[ENGLISH]

Hello, Cloud Gurus, and welcome to this lesson,

which is a summary of everything that we've covered

in the monitoring section, beginning with CloudWatch

which is all about monitoring the performance

and health of your systems.

The main three capabilities include monitoring

default EC2 host-level metrics like CPU,

network, disk, and status check.

Use the CloudWatch agent for operating system-level metrics

like memory usage, anything to do with processes,

and CPU idle time.

CloudWatch Logs allows you to monitor and store your logs

to help you better understand your systems and applications.

And you can use CloudWatch Alarms to create an alarm

to monitor any CloudWatch metric in your account

and generate an alert or take some action.

For instance, you could create an alarm to trigger

if CPU utilization on an EC2 instance exceeds 90%

for a specified period of time.

Use CloudWatch Dashboards to create a customized view

to monitor the metrics that are meaningful to you.

For instance, all of your production systems.

You can display metrics

for multiple regions in the same dashboard.

And if you're configuring a dashboard,

remember to save it so that you can use it again later.

If you would like to receive notifications

based on CloudWatch metrics,

first, create an alarm to notify you

when a specific threshold is hit.

You can create an alarm for any metric,

for instance, associated with CPU utilization

and CloudWatch can be used

to send you an email notification using an SNS topic.

Be sure to understand the differences

between CloudWatch and CloudTrail.

And CloudWatch, of course, is used to monitor

performance and metrics

to centralize application and system logs

and create alarms.

So ask yourself, do I need to monitor the performance

of AWS resources?

If so, you need CloudWatch.

Whereas CloudTrail is used to record the API calls

that are made in your AWS account.

So it records API activity history related to creating,

deleting, and modifying AWS resources.

So ask yourself, do I need an audit log of user activity

in my AWS account?

If so, you need CloudTrail.

So CloudWatch is all about performance and health metrics

whereas CloudTrail is an audit trail.

There are a few different CloudWatch concepts

that are useful to understand.

As you know, a metric is a variable to monitor.

A CloudWatch namespace is a container

for CloudWatch metrics.

For instance, EC2 uses the AWS/EC2 namespace.

CloudWatch dimensions are like filters.

For example, you can use the instance ID dimension to search

for metrics relating to a specific EC2 instance.

And a CloudWatch dashboard is like a custom homepage

that you create in CloudWatch,

for example, to display important metrics

for all of your production systems in one place.

CloudWatch actions allow you to publish, monitor,

and alert on a variety of metrics.

The PutMetricData API call publishes

metric data points to CloudWatch.

For instance, if your application experiences

a critical error,

it can publish a data point to CloudWatch,

and then the PutMetricAlarm API call creates an alarm

associated with a metric that is going to alert

if a threshold has been reached.

It's important to be able to interpret

common HTTP error codes

and remember that 400 errors are always client side errors.

So remember the common 404 error that you've probably seen

many times when using the internet.

And if you see a 400 error,

check that the requested object exists,

you have access to it,

and that your request is correctly formed.

Whereas 500 errors are always at server side errors.

And just remember that five looks a little bit like an S.

500 errors are generally caused by the server

not responding to your request.

This can be due to high traffic to your website

and the servers being either overwhelmed or unavailable.

So it can be indicative of a capacity or performance issue

or even an internal failure in the server.

So if you see any HTTP error codes beginning with five,

just remember that five looks a little bit like an S

and S is for server side errors.

When it comes to SDK exceptions,

there are a few DynamoDB errors that are worth remembering.

Firstly, there's UnprocessedKeys and this means

that some items were not successfully processed

when you ran a BatchGetItem operation on the table.

ProvisionedThroughputExceededException means that

none of the operations were processed

due to exceeding the provision throughput

on the DynamoDB table.

UnprocessedItems means that some items

were not successfully processed

when you ran a BatchWriteItem operation

on the DynamoDB table.

And possible solutions include reducing the size

of the request,

requesting fewer items using DAX

or DynamoDB Accelerator to cache reads,

or increasing the provision throughput capacity.

We can use CloudWatch Logs Insights to interactively query

and analyze data that is stored in CloudWatch Logs.

We can query the logs directly

and also generate visualizations,

for example, bar graphs, line graphs, or pie charts.

For example, we can use CloudWatch Logs Insights

to display the 25 most recently added log events.

We can search VPC Flow Logs to find out

which IP addresses are using a specific protocol

or even find the most expensive Lambda requests.

We can use EventBridge to easily configure

event-driven systems and even define tasks that can be run

on a predefined schedule.

And EventBridge, of course,

uses the same underlying technology as CloudWatch Events.

Events are state changes that are generated by services

like AWS Config, CloudWatch, or CloudTrail, et cetera.

Rules match events

and then route them to the correct target.

And targets can be services like Lambda, SNS or EC2,

and they respond to the event by taking some action.

EventBridge receives events

relating to state changes in AWS.

So think about an EC2 instance changing state

or a CloudWatch alarm changing state.

We can use EventBridge to create rules

that take actions based on the events it receives,

for example, send us an SNS notification.

And you may see EventBridge also referred

to as CloudWatch Events

because they're using the same underlying technology.

So that is it for this lesson.

Any questions, please let me know.

Otherwise, I will see you in the next one.

Thank you.

[SPANISH]

Hola, Cloud Gurus, y bienvenidos a esta lección.

que es un resumen de todo lo que hemos cubierto

en la sección de monitoreo, comenzando con CloudWatch

que se trata de monitorear el rendimiento

y la salud de sus sistemas.

Las tres capacidades principales incluyen el monitoreo

métricas de nivel de host EC2 predeterminadas como CPU,

de red , disco y estado.

Utilice el agente de CloudWatch para las métricas a nivel del sistema operativo

como uso de memoria, cualquier cosa que tenga que ver con procesos,

y el tiempo de inactividad de la CPU.

CloudWatch Logs le permite monitorear y almacenar sus registros

para ayudarle a comprender mejor sus sistemas y aplicaciones.

Y puede usar CloudWatch Alarms para crear una alarma

para monitorear cualquier métrica de CloudWatch en su cuenta

y generar una alerta o realizar alguna acción.

Por ejemplo, podría crear una alarma para activar

si la utilización de la CPU en una instancia EC2 supera el 90 %

por un período de tiempo específico.

Use CloudWatch Dashboards para crear una vista personalizada

para monitorear las métricas que son significativas para usted.

Por ejemplo, todos sus sistemas de producción.

Puede mostrar métricas

para varias regiones en el mismo tablero.

Y si está configurando un tablero,

recuerda guardarlo para que puedas volver a usarlo más tarde.

Si desea recibir notificaciones

basado en las métricas de CloudWatch ,

primero , crea una alarma para notificarte

cuando se alcanza un umbral específico.

Puede crear una alarma para cualquier métrica,

por ejemplo, asociado con la utilización de la CPU

y Se puede utilizar CloudWatch

para enviarle una notificación por correo electrónico utilizando un tema de SNS.

Asegúrese de entender las diferencias

entre CloudWatch y CloudTrail .

Y CloudWatch , por supuesto, se usa para monitorear

rendimiento y métricas

para centralizar los registros de la aplicación y del sistema

y crear alarmas.

Así que pregúntese, ¿necesito monitorear el desempeño

de los recursos de AWS?

Si es así, necesita CloudWatch .

Mientras que CloudTrail se utiliza para registrar las llamadas a la API

que se realizan en su cuenta de AWS.

Por lo tanto, registra el historial de actividad de la API relacionado con la creación,

eliminar y modificar recursos de AWS.

Así que pregúntese, ¿necesito un registro de auditoría de la actividad del usuario?

en mi cuenta de AWS?

Si es así, necesita CloudTrail .

Entonces, CloudWatch tiene que ver con las métricas de rendimiento y salud

mientras CloudTrail es un registro de auditoría.

Hay algunos conceptos diferentes de CloudWatch

que son útiles para entender.

Como sabes, una métrica es una variable a monitorear.

Un espacio de nombres de CloudWatch es un contenedor

para Métricas de CloudWatch .

Por ejemplo, EC2 usa el espacio de nombres AWS/EC2.

de CloudWatch son como filtros.

Por ejemplo, puede usar la dimensión de ID de instancia para buscar

para métricas relacionadas con una instancia EC2 específica.

Y un panel de CloudWatch es como una página de inicio personalizada

que crea en CloudWatch ,

por ejemplo, para mostrar métricas importantes

para todos sus sistemas de producción en un solo lugar.

de CloudWatch le permiten publicar, monitorear,

y alerta sobre una variedad de métricas.

La llamada a la API de PutMetricData publica

métricos apuntan a CloudWatch .

Por ejemplo, si su aplicación experimenta

un error crítico,

puede publicar un punto de datos en CloudWatch ,

y luego la llamada API PutMetricAlarm crea una alarma

asociado a una métrica que va a alertar

si se ha alcanzado un umbral.

Es importante poder interpretar

códigos de error HTTP comunes

y recuerde que los errores 400 son siempre errores del lado del cliente.

Así que recuerda el error 404 común que probablemente hayas visto

muchas veces al usar Internet.

Y si ves un error 400,

comprobar que el objeto solicitado existe,

tienes acceso a ella,

y que su solicitud está correctamente formada.

Mientras que 500 errores siempre son errores del lado del servidor.

Y recuerda que el cinco se parece un poco a una S.

500 errores generalmente son causados por el servidor

no respondiendo a su solicitud.

Esto puede deberse al alto tráfico a su sitio web.

y los servidores están abrumados o no están disponibles.

Por lo tanto, puede ser indicativo de un problema de capacidad o rendimiento.

o incluso una falla interna en el servidor.

Entonces, si ve algún código de error HTTP que comience con cinco,

solo recuerda que el cinco se parece un poco a una S

y S es para errores del lado del servidor.

Cuando se trata de excepciones SDK,

hay algunos errores de DynamoDB que vale la pena recordar.

En primer lugar, hay UnprocessedKeys y esto significa

que algunos elementos no se procesaron correctamente

cuando ejecutó una operación BatchGetItem en la tabla.

ProvisionedThroughputExceededException significa que

ninguna de las operaciones fue procesada

debido a exceder el rendimiento de la provisión

en la tabla de DynamoDB .

UnprocessedItems significa que algunos elementos

fueron procesados exitosamente

cuando ejecutó una operación BatchWriteItem

en la tabla de DynamoDB .

Y las posibles soluciones incluyen reducir el tamaño

de la solicitud,

solicitar menos artículos usando DAX

o Acelerador de DynamoDB para lecturas en caché,

o aumentar la capacidad de rendimiento de suministro.

Podemos usar CloudWatch Logs Insights para consultar de forma interactiva

y analice los datos almacenados en CloudWatch Logs.

Podemos consultar los registros directamente

y también generar visualizaciones,

por ejemplo, gráficos de barras, gráficos de líneas o gráficos circulares.

Por ejemplo, podemos usar CloudWatch Logs Insights

para mostrar los 25 eventos de registro agregados más recientemente.

Podemos buscar registros de flujo de VPC para averiguarlo.

qué direcciones IP están usando un protocolo específico

o incluso encontrar las solicitudes de Lambda más caras.

Podemos usar EventBridge para configurar fácilmente

controlados por eventos e incluso definir tareas que se pueden ejecutar

en un horario predefinido.

Y EventBridge , por supuesto,

utiliza la misma tecnología subyacente que CloudWatch Events.

Los eventos son cambios de estado generados por los servicios.

como AWS Config , CloudWatch o CloudTrail , etcétera.

Eventos de coincidencia de reglas

y luego enrutarlos al objetivo correcto.

Y los objetivos pueden ser servicios como Lambda, SNS o EC2,

y responden al evento tomando alguna acción.

EventBridge recibe eventos

relacionados con los cambios de estado en AWS.

Así que piense en una instancia EC2 que cambia de estado

o un estado de cambio de alarma de CloudWatch .

Podemos usar EventBridge para crear reglas

que toman acciones en base a los eventos que recibe,

por ejemplo, envíenos una notificación SNS.

Y es posible que también se haga referencia a EventBridge

como eventos de CloudWatch

porque están utilizando la misma tecnología subyacente.

Eso es todo por esta lección.

Para cualquier duda, por favor hágamelo saber.

De lo contrario, te veré en la próxima.

Gracias.