

Usando Amazon Web Services para configurar un servidor web Apache

Víctor Fernández Poyatos

1. Qué es Amazon Web Services

Amazon Web Services (AWS) es una plataforma de servicios de nube que ofrece potencia de cómputo, almacenamiento de bases de datos, entrega de contenido y funcionalidad.

La nube de AWS proporciona un amplio conjunto de servicios de infraestructura, ofertados como una utilidad: bajo demanda, disponibles en cuestión de segundos y pagando sólo por lo que utiliza.

Éste es el principio en el que se basa el Cloud Computing: recursos ilimitados bajo demanda y pagando sólo por el uso.

Este tipo de servicios los usan grandes compañías como *Spotify, airbnb, Netflix...*

2. Cómo conseguir una cuenta de AWS

Para conseguir una cuenta en AWS sólo hay que ir a [su página](#) y realizar el registro. Nos pedirán datos como el número de teléfono y el número de cuenta bancaria, pero en este caso, el servicio que vamos a utilizar es completamente gratuito.

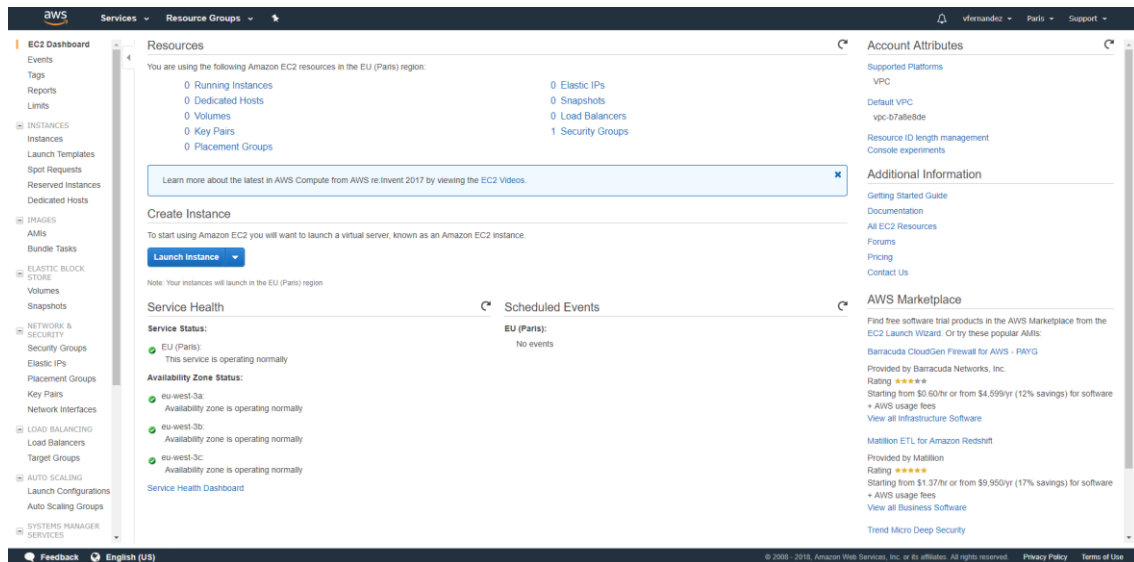
3. Configurando EC2

EC2 (Elastic Compute Cloud) es un servicio web que proporciona capacidad informática en la nube segura y de tamaño modificable. Está diseñado para facilitar a los desarrolladores el uso de la informática en la nube a escala de la web.

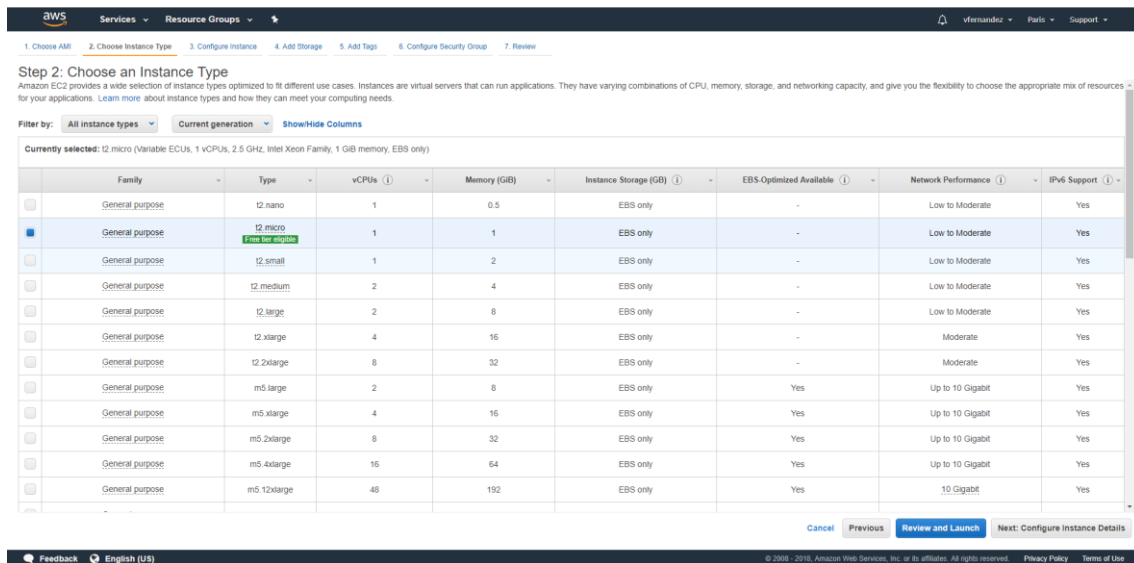
En este caso, lo vamos a configurar de manera que pueda balancear un servidor Apache de manera automática.

Hemos de seguir una serie de pasos para disponer de una configuración activa que nos garantice un sistema de archivos de Amazon EFS, una instancia de EC2 y un sistema de archivos montado en la instancia EC2.

1. Abrimos la [consola](#) de Amazon EC2.
2. Elegimos *Launch Instance*



3. Dentro de este menú, elegimos la opción de *Amazon Linux AMI* que más nos guste. Seleccionamos un tipo de instancia (en nuestro caso la única gratuita) y vamos a configurar los detalles de instancia.



4. Seleccionamos una subnet de cualquier zona de disponibilidad. Seguimos con *Next: Add Storage*.

aws Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 [Launch into Auto Scaling Group](#)

Purchasing option: ☐ Request Spot instances

Network: vpc-b7a8e8de (default) [Create new VPC](#)

Subnet: subnet-699f4e24 (Default in eu-west-3c) [Create new subnet](#)
4091 IP Addresses available

Auto-assign Public IP: ☐ Use subnet setting (Enable)

Placement group: ☐ Add instance to placement group

IAM role: None [Create new IAM role](#)

Shutdown behavior: Stop

Enable termination protection: ☐ Protect against accidental termination

Monitoring: ☐ Enable CloudWatch detailed monitoring
Additional charges apply

Tenancy: ☐ Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy

T2 Unlimited: ☐ Enable
Additional charges may apply

Network interfaces

Device	Network interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-699f4e24	Auto-assign	Add IP	

Cancel Previous **Review and Launch** Next: Add Storage

Feedback English (US) © 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

5. Pinchamos en el botón *Next: Add Tags*.
6. Nombramos la instancia y seguimos con *Next: Configure Security Group*.
7. Configuramos los siguientes parámetros tal y como se muestra en la imagen. Muy importante.

aws Services Resource Groups

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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: launch-wizard-1

Description: launch-wizard-1 created 2018-07-09T22:36:56.970+02:00

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

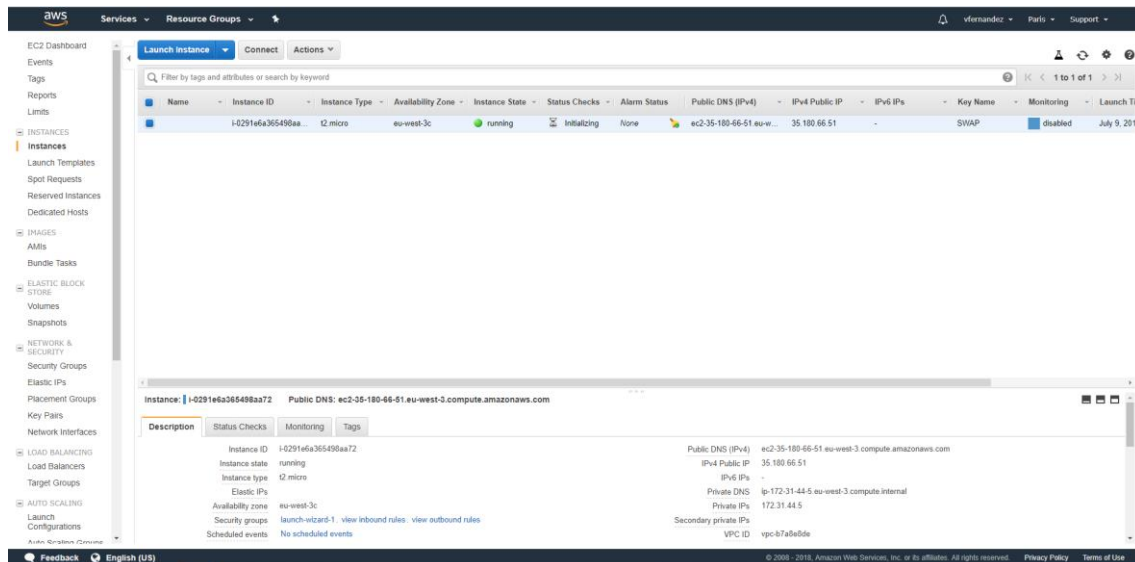
Add Rule

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

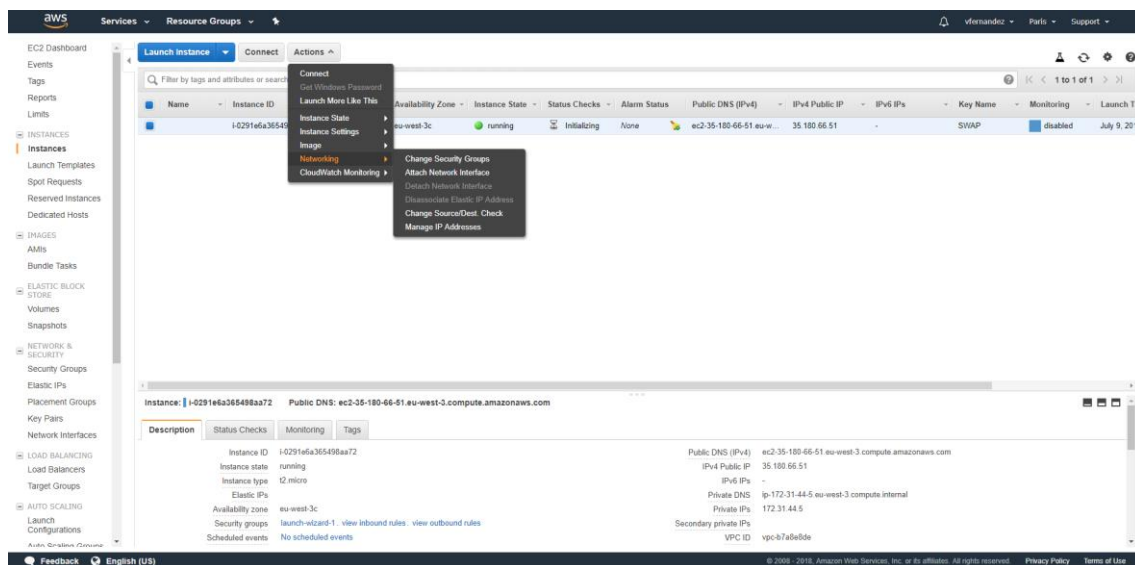
Cancel Previous **Review and Launch**

Feedback English (US) © 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

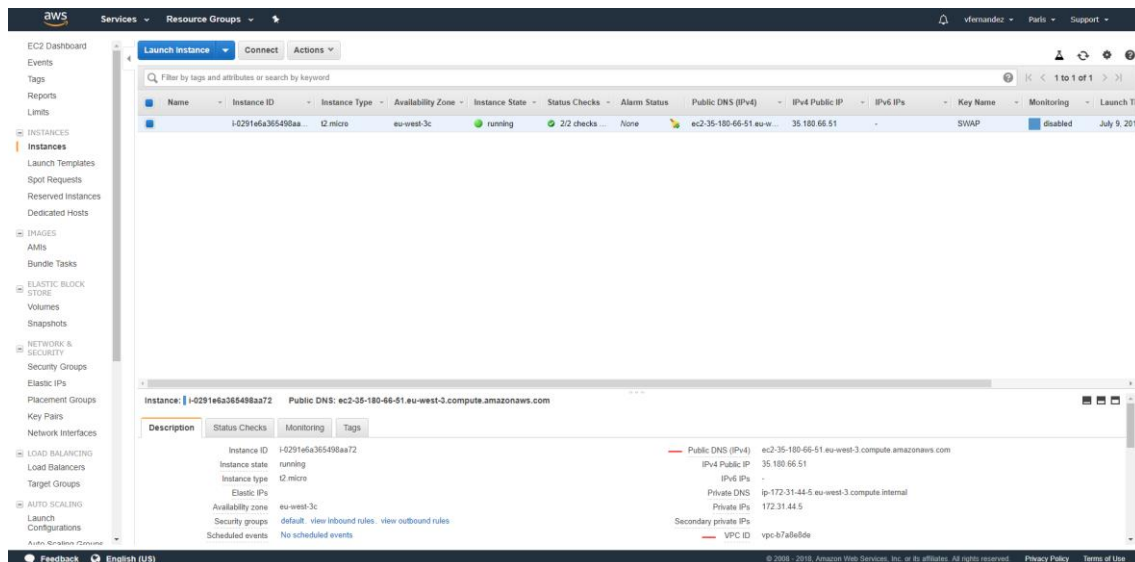
8. Lanzamos las instancias y seleccionamos la opción de *View Instances*, para ver el contenido de éstas. Deberíamos ver algo como esto.



9. El siguiente paso es acceder a la pestaña *Actions > Networking > Change Security Groups*.

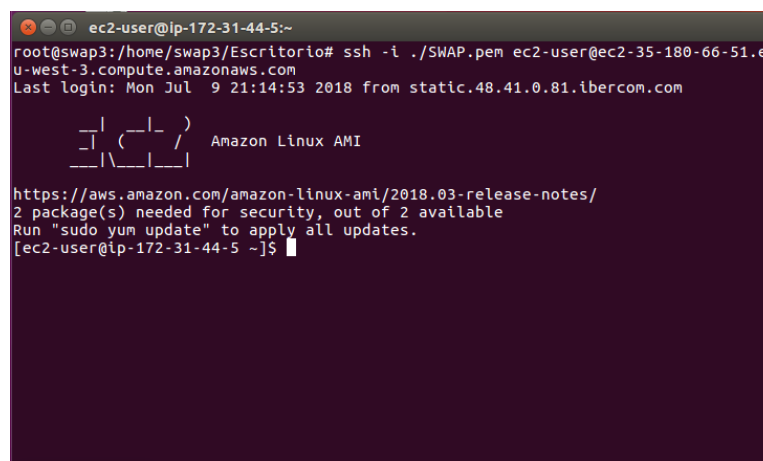
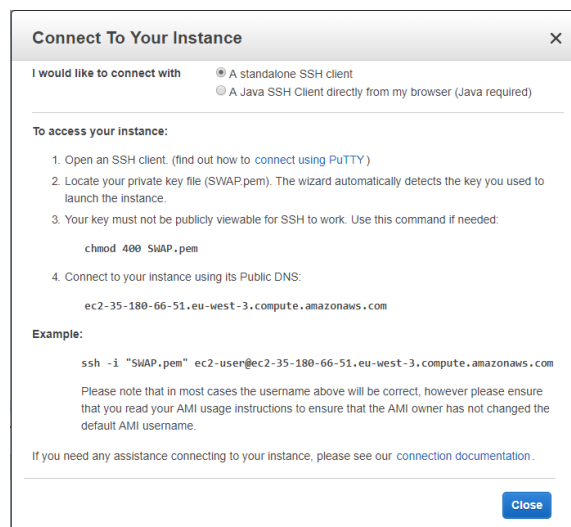


10. Asignamos el grupo de seguridad *default VPC* y guardamos. Ya deberíamos tener configurado nuestro EC2. Ahora debemos apuntar los valores *VPC ID* y *Public DNS* que nos saldrán en la pestaña *Description* al seleccionar nuestra instancia.



Llegados a este punto, debemos conectarnos por SSH a nuestra instancia, usando los datos que hemos recogido previamente.

1. Seleccionando nuestra instancia, pinchamos en *Connect* y seguimos los pasos que nos indica. Los parámetros que aparecen en la siguiente imagen son los míos.



2. Instalamos el servidor Apache e iniciamos servicio con
sudo yum -y install httpd
sudo service httpd start
3. Debemos cambiar la configuración de seguridad de nuestro grupo de seguridad para incluir el protocolo HTTP.

Edit inbound rules ✕

Type ⁱ	Protocol ⁱ	Port Range ⁱ	Source ⁱ	Description ⁱ	
SSH ▾	TCP	22	Custom ▾ 0.0.0.0/0	e.g. SSH for Admin Desktop	✕
SSH ▾	TCP	22	Custom ▾ :::/0	e.g. SSH for Admin Desktop	✕
HTTP ▾	TCP	80	Custom ▾ 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.

Cancel Save

Y listo, ya debería mostrar la página si entramos a nuestra IP pública, la cual tenemos en nuestro panel de instancias. En mi caso es la 35.180.66.51, y como podemos ver a continuación:

