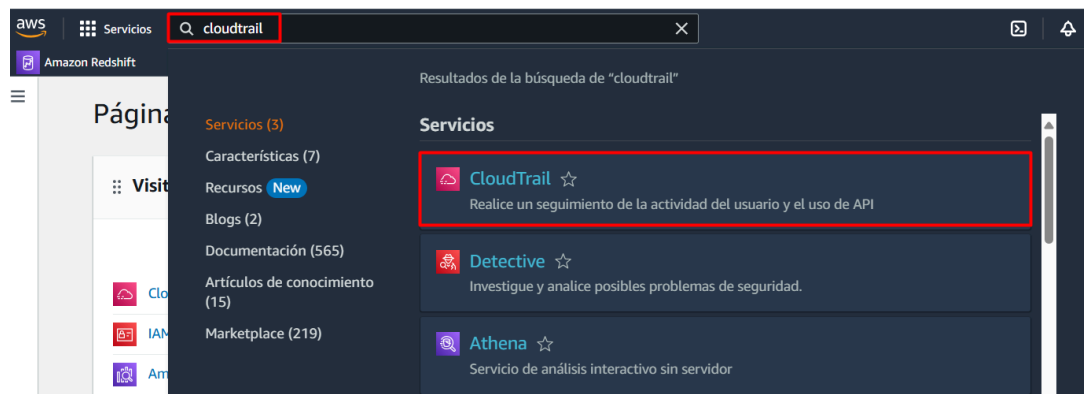


LABORATORIO CLOUDTRAIL Y CLOUDWATCH	2
CLOUDTRAIL EXISTENTE	2
TRAIL NUEVO GUARDAR MÁS DE 90 DIAS	4
CLOUDWATCH	4

LABORATORIO CLOUDTRAIL Y CLOUDWATCH

CLOUDTRAIL EXISTENTE

1. En el buscador digitamos CloudTrail y seleccionamos el servicio:



2. En la consola de AWS CloudTrail damos clic en **Historial de eventos**:



3. Filtramos la búsqueda:

- Tipo de recurso: IAM User
- Fecha y hora: Intervalo absoluto
- Establecemos fecha y hora de inicio
- Establecemos fecha y hora de finalización
- **Aplicar** parámetros de búsqueda

Historial de eventos (10) [Información](#)

El historial de eventos muestra los últimos 90 días de eventos de administración.

Atributos de búsqueda

1 Tipo de recurso Q. AWS::IAM::User 2 Filtros por fecha y hora 3

Intervalo relativo Intervalo absoluto 4

< junio de 2024 julio de 2024 >

dom lun mar mié jue vie sáb dom lun mar mié jue vie sáb

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

21 22 23 24 25 26 27 28 29 30 31

Fecha de inicio Hora de inicio Fecha de finalización Hora de finalización

2024/07/22 00:00:00 2024/07/22 23:59:59

5 6 7 8

El intervalo debe estar comprendido entre hoy y los últimos 90 días. Use el formato de 24 horas.

Zona horaria Zona horaria local

Borrar y descartar Cancelar Aplicar 8

0 / 5 eventos seleccionados

Nombre del evento	Hora del evento	Nombre de usuario	Origen del evento
AddUserToGroup	julio 22, 2024, 23:14:41 (UTC-0...)	root	iam.amazonaws.com
DetachUserPolicy	julio 22, 2024, 22:47:27 (UTC-0...)	root	iam.amazonaws.com
AttachUserPolicy	julio 22, 2024, 22:28:47 (UTC-0...)	root	iam.amazonaws.com
AttachUserPolicy	julio 22, 2024, 21:39:06 (UTC-0...)	root	iam.amazonaws.com
CreateLoginProfile	julio 22, 2024, 21:39:06 (UTC-0...)	root	iam.amazonaws.com
CreateUser	julio 22, 2024, 21:39:05 (UTC-0...)	root	iam.amazonaws.com
AddUserToGroup	julio 07, 2024, 13:02:55 (UTC-0...)	root	iam.amazonaws.com
CreateAccessKey	julio 07, 2024, 12:30:10 (UTC-0...)	root	iam.amazonaws.com
CreateLoginProfile	julio 07, 2024, 12:22:44 (UTC-0...)	root	iam.amazonaws.com
CreateUser	julio 07, 2024, 12:22:44 (UTC-0...)	root	iam.amazonaws.com

AWS CloudTrail nos muestra los eventos que coinciden con la búsqueda que acabamos de hacer:

Historial de eventos (6) [Información](#)

El historial de eventos muestra los últimos 90 días de eventos de administración.

Atributos de búsqueda

¿Qué? Tipo de recurso Q. AWS::IAM::User ¿Quién? 2024-07-22T00:00:00-05:00 — 2024-07-22T23:59:59-05:00

Nombre del evento	Hora del evento	Nombre de usuario	Origen del evento	Tipo de recurso	Nombre del recurso
AddUserToGroup	julio 22, 2024, 23:14:41 (UTC-0...)	root	iam.amazonaws.com	AWS::IAM::User, AWS::IAM::User	test_betek1, admin
DetachUserPolicy	julio 22, 2024, 22:47:27 (UTC-0...)	root	iam.amazonaws.com	AWS::IAM::User, AWS::IAM::User	test_betek1, arn:aws:iam::aws:policy/AdministratorAccess
AttachUserPolicy	julio 22, 2024, 22:28:47 (UTC-0...)	root	iam.amazonaws.com	AWS::IAM::User, AWS::IAM::User	test_betek1, arn:aws:iam::aws:policy/AdministratorAccess
AttachUserPolicy	julio 22, 2024, 21:39:06 (UTC-0...)	root	iam.amazonaws.com	AWS::IAM::User, AWS::IAM::User	test_betek1, arn:aws:iam::aws:policy/IAMUserChangePassword
CreateLoginProfile	julio 22, 2024, 21:39:06 (UTC-0...)	root	iam.amazonaws.com	AWS::IAM::User	test_betek1
CreateUser	julio 22, 2024, 21:39:05 (UTC-0...)	root	iam.amazonaws.com	AWS::IAM::User, AWS::IAM::User	arn:aws:iam::933028198366:user/test_betek1, AIDASSPGQ07P...

Nos muestra para cada evento el nombre (qué se hizo), la hora del evento (cuándo se hizo), el nombre de usuario (quién lo hizo), el origen del evento, el tipo de recurso y el nombre del recurso.

TRAIL NUEVO GUARDAR MÁS DE 90 DIAS

Para crear un trail nuevo:

1. Ir a CloudTrail
2. Crear un nuevo Trail
3. Configurar:
 - Trail name: **Lab-CloudTrail**
 - Storage en S3 (crear bucket nuevo)
 - Activar eventos de management (Read y Write)

Los eventos se separan por:

- Read = Describe, List
- Write = Create, Delete, Modify

CLOUDWATCH

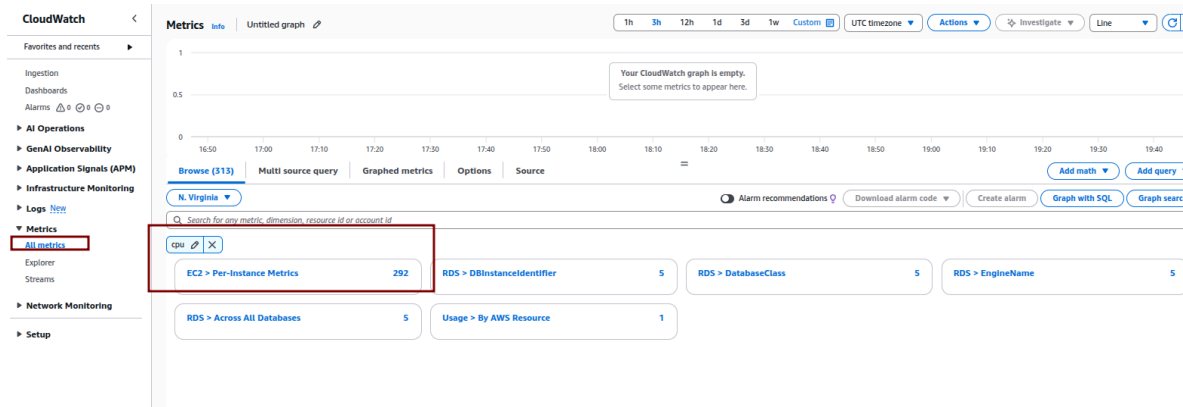
En esta práctica vamos a crear una alarma real y verla dispararse:

Paso 1 — Ir a Métricas

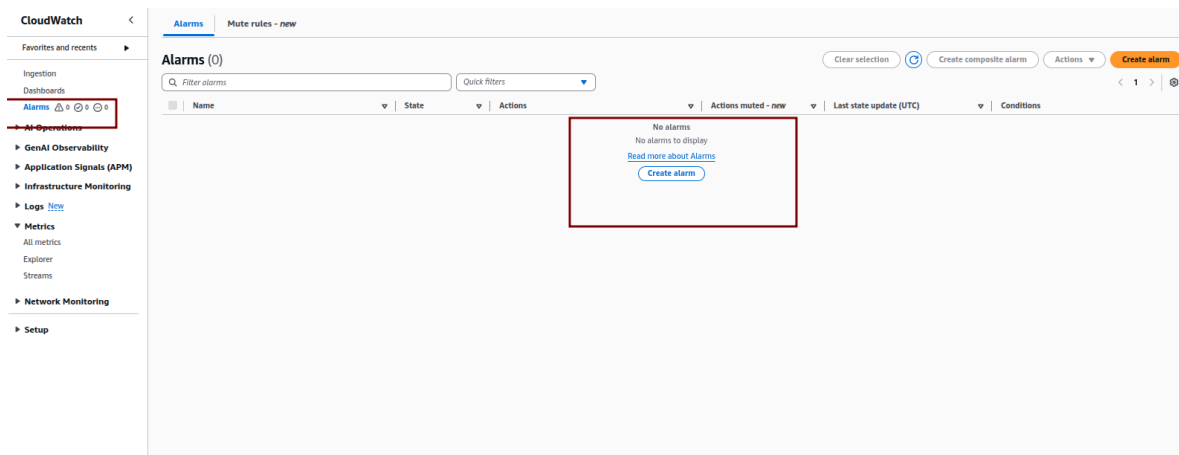
CloudWatch - Metrics - EC2

Selecciona:

CPU Utilization

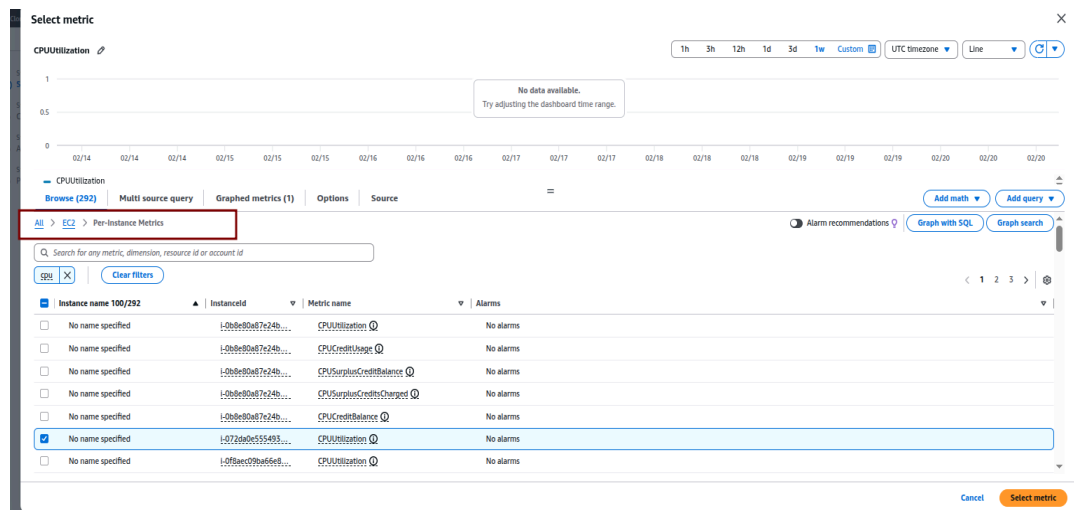


Paso 2 — Crear la alarma

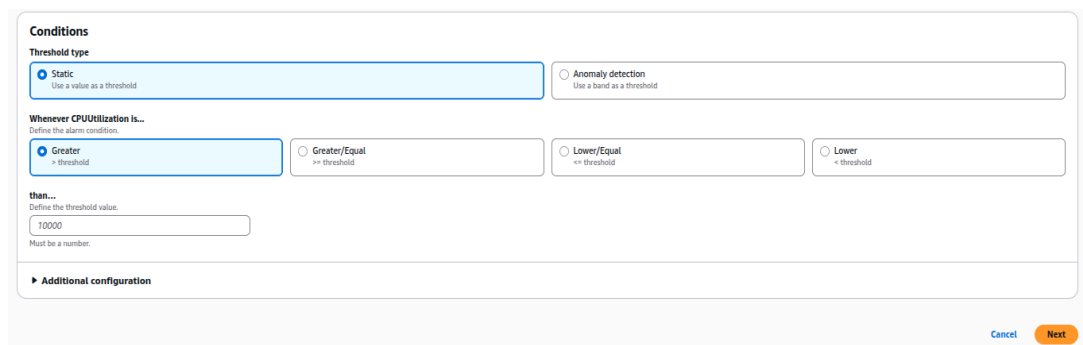


Paso 3 — Configurar de alarma

1. Selecciona la métrica a la cual deseas generar la alarma



2. Selecciona la unidad de medida que deseamos evaluar, por ejemplo, si la CPU supera el 90%



The screenshot shows the 'Conditions' configuration step in AWS CloudWatch. The 'Threshold type' is set to 'Static' with a value of 10000. The 'Whenever CPUUtilization is...' condition is set to 'Greater'.

Conditions

Threshold type

☒ Static
Use a value as a threshold

☐ Anomaly detection
Use a band as a threshold

Whenever CPUUtilization is...

☒ Greater
threshold

☐ Greater/Equal
>= threshold

☐ Lower/Equal
<= threshold

☐ Lower
< threshold

than...

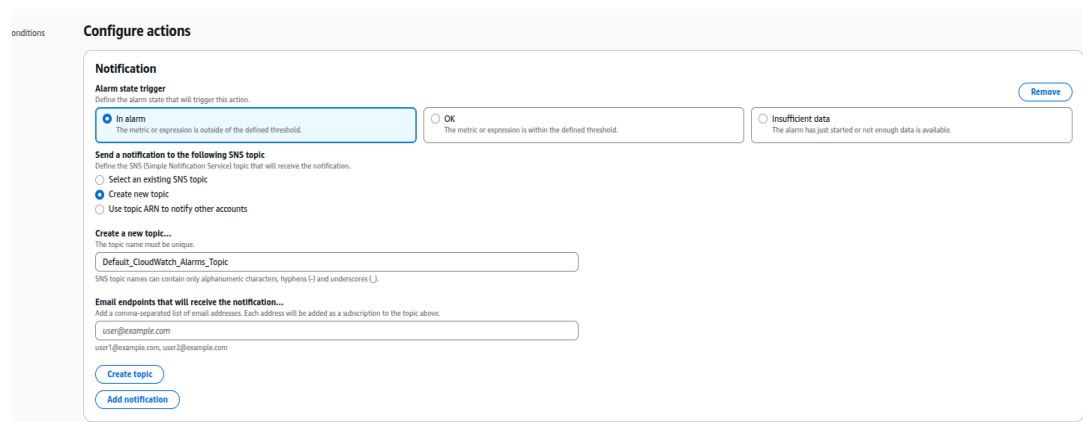
Define the threshold value.

10000

Must be a number.

Additional configuration

3. Selecciona el tipo de envío de alerta para que llegue a el correo



The screenshot shows the 'Configure actions' step in AWS CloudWatch. The 'Notification' action is selected, and the 'Alarm state trigger' is set to 'In alarm'. The 'Send a notification to the following SNS topic' is set to 'Create new topic'.

Configure actions

Notification

Alarm state trigger

☒ In alarm
The metric or expression is outside of the defined threshold.

☐ OK
The metric or expression is within the defined threshold.

☐ Insufficient data
The alarm has just started or not enough data is available.

Send a notification to the following SNS topic.

Define the SNS (Simple Notification Service) topic that will receive the notification.

☐ Select an existing SNS topic

☒ Create new topic

☐ Use topic ARN to notify other accounts

Create a new topic...

The topic name must be unique.

Default_CloudWatch_Alerts_Topic

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification...

Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

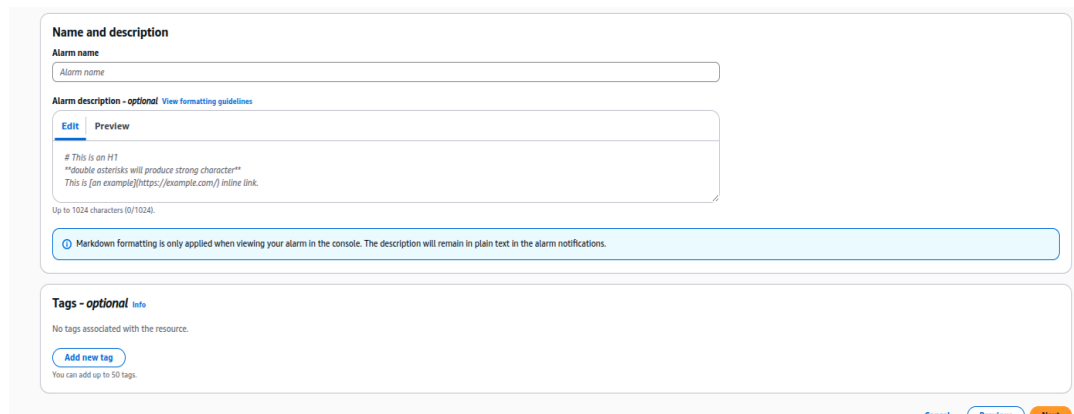
user@example.com

user1@example.com, user2@example.com

Create topic

Add notification

4. Selecciona el mensaje y el asunto que desea en esta alerta



Paso 4 — Conectarse a la EC2 para estresarla

Ejecuta los siguientes comandos:

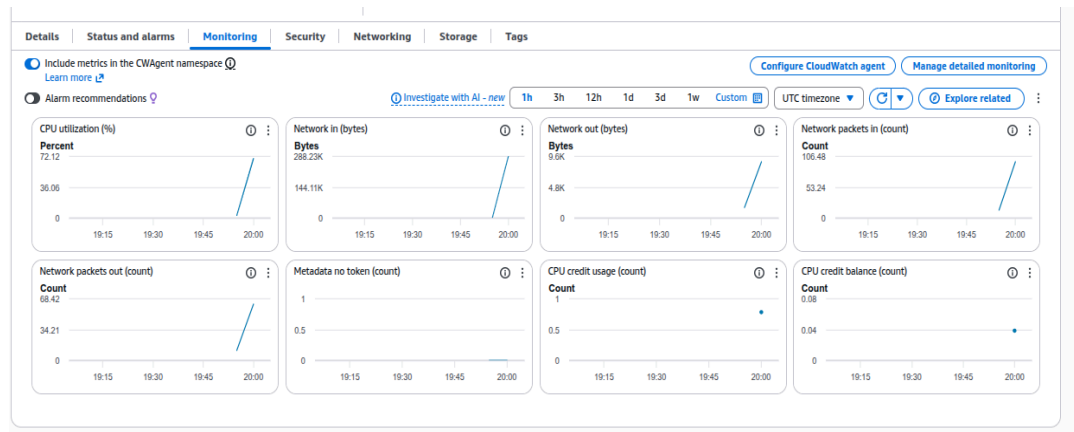
sudo dnf install stress -y —> Instala utilidad para estresar el servidor

stress --cpu \$(nproc) --timeout 300 & —> Envía a segundo plano el test de estrés

Paso 5 — Validar las métricas y la alarma

Pasado un tiempo deberá el consumo verse afectado a nivel de CPU

1. Validarlo desde la consola de cloudwatch



2. Revisa si la alarma llegó de manera correcta

RECUERDA: Eliminar todos los recursos desplegados en esta práctica