



INSTALACIÓN DE DOCKER + MOSQUITTO USANDO AWS

Somoracers



ÍNDICE

3

Crear instancia EC2

5

Configuración del firewall

5

Configurar IP estatica

6

Instalación de docker

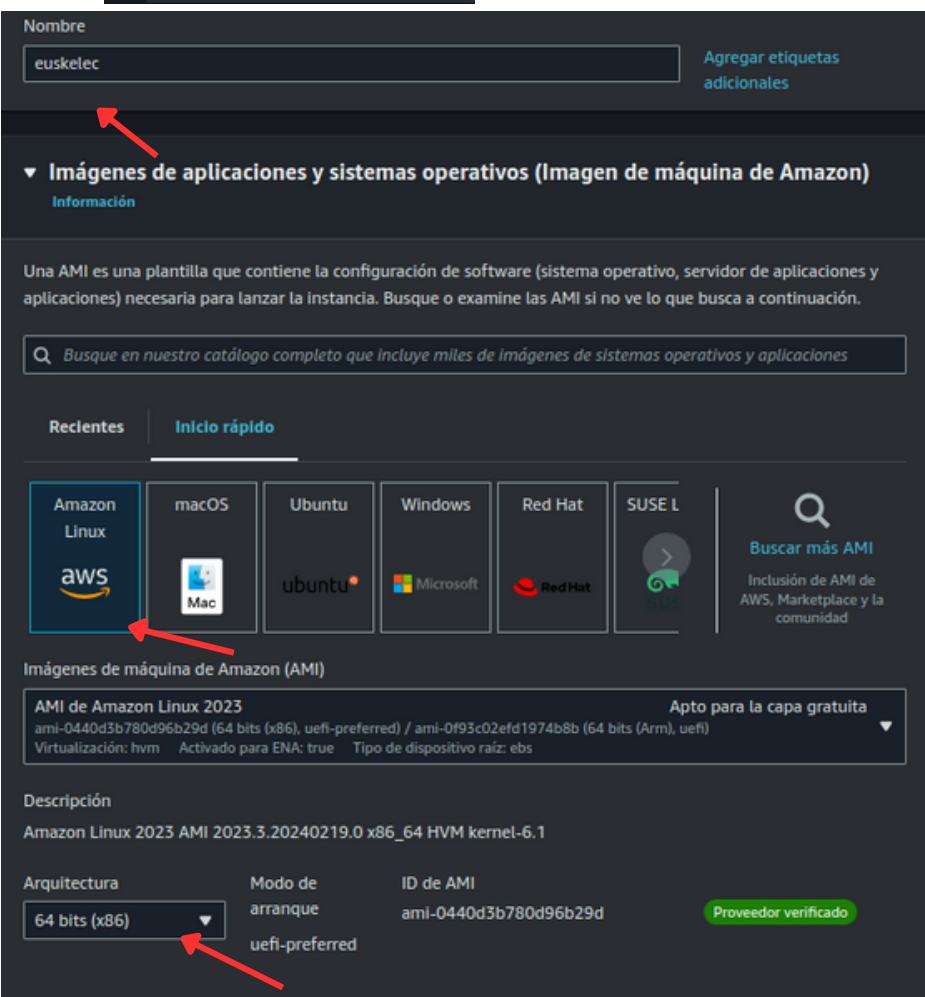
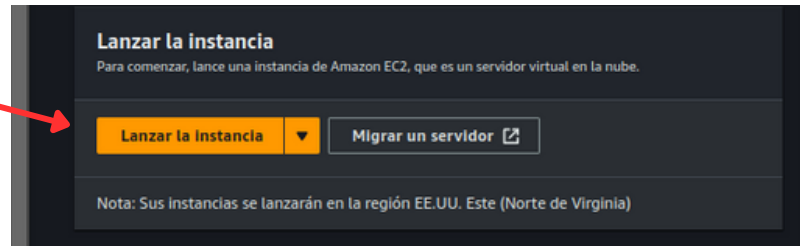
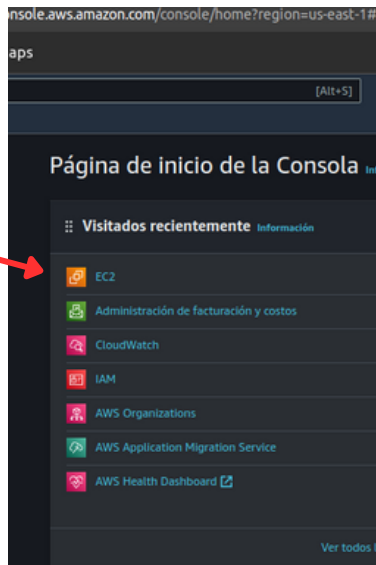
6

Instalación del contenedor de mosquitto


7

Configuración de mosquitto

Crear instancia EC2



Nombre del par de claves - obligatorio

Seleccionar  Crear un nuevo par de claves

▼ Configuraciones de red Información Editar

Red | Información

vpc-02577792aae30f0bf

Subred | Información

Sin preferencias (subred predeterminada en cualquier zona de disponibilidad)

Asignar automáticamente la IP pública | Información

Habilitar

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-6" con las siguientes reglas:

☒ Permitir el tráfico de SSH desde Cualquier lugar 0.0.0.0/0

☐ Permitir el tráfico de HTTPS desde Internet

☒ Permitir el tráfico de HTTP desde Internet

Las reglas con origen 0.0.0.0/0 permiten que todas las direcciones IP tengan acceso a la instancia. Le recomendamos que configure las reglas del grupo de seguridad para permitir el acceso únicamente desde direcciones IP conocidas.

▼ Configurar almacenamiento Información Avanzado

1x GiB Volumen raíz (Sin cifrar)

Los clientes que cumplan los requisitos de la capa gratuita pueden obtener hasta 30 GB de almacenamiento magnético o de uso general (SSD) de EBS

Crear certificado para conerse

Crear par de claves ✕

Nombre del par de claves

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

Escriba el nombre del par de claves

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

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

Cancelar Lanzar instancia

Revisar comandos

Abrir puerto 1883 para TCP

Panel de EC2

Vista global de EC2

Eventos

Console-to-Code

Vista previa

Instancias

Instancias

Tipos de instancia

Plantillas de lanzamiento

Solicitudes de spot

Savings Plans

Instancias reservadas

Alojamiento dedicado

Reservas de capacidad

Reservar capacidad

Imágenes

AMI

Catálogo de AMI

Elastic Block Store

Volúmenes

Instantáneas

Administrador del ciclo de vida

Red y seguridad

Security Groups

Direcciones IP elásticas

Grupos de ubicación

Pares de claves

Interfaz de red

Grupos de seguridad (1/6) Información

Find resources by attribute or tag

Name	Security group ID	Nombre del grupo de seguridad	ID de la VPC	Descripción	Propietario	Número de reglas de entrada
Mosquito + grafana	sg-04a8ca99820175d13	launch-wizard-5	vpc-02577792aae30f0bf	launch-wizard-5 created 2024-02-12T...	939612400909	5 Entradas de permisos
-	sg-0731d1641713852d2	launch-wizard-2	vpc-02577792aae30f0bf	launch-wizard-2 created 2024-02-11T...	939612400909	1 Entrada de permiso
-	sg-0ec500591cca45c86	default	vpc-02577792aae30f0bf	default VPC security group	939612400909	1 Entrada de permiso
-	sg-04f6d45b6182326	launch-wizard-1	vpc-02577792aae30f0bf	launch-wizard-1 created 2024-02-10T...	939612400909	4 Entradas de permisos
-	sg-04401ea1ef2ce1a	launch-wizard-3	vpc-02577792aae30f0bf	launch-wizard-3 created 2024-02-11T...	939612400909	2 Entradas de permisos
Ubuntu + docker	sg-0ab167425efeb09eb	launch-wizard-4	vpc-02577792aae30f0bf	launch-wizard-4 created 2024-02-11T...	939612400909	5 Entradas de permisos

sg-04a8ca99820175d13 - launch-wizard-5

Detalles Reglas de entrada Reglas de salida Etiquetas

Reglas de entrada (5)

Search

Name	ID de la regla del gr...	Versión de IP	Tipo	Protocolo	Intervalo de puertos	Origen	Descripción
------	--------------------------	---------------	------	-----------	----------------------	--------	-------------

TCP personalizado TCP 1883 Anywhere-IPv4 0.0.0.0/0 0.0.0.0/0

Administrar etiquetas Editar reglas de entrada

Crear IP elástica

Acciones

Asignar la dirección IP elástica

Asignar la dirección IP elástica Información

Configuraciones de la dirección IP elástica Información

Grupo de borde de red Información

us-east-1

Grupo de direcciones IPv4 públicas

Grupo de direcciones IPv4 de Amazon

Dirección IPv4 pública que utiliza en la cuenta de AWS con BYOP (opción deshabilitada porque no se encontraron grupos) Más información

Conjunto de direcciones IPv4 propiedad del cliente creado a partir de la red local para su uso con un Outpost. (opción deshabilitada porque no se encontraron grupos propiedad del cliente) Más información

Direcciones IP estáticas globales

AWS Global Accelerator puede proporcionar direcciones IP estáticas globales que se anuncian en todo el mundo mediante difusión por proximidad desde ubicaciones de borde de AWS. Esto puede ayudar a mejorar la disponibilidad y la latencia del tráfico de usuarios mediante el uso de la red global de Amazon. Más información

Crear acelerador

Etiquetas: opcional

Las etiquetas son marcas que se asignan a un recurso de AWS. Cada etiqueta consta de una clave y un valor opcional. Puede utilizarlas para buscar y filtrar los recursos, o para realizar un seguimiento de sus costos de AWS.

No hay etiquetas asociadas a este recurso.

Agregar nueva etiqueta

Puede agregar hasta 50 etiquetas más

Cancelar Asignar

Poner IP elástica de forma estática

Instancias

Tipos de instancia

Plantillas de lanzamiento

Solicitudes de spot

Savings Plans

Instancias reservadas

Alojamiento dedicado

Reservas de capacidad

Reservar capacidad

Imágenes

AMI

Catálogo de AMI

Elastic Block Store

Volúmenes

Instantáneas

Administrador del ciclo de vida

Red y seguridad

Security Groups

Direcciones IP elásticas

Grupos de ubicación

44.214.213.204	IP pública	elipalloc-0fe014ad4084fd43e	-	-
19	IP pública	elipalloc-0b5ac4570f30aa2a2	-	i-094c8b1c1d529a776

Asignar la dirección IP elástica

Ver los detalles

Liberar direcciones IP elásticas

Asociar la dirección IP elástica

Desasociar la dirección IP elástica

Actualizar DNS inverso

Activar transferencias

Desactivar transferencias

Aceptar transferencias

Consulte el uso de la dirección IP y las recomendaciones para liberar las IP no utilizadas con Información sobre la IP pública

44.214.213.204

Resumen Etiquetas

Resumen

Conectarse a la maquina

- `cd /la/ruta/del/certificado`
- `ssh -i "el-nombre-del-certificado.pem" ec2-user@"IP"(pública)`

```
chris [] master 7:60 ~ cd /home/chris/Escritorio/ec2-euskelec1/ EC2-Euskelec2/
chris [] master 7:60 ~ cd /home/chris/Escritorio/ec2-euskelec1/
chris [] master 7:60 ~/Escritorio/ec2-euskelec1 ssh -i ec2-mosquitto-ssh.pem ec2-user@44.214.213.204
```

Instalar docker

- `sudo yum install -y docker`

```
[euskelec@ip-172-31-27-25 historial]$ sudo yum install -y docker
```

Añadir euskelec a grupo docker

- `sudo usermod -a -G docker euskelec`

```
[euskelec@ip-172-31-27-25 historial]$ sudo usermod -a -G docker euskelec
```

Restart docker

- `sudo systemctl restart docker`

```
[euskelec@ip-172-31-27-25 historial]$ sudo systemctl restart docker
```

Listar contenedores activos

- `docker ps`

```
[euskelec@ip-172-31-27-25 historial]$ sudo docker ps
CONTAINER ID   IMAGE     COMMAND   CREATED   STATUS    PORTS     NAMES
[euskelec@ip-172-31-27-25 historial]$
```

Descargar imagen de docker

- `sudo docker pull eclipse-mosquitto`

```
[euskelec@ip-172-31-27-25 ~]$ sudo docker pull eclipse-mosquitto
```

Runnear contenedor

- `sudo docker run -it --name mosquitto -p 1883:1883 eclipse-mosquitto`

```
[euskelec@ip-172-31-27-25 ~]$ sudo docker run -it --name mosquitto -p 1883:1883 eclipse-mosquitto
```

Iniciar contenedor de mosquitto

- `sudo docker start mosquitto`

```
[euskelec@ip-172-31-27-25 ~]$ sudo docker start mosquitto
```

Listar contenedores

- **sudo docker ps**

```
[euskelec@ip-172-31-27-25 ~]$ sudo docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS                               NAMES
08bcd61e84f4   eclipse-mosquitto "/docker-entrypoint..." About a minute ago Up 6 seconds   0.0.0.0:1883->1883/tcp, :::1883->1883/tcp mosquito
```

Entrar al contenedor

- **docker exec -it mosquito sh**

```
[euskelec@ip-172-31-27-25 ~]$ docker exec -it mosquito sh
```

Ir al directorio config

- **cd mosquito/config**

Hacer backup de la configuración

- **cp mosquito.conf mosquito.conf.back**

```
/ # ls
bin                etc                media
dev                home              mnt
docker-entrypoint.sh lib                mosquito
/ # cd mosquito/
/mosquitto # ls
config data log
/mosquitto # cd config/
/mosquitto/config # ls
mosquitto.conf
/mosquitto/config # cp mosquitto.conf mosquitto.back
/mosquitto/config #
```

Editar el mosquitto.conf

- **vi mosquitto.conf**

```
/mosquitto/config # vi mosquitto.conf
```

Habilitar puerto 1883

- **listener 1883**

```
# =====
# Listeners
# =====

# Listen on a port
# multiple times,
# this variable is
# then the default
# The port number
# address or host
# this case, mosq
# address and so
# interface. By d
# Note that for a
# name.
#
# On systems that
# to create a # U
# this case, the
# path must be pr
# listener 0 /tmp
#
# listener port-n
listener 1883
```

Habilitar conexión de los clientes

- **allow_anonymous true**

```
# Security
# =====

# If set, only clients that have a matching prefix on their
# clientid will be allowed to connect to the broker. By default,
# all clients may connect.
# For example, setting "secure-" here would mean a client "secure-
# client" could connect but another with clientid "mqtt" couldn't.
#clientid_prefixes

# Boolean value that determines whether clients that connect
# without providing a username are allowed to connect. If set to
# false then a password file should be created (see the
# password_file option) to control authenticated client access.
#
# Defaults to false, unless there are no listeners defined in the configuration
# file, in which case it is set to true, but connections are only allowed from
# the local machine.
allow_anonymous true
```