



57°

Lab - AWS re/Start

**Monitoreo de las aplicaciones
y la infraestructura**





Interactuando con AWS CloudWatch

Los objetivos son:

- Utilizar el comando de ejecución de AWS Systems Manager para instalar el agente CloudWatch en instancias de Amazon Elastic Compute Cloud (Amazon EC2).
- Monitorizar los logs de las aplicaciones utilizando el agente de CloudWatch y CloudWatch Logs
- Monitorizar métricas del sistema usando el agente CloudWatch y CloudWatch Metrics
- Crear notificaciones en tiempo real mediante CloudWatch Events
- Seguimiento de la conformidad de la infraestructura mediante AWS Config

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-0065c9ac4976268f6

X

Instances

☒

Name

☒

Web Server

☐

Instance ID

☐

i-0065c9ac4976268f6

☐

Instance state

☐

running

☐

Availability zone

☐

us-west-2a

☐

Ping status

☐

Online

☐

Last ping time

☐

3/8/2024 at 11:33:18 GMT-0500 (Peru Standard Time)

☐

Agent version

☐

3.2.222.0

Tarea 01



Luego, procedemos a hacer la configuración en el Parameter Store

Create parameter

Parameter details

Name
Monitor-Web-Server

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
text

Value
}

Con esto definimos los registros que serán enviados a CloudWatch Logs y las métricas, a CloudWatch Metrics. Luego, otra configuración de Run Command

Name
AmazonCloudWatch-ManageAgent

Owner
Amazon

Platform types
Windows, Linux, MacOS

Description
Send commands to Amazon CloudWatch Agent

Document version
Choose the document version you want to run.
8 (Default)

Command parameters

Action
The action CloudWatch Agent should take.
configure

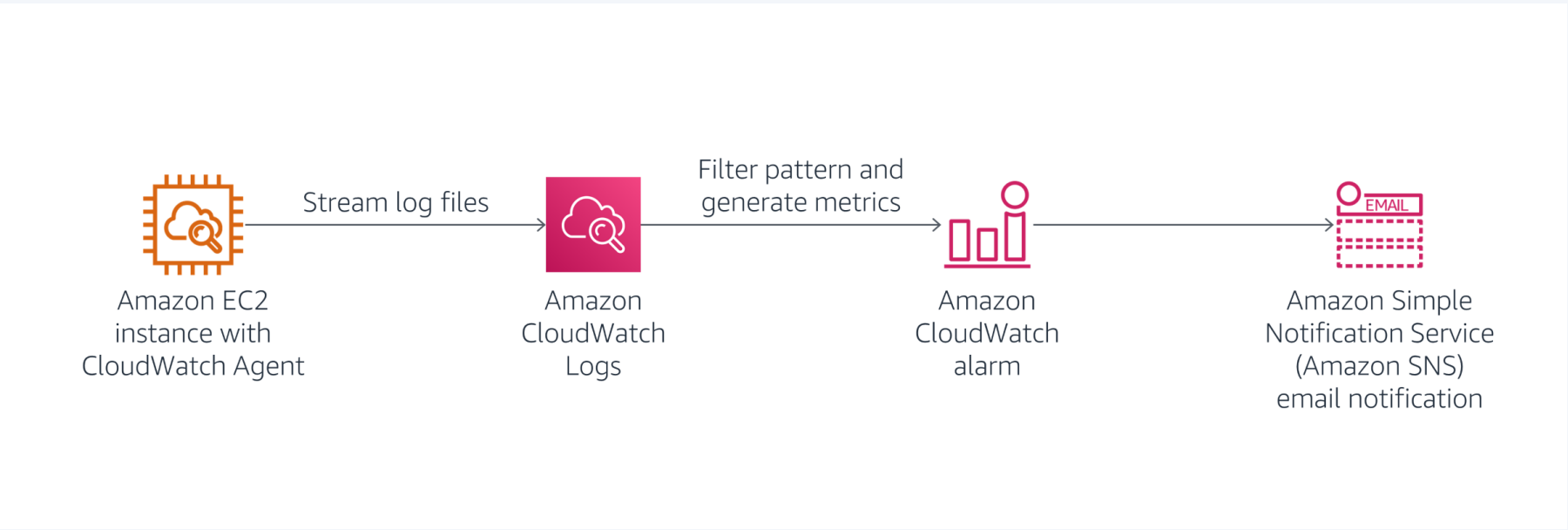
Mode
Controls platform-specific default behavior such as whether to include EC2 Metadata in metrics.
ec2

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

Optional Restart
Only for 'configure' related actions. If 'yes', restarts the agent to use the new configuration. Otherwise the new config will only apply on the next agent restart.
yes

Luego, vamos a monitorear los registros de aplicación utilizando CloudWatch Logs



Tarea 01



Y estos son los registros:

Log events	
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	
<input type="text" value="Filter events"/> Clear 1m 30m 1h 12h Custom Local timezone Display 	
Timestamp	Message
No older events at this moment. Retry	
2024-03-08T12:14:20.027-05:00	18.223.112.207 - - [08/Mar/2024:16:49:30 +0000] "GET /.git/config HTTP/1.1" 404 196 "-" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/535.1 (KHTML, like Gecko) Ubuntu/11.04 Chromium/14.0.825.0 Chrome/14.0.825.0 Safari/535.1"
2024-03-08T12:17:14.028-05:00	20.237.235.106 - - [08/Mar/2024:17:17:09 +0000] "POST /cgi-bin/login.cgi HTTP/1.1" 400 226 "-" "Dark"
2024-03-08T12:19:26.859-05:00	181.176.44.171 - - [08/Mar/2024:17:19:26 +0000] "GET / HTTP/1.1" 403 3630 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36"
2024-03-08T12:19:27.109-05:00	181.176.44.171 - - [08/Mar/2024:17:19:26 +0000] "GET /icons/apache_pb2.gif HTTP/1.1" 200 4234 "http://35.89.105.8/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36"
2024-03-08T12:19:32.027-05:00	181.176.44.171 - - [08/Mar/2024:17:19:27 +0000] "GET /favicon.ico HTTP/1.1" 404 196 "http://35.89.105.8/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36"
2024-03-08T12:19:52.027-05:00	181.176.44.171 - - [08/Mar/2024:17:19:46 +0000] "GET /start HTTP/1.1" 404 196 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36"

Asimismo, podemos realizar un filtro patron para la métrica

Define pattern

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 and count specific terms or extract 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.

Test pattern

Select log data to test

Custom log data

Log event messages

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

```
[83078518-fcc1-4d50-9573-8b9737671438] BENCHMARK: Running Start Crawl for Crawler TestCrawler2
[83078518-fcc1-4d50-9573-8b9737671438] BENCHMARK: Classification complete, writing results to database mygluedatabase
[83078518-fcc1-4d50-9573-8b9737671438] INFO: Crawler configured with SchemaChangePolicy
[83078518-fcc1-4d50-9573-8b9737671438] INFO: Created table guettest in database mygluedatabase
[83078518-fcc1-4d50-9573-8b9737671438] INFO: Created table guettest in database mygluedatabase
[83078518-fcc1-4d50-9573-8b9737671438] BENCHMARK: Finished writing to Catalog
```

Test pattern

Assign metric

Create filter name

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

Filter name

404Errors

Filter pattern

[p, id, user, timestamp, request, status_code=404, size]

Metric details

Metric namespace

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

LogMetrics Create new

Metric name

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

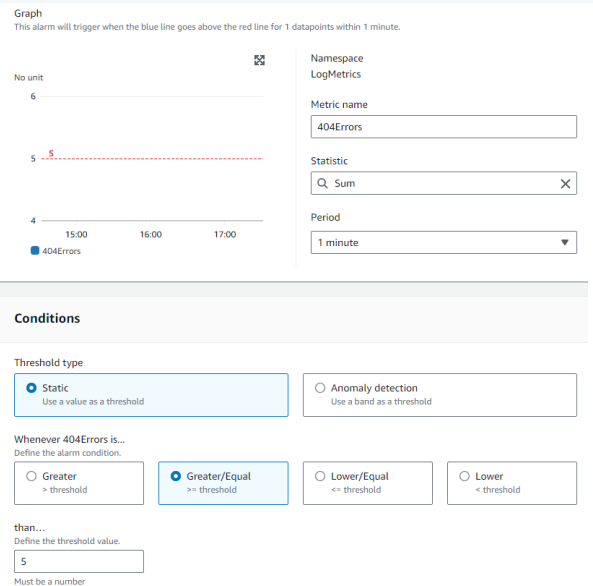
404Errors

Metric value

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

1

Luego, usando este filtro, podremos crear una alarma



CloudWatch > Alarms > Create alarm

Step 1

[Specify metric and conditions](#)

Step 2

[Configure actions](#)

Step 3

[Add name and description](#)

Step 4

[Preview and create](#)

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.

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_Alarms_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.

millonesmam@gmail.com

user1@example.com, user2@example.com

Create topic

Add notification

Add name and description

Name and description

Alarm name

404 Errors

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

Edit Preview

Alert when too many 404s detected on an instance

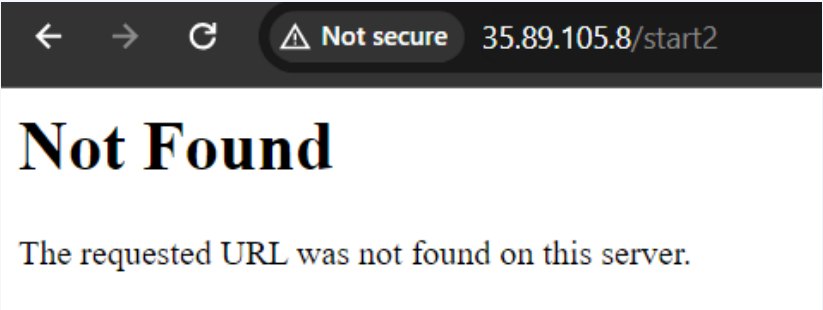
Up to 1024 characters (48/1024)

Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.

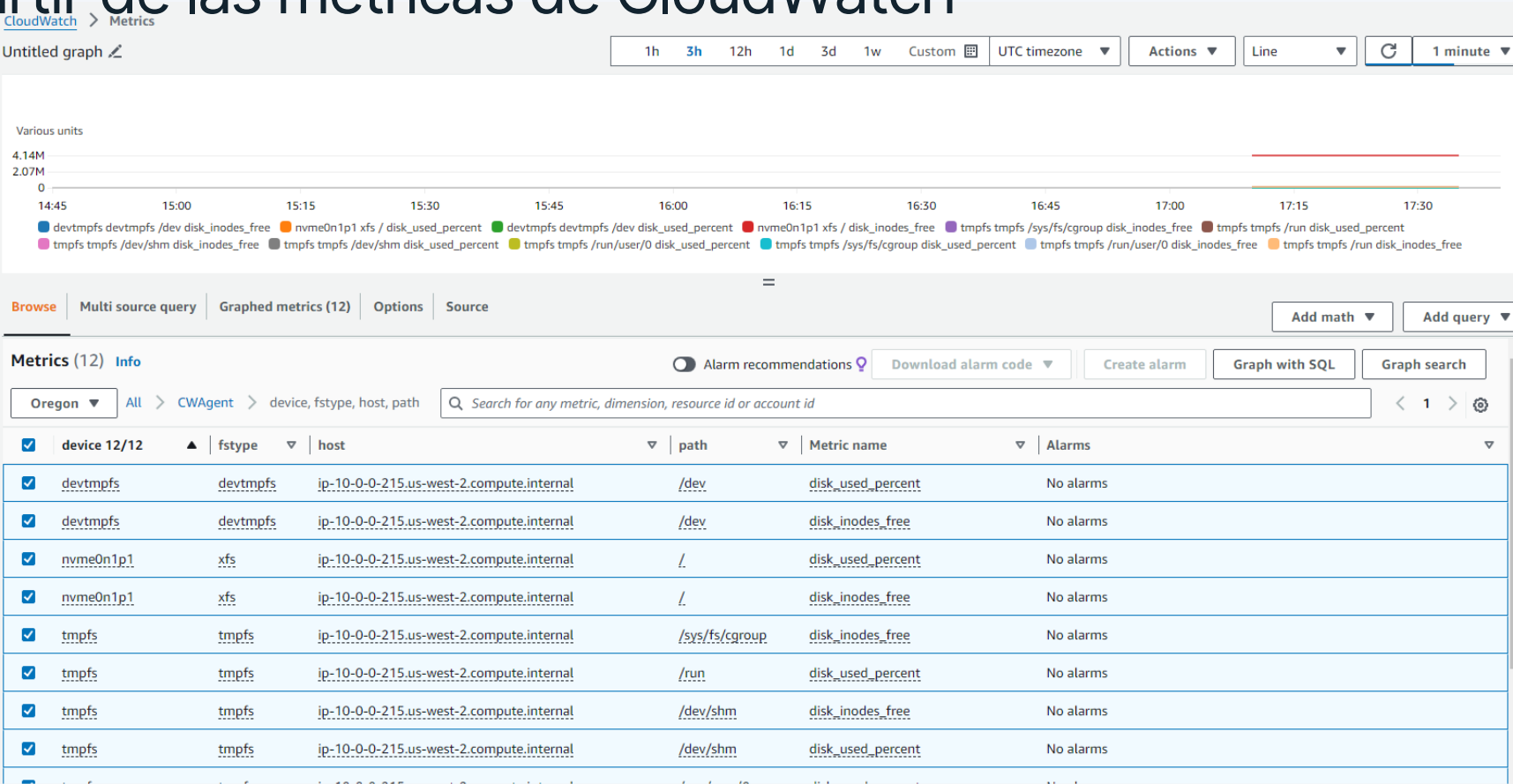
Tarea 01



Luego, probaremos la alarma, se envía el correo



Después de ello, procederemos a monitorear la instancia a partir de las métricas de CloudWatch



Ahora, haremos notificaciones en tiempo real, mediante las reglas de CloudWatch

Tarea 01



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

terminated

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

Select target(s)

Permissions

Note: When using the EventBridge console, EventBridge will automatically configure the proper permissions for the selected targets. If you're using the AWS CLI, SDK, or CloudFormation, you'll need to configure the proper permissions.

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

En el caso se detenga o termine la instancia. Luego, utilizamos Config

AWS Config

Rules

Add rule

Step 1

Specify rule type

Step 2

Configure rule

Step 3

Review and create

Specify rule type

Add rules to define the desired configuration setting of your AWS resources. Customize any of the following rules to suit your needs, or create a custom rule. To create a custom rule, you must create an AWS Lambda function for the rule.

Select rule type

Add AWS managed rule

Customize any of the following rules to suit your needs.

Create custom Lambda rule

Create custom rules and add them to AWS Config. Associate each custom rule with an AWS Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule.

Create custom rule using Guard

Create custom rules using Guard Custom Policy that evaluates whether your AWS resources comply with the rule.

AWS Managed Rules (372)

Q required-

X

1 match

<

1

>

Name	Labels	Supported evaluation mode	Description
required-tags	AWS	DETECTIVE	Checks whether your resources have the tags that you specify.

Parameters

Key	Type	Value	Description
tag1Key	String	project	Key of the required tag.
tag1Value	CSV		Optional value of the required tag. Separate multiple values with commas.
tag2Key	String		Key of a second required tag.
tag2Value	CSV		Optional value of the second required tag. Separate multiple values with commas.
tag3Key	String		Key of a third required tag.
tag3Value	CSV		Optional value of the third required tag. Separate multiple values with commas.
tag4Key	String		Key of a fourth required tag.
tag4Value	CSV		Optional value of the fourth required tag. Separate multiple values with commas.
tag5Key	String		Key of a fifth required tag.
tag5Value	CSV		Optional value of the fifth required tag. Separate multiple values with commas.
tag6Key	String		Key of a sixth required tag.
tag6Value	CSV		Optional value of the sixth required tag. Separate multiple values with commas.

Cancel

Previous

Save

< SWIPE