

PASO 5- INSTANCIA DE EC2

Para que funcione el paso 5 necesitamos crear la instancia en EC2 ya, para ello primero vamos a crear el rol:

IAM→Roles→ Crear rol

The screenshot shows the AWS IAM Roles page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' selected. Under 'Panel', 'Roles' is highlighted with a red arrow. The main content area shows a table of existing roles, each with a checkbox, their names, the service they trust, and the last activity. A red arrow points to the 'Crear rol' (Create role) button at the top right of the table. The top navigation bar shows 'DAVID-TOME (4901-4525-8703)'.

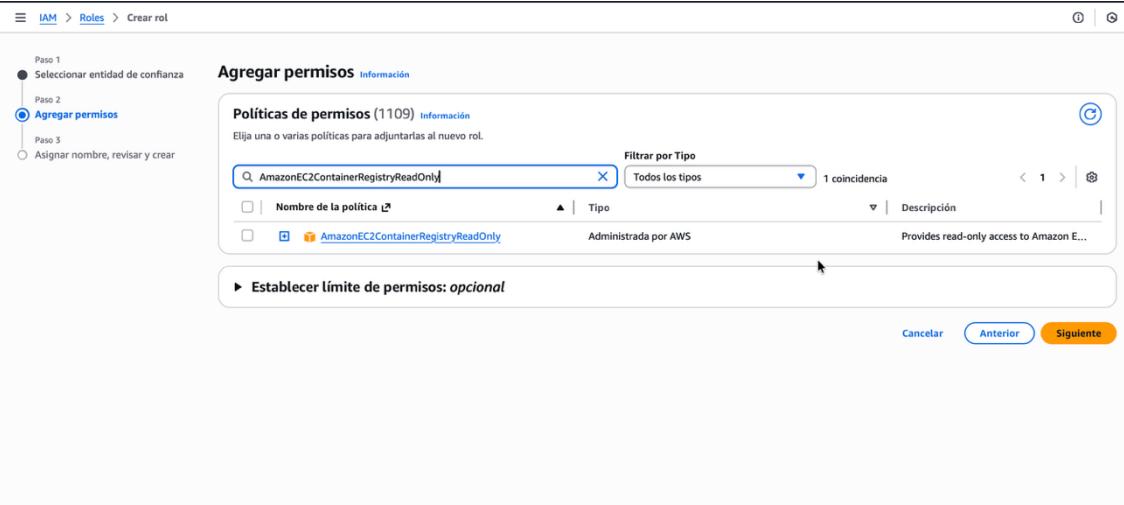
Nombre del rol	Entidades de confianza	Última actividad
AWSServiceRoleForRDS	Servicio de AWS: rds (Rol vinculado)	hace 6 minutos
AWSServiceRoleForResourceExplorer	Servicio de AWS: resource-explorer-	hace 3 horas
AWSServiceRoleForSupport	Servicio de AWS: support (Rol vinculado)	-
AWSServiceRoleForTrustedAdvisor	Servicio de AWS: trustedadvisor (Rol vinculado)	-
EC2-ECR-ReadOnly	Servicio de AWS: ec2	hace 35 minutos
rds-monitoring-role	Servicio de AWS: monitoring.rds	hace 10 minutos

Seleccionamos la opción de “servicio de AWS” y después en caso de uso elegimos EC2. Y damos a siguiente.

The screenshot shows the 'Select Trust Entity' step of the 'Create role' wizard. It has three steps: 'Seleccionar entidad de confianza' (selected), 'Agregar permisos', and 'Asignar nombre, revisar y crear'. A red arrow points to the 'Servicio de AWS' option in the 'Type of trust entity' section. In the 'Use case' section, 'EC2' is selected with a red box around it. The top navigation bar shows 'DAVID-TOME (4901-4525-8703)'.

Buscamos y seleccionamos la opción:

- AmazonEC2ContainerRegistryReadOnly



Paso 1
● Seleccionar entidad de confianza
Paso 2
● Agregar permisos
Paso 3
○ Asignar nombre, revisar y crear

Agregar permisos Información

Políticas de permisos (1109) Información

Elija una o varias políticas para adjuntarlas al nuevo rol.

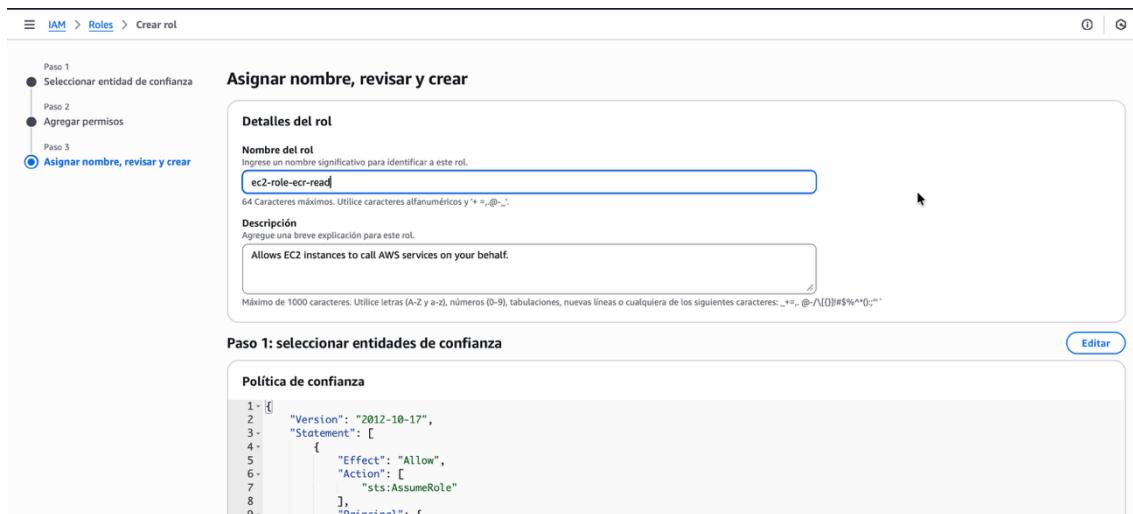
Filtrar por Tipo Todos los tipos 1 coincidencia

Nombre de la política	Tipo	Descripción
AmazonEC2ContainerRegistryReadOnly	Administrada por AWS	Provides read-only access to Amazon E...

▶ Establecer límite de permisos: opcional

Cancelar Anterior Siguiente

Ponemos un nombre al rol y damos a crear.



Paso 1
● Seleccionar entidad de confianza
Paso 2
● Agregar permisos
Paso 3
● Asignar nombre, revisar y crear

Asignar nombre, revisar y crear

Detalles del rol

Nombre del rol
Ingrese un nombre significativo para identificar a este rol.

Descripción
Agregue una breve explicación para este rol.

Máximo de 1000 caracteres. Utilice letras (A-Z y a-z), números (0-9), tabulaciones, nuevas líneas o cualquiera de los siguientes caracteres: _+=_, @-/\\{()#%\$^&`~`

Paso 1: seleccionar entidades de confianza Editar

Política de confianza

```
1 - [ {  
2 -     "Version": "2012-10-17",  
3 -     "Statement": [  
4 -         {  
5 -             "Effect": "Allow",  
6 -             "Action": [  
7 -                 "sts:AssumeRole"  
8 -             ],  
9 -             "Principal": {
```

Ahora vamos a crear la instancia, en nuestro buscador ponemos “EC2”.



aws | Preguntar a Amazon X

IAM >

Identity and Management

Buscar en...

Panel

Administradores

Grupos de personas

Personas

Servicios (13)

Características (58)

Recursos (58)

Publicaciones de blog (47)

Documentación (5337)

Artículos de conocimiento (543)

Tutoriales (19)

Marketplace (4210)

Servicios

Ver los 13 resultados

EC2 Servidores virtuales en la nube

EC2 Image Builder Un servicio administrado para automatizar la creación, personalización e implementaci...

AWS Global View AWS Global View provides a global dashboard and search functionality that lets you fi...

Seleccionamos instancias → lanzar instancias

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with 'Instancias' selected. The main area displays 'Instancias (1) Información' with a single instance listed: 'ec2-demojava...' (ID: i-0c7f4f6c1fac80908, State: En ejecución, Type: t2.micro). At the top right, there's a prominent orange button labeled 'Lanzar instancias' with a red arrow pointing to it.

Ponemos un nombre a nuestra instancia

The screenshot shows the 'Launch instance' wizard. Step 1: 'Nombre y etiquetas'. The instance name is set to 'ec2-manual'. Step 2: 'Resumen'. It shows 'Número de instancias: 1' and 'Imagen de software (AMI): Amazon Linux 2023.9.2... más información'. Step 3: 'Tipo de servidor virtual (tipo de instancia)'. The instance type is selected as 't2.micro'.

Seleccionamos Ubuntu y la versión Ubuntu server 22.04

The screenshot shows the 'Launch instance' wizard. Step 2: 'Imágenes de aplicaciones y sistemas operativos (Imagen de máquina de Amazon)'. The 'Ubuntu' option is selected and highlighted with a red box. The description below states: 'Ubuntu Server 22.04 LTS (HVM), SSD Volume Type' and 'Apto para la capa gratuita'. A red arrow points to the 'ubuntu' link in the description.

Dejamos este tipo de instancia que viene por defecto.

▼ Tipo de instancia [Información](#) | [Obtener asesoramiento](#)

Tipo de instancia

t2.micro

Familia: t2 1 vCPU 1 GiB Memoria Generación actual: true

Bajo demanda RHEL base precios: 0.027 USD por hora

Bajo demanda Linux base precios: 0.0126 USD por hora

Bajo demanda SUSE base precios: 0.0126 USD por hora

Bajo demanda Ubuntu Pro base precios: 0.0144 USD por hora

Bajo demanda Windows base precios: 0.0172 USD por hora

Apto para la capa gratuita

Todas las generaciones

Comparar tipos de instancias

Se aplican costos adicionales a las AMI con software preinstalado

En el apartado de par de claves, pulsamos en crear un nuevo par de claves, aquí se generara un fichero .pem que debemos guardar y tenerlo a mano.

▼ Par de claves (inicio de sesión) [Información](#)

Puede utilizar un par de claves para conectarse de forma segura a la instancia. Asegúrese de que tiene acceso al par de claves seleccionado antes de lanzar la instancia.

Nombre del par de claves - *obligatorio*

Seleccionar

Crear un nuevo par de claves

Lanzar una instancia

Le damos un nombre y pulsamos a crear par de claves.

Crear par de claves

Nombre del par de claves

Con los pares de claves es posible conectarse a la instancia de forma segura.

ejemplo-cicd-ke

El nombre puede incluir hasta 255 caracteres ASCII. No puede incluir espacios al principio ni al final.

Tipo de par de claves

RSA

Par de claves pública y privada cifradas mediante RSA

ED25519

Par de claves privadas y públicas cifradas ED25519

Lanzar una instancia

Formato de archivo de clave privada

.pem

Para usar con OpenSSH

.ppk

Para usar con PuTTY

⚠️ Cuando se le solicite, almacene la clave privada en un lugar seguro y accesible del equipo. Lo necesitará más adelante para conectarse a la instancia. [Más información ↗](#)

Cancelar

Crear par de claves

Seleccionamos el que hemos creado.

▼ Par de claves (inicio de sesión) [Información](#)

Lanzar una instancia

Puede utilizar un par de claves para conectarse de forma segura a la instancia. Asegúrese de que tiene acceso al par de claves seleccionado antes de lanzar la instancia.

Nombre del par de claves - obligatorio

Seleccionar ▾ Continuar sin un par de claves (no recomendado) Valor predeterminado

ejemplo-cicd-key Tipo: rsa

tfg-key Tipo: rsa

Subred | [Información](#)

Sin preferencias (subred predeterminada en cualquier zona de disponibilidad)

[Crear un nuevo par de claves](#) [Editar](#)

En configuración de red, damos a editar.

▼ Configuraciones de red [Información](#)

Red | [Información](#)

vpc-01a8c3c181ec3d071

Subred | [Información](#)

Sin preferencias (subred predeterminada en cualquier zona de disponibilidad)

Asignar automáticamente la IP pública | [Información](#)

Habilitar

Se aplican cargos adicionales cuando no se cumplen los límites del nivel gratuito

Firewall (grupos de seguridad) | [Información](#)

Un grupo de seguridad es un conjunto de reglas de firewall que controlan el tráfico de la instancia. Agregue reglas para permitir que un tráfico específico llegue a la instancia.

Crear grupo de seguridad Seleccionar un grupo de seguridad existente

Crearemos un nuevo grupo de seguridad denominado "launch-wizard-8" con las siguientes reglas:

Permitir el tráfico de SSH desde Ayuda a establecer conexión con la instancia 0.0.0.0/0

Permitir el tráfico de HTTPS desde Internet Para configurar un punto de enlace, por ejemplo, al crear un servidor web

Permitir el tráfico de HTTP desde Internet

[Editar](#)

Escribe estas reglas así, como están en las imágenes. El puerto que pongas en la segunda regla, es decir, en tcp personalizado, es el puerto que luego vas a pasar como variable secreta en APP_PORT, ¡¡cuidado!! Jenkins suele utilizar 8080, para evitar problemas utiliza otro.

Es decir APP_PORT = <intervalo de puertos>

Reglas de grupos de seguridad de entrada

- ▼ Regla del grupo de seguridad 1 (TCP, 22, 79.116.133.90/32)

Tipo Información	Protocolo Información	Intervalo de puertos Información
ssh	TCP	22

Tipo de origen Información	Nombre Información	Descripción - opcional Información
Mi IP	<input type="text"/> Agregue CIDR, lista de prefijos o grupo de s	por ejemplo, SSH para Admin Desktop
	<input type="text"/> 79.116.133.90/32	X
- ▼ Regla del grupo de seguridad 2 (TCP, 8081, 0.0.0.0/0)

Tipo Información	Protocolo Información	Intervalo Lanzar una instancia
TCP personalizado	TCP	8081

Tipo de origen Información	Origen Información	Descripción - opcional Información
Personalizada	<input type="text"/> Agregue CIDR, lista de prefijos o grupo de s	por ejemplo, SSH para Admin Desktop
	<input type="text"/> 0.0.0.0/0	X

En detalles avanzados, seleccionamos el perfil de la instancia de IAM, es decir, el rol que hemos creado poco antes.

▼ Detalles avanzados [Información](#)

Directorio de unión al dominio | [Información](#)

Seleccionar [▼](#) [Crear nuevo directorio](#) ↗

Perfil de instancia de IAM | [Información](#)

ec2-role-ecr-read [arn:aws:iam::490145258703:instance-profile/ec2-role-ecr-read](#) [▼](#) [Crear un nuevo perfil de IAM](#) ↗

Tipo de nombre de anfitrión | [Información](#)

Nombre de IP [▼](#)

Nombre de host de DNS | [Información](#)

Habilitar solicitudes de DNS IPv4 (registro A) de nombre de IP

Habilitar solicitudes de DNS IPv4 (registro A) basado en recursos

Habilitar solicitudes de DNS IPv6 (registro AAAA) basado en recursos [Lanzar una instancia](#)

Recuperación automática de instancias | [Información](#)

Seleccionar [▼](#)

Comportamiento de cierre | [Información](#)

Detener [▼](#)

Ahora vamos a poner una ip fija a nuestra instancia, así cuando se reinicie no cambiara, si no lo haces, cuando reinicies se te cambiaran algunos datos como la IP y un par de variables más que luego te cuento.

En el menú lateral de ec2, seleccionamos la opción de direcciones IP elásticas.

The screenshot shows the AWS Management Console navigation bar at the top with the EC2 logo and the text "EC2 > Instancias > Lanza". Below the navigation bar is a sidebar menu. The menu items are listed under several sections: "Instancias reservadas", "Alojamientos dedicados", "Reservas de capacidad", "Capacity Manager [New](#)", "▼ Imágenes" (which is expanded to show "AMI" and "Catálogo de AMI"), "▼ Elastic Block Store" (which is expanded to show "Volúmenes", "Instantáneas", and "Administrador del ciclo de vida"), "▼ Red y seguridad" (which is expanded to show "Security Groups", "Direcciones IP elásticas" (highlighted in blue), "Grupos de ubicación", "Pares de claves", and "Interfaces de red"), and "▼ Equilibrio de carga".

Selecciono una de las IPs que me figuran ahí. Pulsamos en acciones y elegimos “dirección IP elástica asociada”.

Name	Dirección IPv4 asign...	Tipo	ID de asignación
<input checked="" type="checkbox"/> 176.34.94.150	IP pública	eipalloc-09c5baea41ebbc3ad	
<input type="checkbox"/> 34.246.104.224	IP pública	eipalloc-0647f95aea75255c3	

Elegimos nuestra instancia y damos a asociado.

Dirección IP elástica: 176.34.94.150

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

Instancia
 Fija una instancia
 i-06f0104bb3dc85c8d (ec2-manual) - running
 i-0c7f4fc1fac80908 (ec2-demosql-mongo) - running

Reasociación
Especifique si la dirección IP elástica se puede volver a asociar a un recurso diferente si ya está asociada a un recurso.
 Permitir que se vuelva a asociar esta dirección IP elástica

Cancelar **Asociado**

Si te da error, puede ser porque el admin de la cuenta no tiene permisos full de EC2, habría que buscarlos dentro de IAM e instalarlos, luego te dejaría poner una IP fija.

Ahora vamos a crear las variables secretas que necesitamos para levantar nuestra aplicación y comprobar que el paso 5 funciona correctamente:

EC2_HOST → IP pública o Elastic IP

EC2_USER → ubuntu

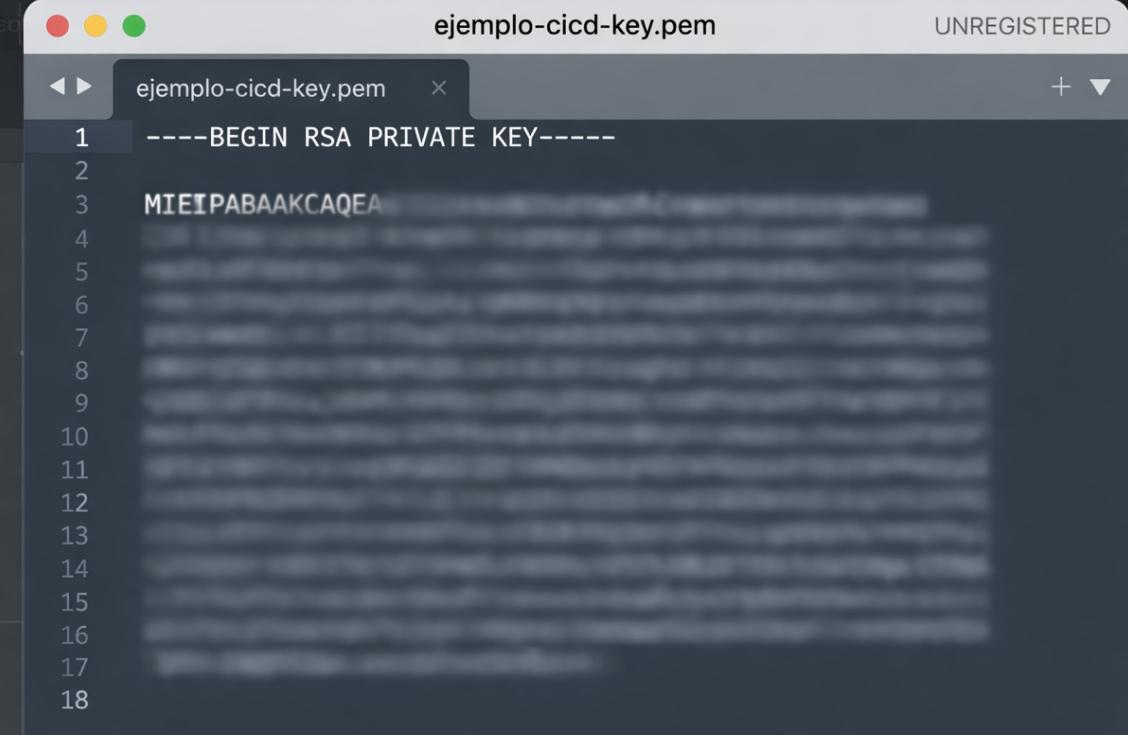
EC2_LLAVE_SSH → clave privada (.pem)

EC2_KNOWN_HOSTS

Para EC2_HOST vamos a la ventana de EC2 dentro de nuestro AWS, entramos en nuestra instancia que hemos creado y vemos nuestra IP pública.

The screenshot shows the AWS Management Console with the EC2 service selected. In the left sidebar, under the 'Instancias' section, 'Instancias' is selected. The main content area displays the 'Resumen de instancia' (Instance Summary) for instance ID i-06f0104bb3dc85c8d. A red arrow points to the 'Dirección IPv4 pública' (Public IPv4 Address) field, which contains '34.250.77.130 | dirección abierta'. Other visible details include the instance's state as 'En ejecución' (Running), its type as 't2.micro', and its VPC ID as 'vpc-01a8c3c181ec3d071'. On the right side, there are sections for private IP addresses, DNS, and elastic IPs, along with a note about AWS Compute Optimizer.

Ahora vamos a descubrir el valor de EC2_LLAVE_SSH, para ello tenemos que abrir el fichero .pem que hemos descargado antes en el paso 4 con nuestra clave. Una vez abierto copiamos todo lo que hay dentro de el y lo insertamos todo como valor de la variable.



```
ejemplo-cicd-key.pem UNREGISTERED
ejemplo-cicd-key.pem
1 -----BEGIN RSA PRIVATE KEY-----
2
3 MIEIPABAACQEA
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
```

Nuestro usuario por defecto es: “ubuntu”.

En el valor de la variable EC2_USER escribimos ubuntu.

Nos faltaría por crear esta variable: EC2_KNOWN_HOSTS

Para ello en nuestro terminal nos posicionamos en la carpeta donde tenemos nuestro .pem y ponemos la siguiente línea sustituyéndolo por nuestros valores

Ssh -i NOMBRE_DEL_PEM.pem USUARIO_EC2@IP_PUBLICA_EC2

```
----- (base) david@MacBook-Pro-de-David TFG % ssh -i ejemplo-cicd-key.pem ubuntu@34.25 0.77.130
```

Si no nos deja entrar, puede ser que nuestra IP haya cambiado dentro de nuestro centro de seguridad de la instancia ec2. Revisar nuestras reglas de entrada y verificar que nuestro origen de SSH sea 0.0.0.0/0.

The screenshot shows the AWS Security Groups console with two identical configurations for the security group 'sg-0a8b875eb32b127 - launch-wizard-8'.

Details:

- Nombre del grupo de seguridad:** launch-wizard-8
- ID del grupo de seguridad:** sg-0a8b875eb32b127
- Descripción:** launch-wizard-8 created 2025-12-30T15:02:54.259Z
- ID de la VPC:** vpc-01a8c3c181ec3d071
- Propietario:** 490145258703
- Número de reglas de entrada:** 2 Entradas de permisos
- Número de reglas de salida:** 1 Entrada de permiso

Reglas de entrada (2):

ID de la regla del gr...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen
sgr-0ef84ad0fc12108b	IPv4	TCP personalizado	TCP	8081	0.0.0.0/0
sgr-0c4da6cee45a7198	IPv4	SSH	TCP	22	0.0.0.0/0

Reglas de entrada (2):

ID de la regla del gr...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen
sgr-0ef84ad0fc12108b	IPv4	TCP personalizado	TCP	8081	0.0.0.0/0
sgr-0c4da6cee45a7198	IPv4	SSH	TCP	22	79.116.129.114/32

Nos salimos de nuestra consola EC2 de nuestra terminal, escribimos esta línea en el terminal para obtener el valor de nuestra variable.

ssh-keyscan -H IP_PUBLICA

Una vez que lo ejecutemos, escribimos esas ultimas líneas que aparecen en la imagen, algo así:

```
"|1|GtaoJ4BDQ63K9hG6ZMFcnTgzZaU=|W4Np2pfa7rWFYxJ9T6PCoXxtrEM= ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAD+4nwm2n3Fbr1RApZo2DuXkmKF6QpryUeLQ6AaNK753
"
```

Ese es nuestro valor de la variable EC2_KNOWN_HOSTS.

```

[ubuntu@ip-172-31-41-174: ~]$ exit 1
logout
Connection to 34.250.77.130 closed.
[(base) david@MacBook-Pro-de-David TFG % ssh-keyscan -H 34.250.77.130 2
# 34.250.77.130:22 SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.13
|1|xzm8p+tgYk9hnISnzdj6s8Hbph4=Dux++41j8ULURC6eGc0Fwq3MKCA= ssh-rsa AAAAB3NzaC1
yc2EAAAQABAAgQCzEzuyXz9Cjrb0RyCvJ8Zl+gbPtJr7yyfK6XjVprksKazfnB01T/DvgR12U3v
r0WLt+ENjVTsRpv9oImJ5SUATYUgHJN0/a14IRVLCrih/TwNP8NJkRXpZG3+UzUAYZxSN/i9J8zZZ1Jc
Xgs3rU83/qjigZGP6LpJL8LRSqkHcNAVTDSkqDXBhpxK3k8katyEx/VAkKzyFWw2BAqdMNJ0iNviXeW
e9599fc8FoUal53fRgSHxF5Cg4R0TxKBbPOdZpQ/MYdb8csH92IonsTQ20d+7P+f7XCTt5Km/F2T+o9R
G9y5+LDvdOtTmU9dx4LhnIM10jEa57iEmHFD7KhLRCVfRPiSFhzf/jneKXNgUoEPZzdu1TYK027+iXPs
xEdA+6JTjQWvG1gh+AaLoXK1NvTlyjo5YCuFoGXVSwug9UUrwCUwM540c0lme9LgPywre9CNnrkAFFFw
AQs6b9npru0C94c0K7dIqnpi74aIb1s0VpLqrbYd5EJ/J4rG5ywM=
# 34.250.77.130:22 SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.13
|1|+mfy+57VcPC5Mma+d8QKIHWAK/E=|YM5dkMGIyAS1JTyKcbPJjIgE5/I= ecdsa-sha2-nistp256
AAAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAIBm1zdHAyNTYAAAABBBFbGZDUEbYwPAi49FcVQdyvo+Lf
imy7UvoBWJG6M+JuT3n4Ic48377RXcgWg13j3bx1pQdbCx1eTgRVpy/CDHjk=
# 34.250.77.130:22 SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.13 3
# 34.250.77.130:22 SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.13
(base) david@MacBook-Pro-de-David TFG %

```

Muy importante, si no tenemos ip fija en nuestra instancia y se reinicia nuestra instancia de EC2, nos va a cambiar los valores de las variables:

EC2_HOST

EC2_KNOWN_HOSTS

Tendríamos que buscarlas y cambiarlos sus valores en nuestros secrets de Git.

Por último vamos a configurar nuestro EC2 por consola, esto solo se hace una vez. En el paso 5 aparece un botón con un fichero .txt que vamos a descargar.

Paso 5 – Comprobar despliegue en EC2

Se comprueba que la aplicación desplegada en una instancia EC2 responde correctamente mediante una petición HTTP.

IP o dominio de EC2
Ej: 52.48.61.1
Puedes poner IP pública o un dominio. No incluyas <http://> ni <https://>.

Puerto
80

Comprobar

Descargar conf EC2 Terminal 

Descarga los comandos necesarios para preparar una instancia EC2 (Docker, Docker Compose y AWS CLI).

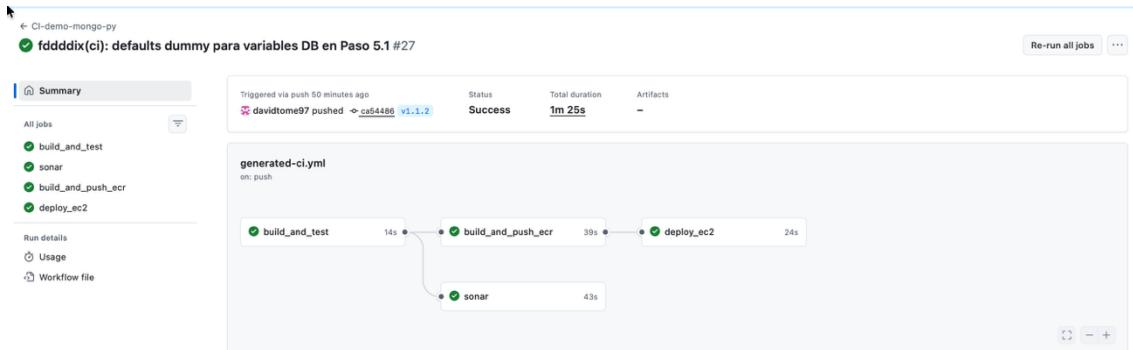
Estado: **OK**
La instancia EC2 responde correctamente (200) en <http://34.250.77.130:8081/>

En nuestro terminal si no estamos dentro de nuestra consola EC2, Ejecuta esta línea sustituyéndolo por tus valores.

Ssh -i NOMBRE_DEL_PEM.pem USUARIO_EC2@IP_PUBLICA_EC2

Una vez dentro copia y pega las líneas de código que tiene el txt. Si se instala todo bien, haciendo el commit y creando una nueva etiqueta.

Debería aparecer nuestro workflow así:



Si hacemos la comprobación ya en el paso 5, debería aparecer OK. Si falla vuelve a revisar todos los pasos.

Te dejo por aquí las líneas de código que hay en le fichero .txt:

```
sudo apt-get update -y
sudo apt-get install -y docker.io
sudo systemctl enable --now docker
sudo systemctl status docker --no-pager | head -n 20
sudo usermod -aG docker ubuntu
docker ps
sudo apt-get update -y
sudo apt-get install -y docker-compose-v2
docker compose versión
sudo rm -rf /home/ubuntu/.docker
mkdir -p /home/ubuntu/.docker
chmod 700 /home/ubuntu/.docker
sudo apt-get update -y
sudo apt-get install -y awscli
aws –version
aws sts get-caller-identity
sudo mkdir -p /usr/lib/docker/cli-plugins
sudo ln -sf /usr/libexec/docker/cli-plugins/docker-compose /usr/lib/docker/cli-plugins/docker-compose
```