**1. Asegurarse de tener configurado un Grupo de Seguridad (Security Group) adecuado**

* Los **Grupos de Seguridad** actúan como un firewall virtual para controlar el tráfico hacia y desde tu instancia EC2.
* Al crear una nueva instancia EC2, debes configurar un Grupo de Seguridad (SG) que defina qué puertos estarán abiertos y accesibles para la instancia.

**Pasos:**

1. En la consola de EC2, selecciona tu **instancia EC2** y dirígete a la sección de **Security**.
2. Si no has creado un Grupo de Seguridad adecuado al lanzar la instancia, puedes crear uno desde la consola de EC2:
   * En el panel izquierdo de EC2, haz clic en **Security Groups** (Grupos de Seguridad) bajo la opción **Network & Security**.
   * Haz clic en **Create Security Group** (Crear Grupo de Seguridad).
   * Especifica un nombre y una descripción para el grupo de seguridad.
   * Asegúrate de agregar las reglas necesarias, por ejemplo:
     + **SSH** en puerto **22** (para acceso remoto) si estás usando Linux/Mac.
     + **HTTP** en puerto **80** (si estás configurando un servidor web).
     + **HTTPS** en puerto **443** (si planeas usar SSL/TLS).
   * Asegúrate de restringir las direcciones IP a un rango seguro (por ejemplo, limitar el acceso SSH solo a tu IP).
3. Asocia este grupo de seguridad a tu instancia EC2 desde la consola de EC2.

**2. Configurar el acceso SSH con claves de par de llaves**

* Para mayor seguridad, debes usar un par de llaves (archivo .pem o .ppk) para autenticarte a tu instancia EC2 en lugar de contraseñas.

**Pasos:**

1. Durante el proceso de lanzamiento de la instancia EC2, se te pedirá que selecciones un **par de llaves** (Key Pair).
2. Si ya tienes un par de llaves, selecciónalo. Si no, crea uno nuevo y **descárgalo**.
   * Guarda el archivo .pem en un lugar seguro, ya que lo necesitarás para conectarte.
3. Asegúrate de dar permisos correctos al archivo .pem (en Linux o Mac):

chmod 400 /path/to/key.pem

**3. Revisar y ajustar reglas del Grupo de Seguridad**

* Asegúrate de que las reglas del grupo de seguridad solo permitan el tráfico necesario, limitando la exposición a Internet.

**Pasos:**

1. Para acceder a tu instancia EC2 de manera segura, asegúrate de que solo los puertos necesarios estén abiertos, y solo para las direcciones IP específicas (por ejemplo, tu IP para SSH).
2. Ejemplo:
   * **SSH**: Solo habilitar acceso desde tu IP o una red confiable (0.0.0.0/0 es riesgoso).
   * **HTTP/HTTPS**: Solo habilitar si tu instancia está sirviendo aplicaciones web.

**4. Deshabilitar el acceso a través de la contraseña (opcional)**

* Por razones de seguridad, es recomendable **deshabilitar el inicio de sesión con contraseña** para evitar accesos no deseados, utilizando solo claves SSH.

**Pasos:**

1. Conéctate a tu instancia EC2 mediante SSH.
2. Edita el archivo de configuración SSH:

sudo nano /etc/ssh/sshd\_config

1. Encuentra la línea que dice:

PasswordAuthentication yes

Y cámbiala a:

PasswordAuthentication no

1. Guarda el archivo y reinicia el servicio SSH para que los cambios surtan efecto:

sudo systemctl restart sshd

**5. Mantener actualizados los sistemas**

* Mantener tu instancia EC2 actualizada con los últimos parches de seguridad es crucial.

**Pasos:**

1. Conéctate a tu instancia EC2.
2. En una instancia de **Linux (por ejemplo, Amazon Linux 2)**, ejecuta los siguientes comandos:

sudo yum update -y # Para actualizar el sistema en Amazon Linux y CentOS.

O, si usas **Ubuntu**:

sudo apt update && sudo apt upgrade -y

**6. Configurar el Firewall (Opcional)**

* AWS utiliza **Grupos de Seguridad** como su firewall, pero también puedes usar herramientas de firewall dentro de tu instancia, como iptables en Linux, para mayor control sobre el tráfico entrante y saliente.

**Pasos:**

1. Para configurar iptables en una instancia EC2, puedes crear reglas específicas.
2. Ejemplo para permitir solo tráfico de SSH desde una dirección IP específica:

sudo iptables -A INPUT -p tcp -s <tu\_ip> --dport 22 -j ACCEPT

**7. Activar la protección contra la terminación (opcional)**

* Si deseas proteger tu instancia EC2 de ser terminada accidentalmente, puedes activar la **protección contra la terminación**.

**Pasos:**

1. En la consola de EC2, selecciona tu instancia y haz clic en **Actions** > **Instance Settings** > **Change Termination Protection**.
2. Activa la opción **Enable** y haz clic en **Apply**.

**8. Configurar CloudWatch Logs (opcional)**

* Para monitorizar la seguridad de tu instancia EC2, puedes usar **Amazon CloudWatch Logs** para hacer un seguimiento de la actividad de la instancia y generar alertas en caso de comportamientos sospechosos.

**Pasos:**

1. En la consola de **CloudWatch**, configura **Alarmas** para monitorear eventos como intentos de inicio de sesión fallidos o cambios en el sistema.
2. Configura la recopilación de logs del sistema, como los logs de SSH o logs de aplicaciones, en **CloudWatch Logs**.

**9. Habilitar Multi-Factor Authentication (MFA) en la cuenta de AWS**

* Aunque esto no es específico de la instancia EC2, es recomendable habilitar la autenticación de múltiples factores (MFA) para tu cuenta de **AWS** para agregar una capa adicional de seguridad.

**Pasos:**

1. En la consola de AWS, ve a **IAM (Identity and Access Management)**.
2. En el panel de la izquierda, selecciona **Users** y elige tu usuario.
3. En la sección **Security Credentials**, habilita el **Multi-Factor Authentication (MFA)**.