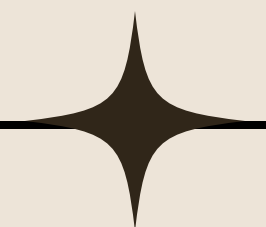


LAB. N° 186

# SUPERVISION DE LA INFRAESTRUCTURA

Sony Etcheverry,  
Michelle Devera,  
Cristofer Gutierrez  
Facundo Morales,  
Fernanda Urman, ,



# Objetivos

Supervisar las aplicaciones y la infraestructura es fundamental para ofrecer servicios de TI confiables y coherentes.

Los requisitos de supervisión van desde la recopilación de estadísticas para análisis a largo plazo hasta la reacción rápida a los cambios y a las interrupciones. La supervisión también puede servir de apoyo a los informes de cumplimiento al verificar de manera continua que la infraestructura cumple los estándares de la organización.

En este laboratorio, se muestra cómo utilizar las métricas de Amazon CloudWatch, Registros de Amazon CloudWatch, Eventos de Amazon CloudWatch y AWS Config para supervisar la infraestructura y las aplicaciones.

Después de completar este laboratorio, podrá hacer lo siguiente:

- Utilizar activar comando de AWS Systems Manager para instalar el agente de CloudWatch en instancias de Amazon Elastic Compute Cloud (Amazon EC2).
- Supervisar los registros de aplicaciones con el agente de CloudWatch y con Registros de CloudWatch.
- Supervisar las métricas del sistema con el agente de CloudWatch y las métricas de CloudWatch.
- Crear notificaciones en tiempo real con Eventos de CloudWatch
- Realizar un seguimiento del cumplimiento de la infraestructura mediante AWS Config.

# Tarea 1: instalar el agente de CloudWatch

Puede utilizar el agente de CloudWatch para recopilar métricas de las instancias de EC2 y de los servidores en las instalaciones, incluidas las siguientes:

- Métricas a nivel de sistema de las instancias de EC2, como la asignación de recursos de la CPU, el espacio libre en el disco y la utilización de la memoria. Estas métricas se recopilan de la propia máquina y complementan las métricas estándar de CloudWatch que recopila CloudWatch.
- Métricas a nivel de sistema de servidores en las instalaciones que permiten la supervisión de entornos híbridos y de servidores no administrados por AWS.
- Registros del sistema y de las aplicaciones de servidores Linux y Windows.
- Métricas personalizadas de aplicaciones y servicios que utilizan los protocolos StatsD y collectd.

En esta tarea, se utilizará Systems Manager para instalar el agente de CloudWatch en una instancia de EC2. Lo configurará para recopilar tanto las métricas de la aplicación como las del sistema.

En esta tarea, se utilizará Systems Manager para instalar el agente de CloudWatch en una instancia de EC2. Lo configurará para recopilar tanto las métricas de la aplicación como las del sistema.



Seleccionamos el botón situado junto a  
AWSConfigureAWSPackage

## Run a command

### Command document

Select the type of command that you want to run.

Q Search by keyword or filter by tag or attributes

< 1 2 3 4 ... >

	Name	Owner	Platform types
<input type="radio"/>	<a href="#">AWS-ApplyAnsiblePlaybooks</a>	Amazon	Linux
<input type="radio"/>	<a href="#">AWS-ApplyChefRecipes</a>	Amazon	Windows, Linux
<input type="radio"/>	<a href="#">AWS-ApplyDSCMofs</a>	Amazon	Windows
<input type="radio"/>	<a href="#">AWS-ApplyPatchBaseline</a>	Amazon	Windows
<input checked="" type="radio"/>	<a href="#">AWS-ConfigureAWSPackage</a>	Amazon	Windows, Linux, MacOS
<input type="radio"/>	<a href="#">AWS-ConfigureCloudWatch</a>	Amazon	Windows
<input type="radio"/>	<a href="#">AWS-ConfigureDocker</a>	Amazon	Windows, Linux
<input type="radio"/>	<a href="#">AWS-ConfigureKernelLivePatching</a>	Amazon	Linux
<input type="radio"/>	<a href="#">AWS-ConfigureWindowsUpdate</a>	Amazon	Windows
<input type="radio"/>	<a href="#">AWS-FindWindowsUpdates</a>	Amazon	Windows

### Command parameters

#### Action

(Required) Specify whether or not to install or uninstall the package.

Install ▼

#### Installation Type

(Optional) Specify the type of installation. Uninstall and reinstall: The application is taken offline until the reinstallation process completes. In-place updates: New or updated files are added to the installation.

Uninstall and reinstall ▼

#### Installation Type

(Optional) Specify the type of installation. Uninstall and reinstall: The application is taken offline until the reinstallation process completes. In-place updates: New or updated files are added to the installation.

Uninstall and reinstall ▼

#### Name

(Required) The package to install/uninstall.

AmazonCloudWatchAgent

#### Version

(Optional) The version of the package to install or uninstall. If you don't specify a version, the system installs the latest published version by default. If a version is specified that is not published, the system returns an error. If no version of the package is installed, the system returns an error.

latest

#### Additional Arguments

(Optional) The additional parameters to provide to your install, uninstall, or update scripts.

{}

Una vez desplegado el menu de los parametros de comando le daremos

- Una acción : Install
- Un nombre : AmazonCloudWatchAgent
- Una version : Latest

En la sección de destinos escogemos las instancias manualmente y seleccionamos el servidor web donde instalaremos CloudWatch

### Target selection

Target selection

Choose a method for selecting targets.

☐ Specify instance tags  
Specify one or more tag key-value pairs to select instances that share those tags.

☒ Choose instances manually  
Manually select the instances you want to register as targets.

☐ Choose a resource group  
Choose a resource group that includes the resources you want to target.

i-027a34061518c0e24

#### Instances

< 1 >

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Availability zone	Ping status	Last ping time
<input checked="" type="checkbox"/>	Web Server	i-027a34061518c0e24	running	us-west-2a	Online	11/7/2024 at 19



Este mensaje nos confirma que el comando con ese ID, se ejecuto correctamente

✔ Command ID: eefc969c-4d1f-4e57-8381-f7a4a8701f05 was successfully sent!

[AWS Systems Manager](#) > [Run Command](#) > Command ID: eefc969c-4d1f-4e57-8381-f7a4a8701f05

Command ID: eefc969c-4d1f-4e57-8381-f7a4a8701f05

↺

Cancel command

Rerun

Copy to new

Command status

Overall status	Detailed status	# targets	# completed	# error	# delivery timed out
✔ Success	✔ Success	1	1	0	0



Expandimos la pestaña de paso 1 y podemos observar un mensaje que nos dice que la ejecución del paso se omitió debido a que no se satisficieron las condiciones previas

Step 1 - Command description and status

Status	Detailed status	Response code	Step name	Start time	Finish time
Success	Success	0	createDownloadFolder	Thu, 11 Jul 2024 23:02:31 GMT	Thu, 11 Jul 2024 23:02:31 GMT

▼ Output

The command output displays a maximum of 24,000 characters. You can view the complete command output in either Amazon S3 or CloudWatch Logs, if you specify an S3 bucket or a logs group when you run the command.

Step execution skipped due to unsatisfied preconditions: '"StringEquals": [platformType, Windows]'. Step name: createDownloadFolder

Copy

Download

► Error

Esta salida por ahora es ignorada ya que vamos a realizar a posterioridad otras configuraciones con el agente de Cloud Watch

Step 2 - Command description and status

Status	Detailed status	Response code	Step name	Start time	Finish time
Success	Success	0	configurePackage	Thu, 11 Jul 2024 23:02:31 GMT	Thu, 11 Jul 2024 23:02:44 GMT

▼ Output

The command output displays a maximum of 24,000 characters. You can view the complete command output in either Amazon S3 or CloudWatch Logs, if you specify an S3 bucket or a logs group when you run the command.

```
Initiating arn:aws:ssm:::package/AmazonCloudWatchAgent 1.300041.0b681
install

Plugin aws:runShellScript ResultStatus Success

install output: Running sh install.sh

create group cwagent, result: 0

create user cwagent, result: 0

Successfully installed arn:aws:ssm:::package/AmazonCloudWatchAgent
1.300041.0b681
```

Copy

Download

**Parameter details**

Name

Monitor-Web-Server

×

When naming a parameter, you can use forward slashes (/) to organize it into a hierarchy. [Learn more about hierarchies](#)

Description — *Optional*

Collect web logs and system metrics

Tier

Parameter Store offers standard and advanced parameters.

☒ Standard

Store up to 10,000 standard parameters. Store parameter values up to 4 KB. Parameter policies and sharing with other AWS accounts are not available. No additional charge.

☐ Advanced

Store up to 100,000 advanced parameters. Store parameter values up to 8 KB. Add parameter policies. Share with other AWS accounts. Charges apply.

Standard parameters cannot be shared with other AWS accounts. [Learn more](#)

Type

☒ String

Any string value.

☐ StringList

Separate strings using commas.

☐ SecureString

Encrypt sensitive data using KMS keys from your account or another account.

Data type

El archivo de configuración en este parametro define la recolección de logs de acceso y errores del servidor web Apache, enviándolos a CloudWatch Logs para análisis.

Creamos un nuevo parámetro que será referenciado al iniciar CloudWatch

Command document

Select the type of command that you want to run.

Search by keyword or filter by tag or attributes

Search: AmazonCloudWatch-ManageAgent

Clear filters

< 1 >

Name	Owner	Platform types
<div><div></div><div><a href="#">AmazonCloudWatch-ManageAgent</a></div></div>	Amazon	Windows, Linux, MacOS

Description

Send commands to Amazon CloudWatch Agent

Document version

Choose the document version you want to run.

8 (Default)

En el icono de búsqueda configuramos para seleccionar nuestro CloudWatch

☆ AmazonCloudWatch-ManageAgent

Delete

Actions ▼

Run command

DescriptionContentVersionsDetails

Document version

8 (Default)

Description	Owner
Send commands to Amazon CloudWatch Agent	Amazon
Platform	Target type
Windows, Linux, MacOS	-
Created	Status
Wed, 21 Dec 2022 17:30:55 GMT	Active
Document version	Latest version
8 (Default)	8
Hash type	Hash

Este parametro permite que las instancias utilicen automáticamente la configuración de monitoreo del servidor web desde AWS Parameter Store a través del agente de AWS Systems Manager

### Command parameters

#### Action

The action CloudWatch Agent should take.

configure ▼

#### Mode

Controls platform-specific default behavior such as whether to include EC2 Metadata in metrics.

ec2 ▼

#### Optional Configuration Source

Only for 'configure' related actions. Use 'ssm' to apply a ssm parameter as config. Use 'default' to apply default config for amazon-cloudwatch-agent. Use 'all' with 'configure (remove)' to clean all configs for amazon-cloudwatch-agent.

ssm ▼

#### Optional Configuration Location

Only for 'configure' related actions. Only needed when Optional Configuration Source is set to 'ssm'. The value should be a ssm parameter name.

Monitor-Web-Server

Este mensaje nos confirma que el comando con ese ID, se ejecuto correctamente

✔ Command ID: 01bdad3f-9d59-4d5f-bbe8-05c06dab52df was successfully sent!

[AWS Systems Manager](#) > [Run Command](#) > Command ID: 01bdad3f-9d59-4d5f-bbe8-05c06dab52df

Command ID: 01bdad3f-9d59-4d5f-bbe8-05c06dab52df

↻

Cancel command

Rerun

Copy to new

Command status

Overall status	Detailed status	# targets	# completed	# error	# delivery timed out
✔ Success	✔ Success	1	1	0	0

Targets and outputs

View output

🔍 Search command invocations

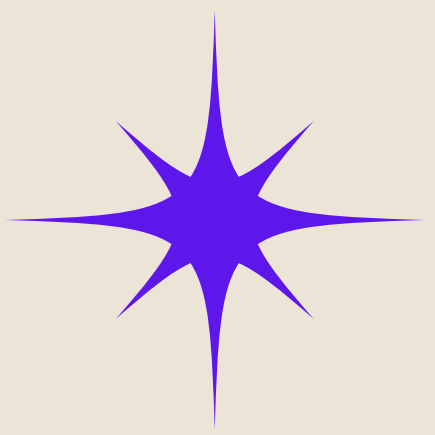
< 1 >

Instance ID	Instance name	Status	Detailed Status	Start time	File
○ <a href="#">i-027a34061518c0e24</a>	ip-10-0-0-110.us-west-2.compute.internal	✔ Success	✔ Success	Thu, 11 Jul 2024 23:21:52 GMT	TI

El agente de CloudWatch ahora se está ejecutando en la instancia y envía datos de registro y métricas a CloudWatch.

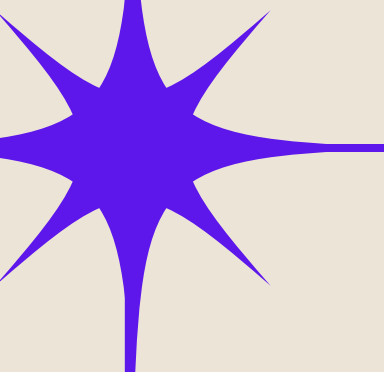


# Tarea 2: Supervisar registros de aplicaciones mediante Registros de CloudWatch

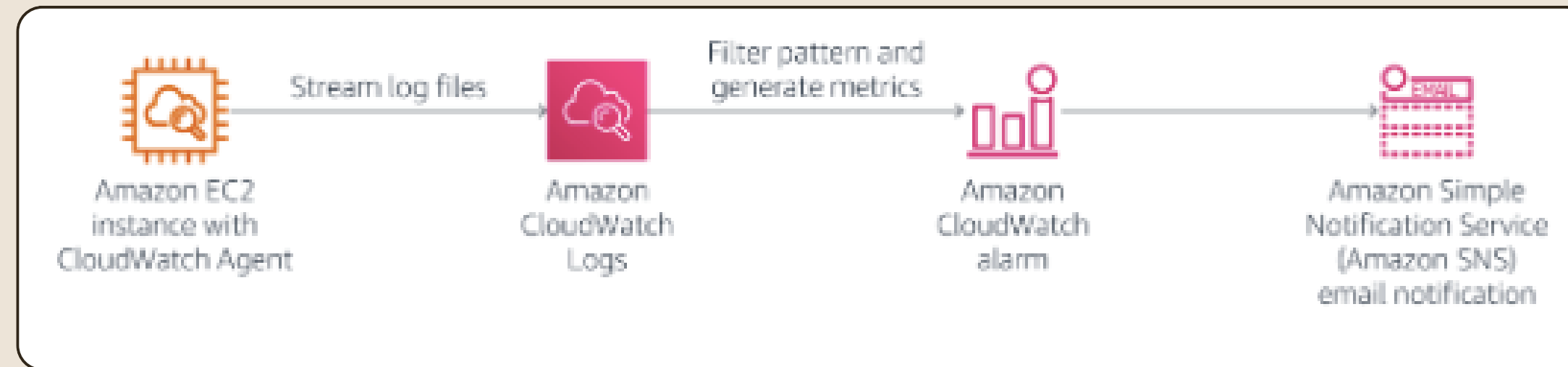


Puede utilizar Registros de CloudWatch para supervisar las aplicaciones y los sistemas con datos de registro. Por ejemplo, Registros de CloudWatch puede hacer un seguimiento del número de errores que se producen en los registros de la aplicación y enviarle una notificación cuando la tasa de errores supere el umbral que especifique.

Registros de CloudWatch utiliza sus datos de registro existentes para la supervisión, por lo que no se requieren cambios en el código. Por ejemplo, puede supervisar los registros de la aplicación en busca de términos literales específicos (como “NullPointerException”) o contar el número de apariciones de un término literal en una posición concreta de los datos de registro (como los códigos de estado 404 en un registro de acceso al servidor web). Cuando se encuentra el término que busca, Registros de CloudWatch informa los datos a una métrica de CloudWatch que usted especifica. Los datos del registro se cifran mientras están en tránsito y en reposo.



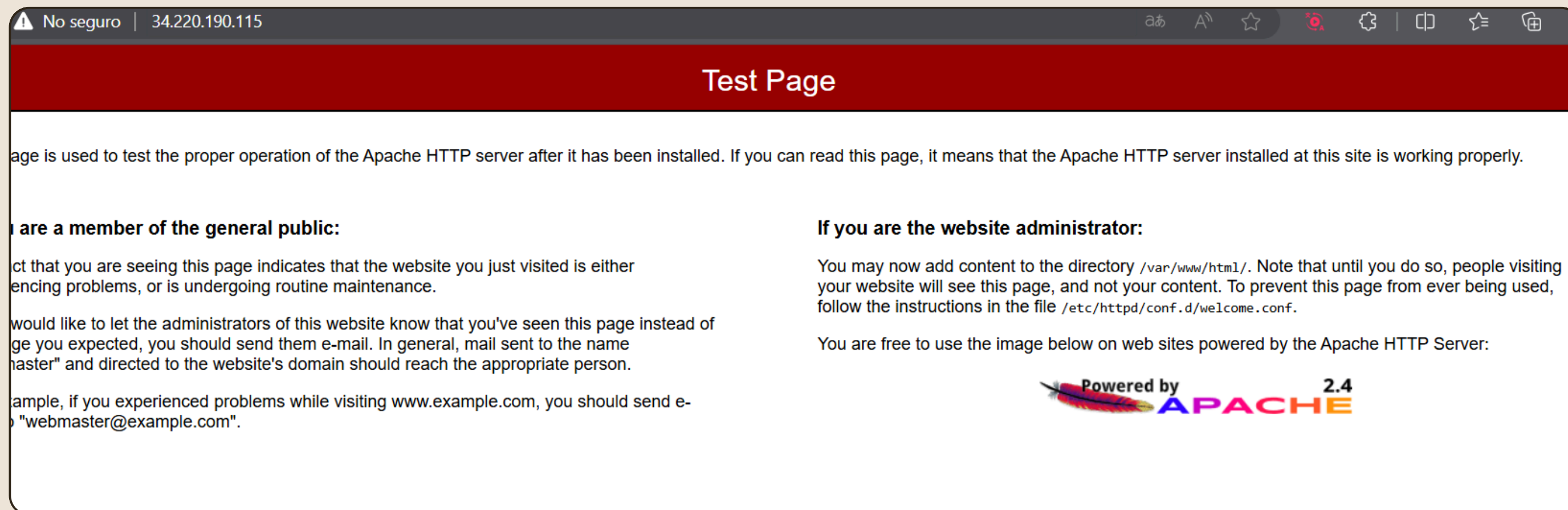
En esta tarea, generará datos de registro en el servidor web y, luego, supervisará los registros mediante Registros de CloudWatch.



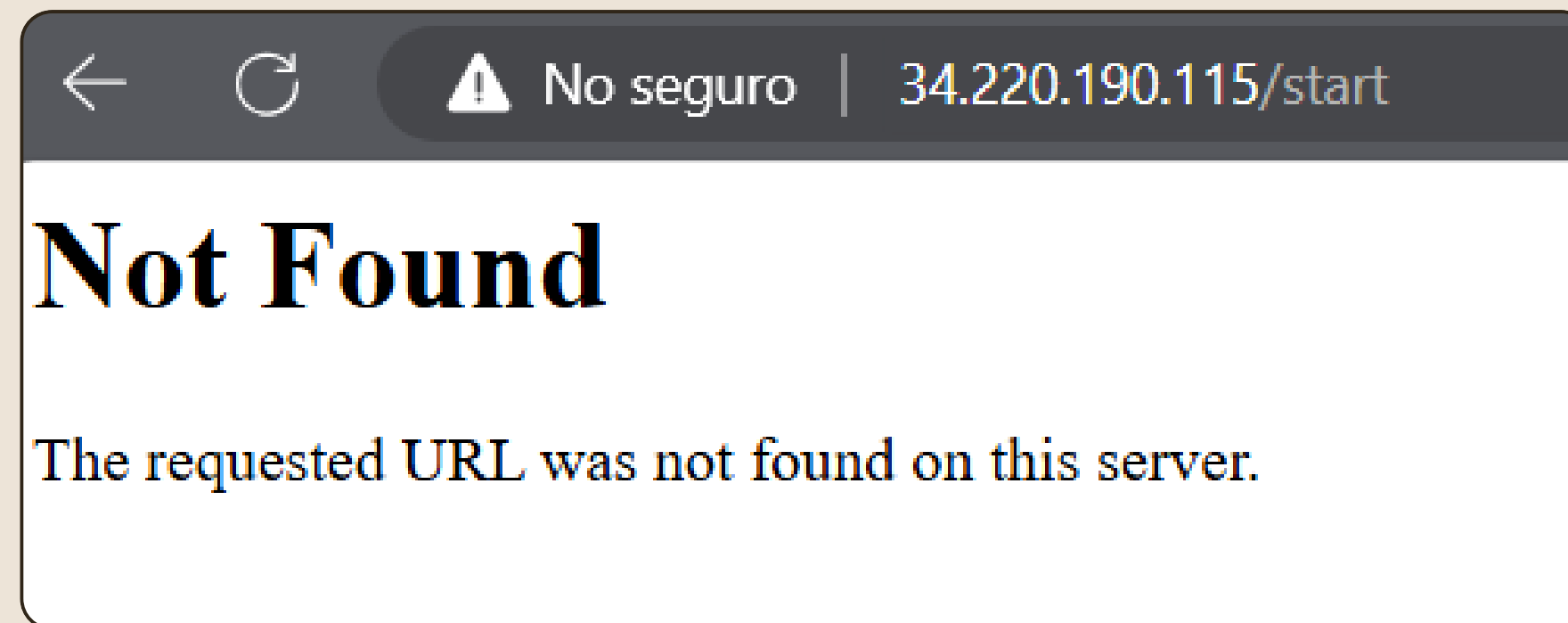
El servidor web genera dos tipos de datos de registro:

- registros de acceso
- registros de error

Luego procedemos a copiar nuestra IP de nuestro servidor web en una pestaña de nuestro navegador y vemos una página de prueba



Luego de agregarle “/start” a nuestra url podemos ver que nos envia un mensaje de error ya que la pagina no existe. Esto está bien asi podemos generar registros para enviar a CloudWatch



Seleccionando el flujo de logs con el mismo nombre que la instancia se visualizan datos de solicitudes GET al servidor web, incluyendo detalles del cliente como navegador y sistema operativo.

Log events

Actions ▼

Start tailing

Create metric filter

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Filter events - press enter to search

Clear

1m

30m

1h

12h

Custom

UTC timezone ▼

Display ▼

	Timestamp	Message
		No older events at this moment. <a href="#">Retry</a>
	2024-07-11T23:24:29.645Z	167.61.70.173 - - [11/Jul/2024:23:24:29 +0000] "GET / HTTP/1.1" 403 3630 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)..."
	2024-07-11T23:24:29.895Z	167.61.70.173 - - [11/Jul/2024:23:24:29 +0000] "GET /icons/apache_pb2.gif HTTP/1.1" 200 4234 "http://34.220.190.115/" "..."
	2024-07-11T23:24:33.978Z	167.61.70.173 - - [11/Jul/2024:23:24:29 +0000] "GET /favicon.ico HTTP/1.1" 404 196 "http://34.220.190.115/" "Mozilla/5.0..."
	2024-07-11T23:25:44.979Z	167.61.70.173 - - [11/Jul/2024:23:25:40 +0000] "GET /start HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0"
		No newer events at this moment. Auto retry paused. <a href="#">Resume</a>

# Aquí crearemos un filtro de métricas en los registros de CloudWatch

En Grupos de registros marcamos la verificación junto a HttpAccessLog. Luego en Acciones, seleccionamos Crear un filtro de métricas.

La siguiente línea en la casilla Patrón de filtro la usamos para especificar como queremos filtrar

**Create filter pattern**

You can use metric filters to monitor events in a log group as they are sent to CloudWatch Logs. You can monitor values from log events and associate the results with a metric. [Learn more about pattern syntax.](#)

**Filter pattern**

Specify the terms or pattern to match in your log events to create metrics.



Luego para probar el patrón, en el menú para seleccionar el ID de la instancia de EC2.

Seleccionamos nuestro Log

- Seleccionamos “Probar patrón”.
- En “Resultados”, seleccionamos “Mostrar resultados de la prueba”.
- Allí podemos ver un par de resultados con “\$status\_code de 404”. Es decir, este código de estado indica que se solicitamos una página que no se encontró.

Test pattern

Select log data to test

i-027a34061518c0e24

Log event messages

Type log data to test with your Filter Pattern. Please use line breaks to separate log events.

167.61.70.173 -- [11/Jul/2024:23:24:29 +0000] "GET / HTTP/1.1" 403 3630 "-"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0"  
167.61.70.173 -- [11/Jul/2024:23:24:29 +0000] "GET /icons/apache\_pb2.gif HTTP/1.1"  
200 4234 "http://34.220.190.115/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.0.0 Safari/537.36 Edg/126.0.0.0"

Test pattern

Results

Found 2 matches out of 4 event(s) in the sample log.

Show test results

	\$status_code	\$timestamp
rome/126.0.0.0 Safari/537.36 Edg/126.0.0.0"	404	11/Jul/2024:23:24:29 +0000
537.36 Edg/126.0.0.0"	404	11/Jul/2024:23:25:40 +0000



En la sección "Crear nombre de filtro", ingresamos "404Error" en el campo de nombre del filtro.

En la sección "Detalles de métrica", configuramos la siguiente información:

- Namespace de la métrica: Ingresamos "LogMetrics".
- Nombre de la métrica: Ingresamos "404Errors".
- Valor de la métrica: Ingresamos "1".

### Create filter name

Log events that match the pattern you define are recorded to the metric that you specify. You can graph the metric.

Filter name

Filter pattern

### Metric details

Metric namespace

Namespaces let you group similar metrics. [Learn more](#)

☒ Create

Namespaces can be up to 255 characters long; all characters are valid except for colon(:) at the start of the name.

Metric name

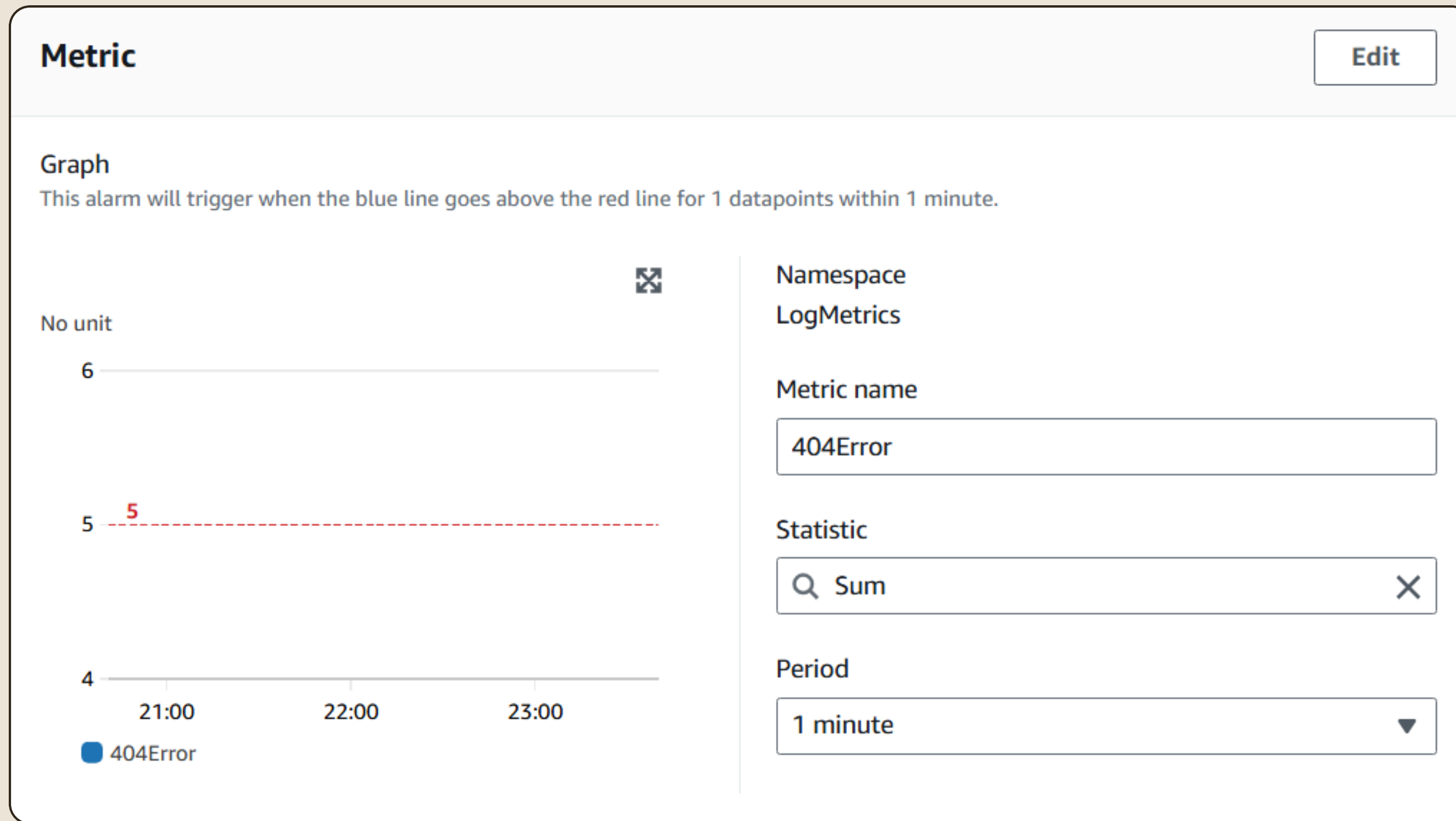
Metric name identifies this metric, and must be unique within the namespace. [Learn more](#)

Metric name can be up to 255 characters long; all characters are valid except for colon(:), asterisk(\*), dollar(\$), and space( ).

Metric value

Metric value is the value published to the metric name when a Filter Pattern match occurs.

En esta zona se visualiza la métrica en si



# Crear una alarma utilizando el filtro

Al crear nuestra alarma configuramos los siguientes ajustes:

- En la sección de Métricas, para Periodo, seleccionamos 1 minuto.
- En la sección de Condiciones, seleccionamos lo siguiente:
- Cuando 404Errors sea:  
Seleccionamos "Mayor o igual que".
- Que sea mayor o igual a:  
Ingresamos "5".

### Conditions

Threshold type

☒ Static  
Use a value as a threshold

☐ Anomaly detection  
Use a band as a threshold

Whenever 404Error is...  
Define the alarm condition.

☐ Greater  
> threshold

☒ Greater/Equal  
≥ threshold

☐ Lower/Equal  
≤ threshold

☐ Lower  
< threshold

than...  
Define the threshold value.

Must be a number

En Notificación, configuramos lo siguiente:

- Seleccione un tema de SNS: Crear un tema nuevo.
- Puntos de enlace de correo electrónico que recibirán la notificación: ingresamos nuestro correo
- Seleccionamos Crear un tema.
- Y luego siguiente

### Configure actions

#### Notification

Alarm state trigger  
Define the alarm state that will trigger this action.

☒ 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.

Remove

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

Send a notification to...

Default\_CloudWatch\_Alarms\_Topic

X

Only topics belonging to this account are listed here. All persons and applications subscribed to the selected topic will receive notifications.

Email (endpoints)  
luchogutmai06@gmail.com - [View in SNS Console](#)

Add notification

Para el nombre y la descripción, configuramos los siguientes ajustes:

- Nombre de la alarma:  
Ingresamos "404 Errors".
- Descripción de la alarma:  
Ingresamos "Alerta cuando se detectan demasiados errores 404 en una instancia".

**Name and description**

Alarm name

404 Error

Alarm description - *optional* [View formatting guidelines](#)

Edit


Preview


Alert when too many 404s detected on an instance.

Up to 1024 characters (49/1024)

Luego en nuestro correo confirmamos la subscripción para recibir las alertas

**AWS Notification - Unsubscribe Confirmation** Recibidos x


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

 Traducir al español ×

Your subscription to the topic below has been deactivated:  
**arn:aws:sns:us-west-2:639565736024:Default\_CloudWatch\_Alarms\_Topic**

If this was in error or you wish to resubscribe, click or visit the link below:  
[Resubscribe](#)

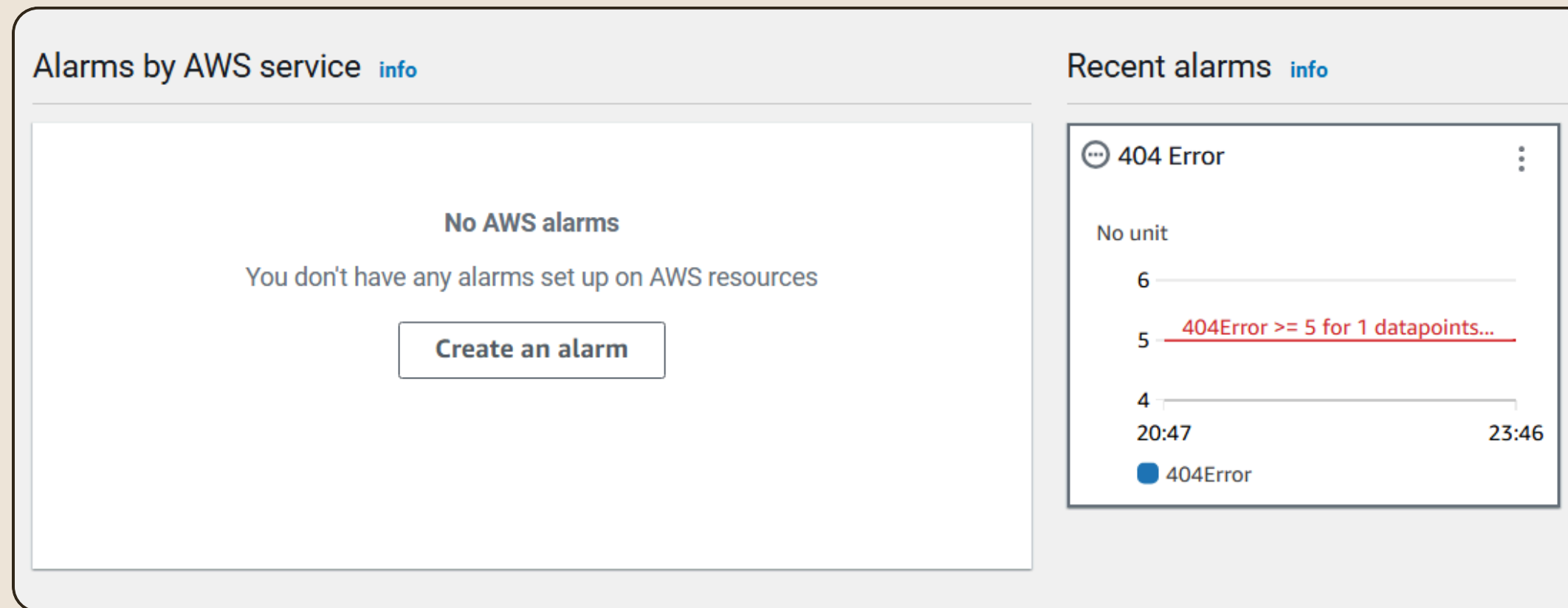
Please do not reply directly to this email. If you have any questions or comments regarding this email, please visit [AWS Support](#).

 Simple Notification Service

**Subscription confirmed!**  
You have successfully subscribed.  
Your subscription's id is:  
**arn:aws:sns:us-west-2:639565736024:Default\_CloudWatch\_Alarms\_Topic:3d93d9cc-9ffc-4dcc-b912-8b8a90f8caee**  
If it was not your intention to subscribe, [click here to unsubscribe](#).

Espere 1 o 2 minutos para que la alarma se active.

El gráfico que se muestra en la página de CloudWatch debería volverse rojo para indicar que está en el estado Alarma.

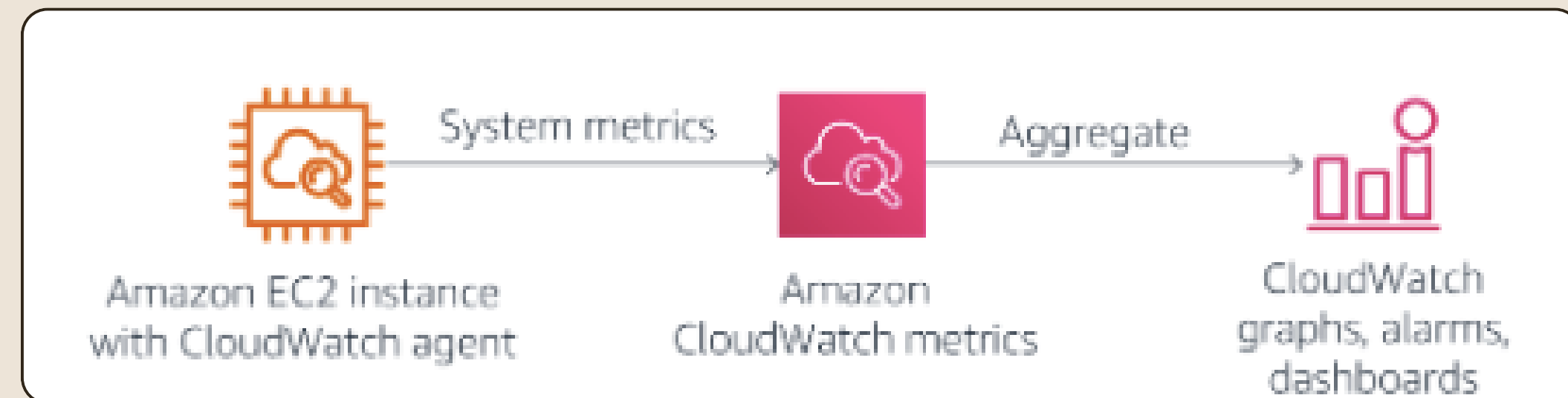




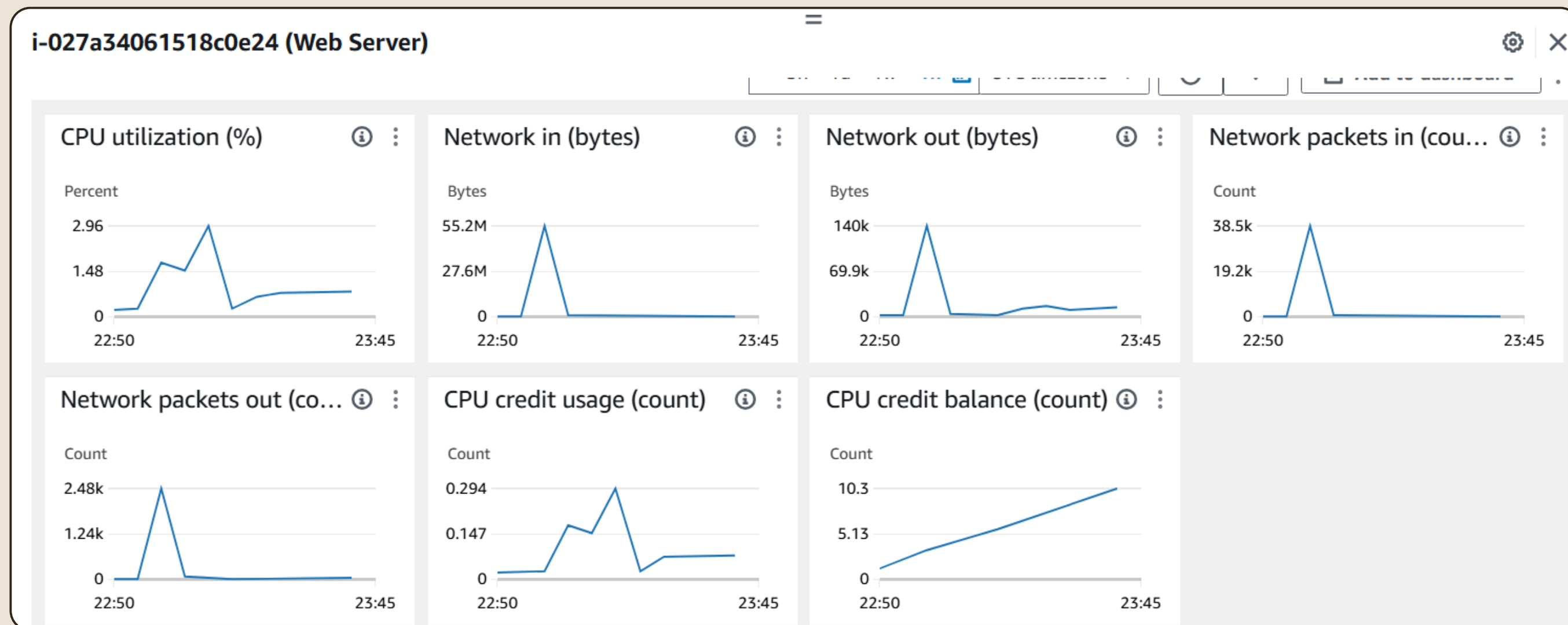
# Tarea 3: Supervisar métricas de las instancias mediante CloudWatch

Las métricas son datos sobre el rendimiento de los sistemas. CloudWatch almacena las métricas de los servicios de AWS que utiliza. También puede publicar las métricas de su aplicación a través del agente de CloudWatch o de manera directa desde su aplicación. CloudWatch puede presentar las métricas para su búsqueda o para representarlas en gráficos, paneles y alarmas.

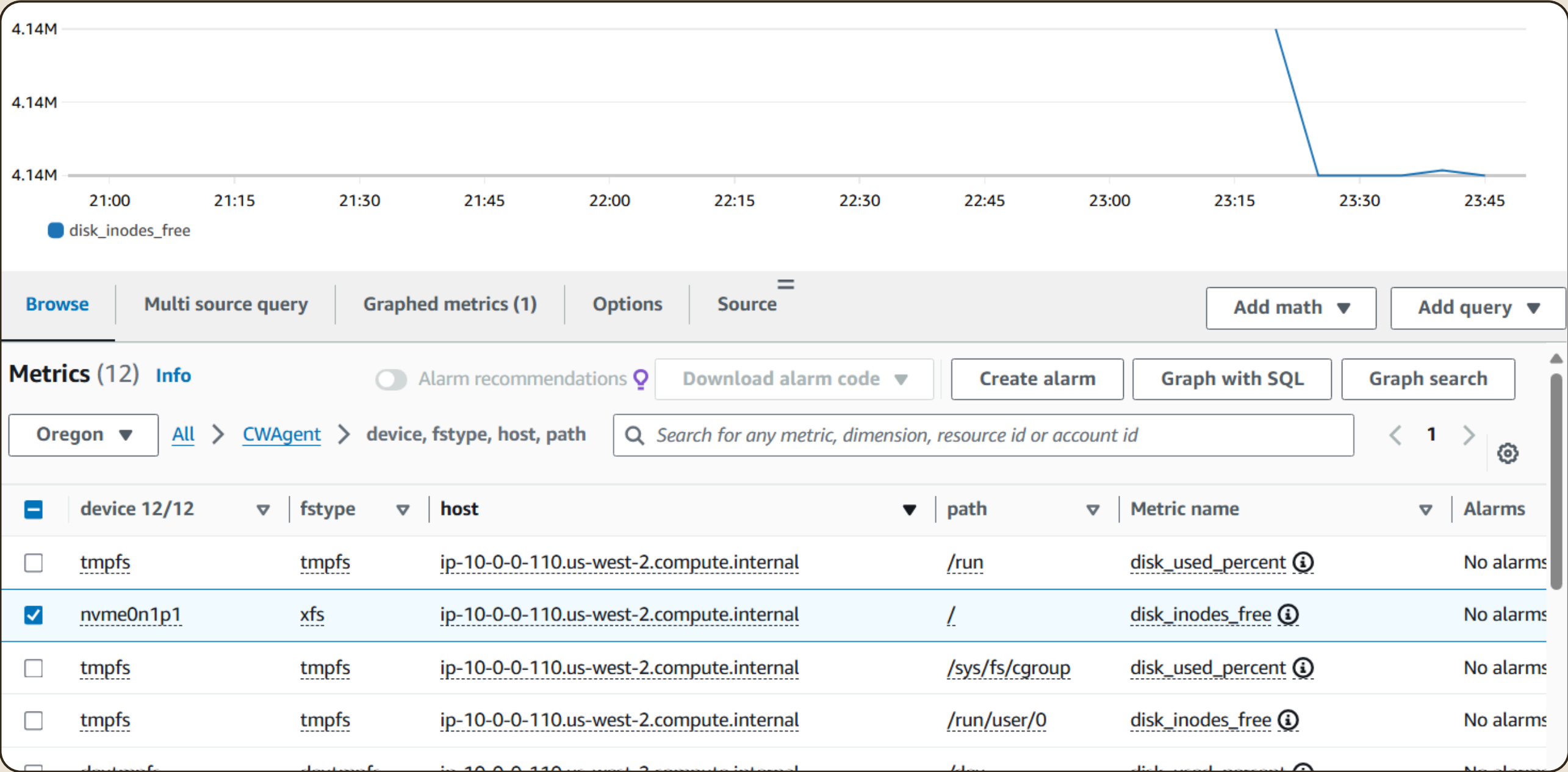
En esta tarea, se utilizarán las métricas que proporciona CloudWatch.



En esta zona pueden visualizarse esas métricas e información relacionada a nuestra EC2



Seleccione CW Agent y, luego, device, fstype, host, path. Esto con el fin de ver las métricas de espacio en disco que captura el agente de CloudWatch.

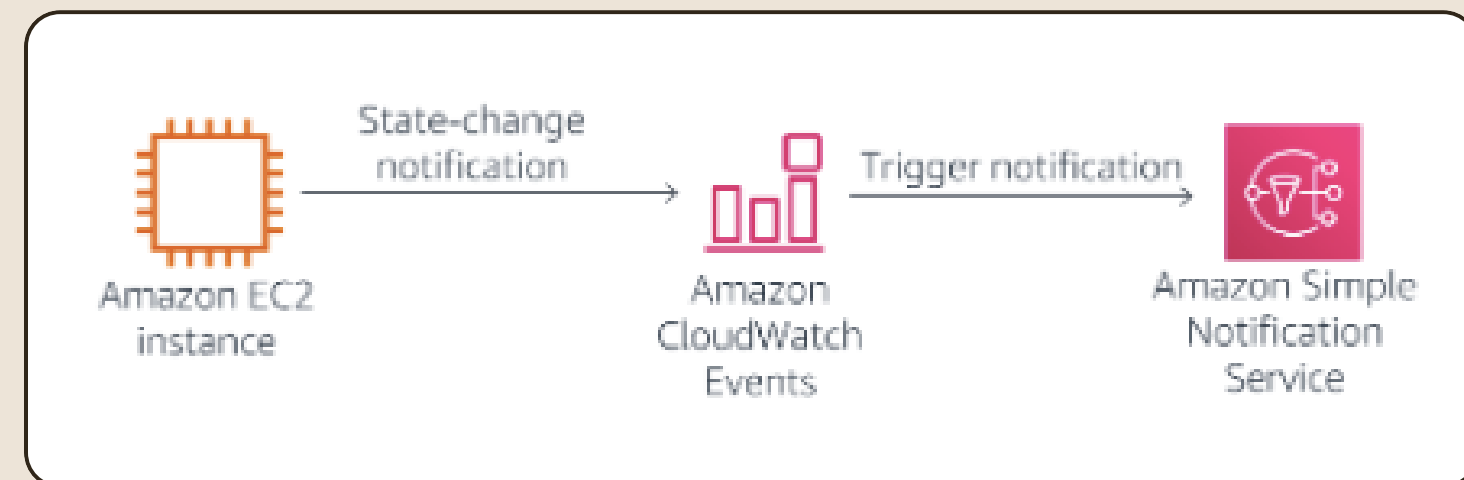


# Tarea 4: Crear notificaciones en tiempo real

Eventos de CloudWatch proporciona un flujo casi en tiempo real de eventos del sistema que describen cambios en los recursos de AWS. Las reglas simples pueden hacer coincidir eventos y dirigirlos a una o más funciones o flujos de destino. Eventos de CloudWatch registra los cambios operativos a medida que se producen.

Eventos de CloudWatch responde a estos cambios operativos y toma las medidas correctivas necesarias enviando mensajes para responder al entorno, activando funciones, realizando cambios y recopilando información sobre el estado. También puede utilizar Eventos de CloudWatch para programar acciones automatizadas que se activen por su cuenta en determinados momentos a través de expresiones cron o rate.

En esta tarea, creará una notificación en tiempo real que le informará cuando una instancia se detiene o termina.



En los detalles de la regla lo configuramos con estos datos y definimos el evento

Rule detail

Name

EC2

Maximum of 64 characters consisting of numbers, lower/upper case letters, ., -, \_.

Description - optional

EC2 Instance State-change Notification

Event bus [Info](#)

Select the event bus this rule applies to, either the default event bus or a custom or partner event bus.

default

☒ Enable the rule on the selected event bus

Rule type [Info](#)

☒ Rule with an event pattern

A rule that runs when an event matches the defined event pattern. EventBridge sends the event to the specified target.

☐ Schedule

A rule that runs on a schedule

Event pattern [Info](#)

Event source

AWS service or EventBridge partner as source

AWS services

AWS service

The name of the AWS service as the event source

EC2

Event type

The type of events as the source of the matching pattern

EC2 Instance State-change Notification

Event Type Specification 1

☐ Any state

☒ Specific state(s)

Specific state(s)

stopped X terminated X

Event Type Specification 2

☒ Any instance

☐ Specific instance Id(s)

Event pattern

Event pattern, or filter to match the events

```
1 {
2   "source": ["aws.ec2"],
3   "detail-type": ["EC2 Instance State-change Notification"]
4   "detail": {
5     "state": ["stopped", "terminated"]
6   }
7 }
```

Copy

Test pattern

Edit pattern

Y terminamos de configurar nuestra regla colocandole la SNS topic para luego crearla

**Target 1**

**Target types**  
Select an EventBridge event bus, EventBridge API destination (SaaS partner), or another AWS service as a target.

☐ EventBridge event bus

☐ EventBridge API destination

☒ AWS service

Select a target [Info](#)  
Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)

SNS topic

▼

Topic

Default\_CloudWatch\_Alarms\_Topic

▼

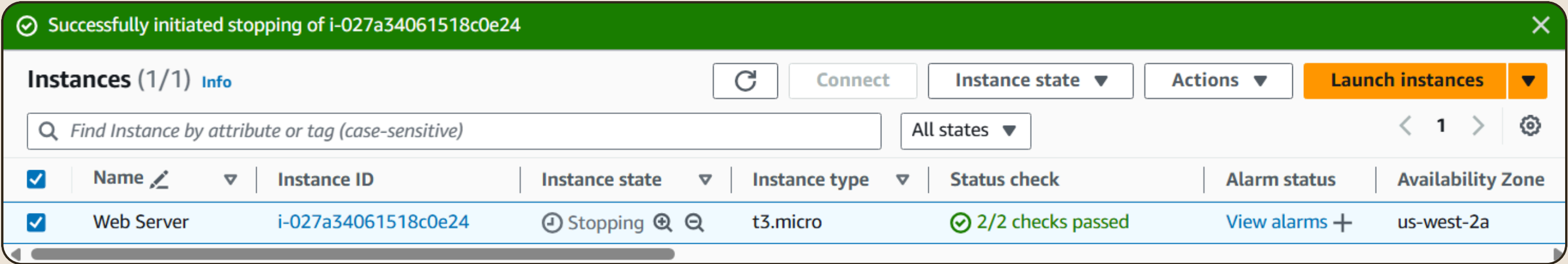
↺

► Additional settings

Luego podemos ver el mensaje de que se creó correctamente

✔ Rule error was created successfully

Detenemos la instancia de Web Server, acá podemos ver como se detuvo correctamente



Luego revisamos el correo y vemos que recibimos la notificación de que nuestra instancia se detuvo exitosamente



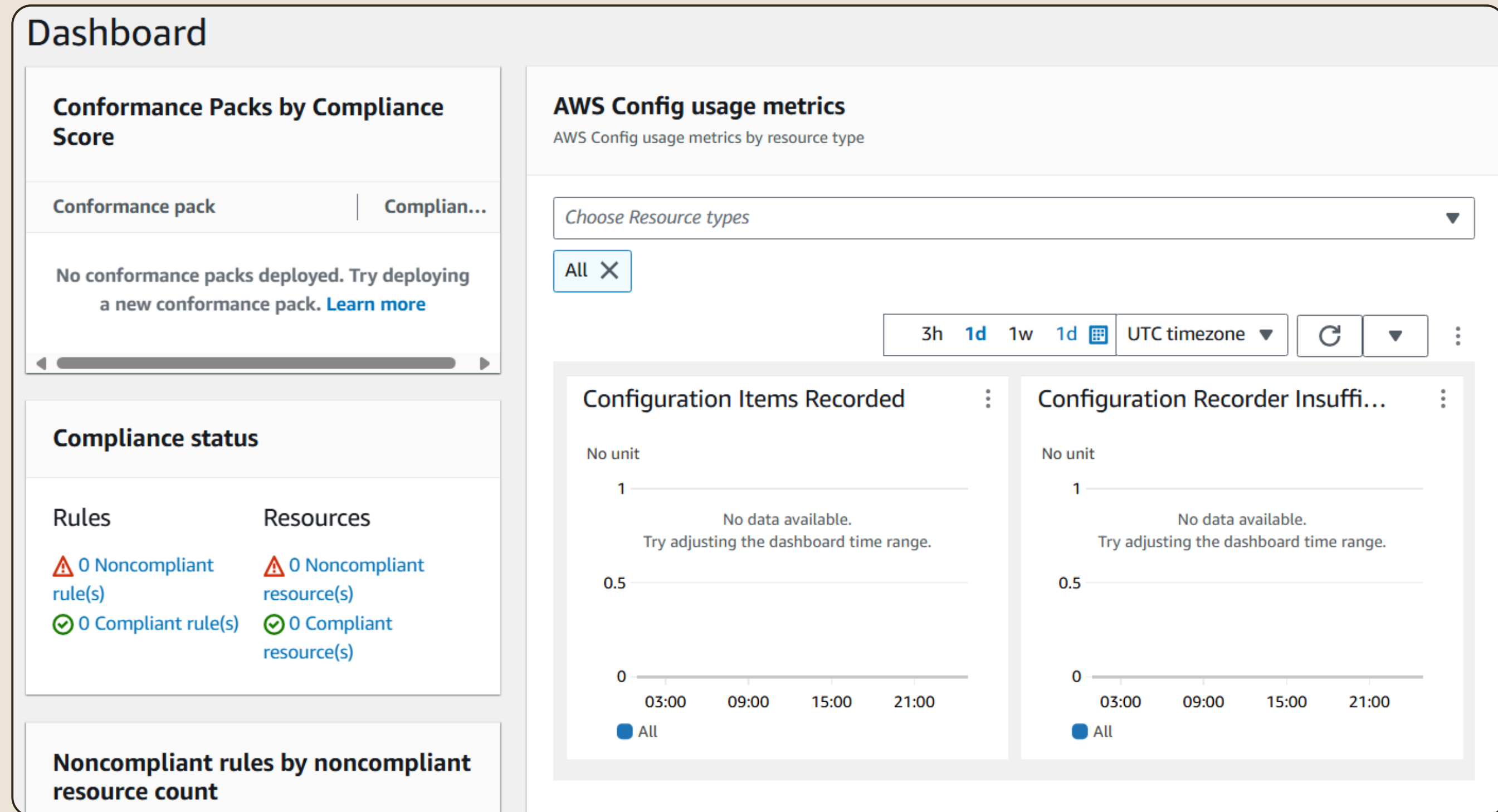
# Tarea 5: Crear notificaciones en tiempo real

AWS Config es un servicio que permite examinar, auditar y evaluar las configuraciones de los recursos de AWS. AWS Config supervisa y registra de manera continua sus configuraciones de recursos de AWS y le permite automatizar la evaluación de las configuraciones registradas comparándolas con las configuraciones deseadas.

AWS Config puede revisar los cambios en las configuraciones y las relaciones entre los recursos de AWS, examinar a profundidad historiales detallados de configuraciones de recursos y determinar el cumplimiento general con las configuraciones especificadas en las pautas internas. AWS Config le permite simplificar la auditoría del cumplimiento, los análisis de seguridad, la administración de los cambios y la solución de problemas operativos.

En esta tarea, activará las reglas de AWS Config para garantizar el cumplimiento del etiquetado y de los volúmenes de Amazon Elastic Block Store (Amazon EBS).

# Accedemos al dashboard de CloudTrail



En la sección Reglas administradas por AWS, del campo de búsqueda, ingrese “required-tags”.

Select rule type

☒ Add AWS managed rule  
Deploy the following managed rules in their default state or customize to suit your needs.

☐ Create custom Lambda rule  
Use a Lambda function with your custom code to evaluate whether your AWS resources comply with the rule.

☐ Create custom rule using Guard  
Use Guard Custom policy that you write to evaluate whether your AWS resources comply with the rule.

AWS Managed Rules (390)

required-

×

1 match

< 1 > ⚙

	Name ▲	Labels	Supported evaluation mode	Description
<input checked="" type="radio"/>	required-tags	AWS	DETECTIVE	Checks whether your resources have the tags that you specify.

Cancel

Next

Luego configuramos los parámetros en la parte de configurar regla  
Esta regla buscará los recursos que no contienen la etiqueta project

Parameters

Rule parameters define attributes that your resources must adhere to for compliance with the rule. Exam parameters that are not valid, such as missing a key or a value, will not be saved.

Key

Value

tag1Key

project

En la sección AWS Manageg Rules, ingresamos “ec2-volume-inuse-check”. Y luego seleccionamos la casilla al lado

AWS Managed Rules (390)

ec2-vol

1 match

	Name	Labels	Supported evaluation mode	Description
<input checked="" type="checkbox"/>	ec2-volume-inuse-check	EC2	DETECTIVE	Checks whether EBS volumes are attached to EC2 instances.

Esperamos hasta que al menos una de las reglas haya completado la evaluación  
Seleccionamos cada una de las reglas para consultar los resultados de las auditorías.

Resources in scope

View details

Remediate

Compliant

< 1 >

	ID	Type	Status	Annotation	Compliance
<input type="radio"/>	vol-0ff18aa64ecdd3983	EC2 Volume	-	-	Compliant

Resources in scope

View details

Remediate

Compliant

< 1 >

	ID	Type	Status	Annotation	Compliance
<input type="radio"/>	i-027a34061518c0e24	EC2 Instance	-	-	Compliant

GRACIAS  
POR LEER