

# 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

<b>Objetivos y servicios</b>	<b>2</b>
<b>Crear instancias de EC2</b>	<b>3</b>
Conexión a las instancias:	4
SSH:	4
EC2 Instance Connect:	6
Conectividad entre instancias	7
<b>Configurar Amazon CloudWatch</b>	<b>9</b>
<b>Configurar AWS SNS</b>	<b>12</b>
<b>Vincular la alarma de CloudWatch con SNS</b>	<b>14</b>
<b>Comprobación</b>	<b>16</b>

## 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, generé 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

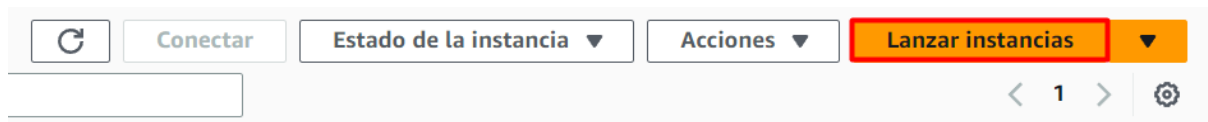
1. **AWS EC2** (Elastic Compute Cloud): Para lanzar un par de instancias de servidor como recursos para monitorear.
2. **Amazon CloudWatch**: Para monitorear las instancias de EC2 y recoger métricas de uso y rendimiento.
3. **AWS SNS** (Simple Notification Service): Para enviar notificaciones cuando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

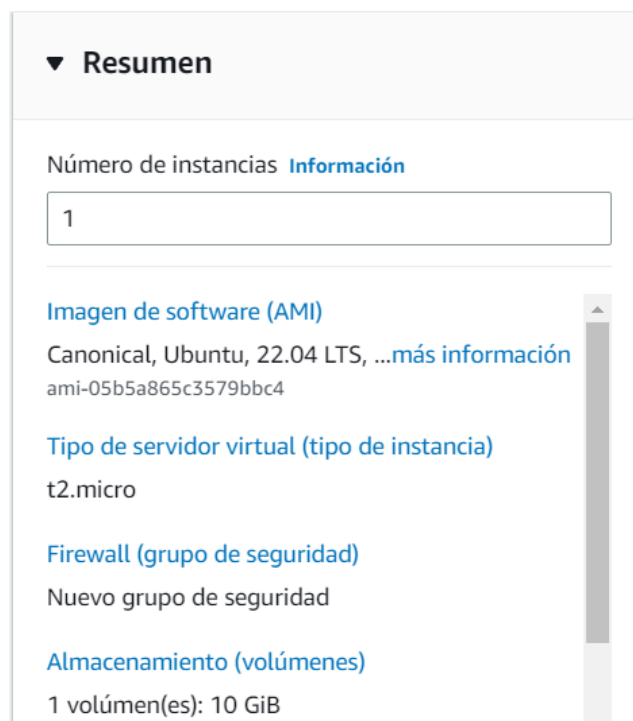


Tendrá las siguientes características:

- **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.

<input type="checkbox"/>	Name ▾	ID de la instancia	Estado de la i... ▾	Tipo de inst... ▾
<input type="checkbox"/>	jcandon_MV1	i-076569db474ce73cd	✓ En ejecución 🔍	t2.micro
<input type="checkbox"/>	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:

```
ubuntu@ip-172-31-39-51: ~
PS C:\Users\Jose\Downloads> ssh -i .\jcandon_MV1.pem ubuntu@35.181.152.155
The authenticity of host '35.181.152.155 (35.181.152.155)' can't be established.
ECDSA key fingerprint is SHA256:uVi4h0kH1Uk38RHbjvqgky06yIWSkkEhKYD0As/vSkg.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '35.181.152.155' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-1025-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat May 20 10:11:24 UTC 2023

System load:  0.0               Processes:           95
Usage of /:   16.4% of 9.51GB    Users logged in:    0
Memory usage: 24%              IPv4 address for eth0: 172.31.39.51
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

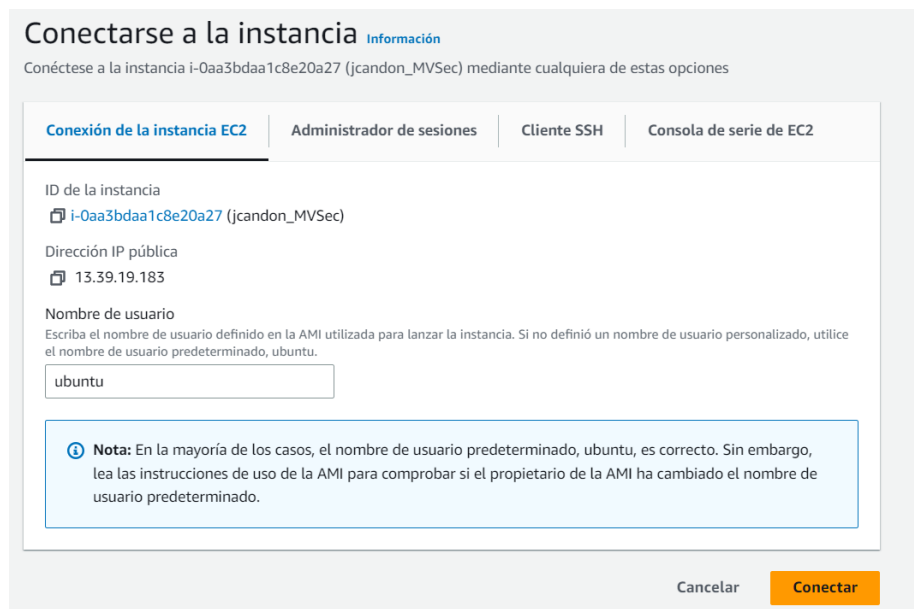
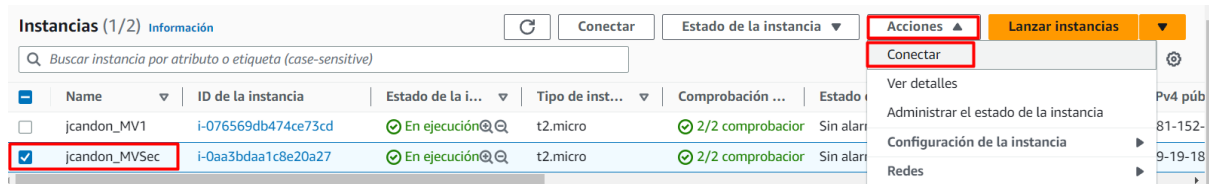
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-39-51: $
```

## 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:

```
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.19.0-1025-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Sat May 20 10:15:50 UTC 2023

System load:  0.16015625      Processes:            96
Usage of /:   16.5% of 9.51GB  Users logged in:     0
Memory usage: 23%            IPv4 address for eth0: 172.31.32.54
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Last login: Sat May 20 10:05:53 2023 from 35.180.112.83
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-32-54:~$
```

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:

Editar reglas de entrada [Información](#)

Las reglas de entrada controlan el tráfico entrante que puede llegar a la instancia.

ID de la regla del grupo de seguridad	Tipo <a href="#">Información</a>	Protocolo <a href="#">Información</a>	Intervalo de puertos <a href="#">Información</a>	Origen <a href="#">Información</a>	Descripción: opcional <a href="#">Información</a>	
sgr-0f7c1f310a32bb5be	SSH	TCP	22	Person... <input type="text" value="Q"/>		Eliminar
-	Todos los ICMP IPv4	ICMP	Todo	Anywh... <input type="text" value="Q"/>		Eliminar

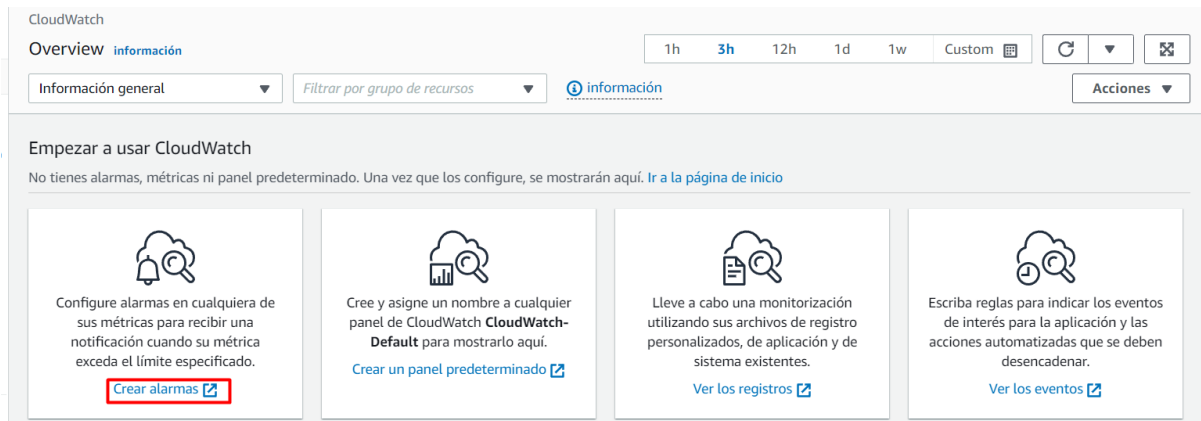


Vemos que ahora sí nos permite usar ping entre instancias y así confirmamos que hay conectividad:

```
jcondon@ip-172-31-39-51:~$ ping 172.31.32.54
PING 172.31.32.54 (172.31.32.54) 56(84) bytes of data.
64 bytes from 172.31.32.54: icmp_seq=1 ttl=64 time=0.657 ms
64 bytes from 172.31.32.54: icmp_seq=2 ttl=64 time=0.352 ms
64 bytes from 172.31.32.54: icmp_seq=3 ttl=64 time=0.509 ms
64 bytes from 172.31.32.54: icmp_seq=4 ttl=64 time=0.403 ms
64 bytes from 172.31.32.54: icmp_seq=5 ttl=64 time=0.416 ms
```

## Configurar Amazon CloudWatch

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



CloudWatch  
Overview **información**

1h 3h 12h 1d 1w Custom

Información general Filtar por grupo de recursos información Acciones

**Empezar a usar CloudWatch**  
No tienes alarmas, métricas ni panel predeterminado. Una vez que los configure, se mostrarán aquí. [Ir a la página de inicio](#)

Configure alarmas en cualquiera de sus métricas para recibir una notificación cuando su métrica exceda el límite especificado.  
**Crear alarmas**

Cree y asigne un nombre a cualquier panel de CloudWatch **CloudWatch-Default** para mostrarlo aquí.  
[Crear un panel predeterminado](#)

Lleve a cabo una monitorización utilizando sus archivos de registro personalizados, de aplicación y de sistema existentes.  
[Ver los registros](#)

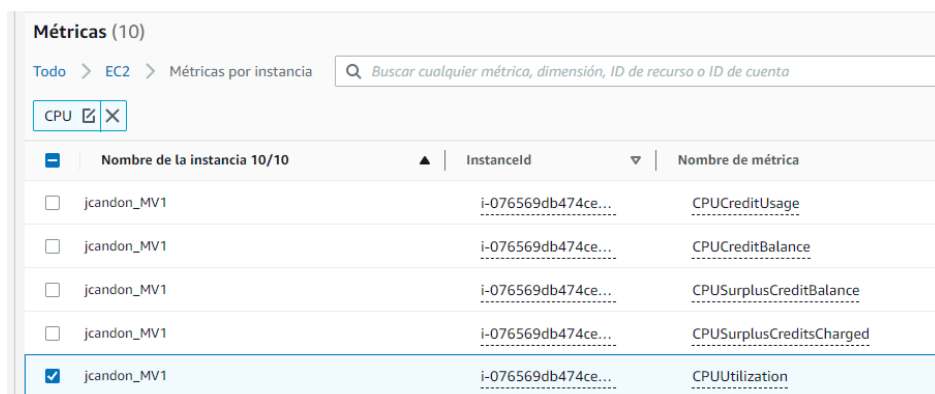
Escriba reglas para indicar los eventos de interés para la aplicación y las acciones automatizadas que se deben desencadenar.  
[Ver los eventos](#)

**Alarmas (0)** ☒ Ocultar alarmas de Auto Scaling Borrar selección Crear alarma compuesta Acciones **Crear alarma**

Buscar Cualquier es... Cualquier tipo Cualquier es... < 1 > ⚙

Nombre	Estado	Última actualización del estado	Condiciones	Acciones
--------	--------	---------------------------------	-------------	----------

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



**Métricas (10)**

Todo > EC2 > Métricas por instancia

CPU

	Nombre de la instancia 10/10	Instanceld	Nombre de métrica
<input type="checkbox"/>	jcandon_MV1	i-076569db474ce...	CPUCreditUsage
<input type="checkbox"/>	jcandon_MV1	i-076569db474ce...	CPUCreditBalance
<input type="checkbox"/>	jcandon_MV1	i-076569db474ce...	CPUSurplusCreditBalance
<input type="checkbox"/>	jcandon_MV1	i-076569db474ce...	CPUSurplusCreditsCharged
<input checked="" type="checkbox"/>	jcandon_MV1	i-076569db474ce...	CPUUtilization

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.

### Condiciones

Tipo de límite



Estático

Utilice un valor como límite



Detección de anomalías

Utilice una banda como límite

Cuando CPUUtilization\_MV1 sea...

Defina la condición de la alarma.



Mayor

> límite



Mayor/Igual

>= límite



Menor/Igual

<= límite



Menor

< límite

que...

Defina el valor del límite.

0,8

Debe ser un número

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:

### Notificación

Agregarr notificación

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

### Nombre y descripción

Nombre de la alarma

Descripción de la alarma - *opcional* [Ver las pautas de formato](#)

Editar

Vista previa

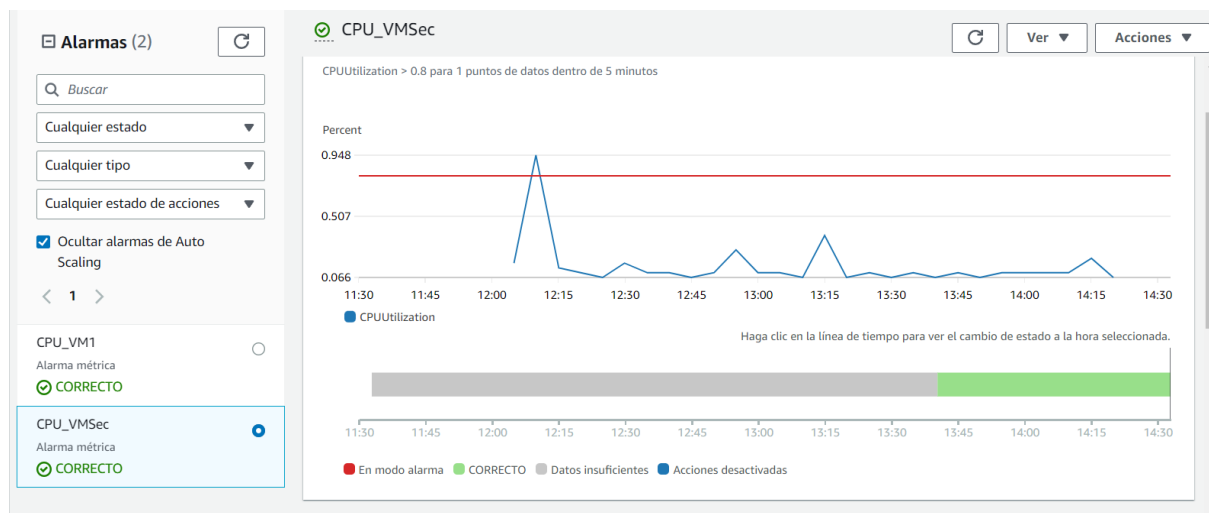
# Alarma. El uso de CPU de VM1 está demasiado alto

\*\*Se recomienda tomar acciones YA\*\*

Hasta 1024 caracteres (87/1024)

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:

### Crear un tema

#### Nombre del tema

Un tema es un canal de mensajes. Cuando se publica un mensaje en un tema, se distribuye el mensaje a todos los puntos de enlace suscritos.

**Paso siguiente**

[Comenzar con la información general](#)

Ahora se agrega una suscripción:

[Suscripciones](#) | [Política de acceso](#) | [Política de protección de datos](#) | [Política de reintentos de entrega \(HTTP/S\)](#) | [Registro del estado de entr](#) >

**Suscripciones (0)** [Editar](#) [Eliminar](#) [Solicitar la confirmación](#) [Confirmar la suscripción](#) [Crear una suscripción](#)

ID▲ | Punto de enlace▼ | Estado▼ | Protocolo▼

No se ha encontrado ninguna suscripción  
No tiene ninguna suscripción a este tema.  
[Crear una suscripción](#)

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:

Crear una suscripción

**Detalles**

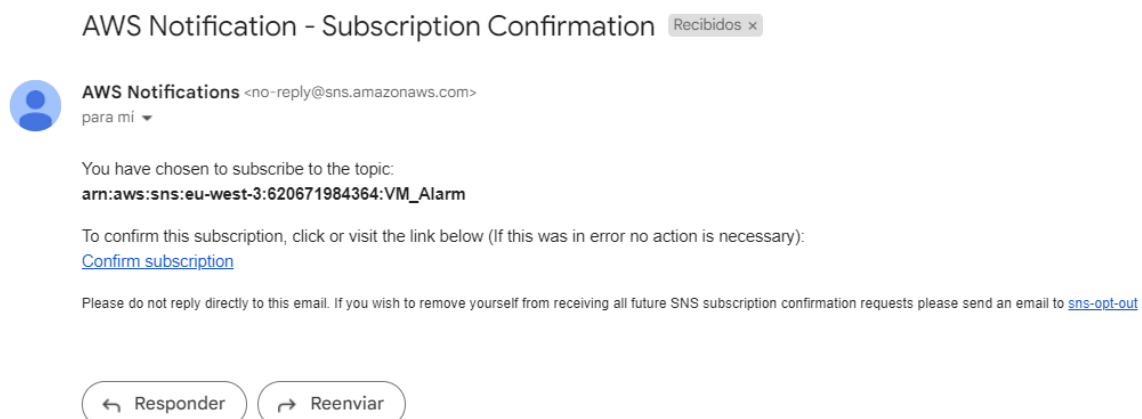
ARN del tema  
arn:aws:sns:eu-west-3:620671984364:VM\_Alarm

Protocolo  
El tipo de punto de enlace para suscribirse  
Correo electrónico

Punto de enlace  
Una dirección de correo electrónico que puede recibir notificaciones de Amazon SNS.  
chatmingo@gmail.com

Una vez creada la suscripción, debe confirmarla. [Información](#)

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



Simple Notification Service

**Subscription confirmed!**

You have successfully subscribed.

Your subscription's id is:

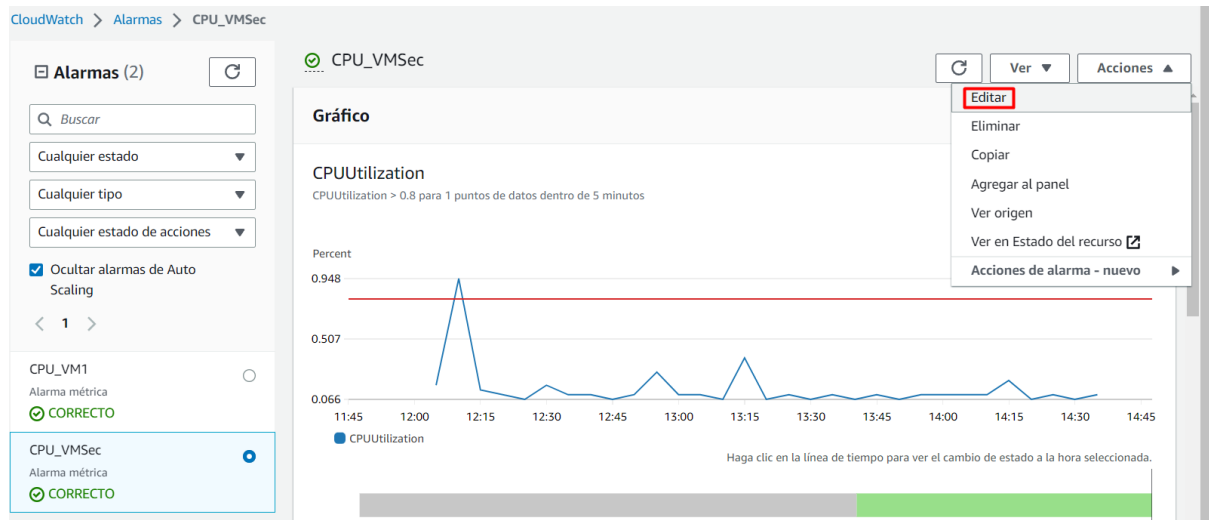
arn:aws:sns:eu-west-3:620671984364:VM\_Alarm:2c0546d3-291c-4fde-95a5-68f1cce6ab9b

If it was not your intention to subscribe, [click here to unsubscribe](#).

## 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:

**Paso 1 - opcional**  
Especifique la métrica y las condiciones

**Paso 2 - opcional**  
**Configurar las acciones**

**Paso 3 - opcional**  
Agregar nombre y descripción

**Paso 4 - opcional**  
Ver la vista previa y crear

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:

### Configurar las acciones - *opcional*

**Notificación**

Activador de estado de alarma  
Definir el estado de alarma que activará esta acción.

☒ En modo alarma  
La métrica o expresión se encuentra fuera del límite definido.

☐ CORRECTO  
La métrica o expresión está dentro del límite definido.

☐ Datos insuficientes  
La alarma se acaba de iniciar o no hay suficientes datos disponibles.

Eliminar

Enviar una notificación al siguiente tema de SNS  
Defina el tema de SNS (Simple Notification Service) que recibirá la notificación.

☒ Seleccione un tema de SNS existente  
☐ Crear un tema nuevo  
☐ Usar ARN del tema para notificar a otras cuentas

Enviar una notificación a...

Q VM\_Alarm X

Solo están disponibles las listas de direcciones de correo electrónico de esta cuenta.

Correo electrónico (puntos de enlace)  
chatmingo@gmail.com - [Abrir en la consola de SNS](#)

Agregarr notificación

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:

Buscar					En modo ala...	Cualquier tipo	Cualquier
<input type="checkbox"/>	Nombre	Estado	Última actualización del estado	Condiciones			
<input type="checkbox"/>	CPU_VM1	En modo alarma	2023-05-20 17:26:53	CPUUtilization > 0.8 para 1 puntos de datos dentro de 5 minutos			

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

ALARM: "CPU\_VM1" in EU (Paris) Recibidos x

**AWS Notifications** <no-reply@sns.amazonaws.com>  
para mí

17:26 (hace 6 minutos) ☆ ↶ ⋮

🌐 inglés > 🇪🇸 español Traducir mensaje Desactivar para: inglés x

You are receiving this email because your Amazon CloudWatch Alarm "CPU\_VM1" in the EU (Paris) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [48.95625128844033 (20/05/23 15:21:00)] was greater than the threshold (0.8) (minimum 1 datapoint for OK -> ALARM transition)." at "Saturday 20 May, 2023 15:26:53 UTC".

View this alarm in the AWS Management Console:  
[https://eu-west-3.console.aws.amazon.com/cloudwatch/deeplink.js?region=eu-west-3#alarmsV2:alarm/CPU\\_VM1](https://eu-west-3.console.aws.amazon.com/cloudwatch/deeplink.js?region=eu-west-3#alarmsV2:alarm/CPU_VM1)

**Alarm Details:**

- Name: CPU\_VM1
- Description: # Alarma. El uso de CPU de VM1 está demasiado alto

**\*\*Se recomienda tomar acciones YA\*\***

- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [48.95625128844033 (20/05/23 15:21:00)] was greater than the threshold (0.8) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Saturday 20 May, 2023 15:26:53 UTC
- AWS Account: 620671984364
- Alarm Arn: arn:aws:cloudwatch:eu-west-3:620671984364:alarm:CPU\_VM1

**Threshold:**

- The alarm is in the ALARM state when the metric is GreaterThanThreshold 0.8 for at least 1 of the last 1 period(s) of 300 seconds.

**Monitored Metric:**

- MetricNamespace: AWS/EC2
- MetricName: CPUUtilization
- Dimensions: [InstanceId = i-076569db474ce73cd]
- Period: 300 seconds
- Statistic: Average