[ENGLISH]

Hello Cloud Gurus and welcome

to this lesson where we'll get our hands dirty

with CloudWatch and we'll begin

by launching an EC2 instance.

And we're going to attach an identity

and access management role with permissions to

send CloudWatch agent metrics into CloudWatch.

And we'll use the CloudWatch agent server policy

managed policy to give us those permissions.

Next, we're going to install the CloudWatch agent

on our EC2 instance

and we'll configure the agent to send operating

system metrics and system logs to CloudWatch.

And then after a few minutes we'll be able

to view the metrics in CloudWatch and we should be able

to see the EC2 default metrics as well as the metrics

and logs that are sent by the CloudWatch agent.

So if you're ready to get started with CloudWatch

I'll see you in the AWS console from the console.

Search for identity and access management.

Select roles from the left hand menu and create role.

Make sure that AWS service is selected.

Scroll down and under common use cases,

select EC2.

Then hit next.

And we're going to add an AWS managed policy to our role

and it's called the CloudWatch Agent Server policy.

So search for CloudWatch agent server policy and hit enter.

And there is our managed policy.

And this one just provides the permissions required to

use the CloudWatch agent on your EC2 instance.

So select the policy, hit next.

We'll give our role a name,

scroll down and create role.

Next, let's create our EC2 instance.

So search for EC2,

launch instance,

call it my EC2 instance.

Scroll down, we'll use the Amazon Linux AAMI by default

it's giving me the latest AMI,

scroll down to instance type

and select T3 micro.

We can proceed without a key pair.

Then scroll down to advanced details at the bottom.

Open the dropdown under IAM instance profile.

Select the role that we just created a minute ago.

Then scroll right down to the end of the page

until you get to the user data section.

And this is where we're going to add a bootstrap script

And you will find this script

in the resources for this lesson.

So this is what I've provided in the lesson resources

and here is the little bootstrap script here.

So just copy that.

And this is just gonna update the operating system.

And if you haven't used DNF before

it's just the new package manager

for the latest Amazon Linux operating system.

And yum is going to be deprecated eventually.

So back on our instance

paste in our script and launch instance.

So now let's select our instance ID

and we can watch the progress of our instance initializing.

As soon as your instance has finished initializing

we can log in.

So select your instance,

hit connect.

We'll use EC2 instance connect.

So select connect.

And now that we are logged into our instance

there are a few different commands that we need to run

in order to configure the CloudWatch agent.

And you will find all

of these commands in the resources for this course.

So the next thing that we need to do is install our Syslog.

And this is gonna generate a readable text file

of the operating system messages in VAR log messages.

So these are the commands that we'll use to do that.

So first of all, we'll run pseudo SU

because we need to do all of this as the root user.

I'll clear my screen.

Next, we'll run DNF, install our Syslog.

So this is just gonna install Syslog.

Answer yes to this question.

Next we'll start our Syslog and enable it to start

at boot time.

After that, we are ready to install the CloudWatch agent

and here's the command that we use to do that.

So that's just downloaded all the packages needed

for the CloudWatch agent and installed them.

The next command is what we use

to configure the CloudWatch agent,

and it actually uses a configuration wizard

with lots of different questions

that we need to answer.

And then at the end it's going to create the

CloudWatch agent configuration file.

So I'll copy that command

and paste.

So it's going to ask us lots of different questions

and for most of them we can accept the defaults.

But here and there we need to deviate from the defaults.

So first of all, which operating system are we running?

Well, we are running Linux so we can accept the default.

So as hit enter, we're using EC2.

So accept the default and hit enter.

We'll run the agent as route.

So accept the default.

We are gonna turn on the stats D demon

and stats D is just a demon that collects metrics

on your system.

So hit enter.

We can accept the default port

and the default interval as well.

And I'm gonna select an aggregation interval of 10 seconds.

So that's gonna be number two and hit enter.

Do we want to monitor metrics

from collect D and no, we don't

because we don't have collect D installed on this system.

And if you select this,

then the agent is gonna fail to start.

So make sure that you've selected

number two here and hit enter.

Do we want to monitor any host metrics?

Yes, we do.

So hit enter CPU metrics.

Yes, so hit enter EC2 dimensions.

Yes, so hit enter.

Do we want to aggregate?

Yes, so hit enter.

Do we want to use higher resolution metrics?

And I'm gonna change this to one second resolution

just so it's a little bit faster.

So I'm gonna select option one and hit enter.

Now we're going to go for standard metrics.

So that is option number two.

So select two for this question and hit enter.

Are we satisfied?

Select one for yes.

So we can just hit enter.

Do we have an existing CloudWatch agent?

No, we don't.

So that's number two.

Hit enter.

Do we want to monitor any log files?

Well, yes, we do.

So that's gonna be number one.

So we can just go ahead and hit enter.

And the log file path is going to be VAR log messages.

And this is the log file created by the rsyslogd daemon.

Once you've added that,

hit enter,

accept the default log group name,

which is messages, and the log stream name

which is our instance ID.

Log group retention,

I'm gonna set for one day.

So type two.

Do we want to specify any additional log files?

No, so type two.

But if we did have additional application log files

that we wanted to monitor,

we can add them in here.

Do we want to store the config in SSM parameter store?

No, we don't.

And that is the CloudWatch agent configured.

So now if we change directory to opt AWS,

Amazon CloudWatch agent bin,

type LS.

Here is our configuration file

and it's called config.Json.

And if we open up that config file,

here is the configuration that we just set up.

So here's the path to our messages file that we defined

and then down here you'll find the metrics

that it's going to collect.

So these are the metrics that the agent is gonna gather

from your operating system.

So it's things like CPU metrics.

Down here we've got some disc metrics down here

there's disc IO metrics,

memory metrics,

and swap as well.

So now we are ready to go ahead

and start the CloudWatch agent.

I'll clear my screen.

And then down here,

this is the command that we're gonna use

to start the CloudWatch agent.

So this is just starting up the CloudWatch agent

and it's telling it where to find the configuration file.

And if it's all worked successfully

this is what it should look like.

So first of all, it's fetching the config

it then validates the config

and then it starts up the CloudWatch agent.

Now at the moment, we don't have anything running

on our system,

so I want to generate some CPU activity

so that we've got some interesting metrics

when we take a look at CloudWatch.

And I'm gonna install a utility called stress

so that we can generate some CPU load.

And here's the command that we're gonna use to do that.

So it's DNF install stress minus Y,

and then after that's been installed,

we can just type stress minus minus CPU

and then the number one and hit enter.

And this is just gonna create some CPU load on our system.

So just run that command

and leave it running in this session.

And in a few minutes we should start to

see some metrics appearing in CloudWatch.

So using the search box, we're gonna search

for CloudWatch and open it up in a new tab

select metrics on the left hand menu and select all metrics.

Then under CW agent

this is where we can find the metrics

that are being produced by the agent

that's running on our instance.

And these are all the metrics that it's producing.

So I'm gonna select instance ID

and here are the metrics that it's collecting.

And if we select a metric down here

so lets select CPU usage user,

and I'm gonna select metrics to be displayed

from the last hour.

So select one H up here.

And if you start to select metrics down here

then you'll notice that they start getting plotted

on the graph up here.

And it might just take a few moments

for the metrics to actually appear in the graph.

So these are the operating system level metrics

that are being sent to CloudWatch by the CloudWatch agent.

So we've got metrics relating to swap usage,

memory usage, CPU usage,

disc IO, and disc percentage.

But I'm gonna de-select these metrics for now

and come back to all metrics.

So select all under metrics,

scroll down and select EC2,

select per instance metrics.

And this is where you'll find all of the default

EC2 metrics that CloudWatch always collects

from every EC2 instance.

And under this view,

it's showing the metrics on a per instance basis.

And we can actually search for our own instance ID.

So I'm gonna find my instance ID

there it is, just copy that.

Then back in CloudWatch search for the instance

ID and here are all the default metrics that

it's collecting for my particular instance ID.

And you can go in and select a metric for this

and add it to your graph up here.

So that is the CloudWatch agent metrics

but what about the logs?

Well, if you head over to logs on the left hand side

and select log groups,

then select messages because that was the name

of our log group.

Then scroll down and here is our log stream.

And if you remember, it was named after our instance ID.

So select the log stream

and this is gonna take you straight into the log.

And these are all the messages appearing in the

VAR log messages on our EC2 instance.

So this is the log file that we asked the

CloudWatch agent to monitor.

So that is CloudWatch.

And in summary, we launched an EC2 instance.

We attached an identity and access management role

with permissions to send the CloudWatch agent metrics

into CloudWatch, and we used a managed policy

called the CloudWatch agent server policy

to give us those permissions.

Next, we installed the CloudWatch agent on our instance

and we configured the agent to send the operating

system metrics and the logs into CloudWatch.

Then finally, we were able to view the metrics in CloudWatch

and we could see the EC2 default metrics as well

as the metrics and logs that were being sent

by this instance using the CloudWatch agent.

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 donde nos ensuciamos las manos

con CloudWatch y comenzaremos

lanzando una instancia EC2.

Y vamos a adjuntar una identidad

y función de administración de acceso con permisos para

enviar Métricas del agente de CloudWatch en CloudWatch .

Y usaremos la política del servidor del agente de CloudWatch

administrada para darnos esos permisos.

A continuación, vamos a instalar el agente de CloudWatch.

en nuestra instancia EC2

y configuraremos el agente para enviar operaciones

métricas del sistema y registros del sistema a CloudWatch .

Y luego de unos minutos podremos

para ver las métricas en CloudWatch y deberíamos poder

para ver las métricas predeterminadas de EC2, así como las métricas

y registros que envía el agente de CloudWatch .

Entonces, si está listo para comenzar con CloudWatch

Nos vemos en la consola de AWS desde la consola.

Búsqueda de identidad y gestión de accesos.

Seleccione roles en el menú de la izquierda y cree un rol.

Asegúrese de que el servicio de AWS esté seleccionado.

Desplácese hacia abajo y debajo de casos de uso comunes,

seleccione EC2.

Luego presiona siguiente.

Y vamos a agregar una política administrada por AWS a nuestro rol

y se denomina política del servidor del agente de CloudWatch .

Así que busque la política del servidor del agente de CloudWatch y presione Intro.

Y ahí está nuestra política administrada.

Y este solo proporciona los permisos necesarios para

utilice el agente de CloudWatch en su instancia EC2.

Así que seleccione la política, presione siguiente.

Le daremos un nombre a nuestro rol,

desplácese hacia abajo y cree un rol.

A continuación, creemos nuestra instancia EC2.

Así que busque EC2,

instancia de lanzamiento ,

llámelo mi instancia EC2.

Desplácese hacia abajo, usaremos Amazon Linux AAMI de forma predeterminada

está dando la última AMI,

desplácese hacia abajo hasta el tipo de instancia

y seleccione T3 micro.

Podemos continuar sin un par de claves.

Luego, desplácese hacia abajo hasta los detalles avanzados en la parte inferior.

Abra el menú desplegable en el perfil de instancia de IAM.

Seleccione el rol que acabamos de crear hace un minuto.

Luego, desplácese hacia abajo hasta el final de la página.

hasta llegar a la sección de datos de usuario.

Y aquí es donde vamos a agregar un script de arranque

Y encontrarás este script

en los recursos para esta lección.

Así que esto es lo que proporcioné en los recursos de la lección.

y aquí está el pequeño script de arranque aquí.

Así que copia eso.

Y esto solo va a actualizar el sistema operativo.

Y si no has usado DNF antes

es solo el nuevo administrador de paquetes

para el último sistema operativo Amazon Linux.

Y yum eventualmente quedará en desuso.

Así que de vuelta en nuestra instancia

pegue en nuestro script y ejecute la instancia.

Así que ahora seleccionemos nuestra ID de instancia

y podemos ver el progreso de la inicialización de nuestra instancia.

Tan pronto como su instancia haya terminado de inicializarse

podemos iniciar sesión.

Así que seleccione su instancia,

pulsa conectar.

Usaremos la conexión de instancia EC2.

Así que selecciona conectar.

Y ahora que estamos logueados en nuestra instancia

hay algunos comandos diferentes que necesitamos ejecutar

para configurar el agente de CloudWatch .

Y encontrarás todo

de estos comandos en los recursos de este curso.

Entonces, lo siguiente que debemos hacer es instalar nuestro Syslog.

Y esto va a generar un archivo de texto legible

de los mensajes del sistema operativo en los mensajes de registro VAR.

Así que estos son los comandos que usaremos para hacer eso.

Entonces, antes que nada, ejecutaremos pseudo SU

porque necesitamos hacer todo esto como usuario root.

Borraré mi pantalla.

A continuación, ejecutaremos DNF, instalaremos nuestro Syslog.

Así que esto solo va a instalar Syslog.

Responda sí a esta pregunta.

A continuación, iniciaremos nuestro Syslog y habilitaremos su inicio

en el momento del arranque.

Después de eso, estamos listos para instalar el agente de CloudWatch .

y aquí está el comando que usamos para hacer eso.

Así que solo descargué todos los paquetes necesarios

para el agente de CloudWatch y los instaló.

El siguiente comando es el que usamos.

para configurar el agente de CloudWatch ,

y en realidad usa un asistente de configuración

con muchas preguntas diferentes

que tenemos que responder.

Y luego al final va a crear el

Archivo de configuración del agente de CloudWatch .

Así que copiaré ese comando.

y pegar

Así que nos va a hacer muchas preguntas diferentes

y para la mayoría de ellos podemos aceptar los valores predeterminados.

Pero aquí y allá necesitamos desviarnos de los valores predeterminados.

Entonces, antes que nada, ¿qué sistema operativo estamos ejecutando?

Bueno, estamos ejecutando Linux, por lo que podemos aceptar el valor predeterminado.

Entonces, al presionar enter, estamos usando EC2.

Así que acepte el valor predeterminado y presione enter.

Ejecutaremos el agente como ruta.

Así que acepta el valor predeterminado.

Vamos a encender el demonio stats D

y stats D es solo un demonio que recopila métricas

en su sistema.

Así que pulsa enter.

Podemos aceptar el puerto predeterminado

y el intervalo predeterminado también.

Y voy a seleccionar un intervalo de agregación de 10 segundos.

Entonces ese será el número dos y presiona enter.

¿Queremos monitorear las métricas ?

de recoger D y no, no lo hacemos

porque no tenemos Collect D instalado en este sistema.

Y si seleccionas esto,

entonces el agente no podrá iniciarse.

Así que asegúrese de haber seleccionado

número dos aquí y presione enter.

¿Queremos monitorear alguna métrica del host?

Sí.

Así que presione ingresar métricas de CPU.

Sí, presione ingresar las dimensiones de EC2.

Sí, así que presiona enter.

¿Queremos agregar?

Sí, así que presiona enter.

¿Queremos usar métricas de mayor resolución?

Y voy a cambiar esto a una resolución de un segundo

solo para que sea un poco más rápido.

Así que seleccionaré la opción uno y presionaré enter.

Ahora vamos a buscar métricas estándar.

Así que esa es la opción número dos.

Así que seleccione dos para esta pregunta y presione enter.

¿Estamos satisfechos?

Seleccione uno para sí.

Así que podemos presionar enter.

Tenemos un agente de CloudWatch existente?

No, no lo hacemos.

Así que ese es el número dos.

Presione enter.

¿Queremos monitorear algún archivo de registro?

Bueno, sí, lo hacemos.

Así que ese va a ser el número uno.

Así que podemos seguir adelante y presionar enter.

Y la ruta del archivo de registro será mensajes de registro VAR.

Y este es el archivo de registro creado por el demonio rsyslogd .

Una vez que haya agregado eso,

pulsa enter,

aceptar el nombre del grupo de registro predeterminado,

que es mensajes, y el nombre del flujo de registro

que es nuestra ID de instancia.

Retención de grupos de registro,

Me voy a fijar para un día.

Así que escribe dos.

¿Queremos especificar algún archivo de registro adicional?

No, entonces escriba dos.

Pero si tuviéramos archivos de registro de aplicaciones adicionales

que queríamos monitorear,

podemos agregarlos aquí.

Queremos almacenar la configuración en el almacén de parámetros de SSM?

No, no lo hacemos.

Y ese es el agente de CloudWatch configurado.

Entonces, si cambiamos de directorio para optar por AWS,

de Amazon CloudWatch ,

tipo LS.

Aquí está nuestro archivo de configuración

y se llama config.Json .

Y si abrimos ese archivo de configuración ,

aquí está la configuración que acabamos de establecer.

Así que aquí está la ruta a nuestro archivo de mensajes que definimos

y luego aquí abajo encontrarás las métricas

que va a recoger.

Estas son las métricas que el agente recopilará

de su sistema operativo.

Así que son cosas como las métricas de la CPU.

Aquí abajo tenemos algunas métricas de disco aquí abajo

hay métricas de E/S de disco,

de memoria ,

y permuta también.

Así que ahora estamos listos para seguir adelante.

e inicie el agente de CloudWatch .

Borraré mi pantalla.

Y luego aquí abajo,

este es el comando que vamos a usar

para iniciar el agente de CloudWatch .

Así que esto es solo iniciar el agente de CloudWatch.

y le dice dónde encontrar el archivo de configuración.

Y si todo ha funcionado con éxito

esto es lo que debería verse.

Entonces, antes que nada, está obteniendo la configuración

luego valida la configuración

y luego inicia el agente de CloudWatch .

Ahora por el momento no tenemos nada funcionando

en nuestro sistema,

entonces quiero generar algo de actividad de CPU

para que tengamos algunas métricas interesantes

cuando echamos un vistazo a CloudWatch .

Y voy a instalar una utilidad llamada stress

para que podamos generar algo de carga de CPU.

Y aquí está el comando que vamos a usar para hacer eso.

Entonces es estrés de instalación DNF menos Y,

y luego de que se haya instalado,

podemos escribir estrés menos menos CPU

y luego el número uno y presione enter.

Y esto solo creará algo de carga de CPU en nuestro sistema.

Así que solo ejecuta ese comando

y dejarlo funcionando en esta sesión.

Y en unos minutos deberíamos empezar a

vea algunas métricas que aparecen en CloudWatch .

Usando el cuadro de búsqueda, vamos a buscar

para CloudWatch y ábralo en una nueva pestaña

seleccione métricas en el menú de la izquierda y seleccione todas las métricas.

Luego bajo el agente de CW

aquí es donde podemos encontrar las métricas

que están siendo producidos por el agente

que se está ejecutando en nuestra instancia.

Y estas son todas las métricas que está produciendo.

Así que voy a seleccionar el ID de instancia

y aquí están las métricas que está recopilando.

Y si seleccionamos una métrica aquí abajo

entonces vamos a seleccionar el usuario de uso de la CPU,

y voy a seleccionar las métricas que se mostrarán

de la última hora.

Así que seleccione una H aquí.

Y si empiezas a seleccionar métricas aquí abajo

entonces notarás que comienzan a trazarse

en el gráfico aquí arriba.

Y puede que sólo tome unos momentos

para que las métricas aparezcan realmente en el gráfico.

Estas son las métricas a nivel del sistema operativo

que el agente de CloudWatch envía a CloudWatch .

Así que tenemos métricas relacionadas con el uso de intercambio,

de memoria , uso de CPU,

disco IO y porcentaje de disco.

Pero voy a anular la selección de estas métricas por ahora

y volver a todas las métricas.

Así que seleccione todo bajo métricas,

desplácese hacia abajo y seleccione EC2,

seleccionar métricas por instancia.

Y aquí es donde encontrará todos los valores predeterminados

Métricas de EC2 que CloudWatch siempre recopila

de cada instancia de EC2.

Y bajo esta vista,

muestra las métricas por instancia.

Y en realidad podemos buscar nuestra propia ID de instancia.

Así que voy a encontrar mi ID de instancia

ahí está, solo copia eso.

Luego, de vuelta en CloudWatch, busque la instancia.

ID y aquí están todas las métricas predeterminadas que

está recopilando para mi ID de instancia particular.

Y puede ingresar y seleccionar una métrica para esto

y agréguelo a su gráfico aquí arriba.

Esas son las métricas del agente de CloudWatch

pero ¿qué pasa con los registros?

Bueno, si te diriges a los registros en el lado izquierdo

y seleccionar grupos de registro,

luego seleccione mensajes porque ese era el nombre

de nuestro grupo de registro.

Luego desplácese hacia abajo y aquí está nuestro flujo de registro.

Y si recuerda, recibió el nombre de nuestra ID de instancia.

Así que seleccione el flujo de registro

y esto te llevará directamente al registro.

Y estos son todos los mensajes que aparecen en el

Mensajes de registro VAR en nuestra instancia EC2.

Así que este es el archivo de registro que le pedimos al

de CloudWatch para monitorear.

Eso es CloudWatch .

Y en resumen, lanzamos una instancia EC2.

Adjuntamos un rol de administración de identidad y acceso

con permisos para enviar las métricas del agente de CloudWatch

en CloudWatch y usamos una política administrada

denominada política del servidor del agente de CloudWatch

para darnos esos permisos.

A continuación, instalamos el agente de CloudWatch en nuestra instancia

y configuramos el agente para enviar el operativo

del sistema y los registros en CloudWatch .

Finalmente, pudimos ver las métricas en CloudWatch

y también pudimos ver las métricas predeterminadas de EC2

como las métricas y registros que se enviaban

por esta instancia mediante el agente de CloudWatch .

Eso es todo por esta lección.

Para cualquier duda, por favor hágamelo saber.

De lo contrario, te veré en la próxima.

Gracias.