

# Instalación Servidor Virtual en la nube de Amazon

# 1. Cómo crear un servidor virtual en la nube de Amazon Web Services

Existen muchas empresas que ofrecen servicios en la nube, pero hemos optado por Amazon Web Services (AWS) teniendo en cuenta el prestigio de esta empresa y la gran infraestructura que la soporta.

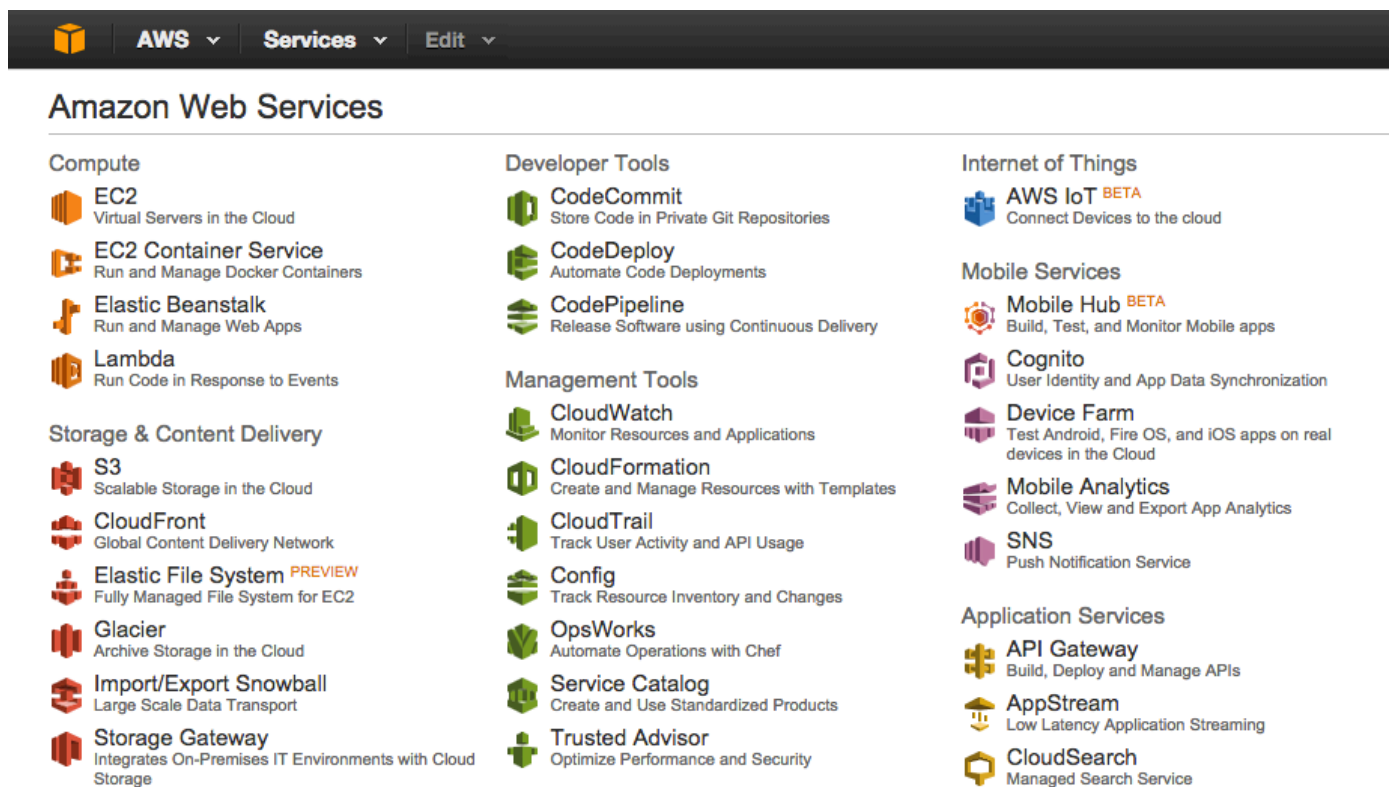
Lo primero que debemos hacer es darnos de alta en la página web de AWS:

<https://aws.amazon.com/es/>

El proceso de registro es muy parecido a cualquier otra web. Te solicitarán tus datos personales o de empresa, además los datos de tu tarjeta de crédito o cuenta bancaria donde se cargarían los recibos en caso de que utilices alguno de sus servicios de pago. También introducirás como datos de acceso, tu email y una contraseña. Como resultado del proceso de registro te enviarán un email con los enlaces para acceder a la consola de cliente.

<https://console.aws.amazon.com/console/home>

Una vez entramos en la consola de cliente de AWS, veremos la siguiente imagen:



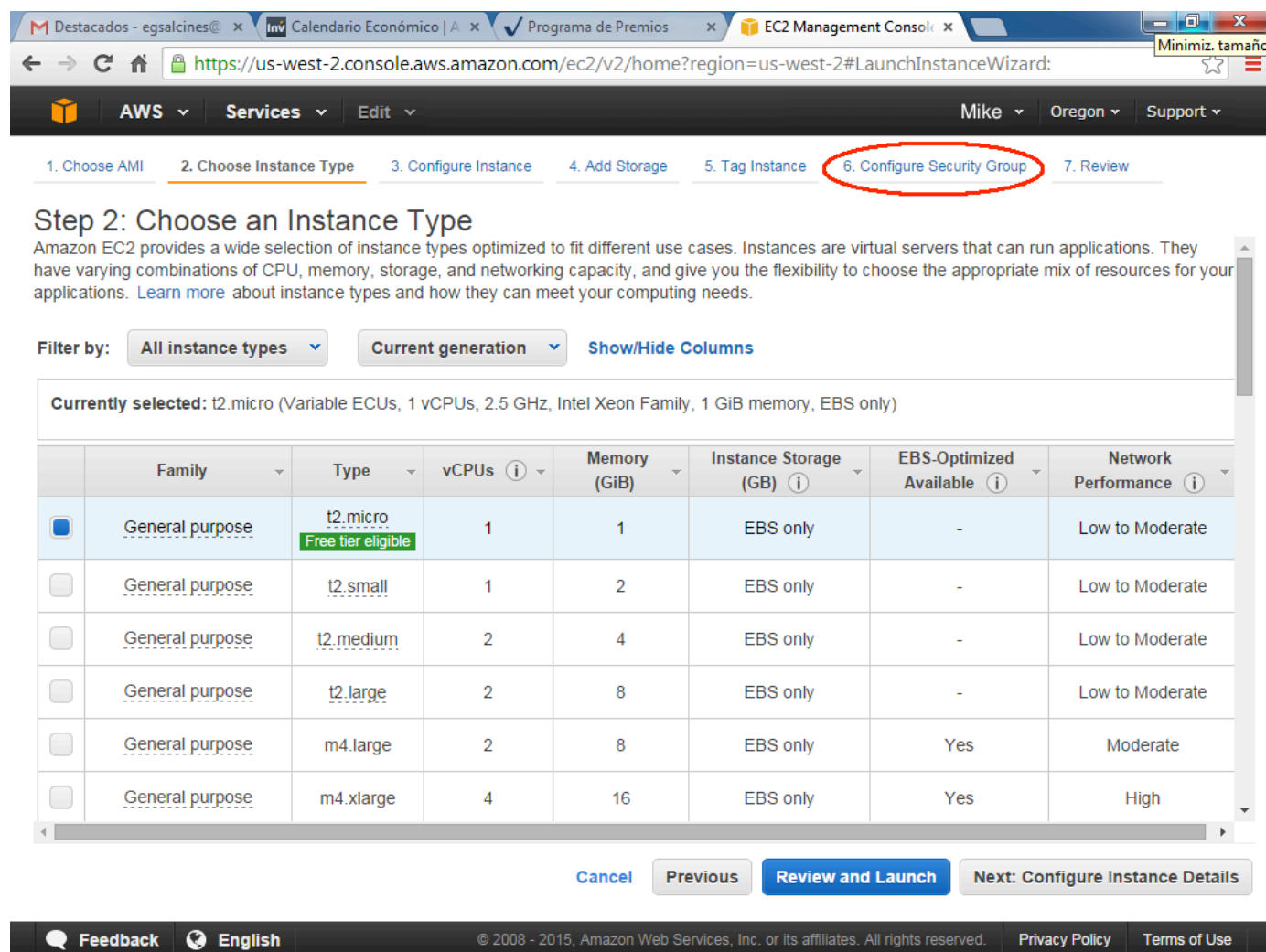
En la pantalla anterior debemos pulsar en la primera opción EC2 “Virtual Servers in the Cloud” y esto nos llevará a la pantalla “EC2 Dashboard” o el Escritorio EC2, desde donde puedes gestionar todos tus servidores virtuales.

The screenshot shows the AWS Management Console for the EC2 service in the us-west-2 region. The left sidebar contains a navigation menu with categories like EC2 Dashboard, INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, and LOAD BALANCING. The main content area is divided into several sections: Resources (listing 1 Running Instance, 1 Elastic IP, etc.), Create Instance (with a 'Launch Instance' button), Service Health (showing 'US West (Oregon): This service is operating normally'), and Account Attributes (showing supported platforms and VPC). A 'Launch Instance' button is highlighted in the 'Create Instance' section.

Ya en el Dashboard, pulsamos el botón azul **“Launch Instance”** y nos muestra la siguiente pantalla donde seleccionaremos el sistema operativo que queremos para nuestro servidor virtual. En nuestro caso, instalaremos Microsoft Windows Server 2012 de 64 bits. Pulsamos el botón azul **“Select”**.

The screenshot shows the 'Step 1: Choose an Amazon Machine Image (AMI)' screen. It features a progress bar at the top with steps: 1. Choose AMI (active), 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Tag Instance, 6. Configure Security Group, and 7. Review. Below the progress bar, there are three AMI options listed: SUSE Linux Enterprise Server 12 (HVM), SSD Volume Type - ami-d7450be7; Ubuntu Server 14.04 LTS (HVM), SSD Volume Type - ami-5189a661; and Microsoft Windows Server 2012 R2 Base - ami-dfcd1ef. The Microsoft Windows Server 2012 R2 Base option is circled in red, and its 'Select' button is highlighted. Each option includes details about the root device type, virtualization type, and architecture (64-bit).

En la siguiente pantalla seleccionaremos la opción que sale por defecto de tipo de servidor que es la **Type: t2.micro** que es la capa gratuita de AWS.



The screenshot shows the AWS Management Console interface for the 'Launch Instance Wizard'. The top navigation bar includes 'AWS', 'Services', 'Edit', and user information. The wizard steps are: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Tag Instance, 6. Configure Security Group (highlighted with a red circle), and 7. Review.

### 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
<input checked="" type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	m4.large	2	8	EBS only	Yes	Moderate
<input type="checkbox"/>	General purpose	m4.xlarge	4	16	EBS only	Yes	High

Buttons: [Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Instance Details](#)

Footer: Feedback English © 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Antes de lanzar la instancia creada, debemos configurar un nuevo grupo de seguridad para que sólo se pueda acceder a nuestra instancia desde la dirección IP de nuestro ordenador. Para averiguar la IP pública de nuestro ordenador debemos consultar las propiedades de nuestra conexión de red, o si lo preferís podéis consultar la siguiente página web que te muestra directamente tu dirección IP:

<http://cual-es-mi-ip-publica.com/>

Una vez tengamos la IP, pulsamos en la opción 6 del menú superior denominada **“Configure Security Group”** en la pantalla anterior mostrando la siguiente pantalla.

**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 <small>i</small>	Protocol <small>i</small>	Port Range <small>i</small>	Source <small>i</small>
RDP	TCP	3389	My IP <input type="text" value="71.XX.128.255/32"/>

En el campo Source que originalmente pone “AnyWhere” debemos cambiarla por “My IP” y en el cuadro de texto a la derecha que pone 0.0.0.0/0 lo cambiamos por nuestra IP pública que averiguamos en el paso anterior (ver zona roja seleccionada)

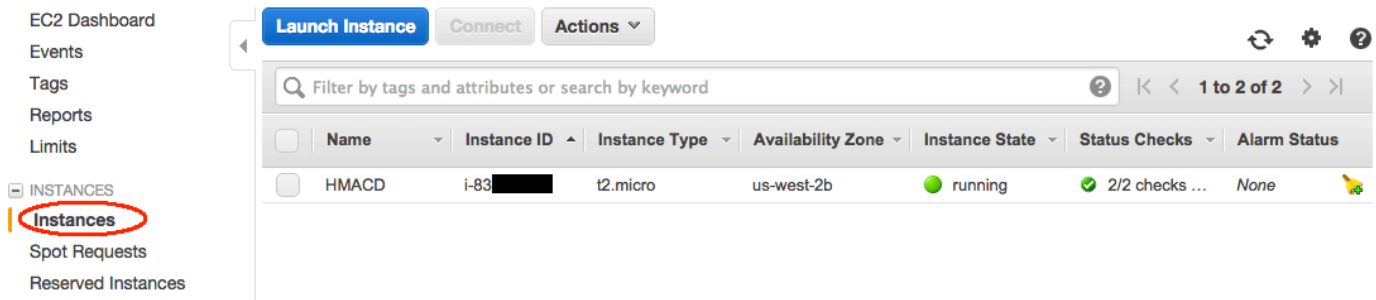
Posteriormente pulsamos el botón azul “Review and Launch” y ya tenemos lanzado nuestro servidor. El mensaje obtenido es el siguiente:

## Launch Status

**Your instances are now launching**  
 The following instance launches have been initiated: [i-b2dde477](#) [View launch log](#)

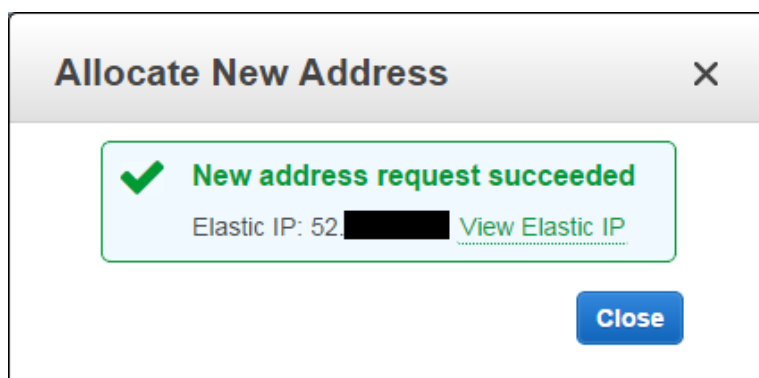
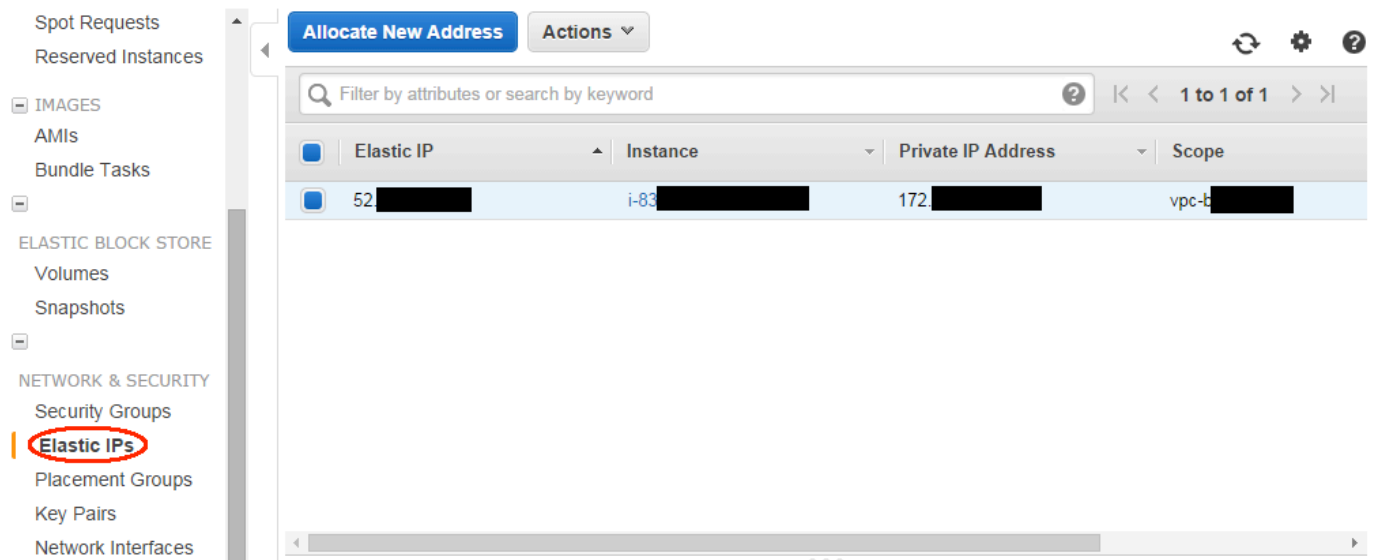
**Get notified of estimated charges**  
[Create billing alerts](#) to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

Si pulsamos en el panel lateral izquierdo la opción “Instances” nos mostrará a la derecha la instancia que hemos creado y que se está ejecutando.

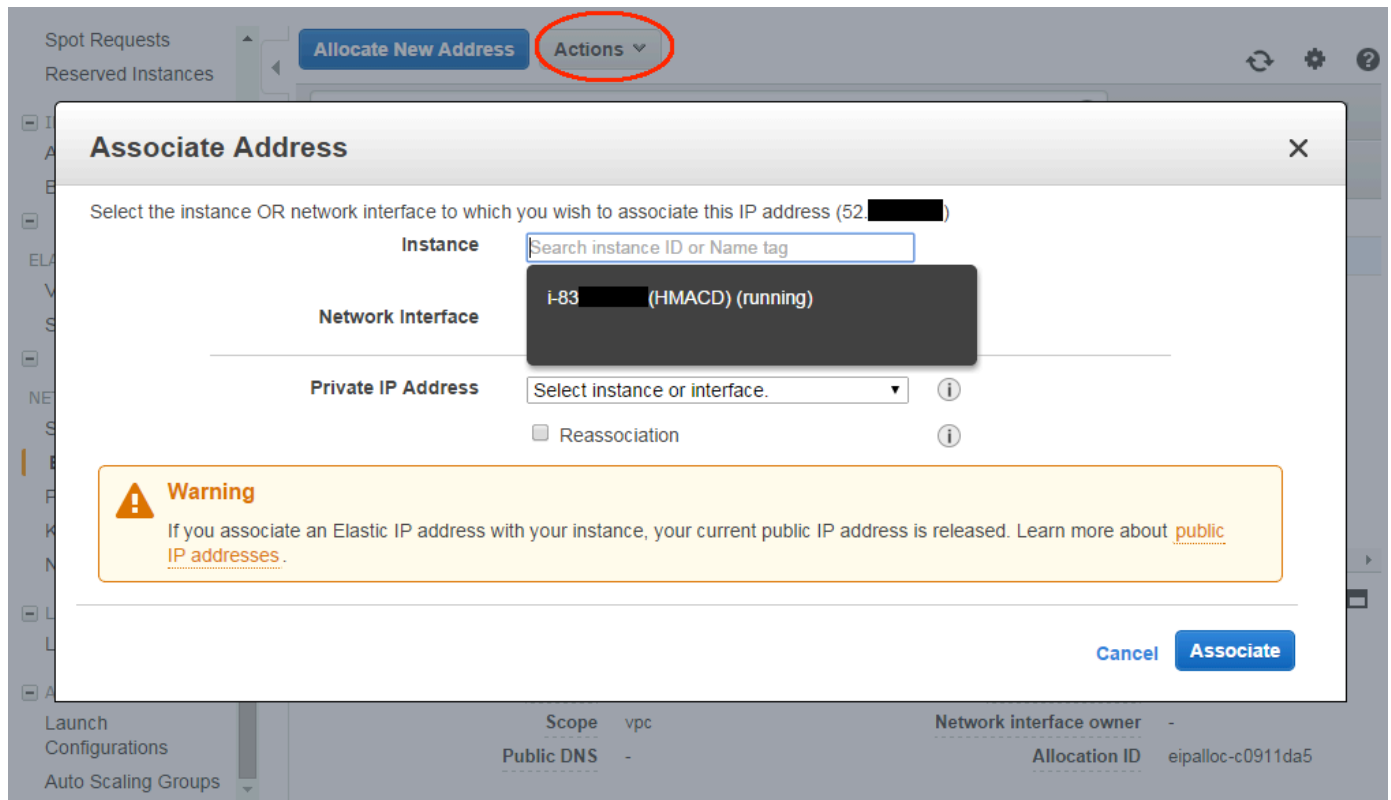


Ya tenemos creada nuestra instancia con un servidor Windows Server 2012.

Lo primero que debemos hacer es crear una IP pública para asociarla después a nuestra instancia- Esta será la dirección IP a la que nos conectaremos desde nuestro ordenador. Para ello, pulsamos en la opción **“Elastic IP”** en el panel de la izquierda y en la pantalla que nos muestra a la derecha pulsamos el botón azul **“Allocate New Address”**. Como resultado debemos obtener la siguiente pantalla. En el campo IP obtendréis una dirección del tipo AA.XX.YY.ZZ/32, por ejemplo 31.115.12.33/32.



Una vez creada la IP elástica debemos asociarla a nuestra instancia. Para ello debemos pulsar el botón gris **“Actions”**, se abrirá un submenú y seleccionamos **“Associate Address”**, abriéndose un cuadro de diálogo como el de la siguiente pantalla:

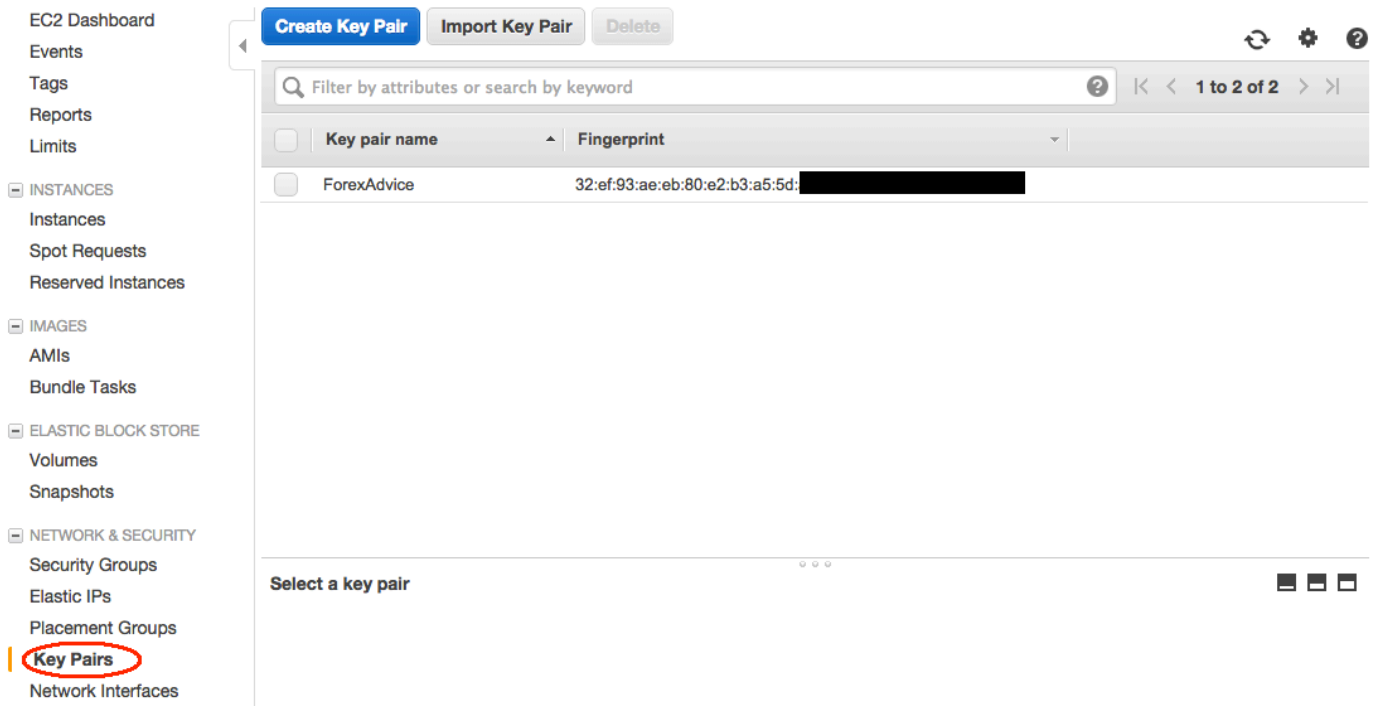


En el cuadro de texto Instance: seleccionamos nuestra instancia y pulsamos el botón azul “Associate”.

Ya sólo queda crear el par de claves pública y privada para conectarnos de manera segura a nuestro servidor remoto. En inglés a este par se le denomina KeyPairs. El recurso Keypairs es uno de los mas importantes ya que es el que permite la comunicación entre nuestra instancia o maquina virtual y un cliente, gracias a un intercambio de llave publica y una llave privada.

Al realizar el proceso de crear una instancia o maquina virtual de cero es muy importante generar, descargar y guardar la llave privada entregada por el dashboard, ya que es el "contrato" entre nuestra instancia o maquina virtual y con el (los) cliente(s) que queremos interactuar. Dentro de las operaciones que podemos realizar con el recurso keypairs se encuentra borrar, adicionar e importar keypairs.

Para crear un nuevo KeyPair, pulsamos en la opción “KeyPair” del panel lateral izquierdo y en la pantalla derecha seleccionamos el botón azul “Create Key Pair” que aparece en la pantalla:



Le ponemos un nombre a la KeyPair y pulsamos el botón “Create”.



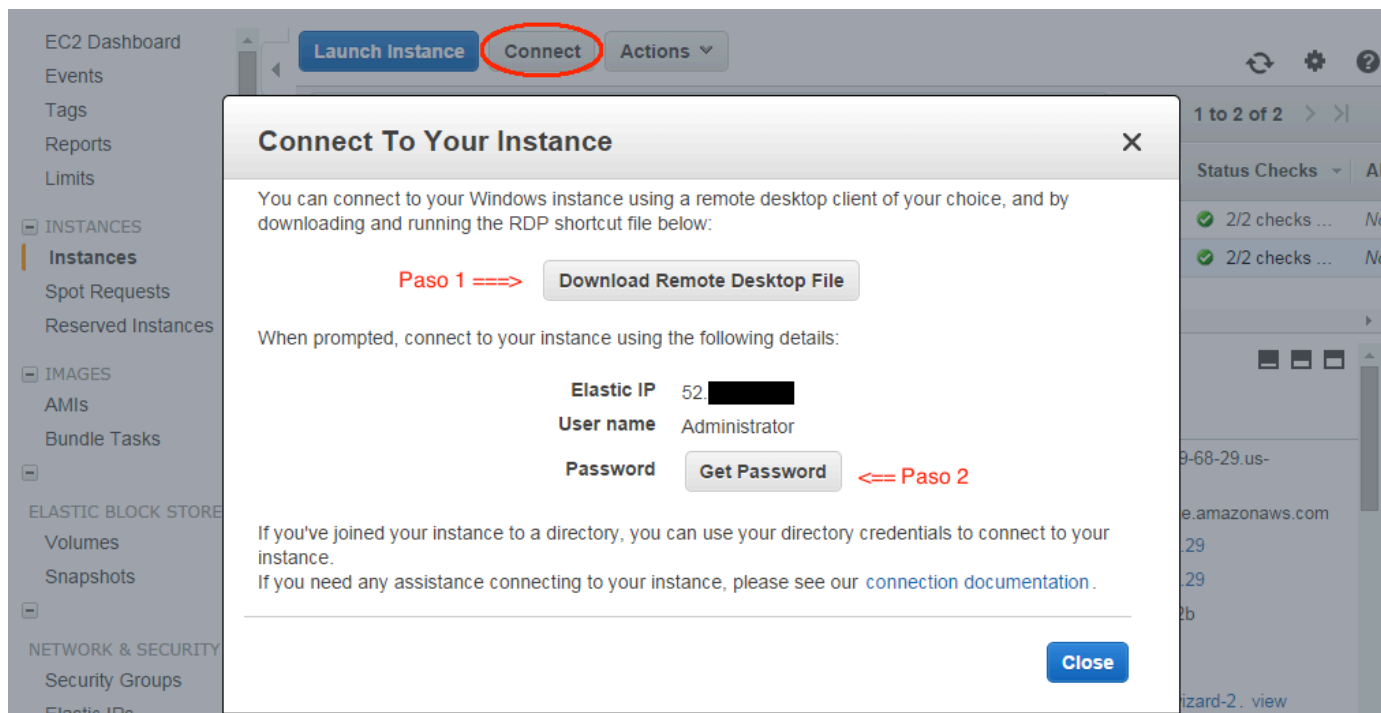
El archivo de claves privado se descarga automáticamente en tu navegador. El archivo tendrá el mismo nombre que le has puesto a la clave y la extensión es .pem. OJO, es importante que guardemos ese archivo en una carpeta que nunca olvidemos, pues más adelante nos pedirán que introduzcamos este archivo para conectar con la instancia. Además, esta es la única oportunidad para guardar este archivo, pues no existe en la consola de AWS ninguna otra opción para descargarlo a posteriori.

Llegados a este punto, ya tenemos todo configurado correctamente para poder conectarnos a nuestro servidor virtual remoto.

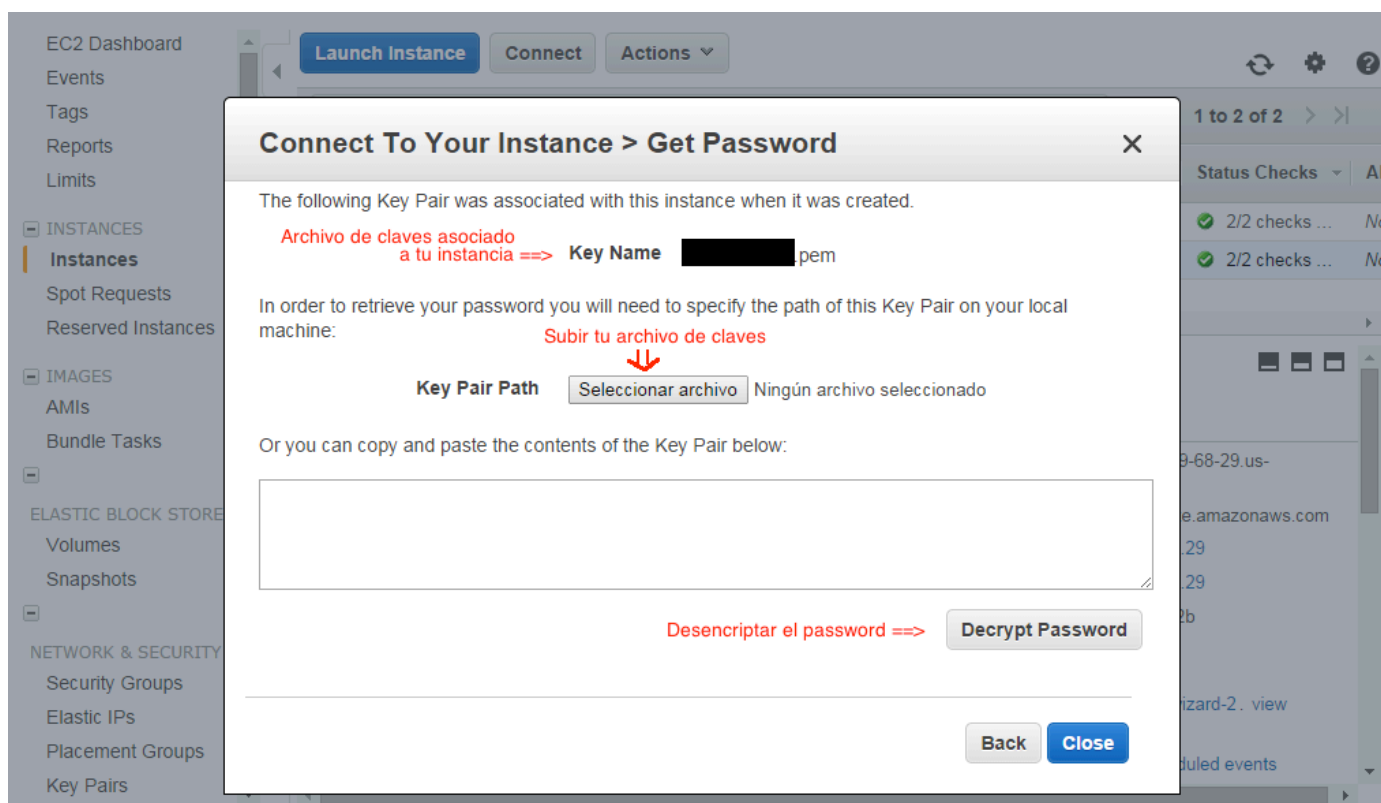
### Conexión a nuestro servidor

1. Volvemos al panel de Instancias, pulsando **“Instances”** en el panel lateral izquierdo.
2. Seleccionamos nuestra servidor virtual y pulsamos el botón gris **“Connect”**. Aparecerá un cuadro de diálogo como el de la pantalla siguiente.
3. Ejecutamos el Paso 1, que es descargar el archivo de conexión .RDP. Para ello, pulsamos en el botón **“Download Remote Desktop File”**, y guardamos este archivo, por ejemplo, en el escritorio Windows de nuestro ordenador personal.

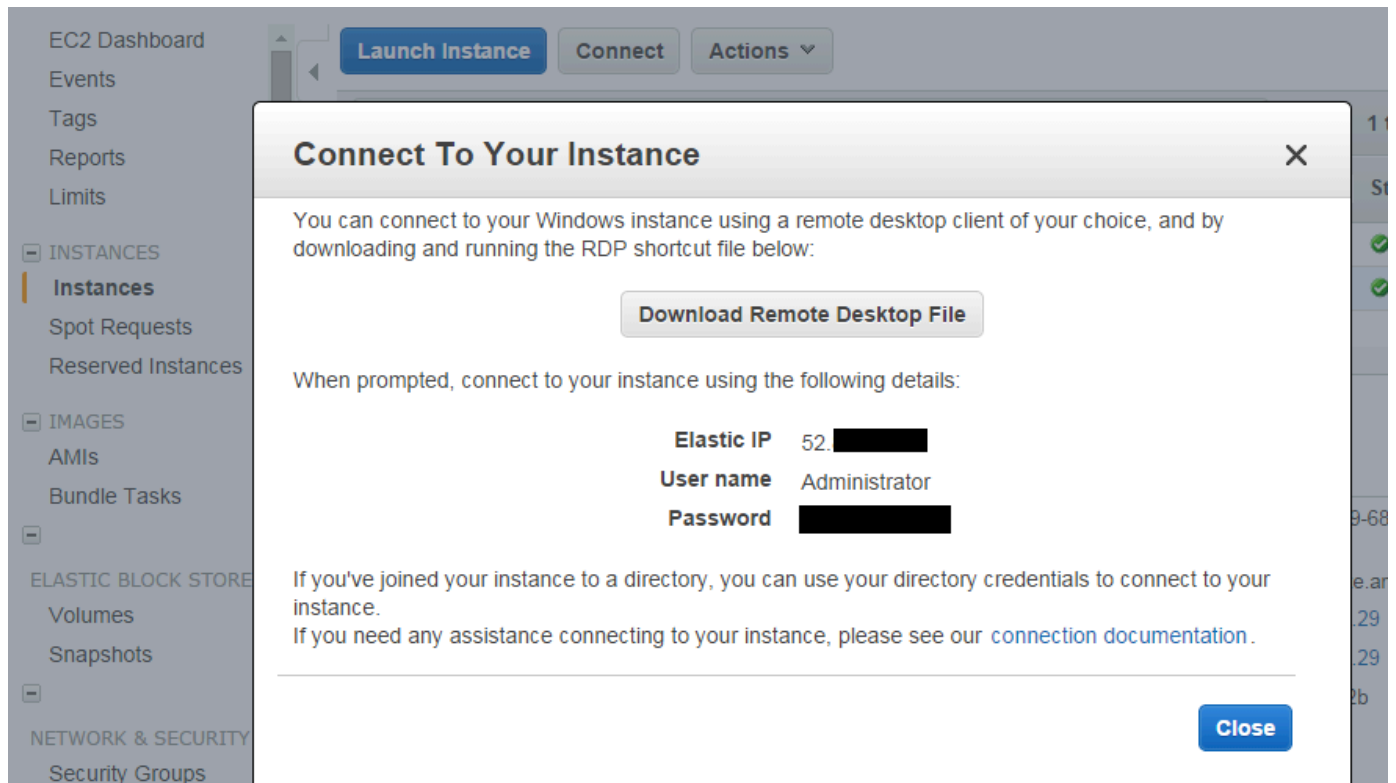




4. Ejecutamos el Paso 2, que es obtener el password para conectarnos a nuestro servidor. Para ello, pulsamos el botón “**GetPassword**” y se abrirá el siguiente cuadro de diálogo. Pulsamos el botón “**Seleccionar archivo**” para subir el archivo de claves **tunombre.pem** que guardamos en el apartado anterior. Una vez subido el archivo, pulsamos el botón “**Decrypt Password**”.

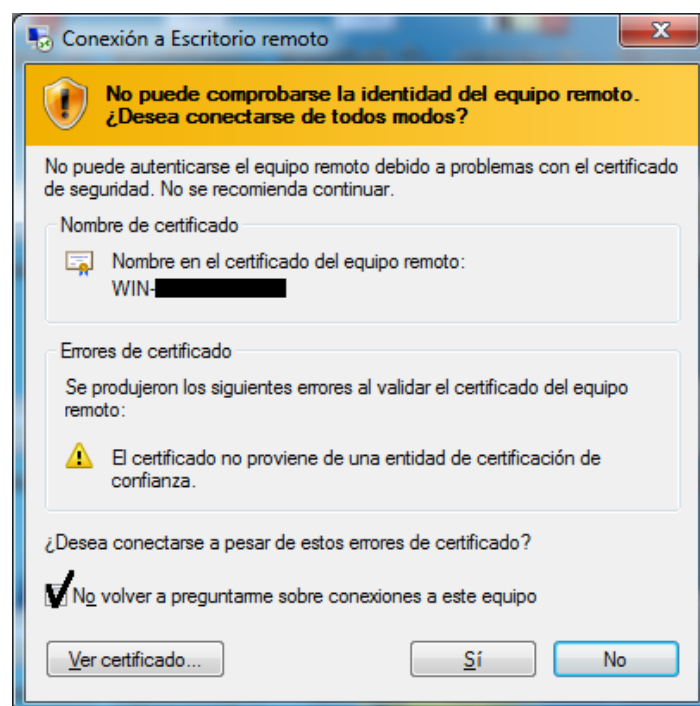


Una vez se ha desencriptado el password, nos muestra la siguiente pantalla con el password desencriptado



La apuntamos en un lugar seguro y ya hemos terminado todo el proceso.

Para conectarnos, basta hacer doble click sobre el archivo .RDP que guardamos en el punto 3 y nos saldrá el siguiente cuadro de diálogo de Conexión a Escritorio Remoto:



Pulsamos el checkbox “No volver a preguntarme...” y pulsamos el botón “Sí”. Inmediatamente te solicitará la contraseña de acceso que guardamos en el punto 4.

Si todo ha ido bien te mostrará una ventana con el escritorio de Windows de nuestro servidor remoto a similitud con la siguiente pantalla.