IES gRAN CAPITÁN



2º FPGS ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED

IMPLANTACIÓN DE APLICACIONES WEB

iaw

# 4.5 Finalizar escenario cluster web

 Otero Gómez, Manuela

2º ASIR

IAW

15.02.2023

Tabla de contenidos

[1. Alta seguridad 4](#_Toc1)

[2. Alto rendimiento 5](#_Toc2)

[3. Alta disponibilidad 6](#_Toc3)

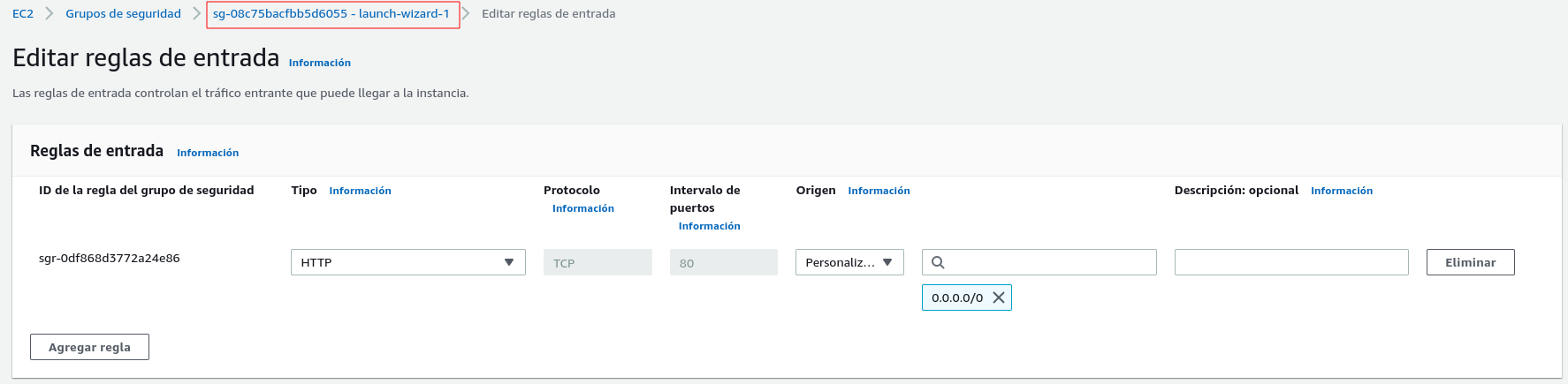
[4. Escalabilidad horizontal y vertical 6](#_Toc4)

# 1. Alta seguridad

Sobre el escenario de las prácticas anteriores, hacemos un resumen de qué políticas de seguridad se han tomado y cómo queda el escenario (todas las instancias están en la misma VPC):

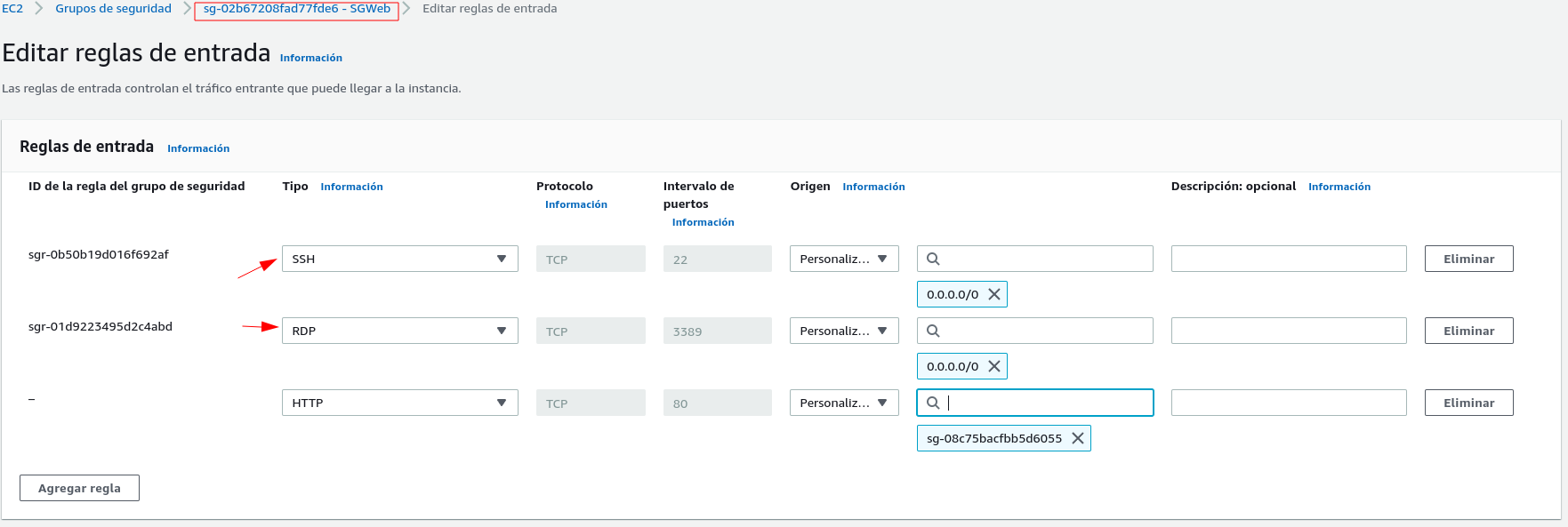
Por un lado tenemos la seguridad en la infraestructura montada: desde el exterior solo se puede acceder al proxy que será el que redirija el tráfico hacia las instancias del *back-end*:

Tenemos en las instancias de tipo EC2 dos grupos de seguridad independientes: el grupo al que pertenece solo la instancia del proxy (launch-wizard-1) tiene las siguientes reglas



Como hemos dicho, solo se puede acceder por el puerto 80 (http) desde cualquier IP.

Todas las instancias EC2, incluida la máquina de Windows que usamos para la administración de la base de datos y será temporal, están en otro grupo llamado SGWeb con las siguientes reglas:

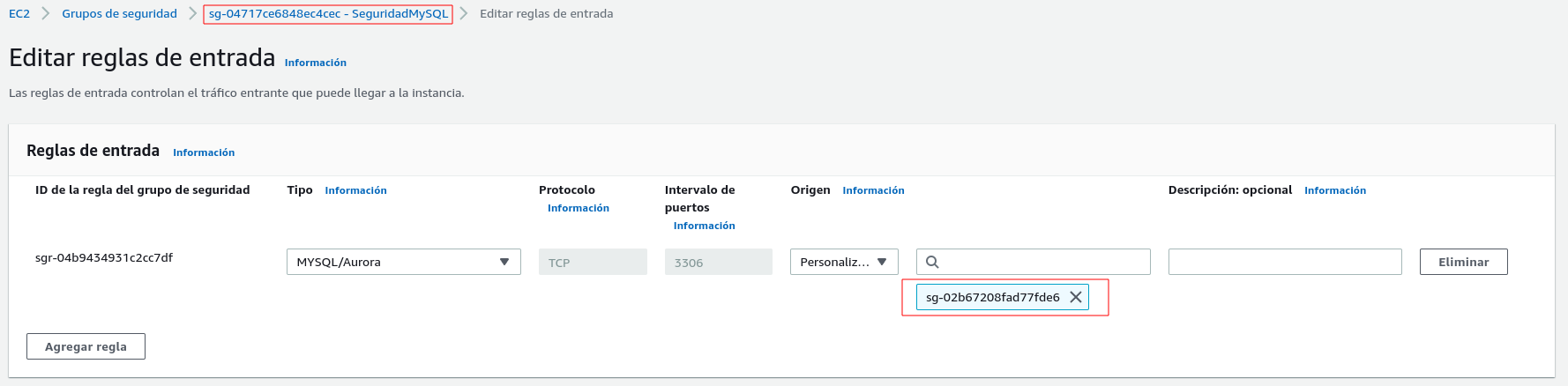


La regla del SSH que permite el trafico desde cualquier origen está solo para la administración de las instancias. Se eliminará al terminal el despliegue.

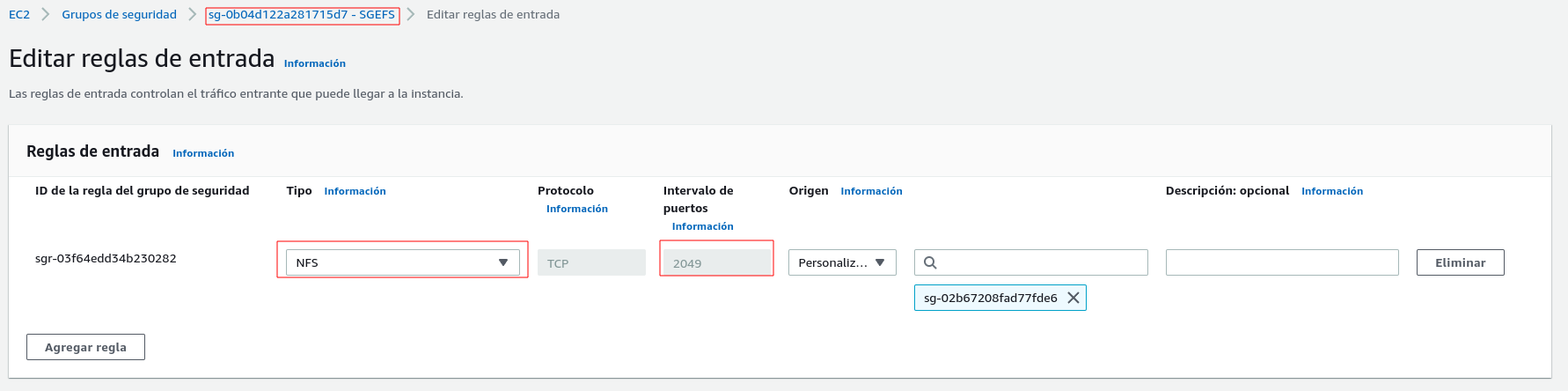
Lo mismo ocurrirá con la regla del RDP, el escritorio remoto de Windows, que se creó para poder conectarnos a la EC2 con Windows Server pero que se eliminará cuando esta instancia también lo haga.

Por último, la regla de HTTP permite la entrada solo desde el grupo de seguridad launch-wizzard-1 al que pertenece el proxi, es decir, solo podrán acceder a estas instancias las conexiones por el puerto 80 que vengan desde el la instancia Proxy.

Hay un grupo de seguridad exclusivo para la base de datos que solo tiene una regla que permite el acceso desde el grupo de seguridad SGWeb, es decir. A la base de datos solo podrán acceder las IPs de los apaches que a su vez vienen redirigidas por el proxy aportando así una capa más de filtrado:

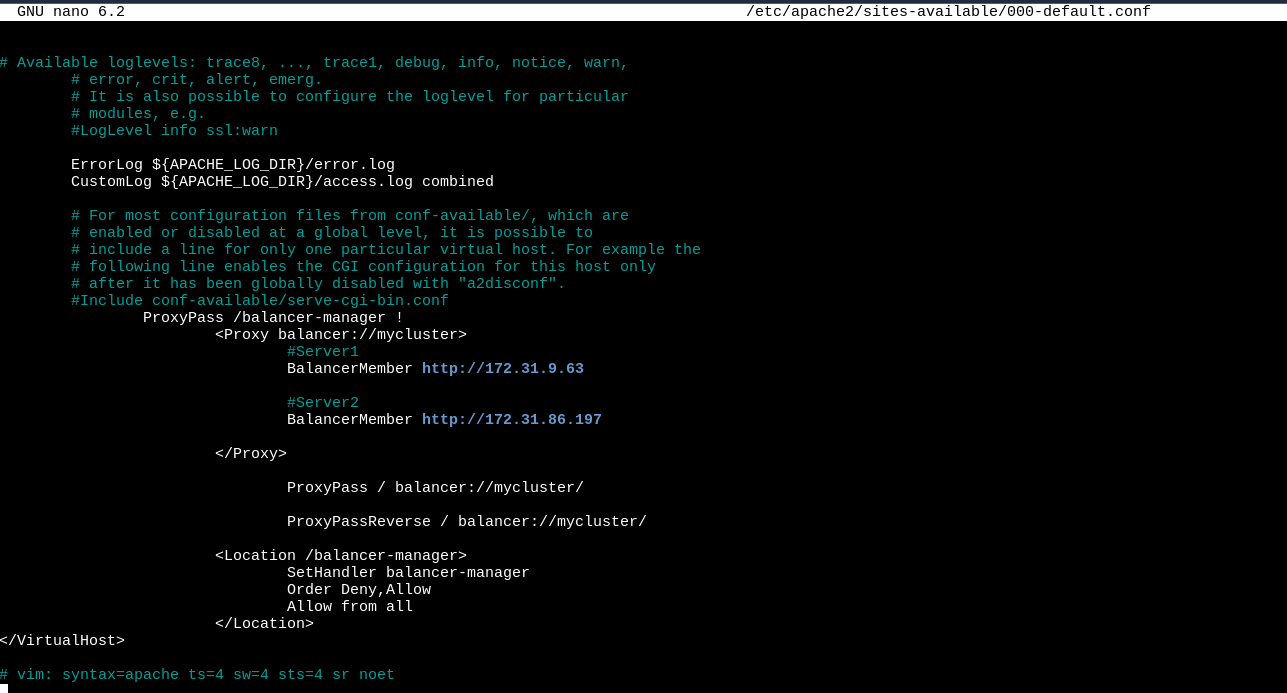


Por último tenemos el grupo de seguridad del almacenamiento EFS. A él solo pueden acceder las máquinas de Apache que tienen montado el directorio efs\_mount donde se almacenan todos los archivos que dan forma a la página web. El puerto es el predeterminado para este tipo de conexión.



# 2. Alto rendimiento

El alto rendimiento se consigue gracias a la duplicidad de las instancias EC2 que proporcionan el servicio web de Apache corriendo sobre un Sistema Operativo Amazon Linux. Estas instancias están conectadas a un servicio de almacenamiento EFS. Además el proxi tiene balanceador de carga, por lo que al aumentar el número de peticiones, estas se van a repartir entre ambas instancias de manera transparente al usuario. La configuración del proxy es la siguiente:



En esta configuración, el cuello de botella lo haría el proxy, que es una sola instancia de Ubuntu Server que tendría que gestionar, redirigir y balancear todas las peticiones hacia las máquinas del *back-end*.

# 3. Alta disponibilidad

En este despliegue tenemos duplicidad tanto en los servidores web con las dos instancias EC2 de Amazon Linux mencionadas antes como en dos instancias de bases de datos RDS configuradas en cluster como se explicó en la práctica anterior. Las instancias multi A-Z se encuentran además en zonas diferentes, por lo que si hay un problema físico en una de las granjas de servidores de Amazon, la otra instancia RDS seguiría funcional.

Respecto a estas instancias, solo se puede leer y escribir en una de ellas, la otra está perfectamente sincronizada, pero solo recibirá los datos provenientes de los apaches si la primera no responde.

Las instancias EC2 tienen IP elástica y es la IP privada la que aparece en el balanceador para que no cambie entre reinicios.

El almacenamiento de todos los archivos necesarios para que nuestra web dinámica funcione están alojados en un servicio EFS. Este servicio de Amazon proporciona un almacenamiento de tipo NFS cuyo montaje en los Apaches está en el directorio /var/www/html/efs\_mount (se ha modificado el document root de Apache para que sea esa la carpeta raiz). Ahí se encuentran tanto el index.html y el sytle.css que da forma a la página como los achivos .php que proporcionan el formulario y la conexión con la base de datos. De esta manera la edición de cualquiera de estos archivos se ve inmediatamente reflejada en la otra instancia puesto que se está modificando el contenido de un punto de montaje externo.

# 4. Escalabilidad horizontal y vertical

Toda la configuración aquí descrita proporciona un entorno bastionado y de alta disponibilidad para el despliegue planteado en las prácticas. Pero no solo es seguro y tiene alta disponibilidad, también se puede ampliar fácilmente si nuestro sitio web requiriese de más infraestructura:

Ya sabemos crear imágenes tipo AMI en amazon, por lo que para levantar más servicios tanto proxy como web solo tendríamos que crear la imagen y levantar tantas instancias como fuesen necesarias, durante la creación los añadimos a los grupos de seguridad pertinentes y funcionarían sin afectar a la disponibilidad del sitio.

Las RDS también son escalables, de hecho, todos los servicios que hemos visto a lo largo del curso tienen la opción de autoescalado por parte de AWS.