



**UNIVERSIDAD  
NACIONAL  
DE LA PLATA**

**Facultad de Informática - UNLP  
Cloud Computing y Cloud Robotics (00A22)  
Curso 2022 - Actividad N°1**

Grupo 14

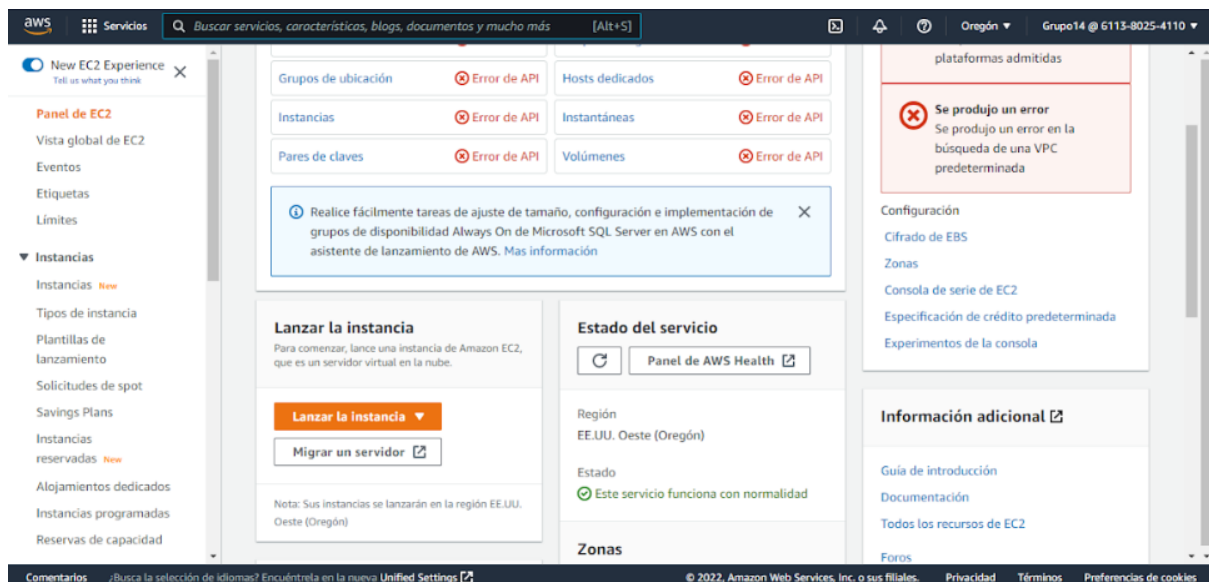
Alumnos: Stella Joaquín, Guerrero Nicolás

## Índice

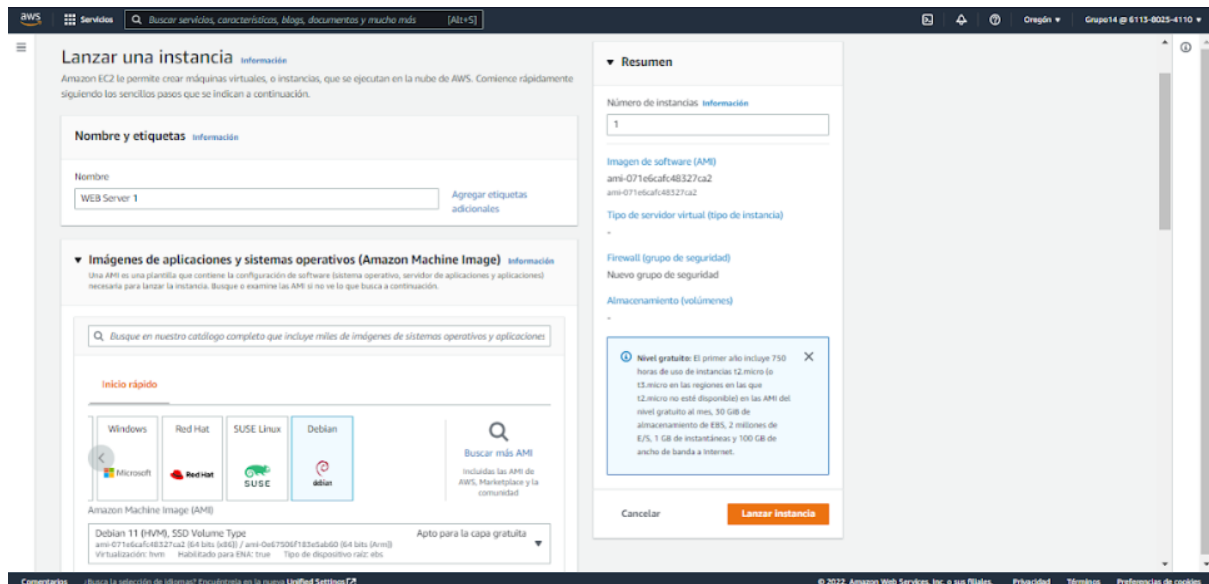
<b>1 - Lanzar instancia EC2 de AWS</b>	<b>3</b>
<b>2 - Realizar conexión SSH</b>	<b>7</b>
<b>3 - Configuración como “WEB Server 1”. Instalación y configuración de Apache</b>	<b>9</b>
<b>4 - Verificación de los tráficos configurados en el grupo de seguridad</b>	<b>10</b>
<b>5 - Reservación y asociación de una IP elástica</b>	<b>11</b>
<b>6 - Verificación de acceso vía navegador WEB con IP elástica</b>	<b>13</b>
<b>7 - Verificación de no pérdida de paquetes con el comando “ping” a la IP elástica</b>	<b>14</b>
<b>8 - Lanzamiento de nueva instancia AWS EC2</b>	<b>14</b>
<b>9 - Conexión y configuración del “WEB Server 2”</b>	<b>15</b>
<b>10 - Reasociación de la IP elástica con la instancia “WEB Server 2”</b>	<b>16</b>
<b>11 - Verificación de la no pérdida de paquetes por consola</b>	<b>17</b>
<b>12 - Verificación de acceso vía navegador WEB</b>	<b>17</b>
<b>13 - Liberar la IP elástica y “terminar” ambas instancias</b>	<b>18</b>
<b>Fuentes</b>	<b>19</b>

# 1 - Lanzar instancia EC2 de AWS

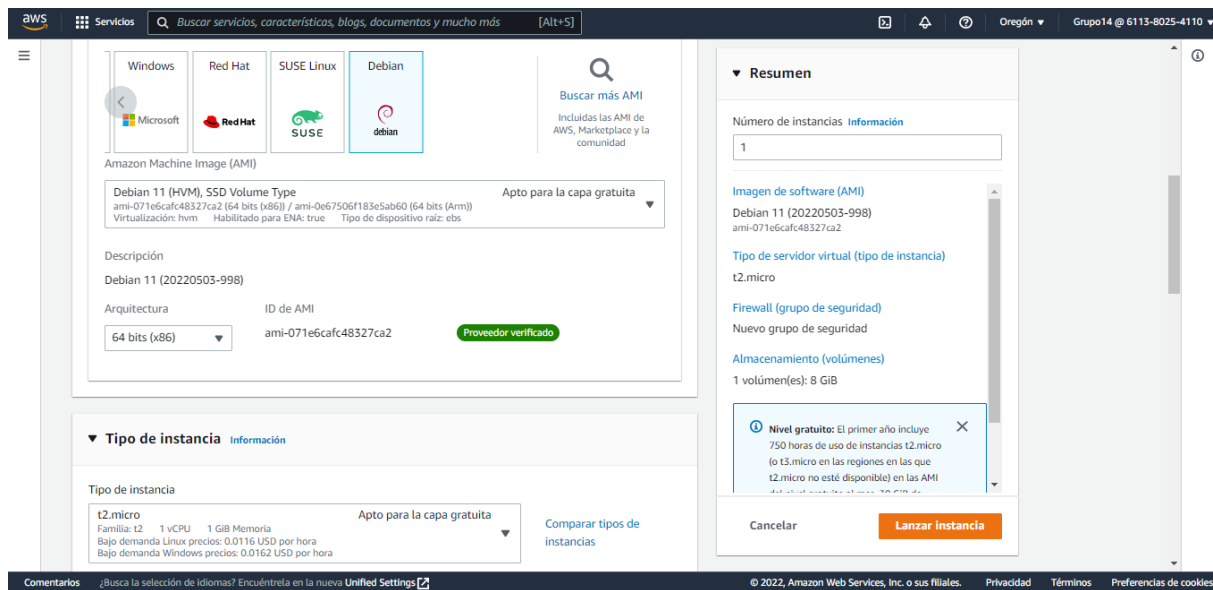
Utilizando el servicio “EC2” de AWS, se va al “Panel de EC2”. Una vez allí, se presiona “Lanzar la Instancia”, abajo a la izquierda del panel de Recursos.



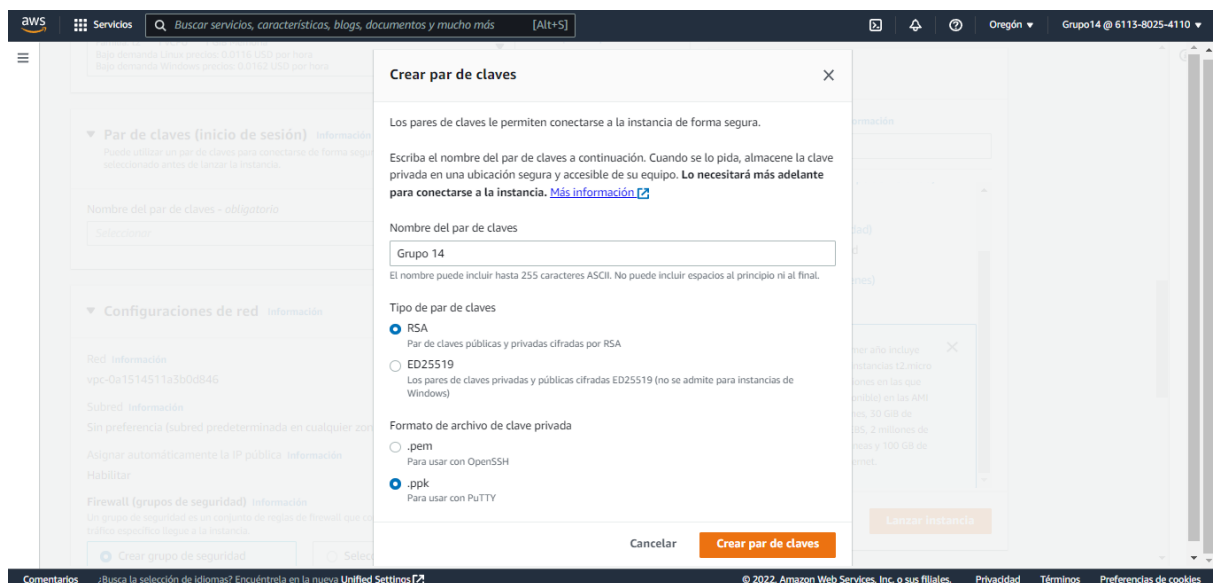
Aparecerá una serie de pasos a seguir para lanzar la instancia: elegiremos como nombre “WEB Server 1”, como AMI (Amazon Machine Image) se escogerá “Debian 11 Bullseye”, disponible para la capa gratuita, y se seleccionará trabajar con una instancia de 64 bits.



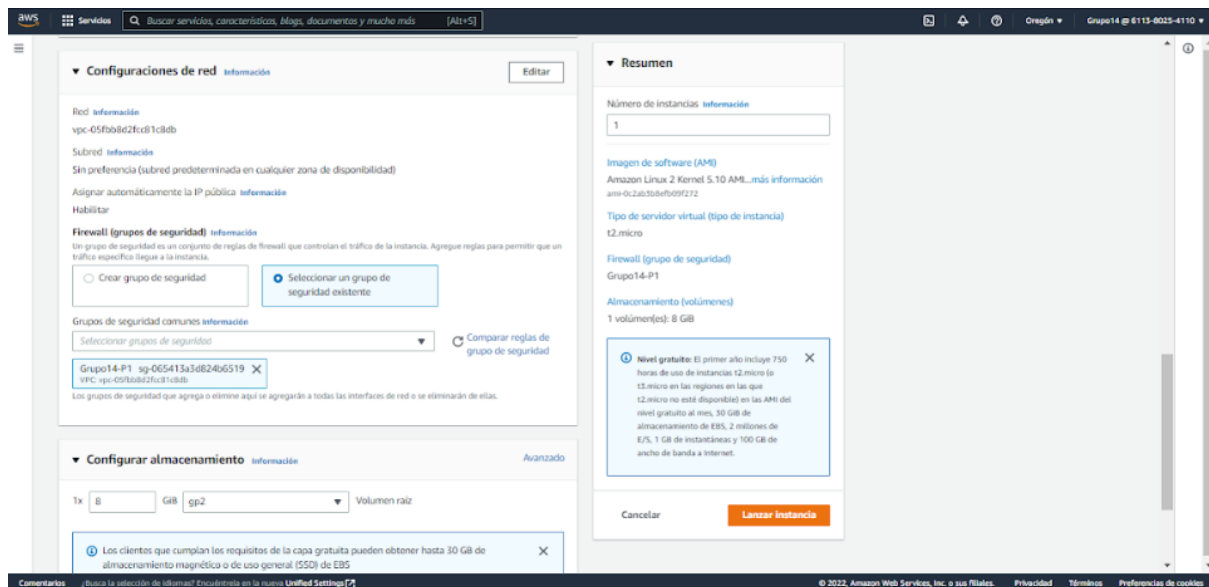
El tipo de instancia a escoger en este caso será el “t2.micro”, apto para la capa gratuita.



Para poder acceder remotamente a la terminal de la instancia, se necesitará un par de claves, las cuales se deben generar utilizando “Crear un nuevo par de claves”. Ya que se está trabajando sobre Windows, se utilizarán llaves del tipo RSA y de formato .ppk, aptas para ser utilizadas en la aplicación PuTTY, un cliente de SSH para ese sistema operativo. Se les da un nombre (“Grupo 14”) y se descarga la llave privada.

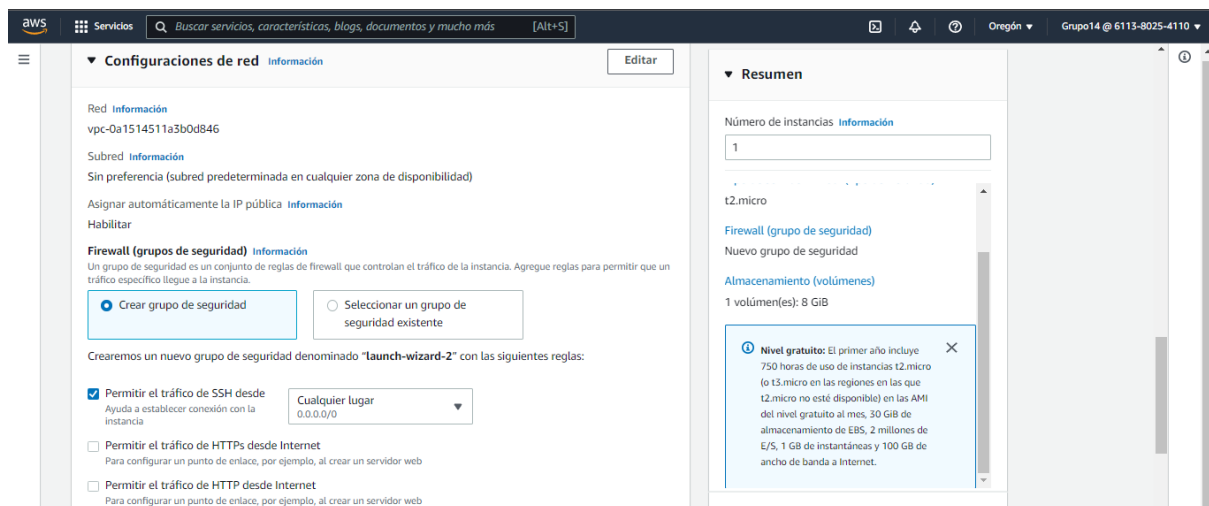


Al llegar al apartado “Configuraciones de red” se debe escoger un “grupo de seguridad”, que trabajará como un firewall definiendo las reglas de tráfico de entrada y salida a la instancia. Se selecciona un grupo de seguridad existente, ya que queremos tener un grupo de seguridad para aplicarlo en distintas instancias.



Para crear un grupo de seguridad, se siguen los siguientes pasos:

1. En el desplegable izquierdo, se va a la pestaña “Red y seguridad”, y se elige “Security Groups”
2. Se podrán ver los grupos de seguridad existentes, y estará la opción de crear uno nuevo, presionando “Crear grupo de seguridad”
3. Se le dará al grupo de seguridad un nombre, una breve descripción y a continuación se les dará las reglas de entrada y de salida
4. Finalizado esto, se hace clic en “Crear grupo de seguridad”, y pasa a estar disponible para aplicarse a instancias que creamos.



Configuramos el grupo de seguridad “Grupo14-P1” con las siguientes reglas:

Detalles Seguridad Redes Almacenamiento Comprobaciones de estado Monitoreo Etiquetas

▼ Detalles de seguridad

Rol de IAM ID de subred

sg-065413a3d824b6519 (Grupo14-P1)

▼ Reglas de entrada

ID de la regla del grupo d...	Intervalo de pu...	Protocolo	Origen	Grupos de seguridad
sgr-0663cfef6714b77ff	80	TCP	0.0.0.0/0	Grupo14-P1
sgr-0352deeca6b99e1fc	22	TCP	163.10.33.192/32	Grupo14-P1

▼ Reglas de salida

ID de la regla del grupo d...	Intervalo de pu...	Protocolo	Destino	Grupos de seguridad
sgr-0149c0ef44d289fad	Todo	ICMPV6	0.0.0.0/0	Grupo14-P1
sgr-0bc947fea0f9f1cef	Todo	ICMP	0.0.0.0/0	Grupo14-P1

## Grupos de seguridad

sg-065413a3d824b6519 (Grupo14-P1)

### ▼ Reglas de entrada

Filtrar reglas				
ID de la regla del grupo d...	Intervalo de pu...	Protocolo	Origen	Grupos de seguridad
sgr-0663cfef6714b77ff	80	TCP	0.0.0.0/0	Grupo14-P1
sgr-0352deeca6b99e1fc	22	TCP	163.10.33.192/32	Grupo14-P1

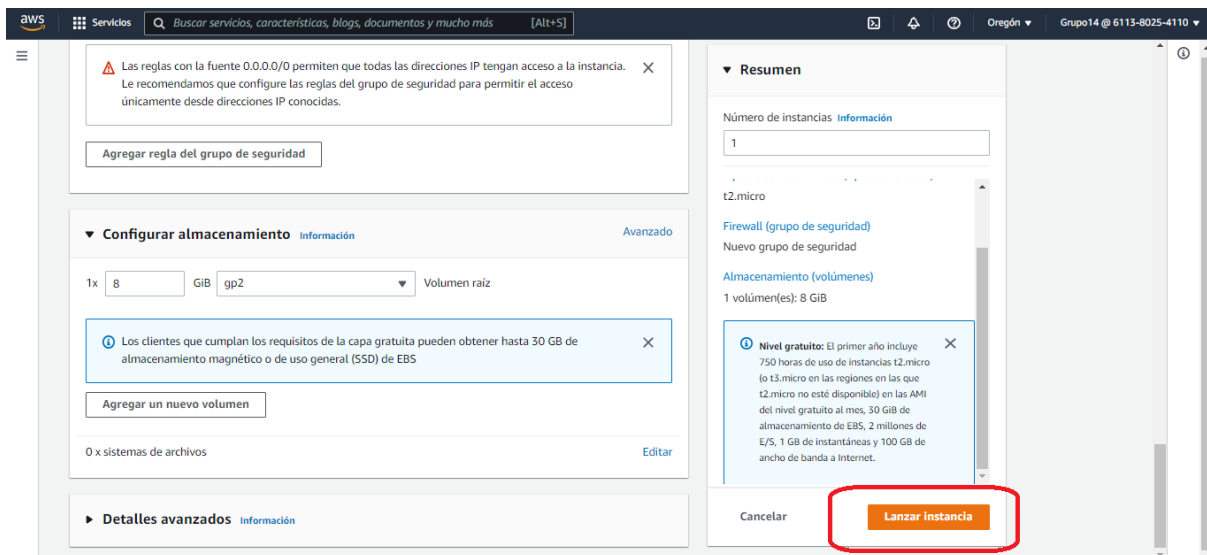
### ▼ Reglas de salida

Filtrar reglas				
ID de la regla del grupo d...	Intervalo de pu...	Protocolo	Destino	Grupos de seguridad
sgr-0149c0ef44d289fad	Todo	ICMPV6	0.0.0.0/0	Grupo14-P1
sgr-0bc947fea0f9f1cef	Todo	ICMP	0.0.0.0/0	Grupo14-P1

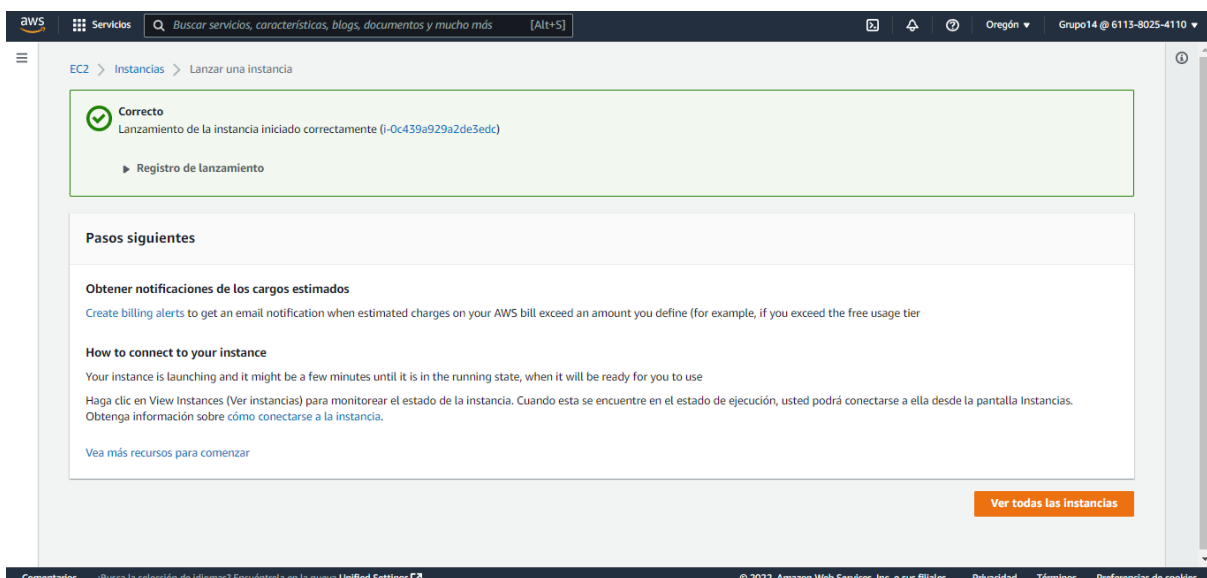
Teniendo ya listo nuestro grupo de seguridad, lo buscamos en el apartado “Grupos de seguridad comunes” y lo asignamos.

En “Configurar almacenamiento” le damos a la instancia 8 GiB de almacenamiento con gp2 (es decir, un disco de estado sólido de uso general). El límite para la capa gratuita es de 30 GiB de EBS.(Elastic Block Store, utilizado para instancias en vez de objetos).

Elegimos en “Resumen” lanzar una única (1) instancia con esta configuración y le damos a “Lanzar instancia”.



A continuación, veremos que nos informa de que la instancia se ha iniciado con éxito.



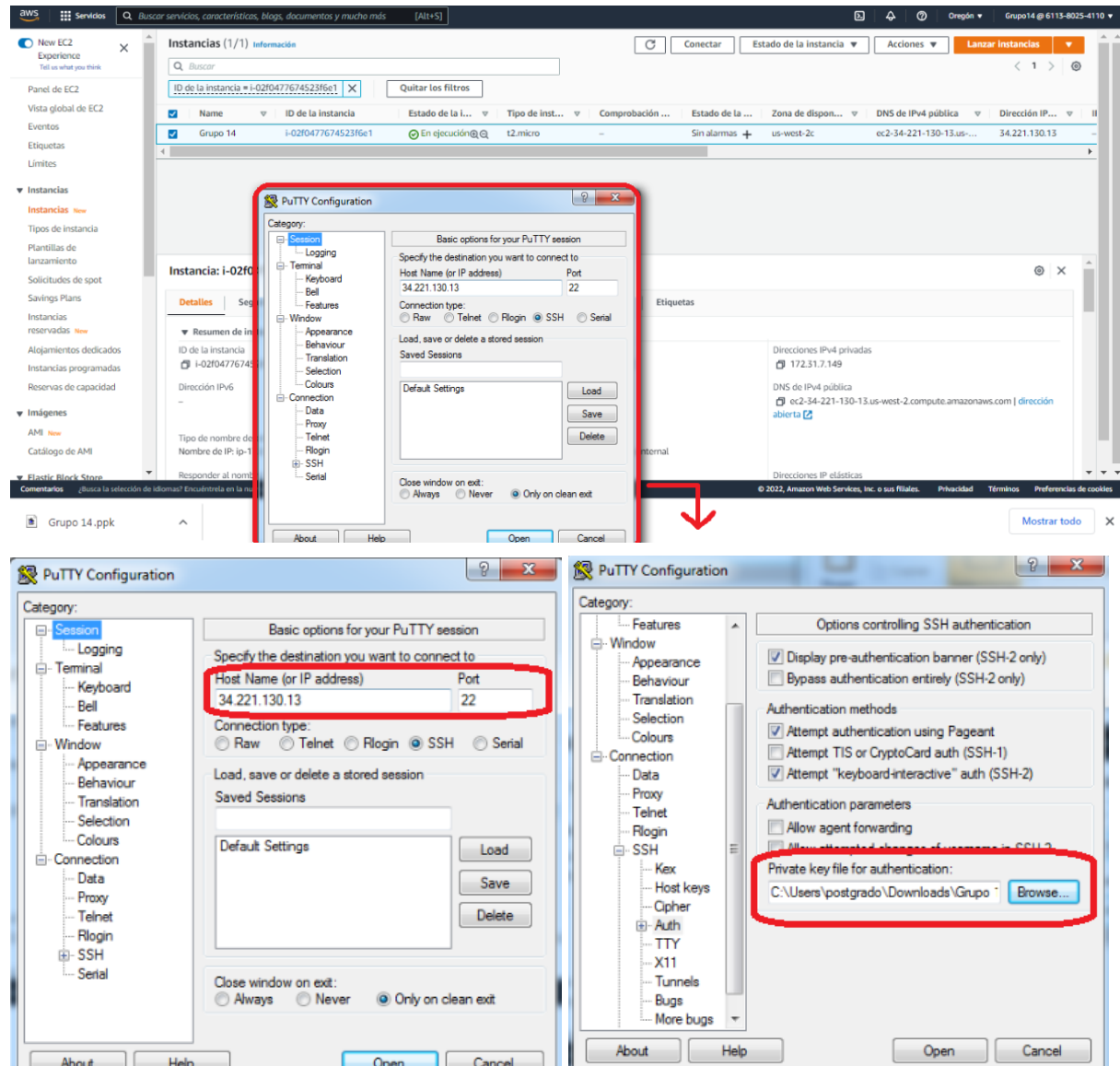
## 2 - Realizar conexión SSH

Para poder realizar la vinculación entre la instancia creada y nuestra computadora personal, se utiliza una comunicación por protocolo SSH ( Secure SHell), haciendo uso del par de llaves generadas durante la creación de la instancia.

Como estamos trabajando en un sistema operativo Windows, se hace uso del programa PuTTY, un cliente telnet para utilizar SSH. Al ingresar en PuTTY se nos solicitará la IP del destino al que quiero conectarme ("Host name (or address IP)", junto con el puerto de conexión.

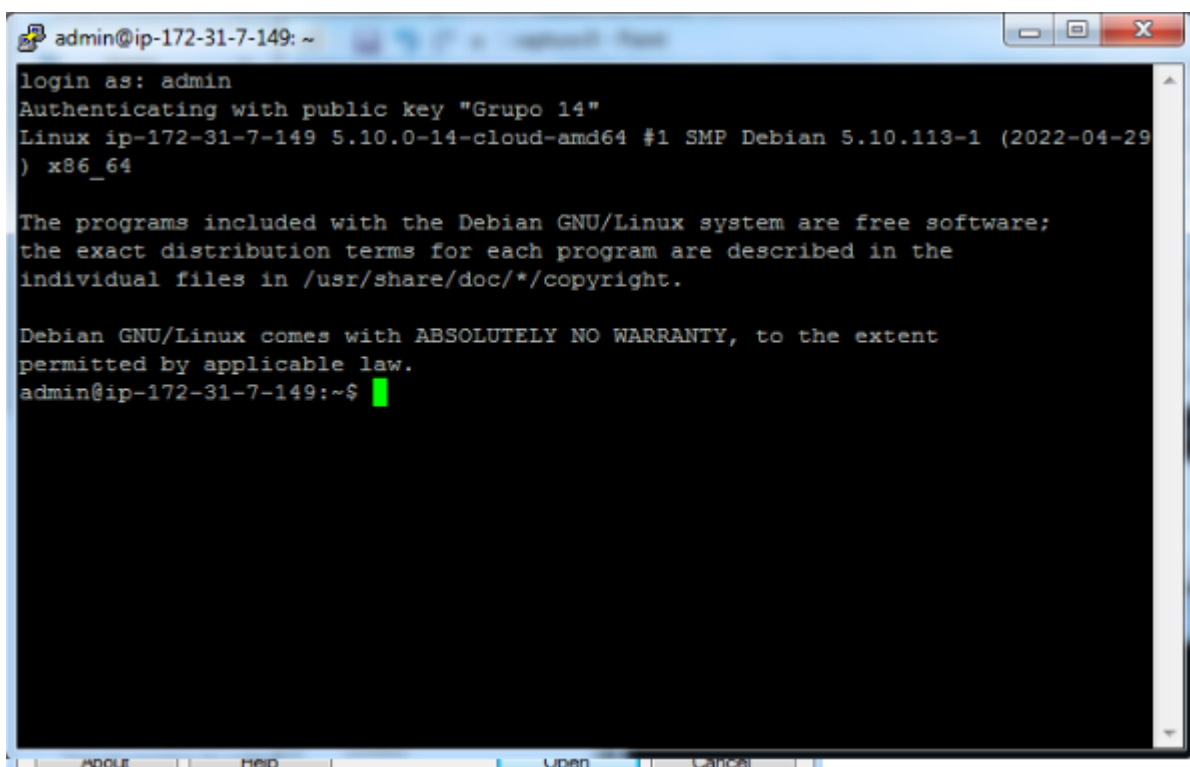
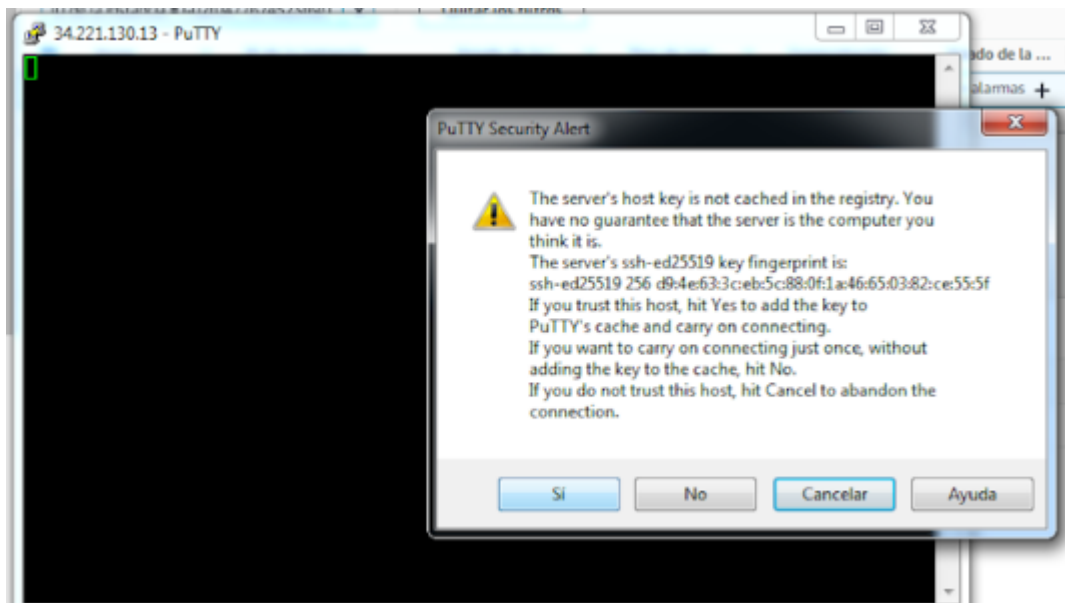
La IP a ingresar será la IP pública de la instancia, que puede encontrarse en la consola de AWS yendo a "EC2>Instancias". Allí, podremos ver información básica de cada instancia en ejecución (o recientemente terminada). Seleccionamos la instancia "WEB Server 1" y copiamos su IP pública.

Ingresamos la IP en PuTTY y después nos movemos por el menú cascada a la izquierda hasta “Connection>SSH>Auth”. Nos pedirá la llave privada, por lo que ingresamos el directorio en el que se encuentra el archivo que descargamos al crear el par de llaves.



Hacemos clic en “Open” y nos aparecerá una terminal, que nos pedirá un nombre de usuario. Le ingresamos el nombre “admin”, ante lo cual se nos darán permisos de administrador en la instancia y podremos ver la terminal Bash de la instancia Debian.





### 3 - Configuración como "WEB Server 1". Instalación y configuración de Apache

Haciendo uso de estos permisos sobre el sistema, actualizamos la lista de repositorios disponibles para instalar con el comando "sudo apt-get update". Después, instalamos Apache2 con el comando "sudo apt-get install apache2". Le decimos al instalador que queremos instalar el paquete con "Y".

Una vez instalado apache, se cambia de lugar el directorio “DocumentRoot”, y se crea el archivo “index.html” dándole como contenido:

```
<head>
  <!DOCTYPE html>
  <html>
    <title> WEB Server 1 </title>
    <meta charset="UTF-8">
</head>
<body>
  <h1>WEB Server 1 - Grupo 14</h1>
</body>
<script>
  (function(){
    var fecha = new Date();
    document.write(fecha);
  })
</script>
</html>
```

## 4 - Verificación de los tráficos configurados en el grupo de seguridad

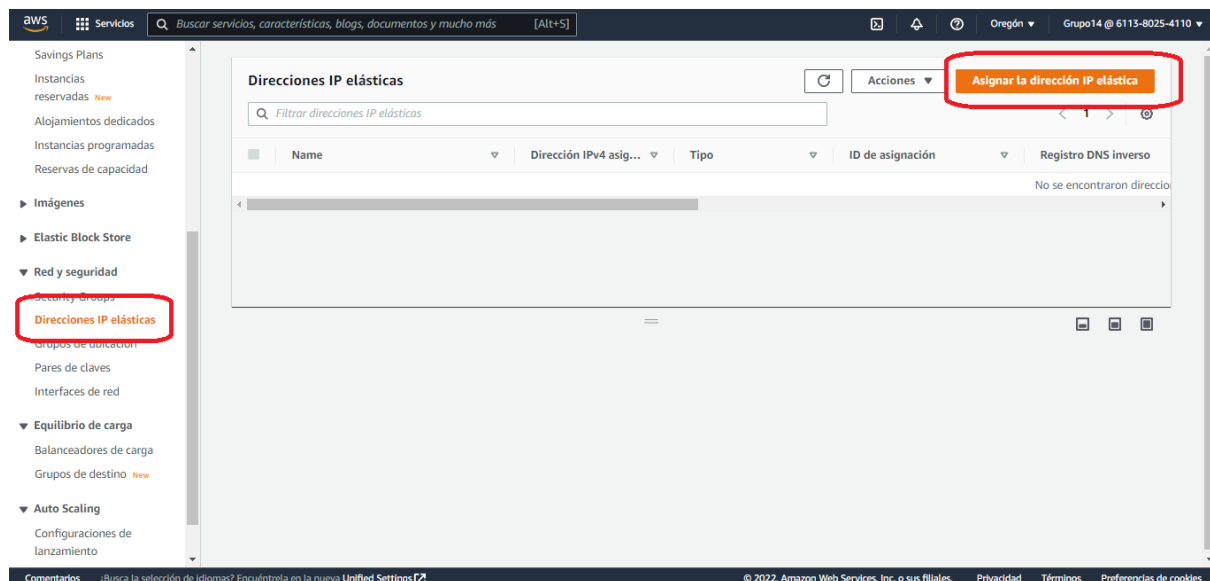
1. Verificando el tráfico en el port TCP 80 (HTTP): bastará con ingresar la dirección IP pública de la instancia agregando un “:80” para indicar que se quiere acceder al puerto 80. Se podrá ver la página html que ingresamos en el directorio “DocumentRoot” en el paso anterior, con título “WEB Server 1” y mostrando la fecha y la hora.



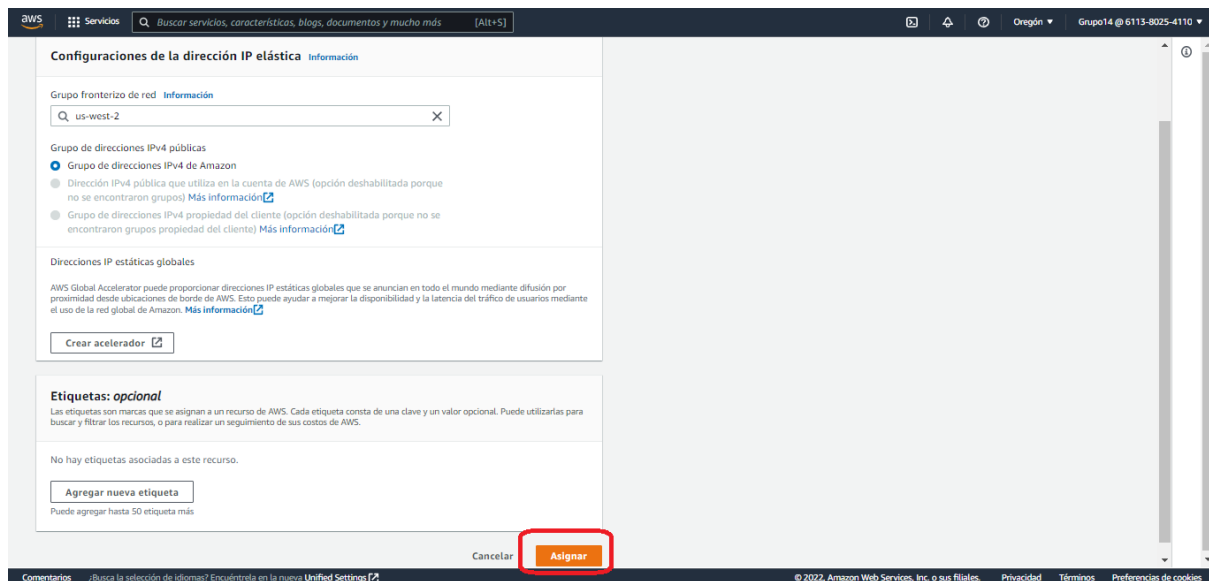
2. Verificando el tráfico en el port TCP 22 (SSH): dado que es el puerto que se utiliza para establecer la conexión SSH y poder utilizar la terminal Bash, ya se ha comprobado que está funcionando correctamente.
3. Verificando tráfico ICMP: para esto, se aplicará desde la terminal "CMD" de Windows un comando "ping", que enviará un paquete ICMP a la dirección que especifiquemos (en este caso, la IP pública de la instancia). Se podrá visualizar en la terminal como los paquetes son enviados y regresan, sin que se produzcan pérdidas.

## 5 - Reservación y asociación de una IP elástica

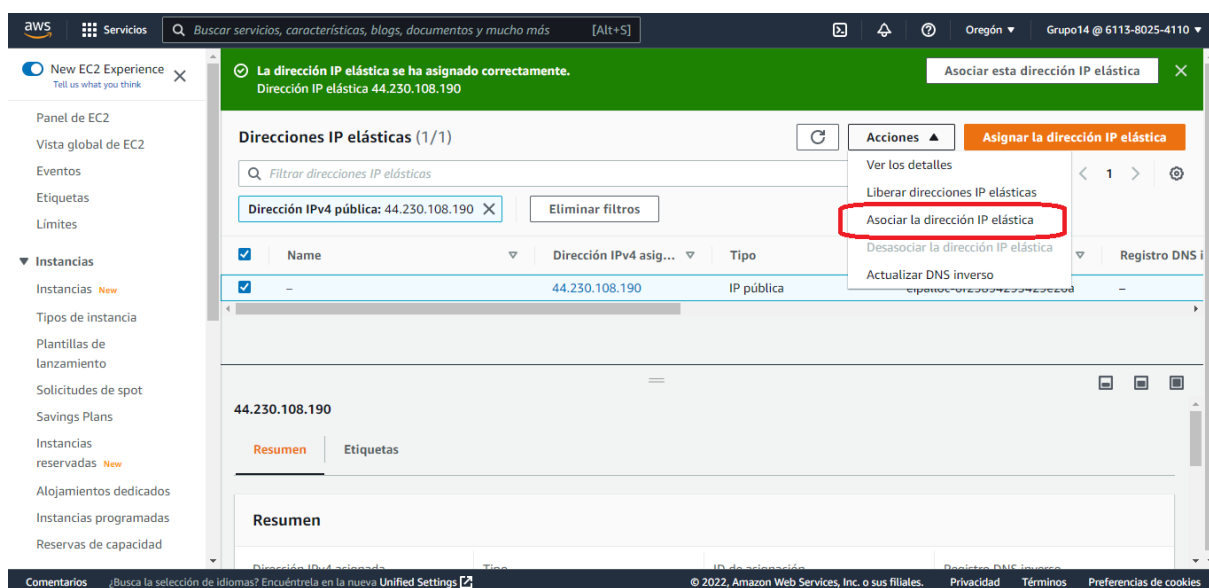
Para asociar una IP elástica a nuestra instancia "WEB Server 1", se deberá ir a la consola de AWS, "EC2>Red y seguridad>Direcciones IP elásticas". Se podrán ver las direcciones actualmente en uso, y estará la opción de asignar una nueva IP elástica seleccionando "Asignar la dirección IP elástica". Se pueden utilizar hasta 3 IP elásticas en la capa gratuita sin costo adicional.



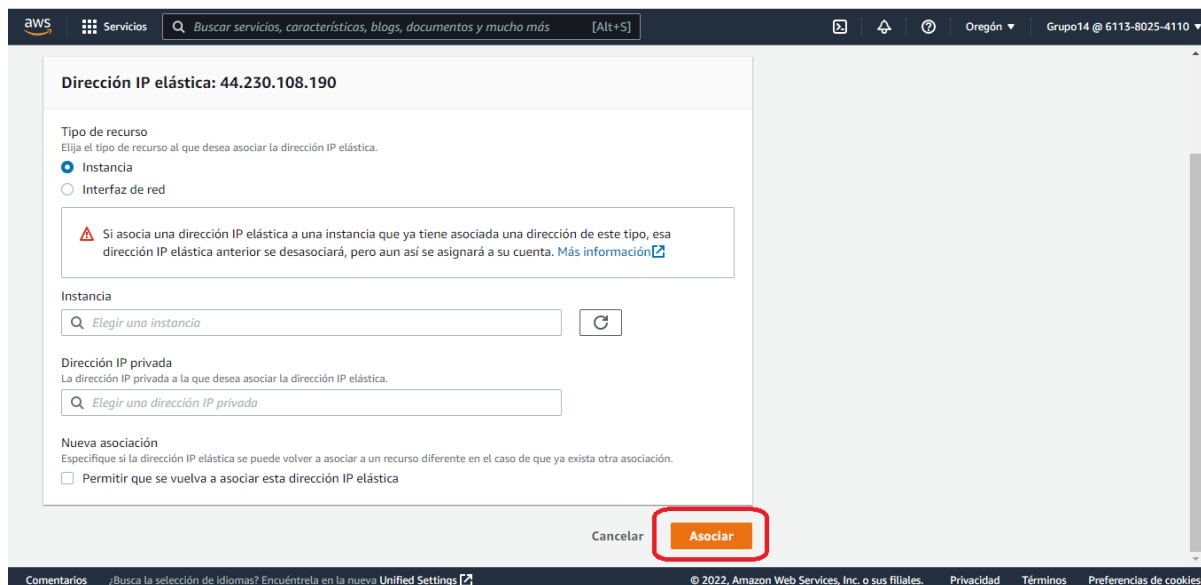
Aparecerá un menú, y nos limitaremos a terminar el proceso haciendo clic en "Asignar".



A continuación, marcaremos nuestra IP elástica y en “Acciones” elegiremos “Asociar la dirección IP elástica”.



En el menú se nos mostrará la IP en cuestión y se nos permitirá buscar nuestra instancia, para después asociarla presionando “Asociar”.



**Dirección IP elástica: 44.230.108.190**

Tipo de recurso  
Elija el tipo de recurso al que desea asociar la dirección IP elástica.

☒ Instancia  
☐ Interfaz de red

⚠ Si asocia una dirección IP elástica a una instancia que ya tiene asociada una dirección de este tipo, esa dirección IP elástica anterior se desasociará, pero aun así se asignará a su cuenta. [Más información](#)

Instancia

Dirección IP privada  
La dirección IP privada a la que desea asociar la dirección IP elástica.

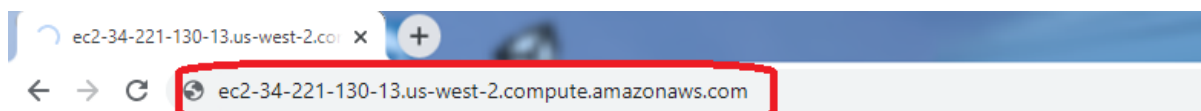
Nueva asociación  
Especifique si la dirección IP elástica se puede volver a asociar a un recurso diferente en el caso de que ya exista otra asociación.  
☐ Permitir que se vuelva a asociar esta dirección IP elástica

Cancelar **Asociar**

En el panel de instancias, podremos comprobar que ahora el campo “Direcciones IP elásticas” correspondiente a nuestra instancia lleva la IP elástica que le asociamos.

## 6 - Verificación de acceso vía navegador WEB con IP elástica

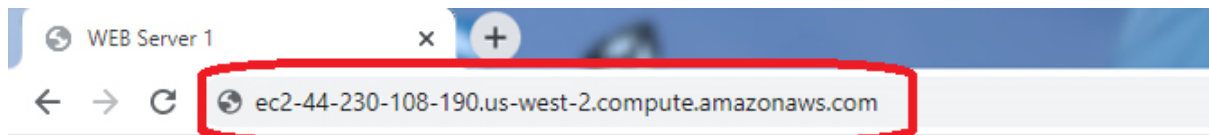
Ahora que nuestra instancia está asociada a una IP elástica, veremos que al querer acceder al DNS de la IP pública utilizada en los pasos anteriores no la encontraremos disponible.



### No se puede acceder a este sitio web

La página **ec2-34-221-130-13.us-west-2.compute.amazonaws.com** ha tardado demasiado tiempo en responder.

Sin embargo, ingresando con la IP elástica veremos la misma página que estaba visible para la conexión con el puerto 80:



## WEB Server 1 - Grupo 14

Wed Sep 7 2022 19:22:56 GMT-0300 (hora estándar de Argentina)

### 7 - Verificación de no pérdida de paquetes con el comando “ping” a la IP elástica

Abriendo la consola, y aplicando el comando “ping” a la IP elástica, veremos que no se produce pérdida de paquetes.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\postgrado>ping 44.230.108.190

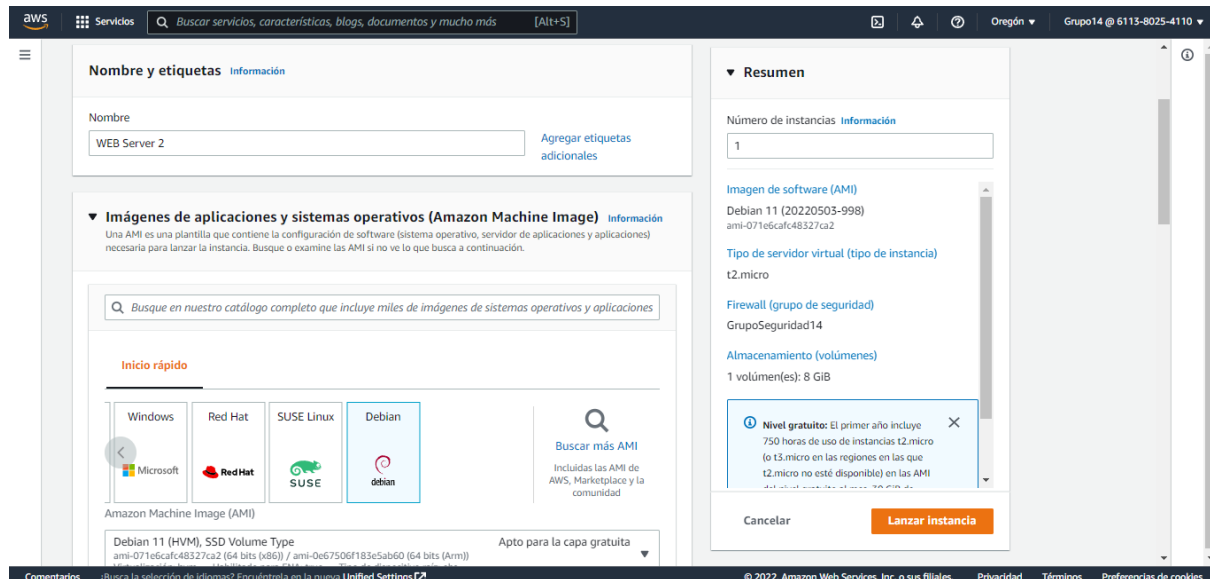
Haciendo ping a 44.230.108.190 con 32 bytes de datos:
Respuesta desde 44.230.108.190: bytes=32 tiempo=156ms TTL=29
Respuesta desde 44.230.108.190: bytes=32 tiempo=156ms TTL=29
Respuesta desde 44.230.108.190: bytes=32 tiempo=156ms TTL=29
Respuesta desde 44.230.108.190: bytes=32 tiempo=156ms TTL=29

Estadísticas de ping para 44.230.108.190:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 156ms, Máximo = 156ms, Media = 156ms

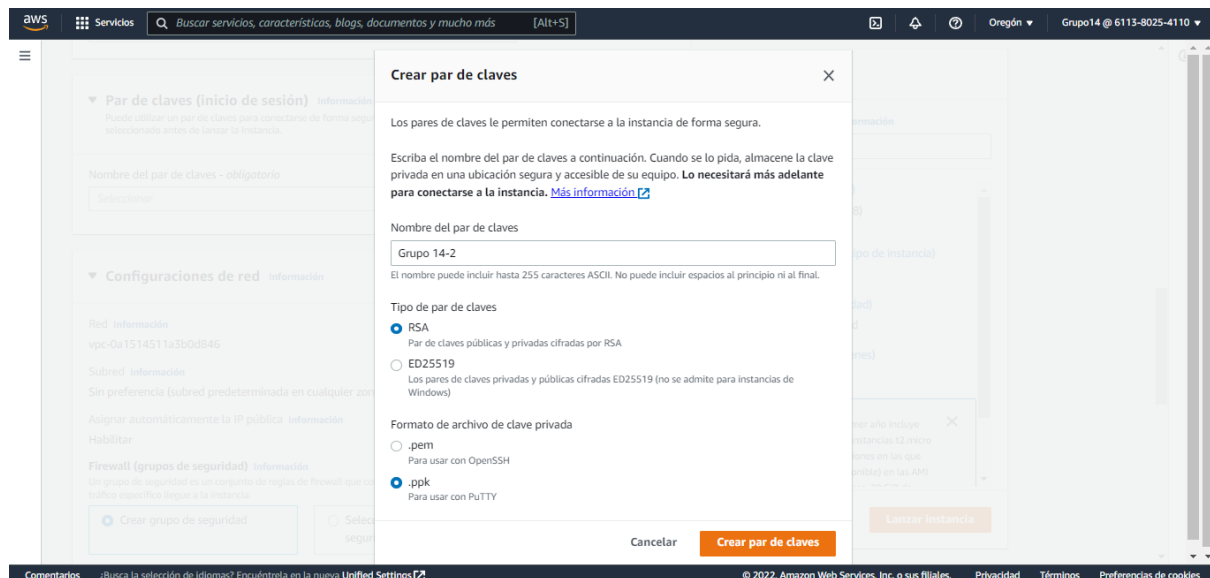
C:\Users\postgrado>
```

### 8 - Lanzamiento de nueva instancia AWS EC2

Para lanzar una nueva instancia, se vuelve al “Panel de EC2”, elige “Lanza la instancia”, y se realiza el mismo proceso visto para lanzar la instancia “Web Server 1”, pero dándole el título “WEB Server 2”. Se lo configura como “t2.micro” y con AMI “Debian 11 Bullseye”.



Se crea un nuevo par de llaves RSA en formato .ppk (“Grupo 14-2”, ya que el anterior se llamaba “Grupo 14”).



El grupo de seguridad a escoger es el que creamos anteriormente (“Grupo14-P1”). Lanzamos la instancia con “Lanzar instancia”.

## 9 - Conexión y configuración del “WEB Server 2”

1. Conexión: Para poder acceder con SSH a la instancia, se sigue el mismo procedimiento que con la otra instancia, pero ingresando en PuTTY su dirección IP pública. En “Connection>SSH>Auth” se aplicará la nueva llave privada, y se

presiona "Open". Se nos pide el nombre "admin" y se nos da acceso a la terminal Bash de la instancia.

2. Configuración: instalamos Apache2 con el mismo procedimiento y agregamos un "index.html" al DocumentRoot, pero esta vez le damos como título a la página "WEB Server 2".

Verificamos la conexión con la instancia por el puerto 80 ingresando la IP pública seguida de ":80", tras lo cuál veremos la página HTML que creamos con la fecha y la hora, pero con título "WEB Server 2".

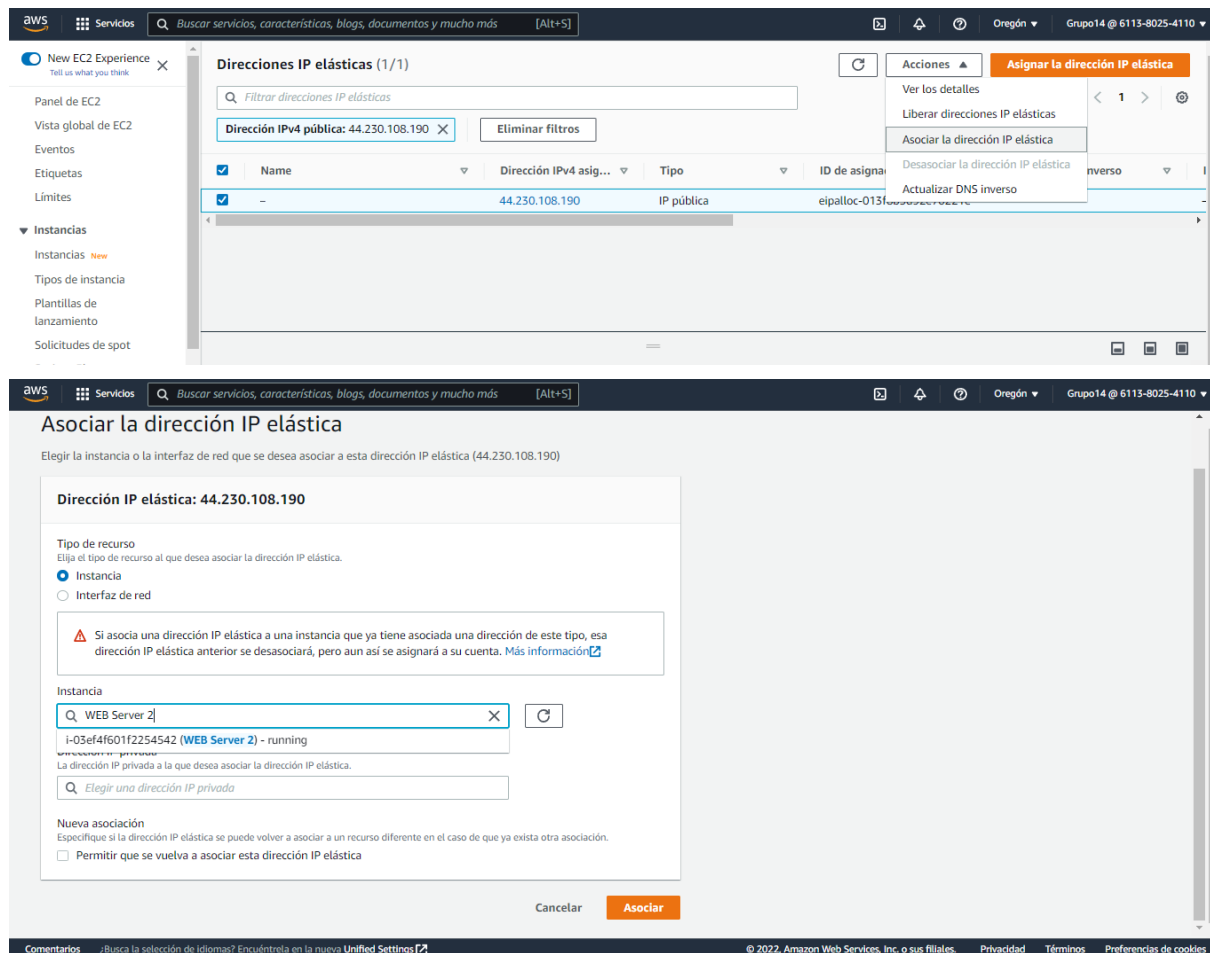


## 10 - Reasociación de la IP elástica con la instancia "WEB Server 2"

Para realizar el cambio, vamos a "EC2>Redes y Seguridad>Direcciones IP elásticas". Seleccionamos la IP elástica que creamos, vamos a "Acciones" y elegimos "Disasociar la dirección IP elástica". Podemos comprobar que el id al que está asociada la IP elástica es el mismo que el de la instancia "WEB Server 1", por lo que aplicamos "Desasociar" y esta deja de tener la IP elástica, sino que solo dispone de una IP pública.

Ahora, la IP elástica estará disponible, por lo que vamos a "Acciones" y a "Asociar la dirección IP elástica", eligiendo "WEB Server 2".





## 11 - Verificación de la no pérdida de paquetes por consola

Una vez asociamos la IP elástica a la nueva instancia, vamos a la terminal de Windows “CMD” y utilizamos el comando “ping” dirigiendo los paquetes ICMP hacia la IP elástica. Podremos comprobar que no se pierden paquetes, sino que todos regresan.

## 12 - Verificación de acceso vía navegador WEB

Actualizando la página con el DNS de la IP elástica, podremos observar que el título de la página cambió: en vez de decir “WEB Server 1”, se verá “WEB Server 2”. Además, nos mostrará la fecha y la hora.

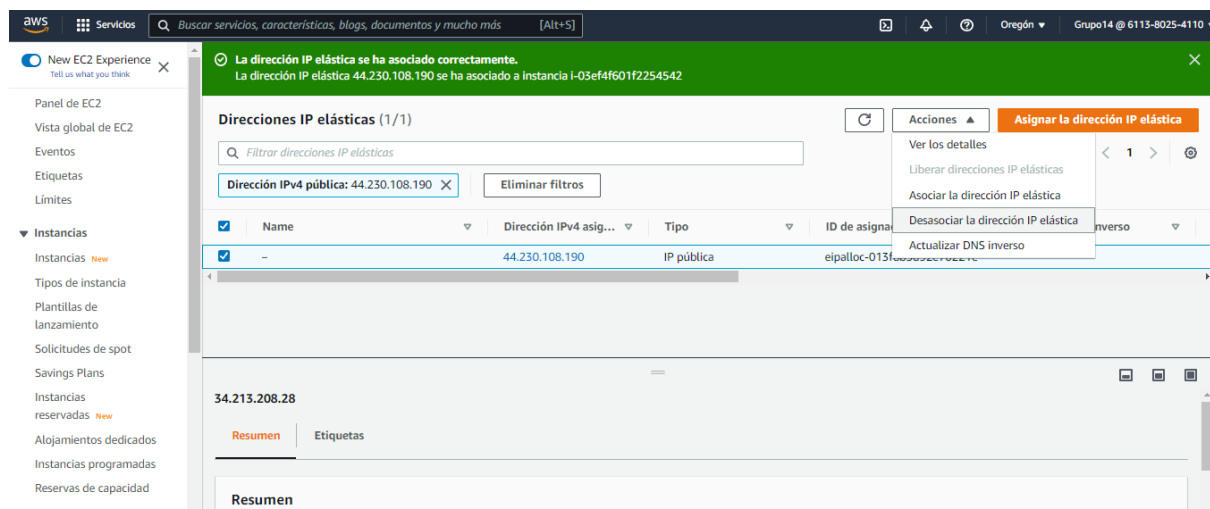


## WEB Server 2 - Grupo 14

Wed Sep 7 2022 19:45:11 GMT-0300 (hora estándar de Argentina)

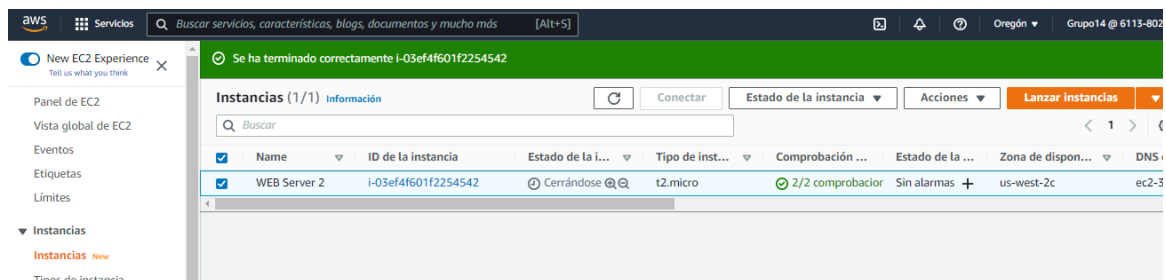
### 13 - Liberar la IP elástica y “terminar” ambas instancias

Finalmente, vamos nuevamente a “EC2>Direcciones IP elásticas” y en “Acciones” elegimos “Disasociar la IP elástica”. Esta vez, veremos que el id de instancia en el menú será el de la instancia “WEB Server 2”. Seleccionamos “Disasociar”.





Después, volvemos a “Acciones” y elegimos “Liberar direcciones IP elásticas”. Para terminar las instancias, vamos a “EC2>Instancias”, elegimos una instancia y en “Estado de la instancia” hacemos clic en “Terminar instancia”. Repetimos esto en ambas instancias. Tras esto, las terminales por las cuales nos comunicamos a las instancias se congelarán, ya que las instancias dejaron de estar disponibles. Veremos en “Instancias” que el estado cambió a “Cerrándose”, y luego “Terminada”.



## Fuentes

- Recursos disponibles en la capa gratuita de Amazon:  
<https://aws.amazon.com/es/free/>
- Más información sobre los Elastic Block Store (EBS) de Amazon:  
[https://docs.aws.amazon.com/es\\_es/AWSEC2/latest/UserGuide/AmazonEBS.html](https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/AmazonEBS.html)
- Cómo conocer la propia IP en Windows:  
<https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig>
- Usar llaves SSH en Windows con PuTTY:  
<https://devops.ionos.com/tutorials/use-ssh-keys-with-putty-on-windows/>
- Modificar directorio “DocumentRoot”:  
<https://hazlolinux.com/apache/como-cambiar-el-directorio-predeterminado-de-apache-documentroot-en-linux/>