticiones desde las EC2 que alojan la instalación de WordPress

2.- Desarrollo

Partimos de un escenario donde ya tenemos una instalación de WordPress en dos niveles, con la base de datos en una instancia RDS y el WordPress instalado en una instancia EC2 con Apache, PHP y WordPress instalado y funcionando correctamente.

Para evitar posibles errores a la hora de crear las dos nuevas instancias EC2, se ha optado por realizar un clonado de la imagen de la instancia EC2, para que a la hora de crear estas nuevas instancias, hacerlo desde la imagen AMI creada a partir de la instancia EC2 inicial.

A partir de la instancia en ejecución, se selecciona dicha instancia y se despliega el menú Acciones de la consola de administración de AWS. En dicho desplegable, seleccionamos el menú **Imagen y Plantillas** → **Crear Imagen**



Damos un nombre a la imagen que se va a crear y una descripción, si es necesario, y pulsamos en Crear Imagen. Una vez finalizada, utilizaremos esta imagen para crear dos nuevas instancias EC2 ya configuradas y con el software de WordPress instalado y configurado para acceder a la base de datos en la instancia RDS

Para crear las instancias EC2 con nuestra imagen, sólo tendremos que seleccionar dicha opción a la hora de crear nuevas instancias. Accedemos a Lanzar instancia, pero en vez de escoger una de las máquinas precargadas que ofrece AWS, seleccionamos la opción "**Mis AMI**", que es nombre que AWS da a las imágenes generadas (clonadas)

The screenshot shows the AWS 'Launch Instance' wizard. The 'Image and Operating System' step is selected, displaying a search bar and filters for 'Owned by me' and 'Shared with me'. The 'Summary' panel on the right shows the following configuration: 1 instance, t2.micro type, new security group, and 8 GB storage. A 'Free tier' warning is displayed, stating that the first year includes 750 hours of use for t2.micro instances. The 'Launch Instance' button is visible at the bottom right of the summary panel.

Una vez seleccionada la imagen que creamos con anterioridad, las dos instancias que creamos serán exactamente iguales a la original, con lo que nos ahorramos el tener que realizar la instalación y configuración del WordPress en estas dos nuevas instancias

Debemos crear estas dos instancias dentro de la misma VPC a la que pertenece la instancia original, y las metemos en el mismo grupo de seguridad. A la hora de crear reglas de acceso, al pertenecer al mismo grupo, tendrán las mismas reglas las tres instancias (que denominaremos a partir de ahora wordpress1, wordpress2 y wordpress3. Asimismo, asignaremos IP Elástica a las dos nuevas instancias EC2 creadas.

En cuanto a las reglas de acceso, esperaremos a tener creada la instancia que hará de balanceador para configurarlas.

Por su lado, la RDS que contiene la base de datos, está en la misma VPC que el resto de instancias, y tiene su propio grupo de seguridad. Modificaremos las reglas de entrada de este grupo de seguridad, permitiendo sólo el acceso por el puerto 3306, y sólo con origen el grupo de seguridad de las EC2 de wordpress

Esto aísla la base de datos del exterior, no siendo accesible desde ninguna IP que no pertenezca al grupo de seguridad de las EC2 de WordPress (wordpress1, wordpress2 y wordpress3)

Nombre: José Fco. Mejías Bendala
Módulo: Implantación de Aplicaciones Web

Ciclo: Administración de Sistemas Informáticos en Red
Fecha: 18/01/23

The screenshot shows the AWS IAM console interface for a security group. At the top, there's a header for 'Grupos de seguridad (1/1)' with a search bar and a 'Crear grupo de seguridad' button. Below this, a table lists security groups. The selected group is 'sg-0424dd4aecc28bb33', which is associated with 'RD5Wordpress' and 'vpc-04e9b51024b7f9db2'. The 'Reglas de entrada' tab is active, showing a single inbound rule. A notification banner at the top of the rules section suggests using the Reachability Analyzer.

Name	ID del grupo de segu...	Nombre del grupo ...	ID de la VPC	Descripción	Propietario	Número de reglas ...	Número de reg
RDS	sg-0424dd4aecc28bb33	RD5Wordpress	vpc-04e9b51024b7f9db2	Created by RDS manag...	022016390894	1 Entrada de permiso	1 Entrada de pe

Name	ID de la regla del g...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
-	sgr-0d806c87889f1f689	-	MYSQL/Aurora	TCP	3306	sg-05f54ebf54ef17cb...	-

La última instancia que tenemos que crear es la que tendrá el rol de balanceador. Será una instancia EC2 igual a las anteriores, pero en ella sólo instalaremos el servicio de Apache.

Será creada en la misma VPC que el resto de instancias, tendrá su propio grupo de seguridad y le asignaremos una IP Elástica. Esta será la única máquina que estará expuesta al exterior (a Internet), con las siguientes reglas de acceso:

The screenshot shows the AWS IAM console interface for a security group. The header indicates the group is 'sg-099ae8b40994ae63c - launch-wizard-1'. The 'Reglas de entrada' tab is active, showing two inbound rules. A notification banner at the top of the rules section suggests using the Reachability Analyzer.

Name	ID de la regla del g...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
-	sgr-0cda0a15bdea9d2e6	IPv4	HTTP	TCP	80	0.0.0.0/0	-
-	sgr-00e8dd6ab21d24...	IPv4	SSH	TCP	22	0.0.0.0/0	-

Es decir, exponemos la máquina a Internet por el puerto 80 (HTTP) y por el puerto 22 (SSH) por motivos de configuración y mantenimiento

Nombre: José Fco. Mejías Bendala
Módulo: Implantación de Aplicaciones Web

Ciclo: Administración de Sistemas Informáticos en Red
Fecha: 18/01/23

En cuanto a la configuración del software, debemos añadir en el archivo `/etc/apache2/sites-available/000-default.conf` el siguiente código:

ProxyPass /balancer-manager !

```
<Proxy balancer://mycluster>
  #Server1
  BalancerMember http://IP_privada_wordpress1 loadfactor=3 timeout=1
  #Server2
  BalancerMember http://IP_privada_wordpress2 loadfactor=2
  #Server3
  BalancerMember http://IP_privada_wordpress3 loadfactor=1
</Proxy>
```

```
ProxyPass "/" "balancer://mycluster"
ProxyPassReverse "/" "balancer://mycluster"
```

```
<Location /balancer-manager>
  SetHandler balancer-manager
  Order Deny,Allow
  Allow from all
</Location>
```

Una vez configurado esta instancia, debemos acceder al grupo de seguridad de los wordpress(1, 2 y 3) para permitir el tráfico desde el exterior por el puerto 22 (SSH) para configuración de las máquinas, y acceso por el puerto 80 (HTTP) sólo desde el grupo de seguridad de la instancia con rol de balanceador, aislando de esta manera la instalación de WordPress en los tres nodos de accesos directos desde Internet:

EC2 > Grupos de seguridad > sg-05f54ebf54ef17cb2 - launch-wizard-2

sg-05f54ebf54ef17cb2 - launch-wizard-2

Detalles

Nombre del grupo de seguridad launch-wizard-2	ID del grupo de seguridad sg-05f54ebf54ef17cb2	Descripción launch-wizard-2 created 2023-01-11T08:09:00.263Z	ID de la VPC vpc-04e9b51024b7f9db2
Propietario 022016390894	Número de reglas de entrada 2 Entradas de permisos	Número de reglas de salida 1 Entrada de permiso	

Reglas de entrada (2)

	Name	ID de la regla del g...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
<input type="checkbox"/>	-	sgr-0a727d686a476de...	-	HTTP	TCP	80	sg-099ae8b40994ae6...	-
<input type="checkbox"/>	-	sgr-00ec50c44059973ea	IPv4	SSH	TCP	22	0.0.0.0/0	-

Nombre: José Fco. Mejías Bendala
Módulo: Implantación de Aplicaciones Web

Ciclo: Administración de Sistemas Informáticos en Red
Fecha: 18/01/23

Una vez que comprobemos que todo funciona correctamente, desactivaremos en los grupos de seguridad las reglas de acceso SSH, para exponer lo menos posible al exterior nuestra infraestructura