Monitoreo de Instancia EC2

Jose Candon Rubio (MingosGit)
22/05/2023
AWS
https://github.com/MingosGit/MingosTinys
https://www.linkedin.com/in/jose-candon/

Índice

Objetivos y servicios

Monitoreo de Infraestructura de Servicios en AWS
Este proyecto te permitirá familiarizarte con la configuración de un sistema de monitoreo para tus recursos en AWS. Conocer el estado de tus sistemas es crucial para mantenerlos operativos y eficientes. El servicio principal que utilizarás será Amazon CloudWatch, que ofrece una gran cantidad de métricas y funcionalidades de monitoreo. A parte, consciente de que no es necesario tener dos instancias para llevar a cabo esta práctica, generó dos para mostrar las diferentes maneras de acceder a una instancia y para demostrar cómo permitir el protocolo ICMP entre dos instancias.

Servicios de AWS a utilizar

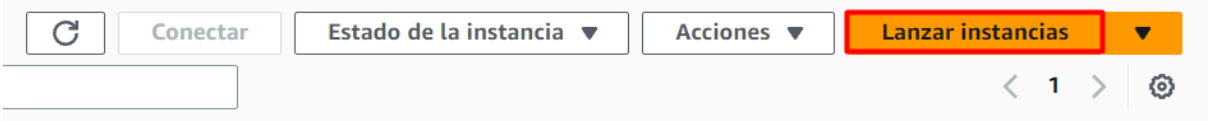
1. **AWS EC2** (Elastic Compute Cloud): Para lanzar un par de instancias de servidor como recursos para monitorear.
2. **Amazon CloudWatch**: Para monitorear las instancias de EC2 y recoger métricas de uso y rendimiento.
3. **AWS SNS** (Simple Notification Service): Para enviar notificaciones cuando ocurren ciertos eventos o cuando las métricas de CloudWatch superan ciertos umbrales.

Pasos a seguir:

1. **Crear un par de instancias de EC2**.
2. Configurar Amazon CloudWatch:
    - Ve a CloudWatch desde el panel de control de AWS.
    - Crea una alarma
    - Selecciona la instancia EC2 y la métrica que quieres monitorear.
    - Establece las condiciones para la alarma.
3. Configurar AWS SNS para notificaciones:
    - Ve a SNS desde el panel de control de AWS y crea un tema.
    - Suscribete a ese tema.
    - Elige "Email" como protocolo y escribe tu dirección de correo.
    - Confirma suscripción.
4. Vincular la alarma de CloudWatch con SNS:
    - Vuelve a la configuración de la alarma en CloudWatch.
    - En "Acciones", elige "Enviar notificación".
    - Selecciona el tema de SNS que acabas de crear.

Crear instancias de EC2

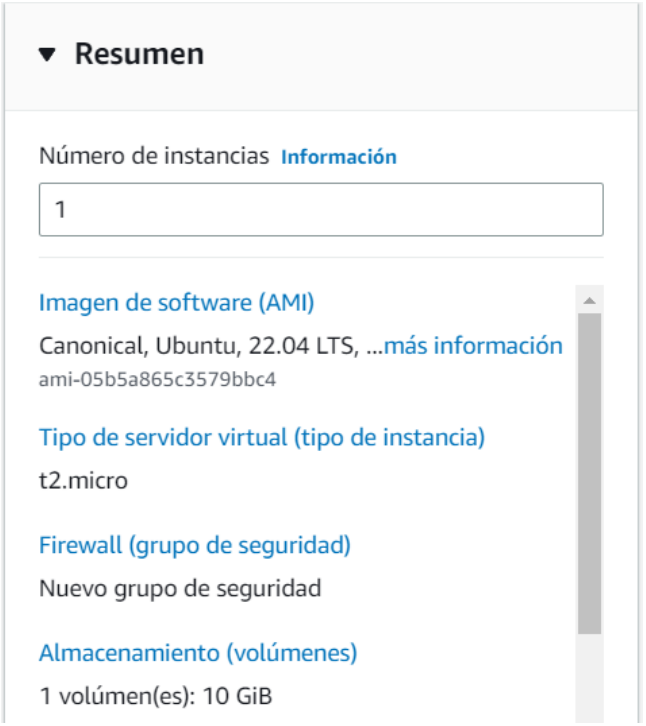
Para garantizar la monitorización efectiva de nuestras instancias y poder identificar cuál está experimentando una mayor carga, primero es necesario crear instancias en Amazon EC2. Si ya las tienes creadas puedes saltar esta explicación. A continuación, se describe el proceso de creación de dos instancias con las siguientes características:



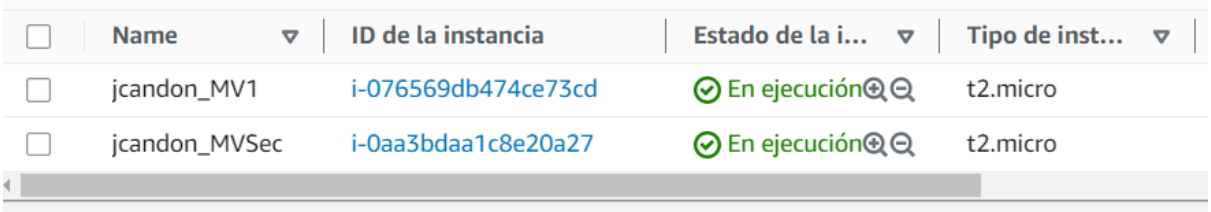
Tendrá las siguientes características:

- **Nombre:** jcandon_MV1
- **OS:** Ubuntu Server 22.04
- **Tipo de instancia:** t2.micro
- **Almacenamiento:** 10GiB gp2

Es importante generar un par de claves para establecer la conexión con las instancias.
A continuación, se proporciona un resumen de la configuración:



Ahora crearemos una segunda instancia con las mismas características, pero con el nombre jcandon_MVSec, de secundaria, para poder diferenciar las máquinas de una manera visualmente más sencilla.



Name	ID de la instancia	Estado de la i...	Tipo de inst...
jcandon_MV1	i-076569db474ce73cd	En ejecución	t2.micro
jcandon_MVSec	i-0aa3bdaa1c8e20a27	En ejecución	t2.micro

Las direcciones IP privadas asignadas a las instancias son las siguientes:

- jcandon_MV1: 172.31.39.51/20
- jcandon_MVSec: 172.31.32.54/20

Conexión a las instancias:

A continuación, se presentan dos métodos para conectarse a las instancias:

SSH:

Deberemos ejecutar el siguiente comando en PowerShell:

```
ssh -i .\Key_Name.pem ubuntu@Instance_Public_IP
```

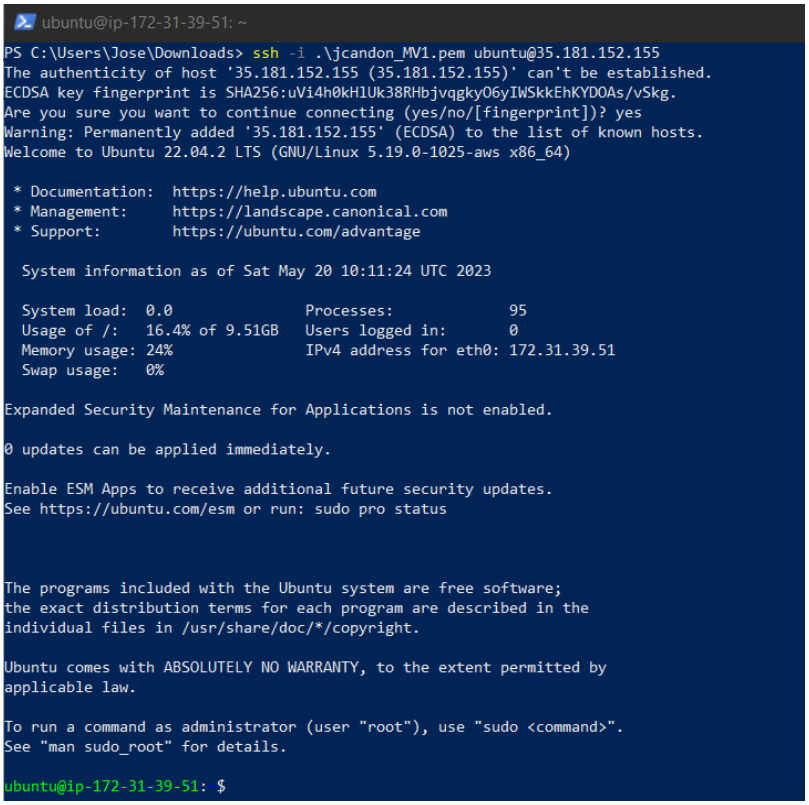
Por ejemplo, en mi caso:

```
ssh -i .\jcandon_MV1.pem ubuntu@35.181.152.155
```

o, por el contrario:

```
ssh -i .\jcandon_MV1.pem
ubuntu@ec2-35-181-152-155.eu-west-3.compute.amazonaws.com
```

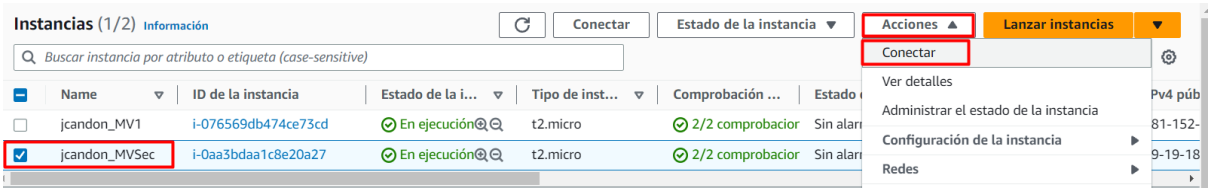
Vemos que nos permite perfectamente acceder vía SSH:

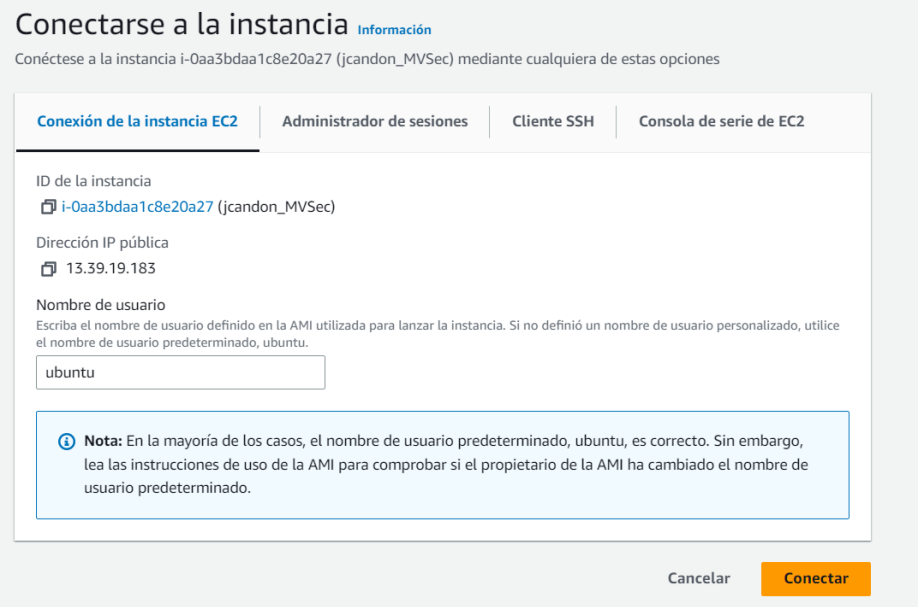


EC2 Instance Connect:

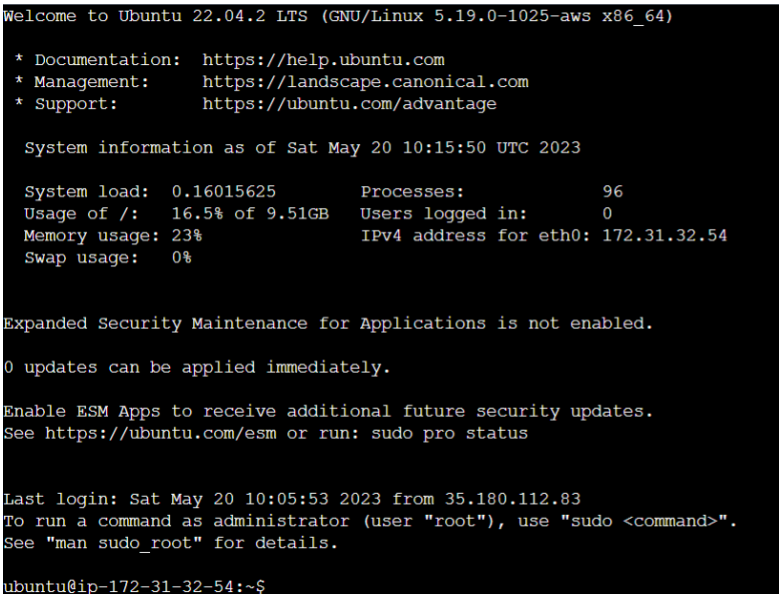
Para poder conectarnos deberemos seguir los siguientes pasos:

1. Seleccionar la instancia en la consola de EC2.
2. Acceder a "Acciones" y seleccionar "Conectar".
3. Dentro de "Conexión de la instancia EC2", hacer clic en "Conectar".
4. Establecer la conexión exitosamente.





Estamos dentro:



Para facilitar la diferenciación entre las máquinas, se crearán los usuarios "jcandon" en la instancia "jcandon_MV1" y "jrubio" en la instancia "jcandon_MVSec". Para crear un usuario, se utilizará el siguiente comando:

```
sudo adduser User_Name
```

Conectividad entre instancias

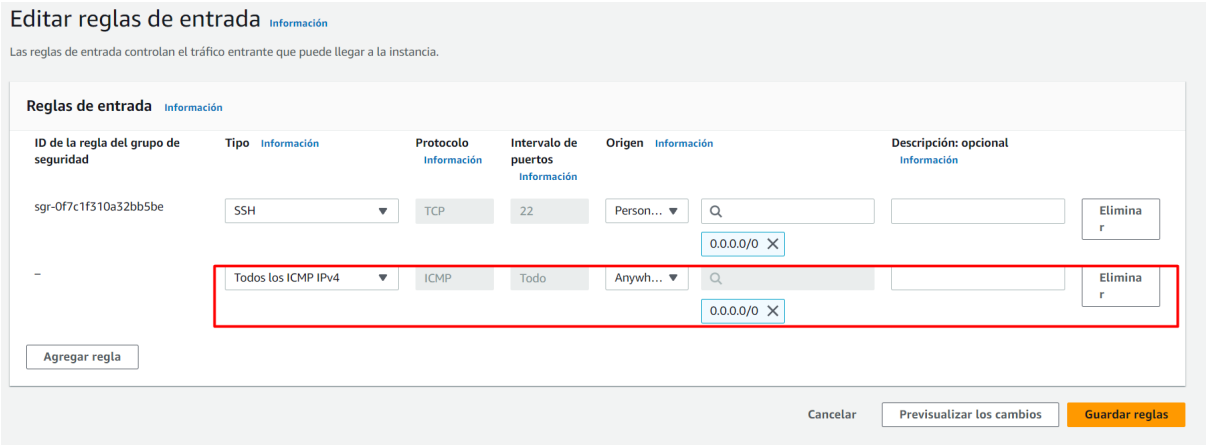
Una vez configurado esto, se puede verificar la conectividad entre las instancias mediante el comando "ping". Si no hay conectividad, es posible que se deba a las restricciones del grupo de seguridad de las instancias. Para permitir el protocolo ICMP, se debe editar el grupo de seguridad y agregar una regla de entrada que permita todo el flujo ICMP.

En este caso, como nuestro grupo de seguridad es nuevo, no están permitidas las conexiones entrantes del protocolo ICMP, por lo que el comando ping no funciona:

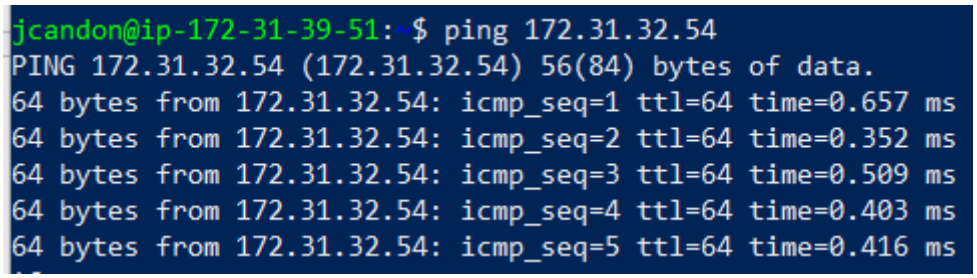
```
jcandon@ip-172-31-39-51:~$ ping 172.31.32.54
PING 172.31.32.54 (172.31.32.54) 56(84) bytes of data.
^C
--- 172.31.32.54 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3080ms

jcandon@ip-172-31-39-51:~$
```

Para poder permitirlo debemos editar nuestro Security Group.

No es necesario tocar las reglas de salida, pero sí la de entrada. Agregaremos la siguiente regla de entrada, permitiendo todo el flujo ICMP, no es la opción más segura, pero para este caso nos vale:

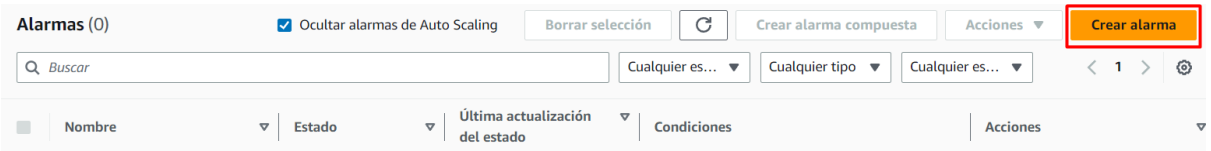


Vemos que ahora sí nos permite usar ping entre instancias y así confirmamos que hay conectividad:

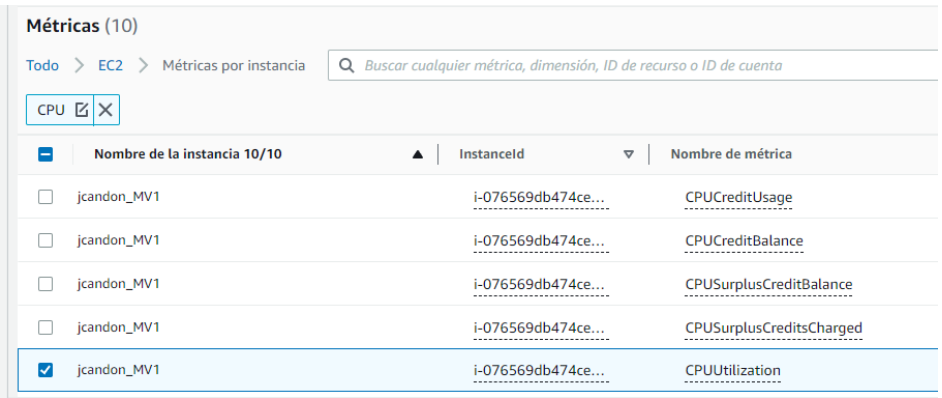


Configurar Amazon CloudWatch

A continuación, se describe el proceso para configurar Amazon CloudWatch:
Nos dirigimos a CloudWatch, donde crearemos una alarma:

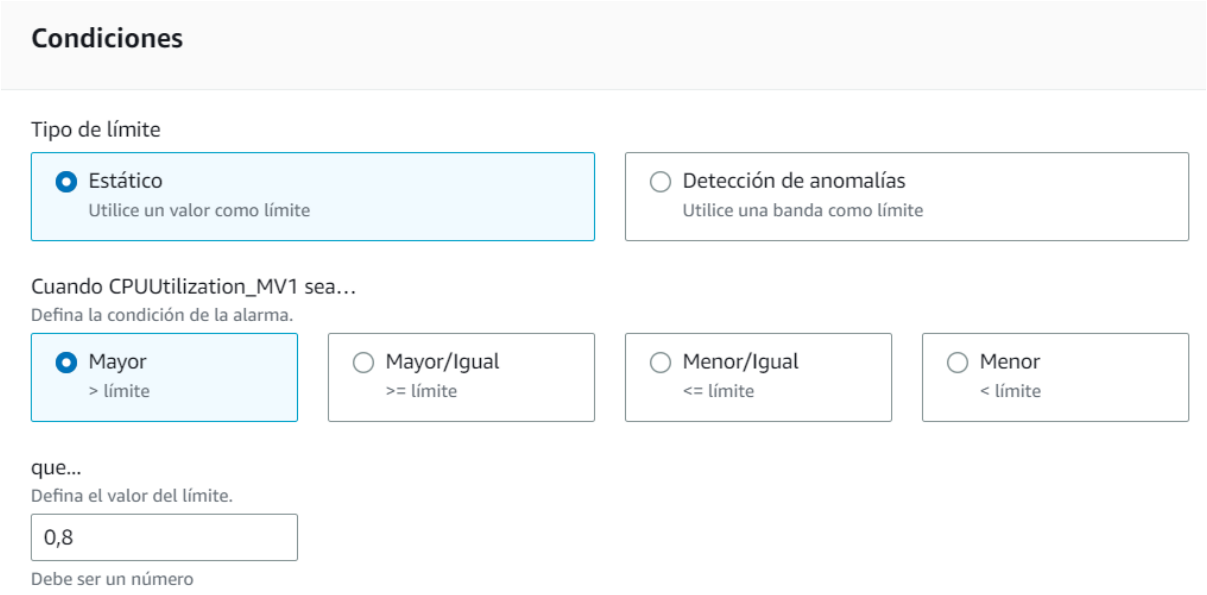


Nos pedirá seleccionar una métrica. Elegimos EC2>>Métricas por instancia>>CPUUtilization de VM1

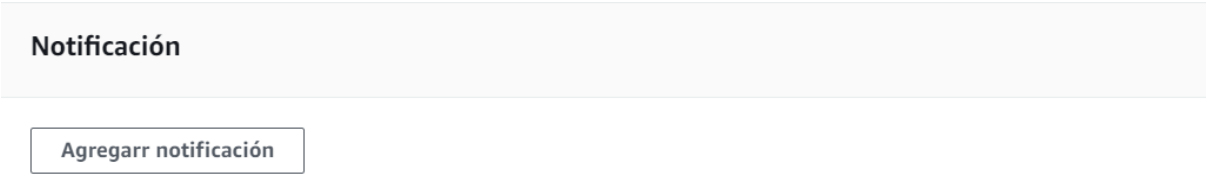


En el apartado de métrica y las condiciones no se ha modificado nada.

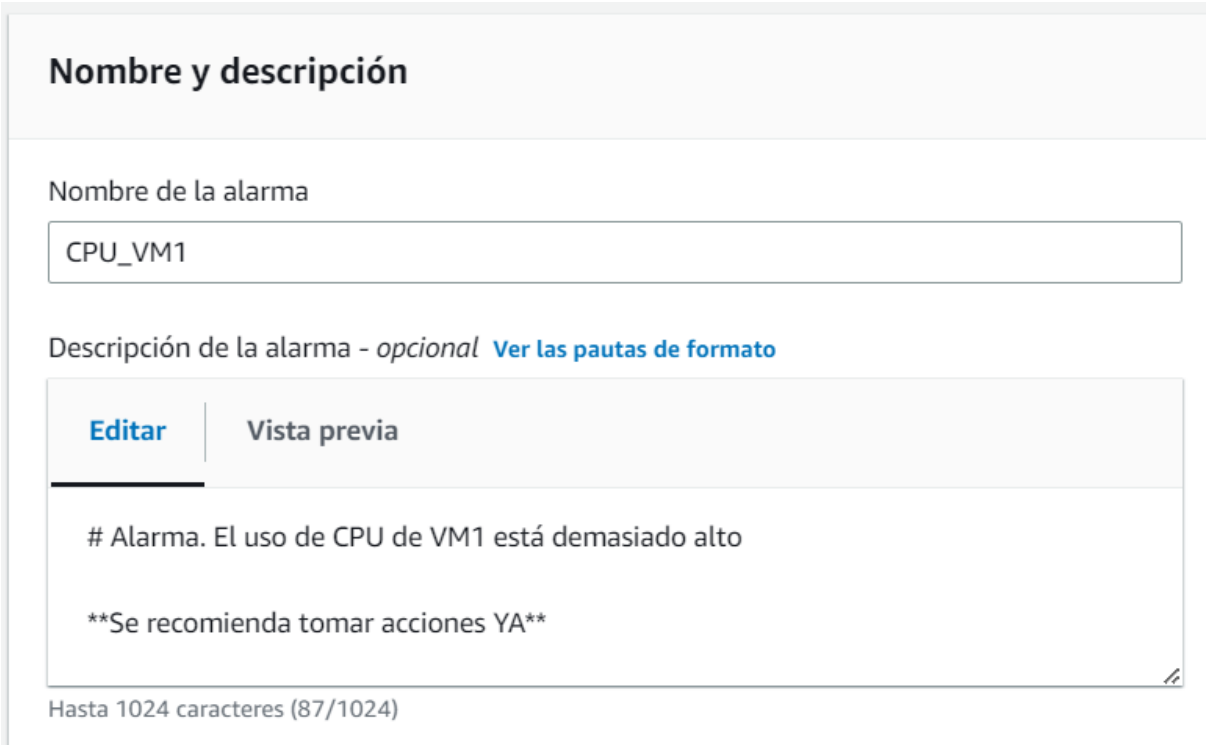
En cuanto a las condiciones, se ha dejado puesto que “salten las alarmas” cuando el uso de CPU sea mayor que 0,8.
Al ser una instancia sencilla no nos resultará difícil estresarla hasta tal punto, muchas veces ya llega hasta ahí con solo encenderla.



En el siguiente paso, se han de eliminar las notificaciones que vienen por defecto, ya que por ahora no tenemos un tema de SNS, entonces, este proceso de vinculación con SNS se explicará más adelante:

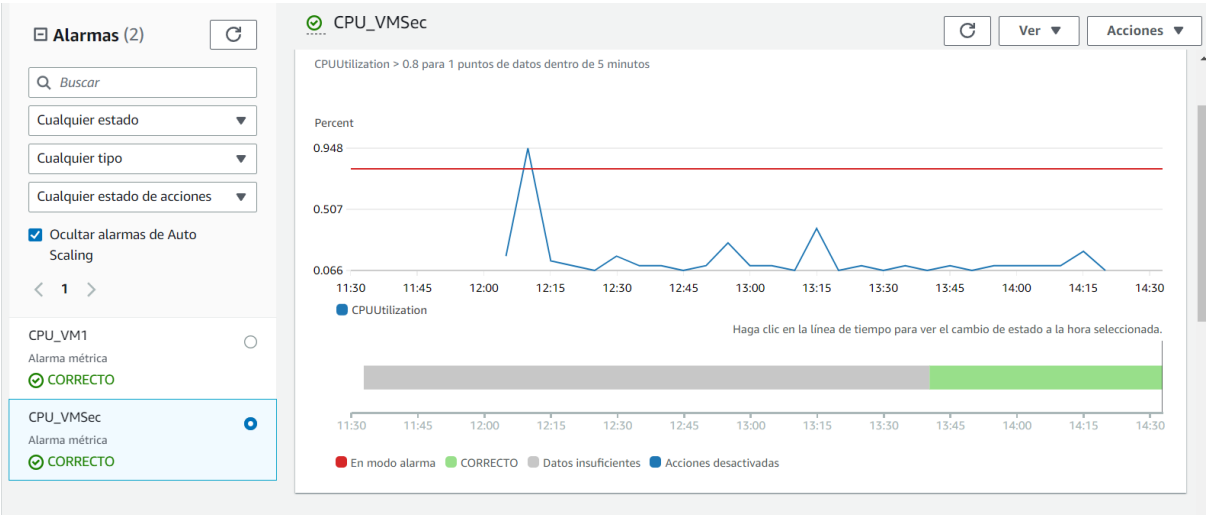


Se proporciona un nombre y una descripción (opcional) para la alarma.



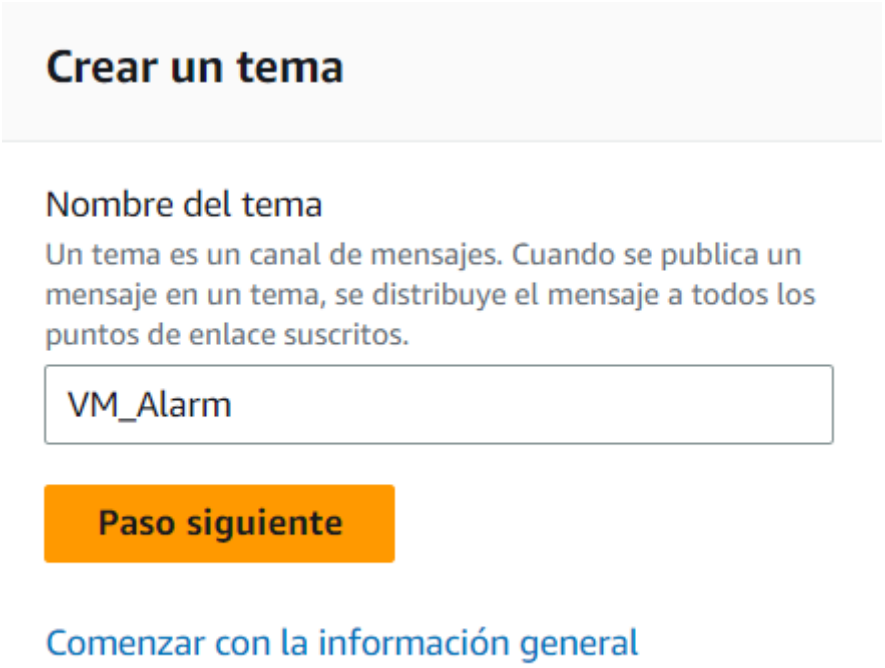
Replicamos los mismos pasos pero con MVSec.

Es posible que al principio tarde un poco en recibir datos, pero después de un breve período de tiempo, se actualizará y se mostrará como correcto.



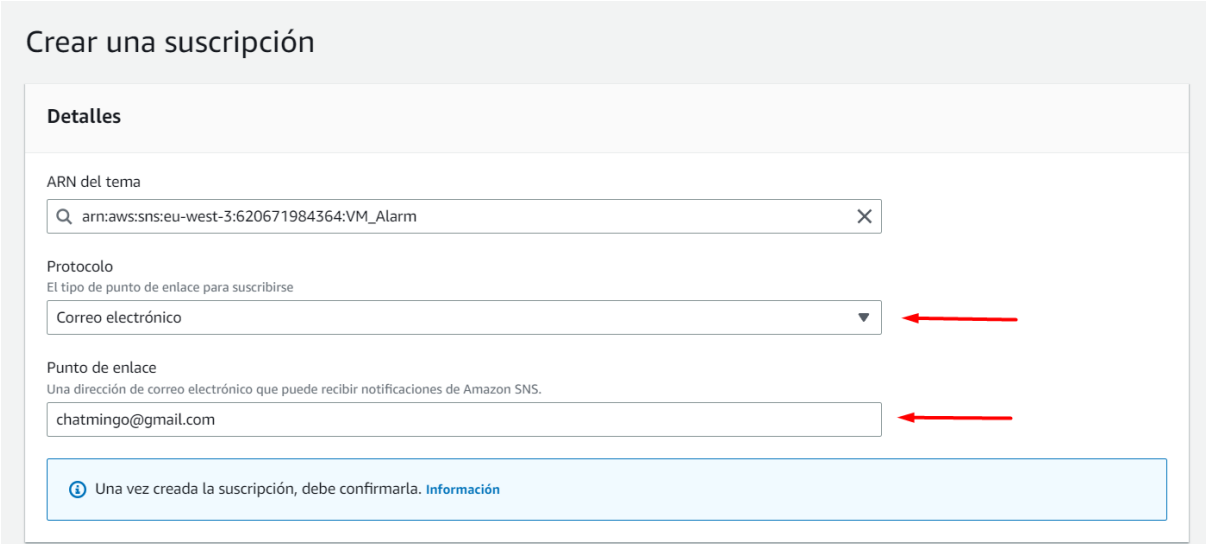
Configurar AWS SNS

Nos dirigimos a SNS y creamos un tema dejándolo todo por defecto:

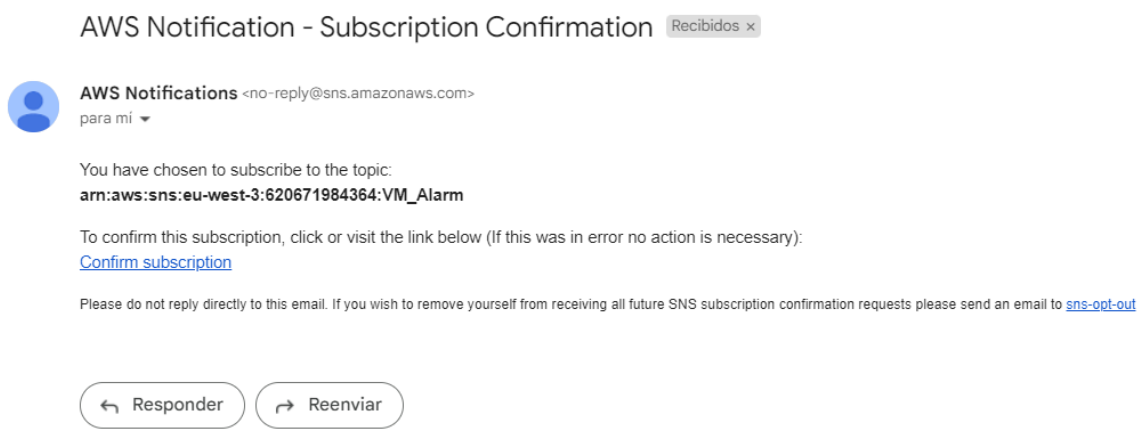


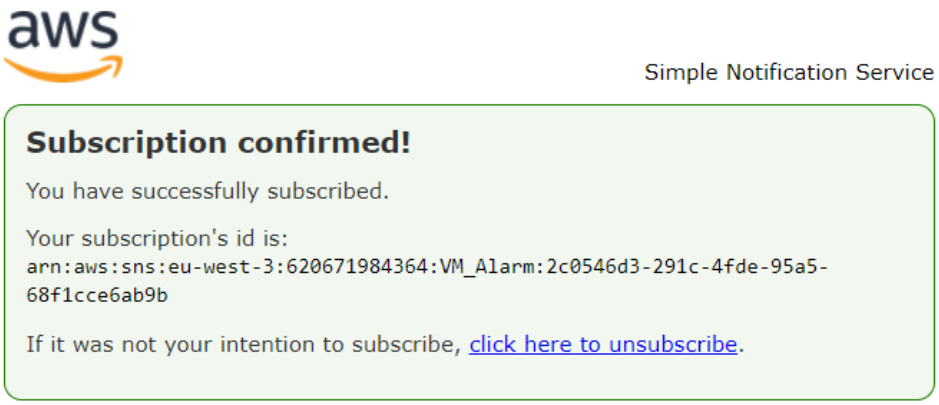
Ahora se agrega una subscripción:

Debemos asignarle “Correo electrónico” como protocolo y proporcionar la dirección de correo electrónico donde se recibirán las alertas, el resto de la configuración seguirá por defecto:



Al correo que hemos puesto le llegará un mail de confirmación, deberemos confirmar la suscripción:

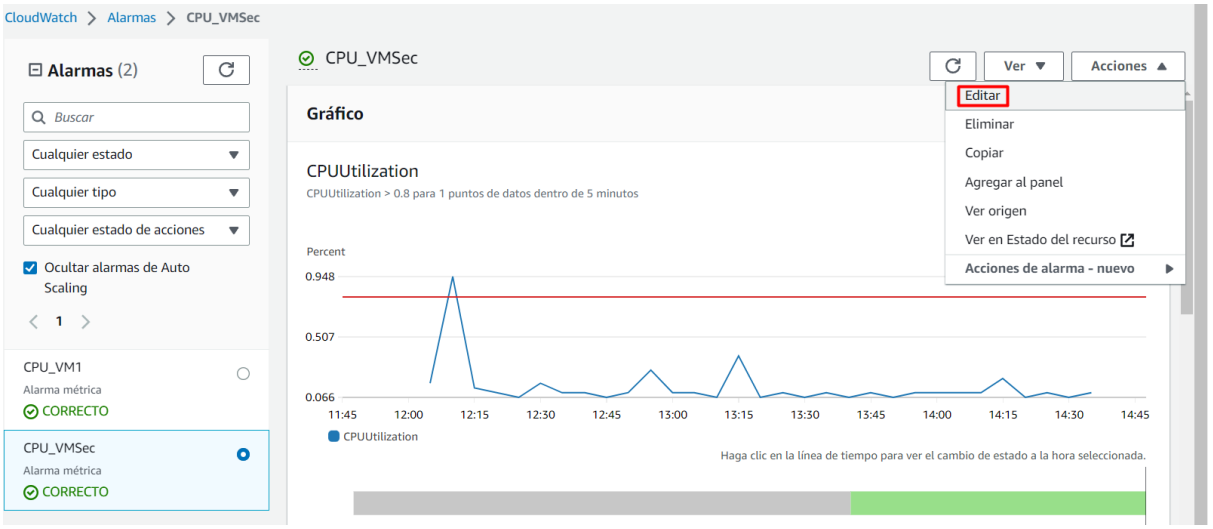




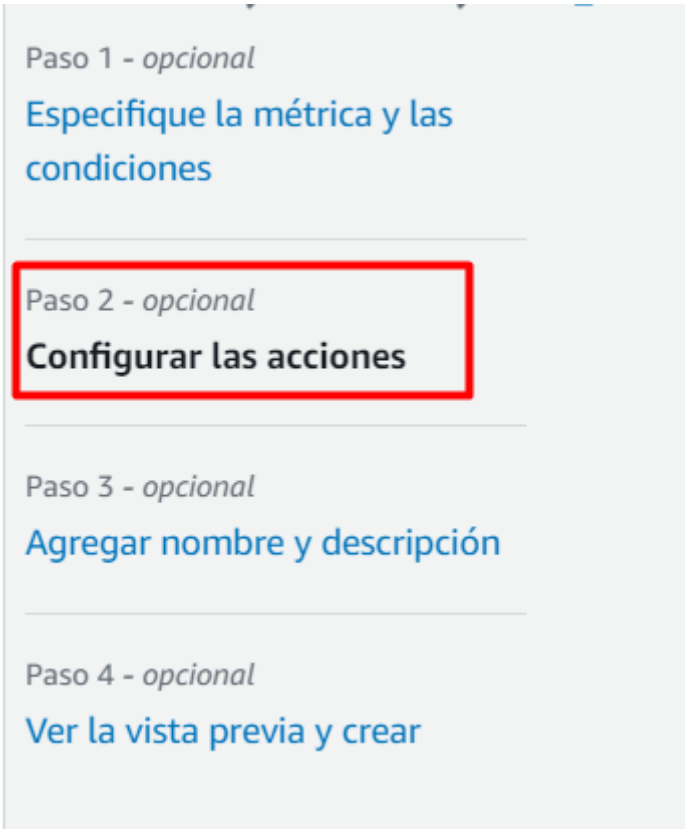
Vincular la alarma de CloudWatch con SNS

Por último, se debe vincular la alarma de CloudWatch con SNS para recibir las alertas correspondientes. A continuación, se detallan los pasos a seguir:

1. Acceder a CloudWatch>>seleccionamos una alarma>>Ver>>Editar

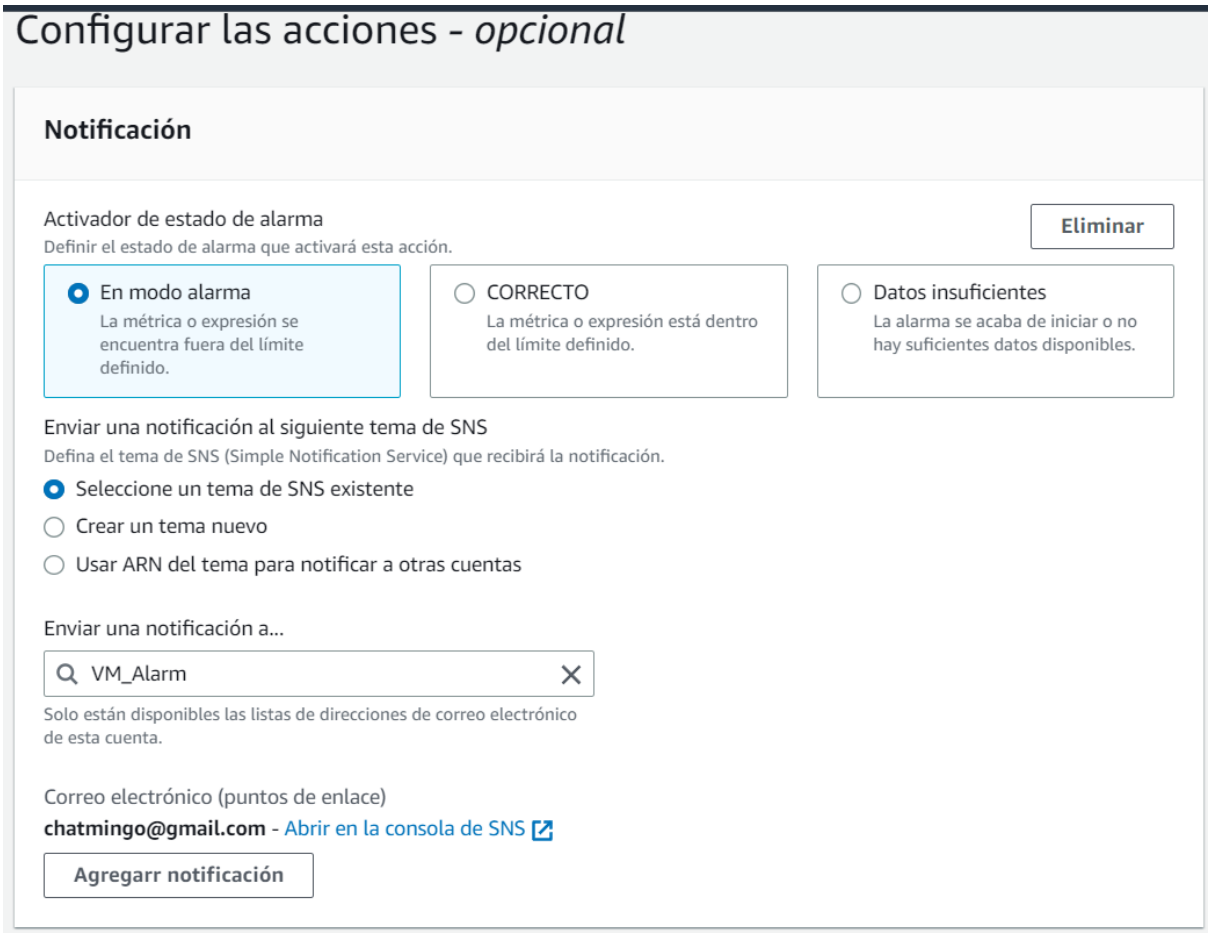


2. Desplazarse al paso 2 de la configuración:



Como antes no teníamos un tema de SNS, no hubiera estado correcto agregar una notificación con las características que deseábamos.
Podríamos crear un tema desde aquí, pero encuentro mejor ir a SNS directamente, ya que a la hora de crearlo te da muchas más opciones de configuración.

3. Seleccionar el tema de SNS ya creado y guardamos:



4. Repetir estos pasos para la alarma de la otra instancia.

Comprobación

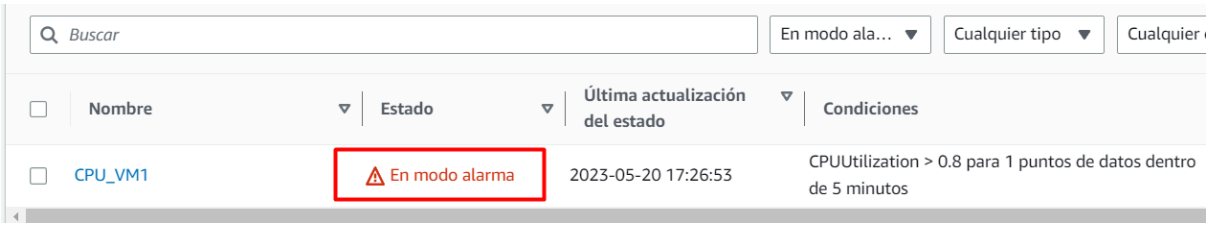
Para activar las alarmas deberemos de tener la CPU a más de 0,8. Para ello vamos a hacer un test de estrés de CPU.
Esta tarea precisa de la herramienta “stress” que podremos descargar con el siguiente comando:

```
apt install stress
```

Usaremos el comando:

```
stress –cpu 0
```

Veremos que está en modo alarma:



Vemos que nos llega un mail conforme se ha superado el límite de CPU, por lo que damos este proceso como exitoso: