

Instituto Tecnológico y de Estudios  
Superiores de Occidente – ITESO



**ITESO**  
Universidad Jesuita  
de Guadalajara

Seguridad

Materia: *Internet of Things*  
Maestro: Héctor Edmundo Ramírez Gómez  
Fecha: 20 de abril de 2020  
Autor: Arpio Fernández, León. IE702086

## Índice

Índice .....	2
Objetivos .....	3
Lambda .....	3
IoT Core .....	10
Crear una política .....	10
Generar certificados .....	12
Reglas .....	14
Dynamo DB .....	18

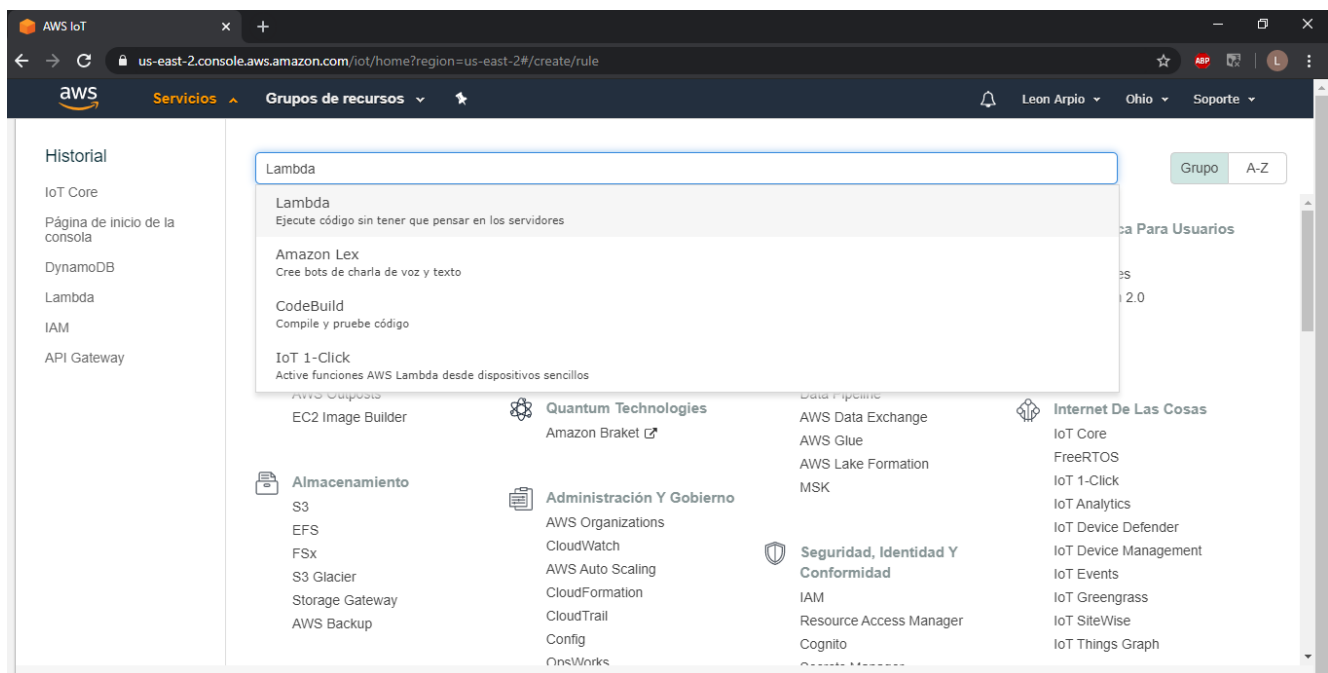
## Objetivos

El objetivo de este documento es el de mostrar paso a paso como configurar *IoT Core* de AWS para que un dispositivo pueda publicar por MQTT, como configurar una función Lambda y generar un *deploy package*, y como configurar Dynamo DB.

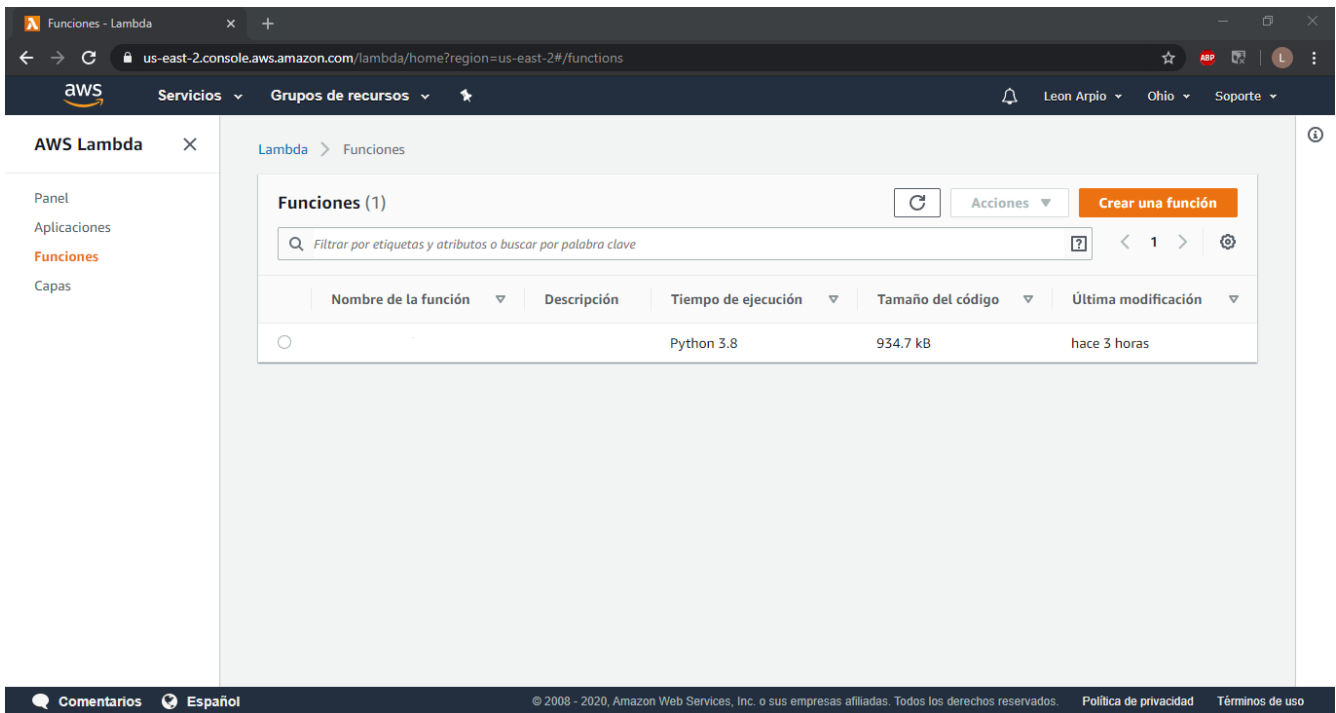
## Lambda

Lo primero que hay que hacer, es crear una cuenta en AWS, siguiendo cuidadosamente los pasos, agregando un número de teléfono, un método de pago, y asegurándose de que este sea correcto, para poder acceder a las funciones de AWS.

Una vez dentro de la plataforma, en la pestaña de *Servicios*, buscar *Lambda*.

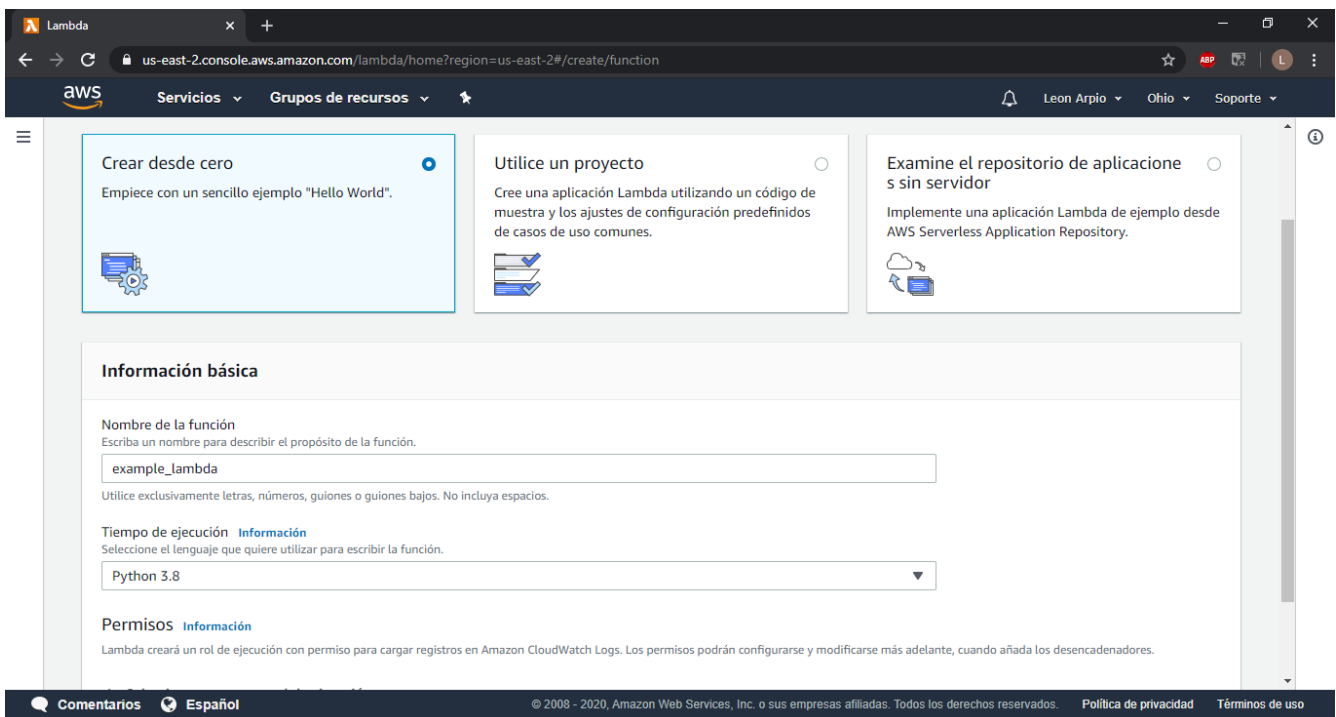


En la pestaña que se abre, presionar *Crear una función*



Seleccionar la opción *Crear desde cero*, se deberá de dar un nombre a la función, y elegir el lenguaje de programación. En este caso, Python 3.8. Presionar *Crear una función*.

**Nota:** Evitar utilizar Python 2.7, ya que pronto será descontinuado.

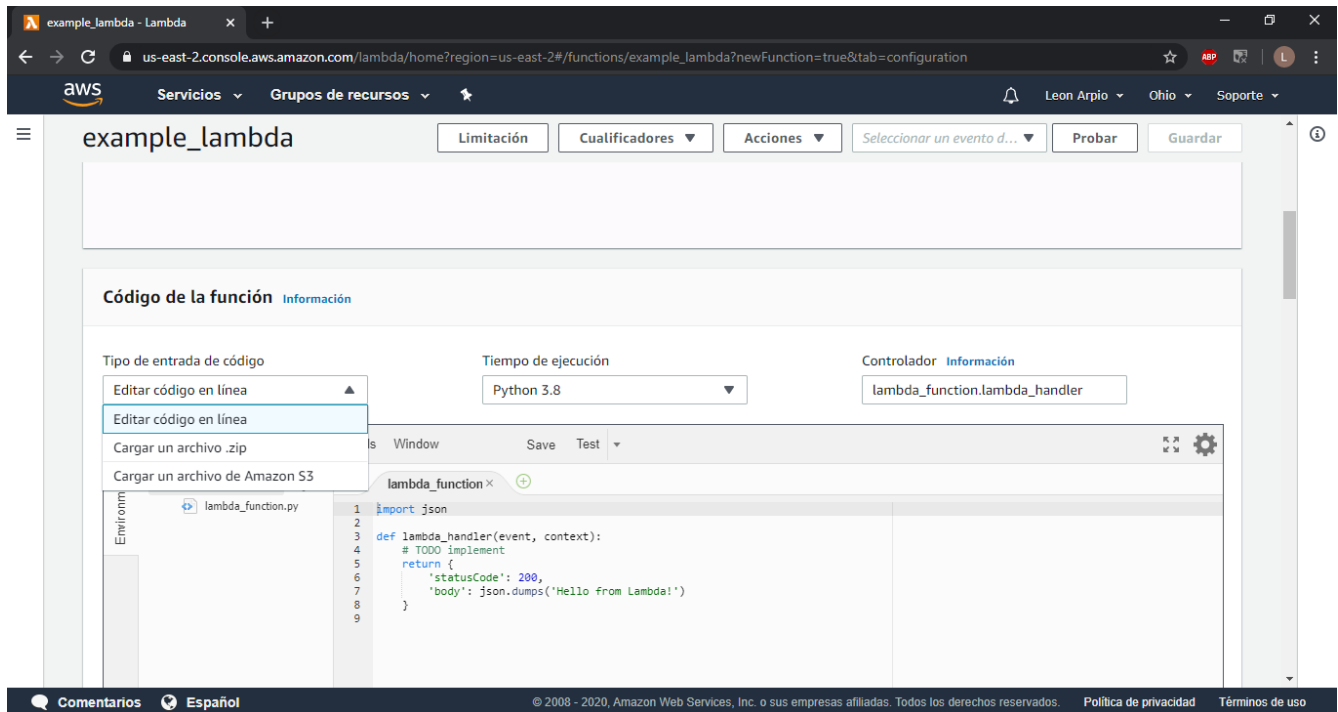


Aparecerá una ventana donde se podrá programar la Lambda, aquí también se puede elegir un archivo .zip del ordenador que contenga un *deploy package*, el cual tiene tanto la función Lambda, como las librerías necesarias para que se ejecute. Para instalar una librería de Python en una carpeta en específico, abrir la ventana de comandos en la carpeta donde se encuentra el *deploy package* y ejecutar el siguiente comando.

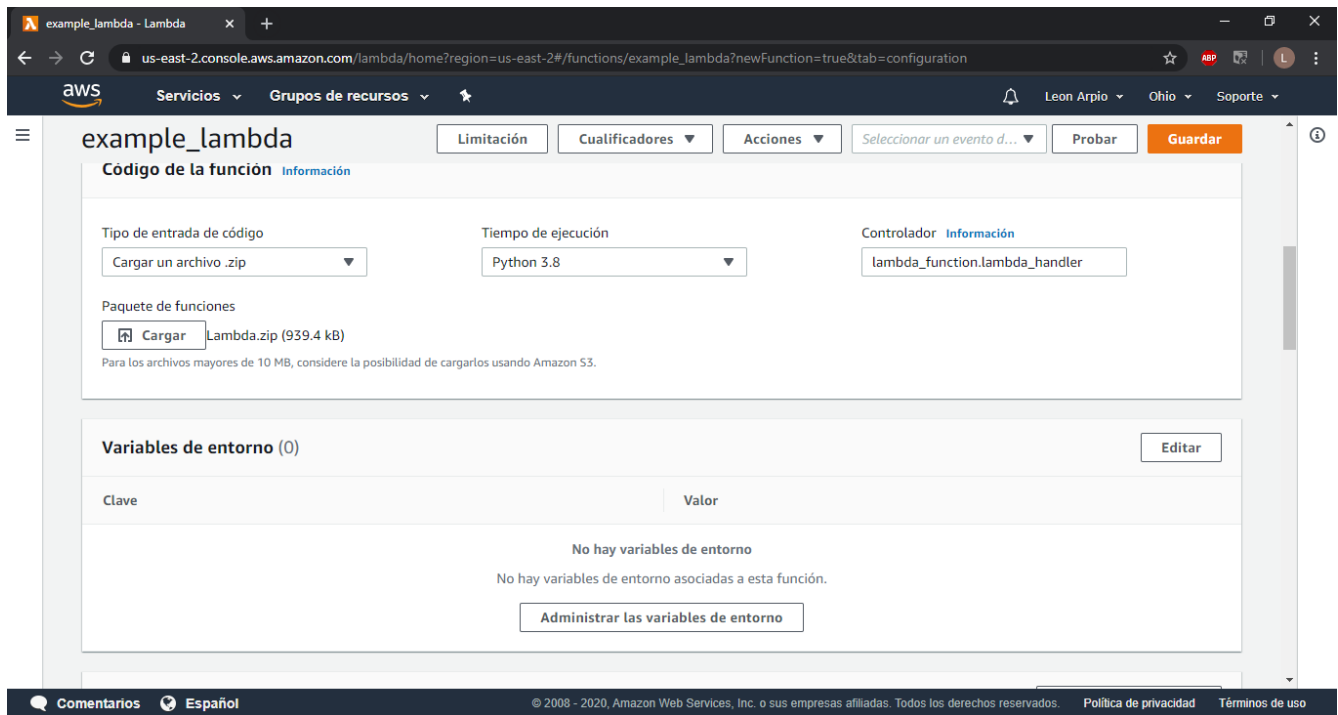
```
pip install my-library -t ..
```

Esto instalará la librería *my-library* en la carpeta actual. Comprimir la carpeta, y en AWS seleccionar la opción Cargar un archivo .zip.

**Nota:** Si no necesitas una librería no soportada por AWS, puedes editar el código en línea sin mayor problema.



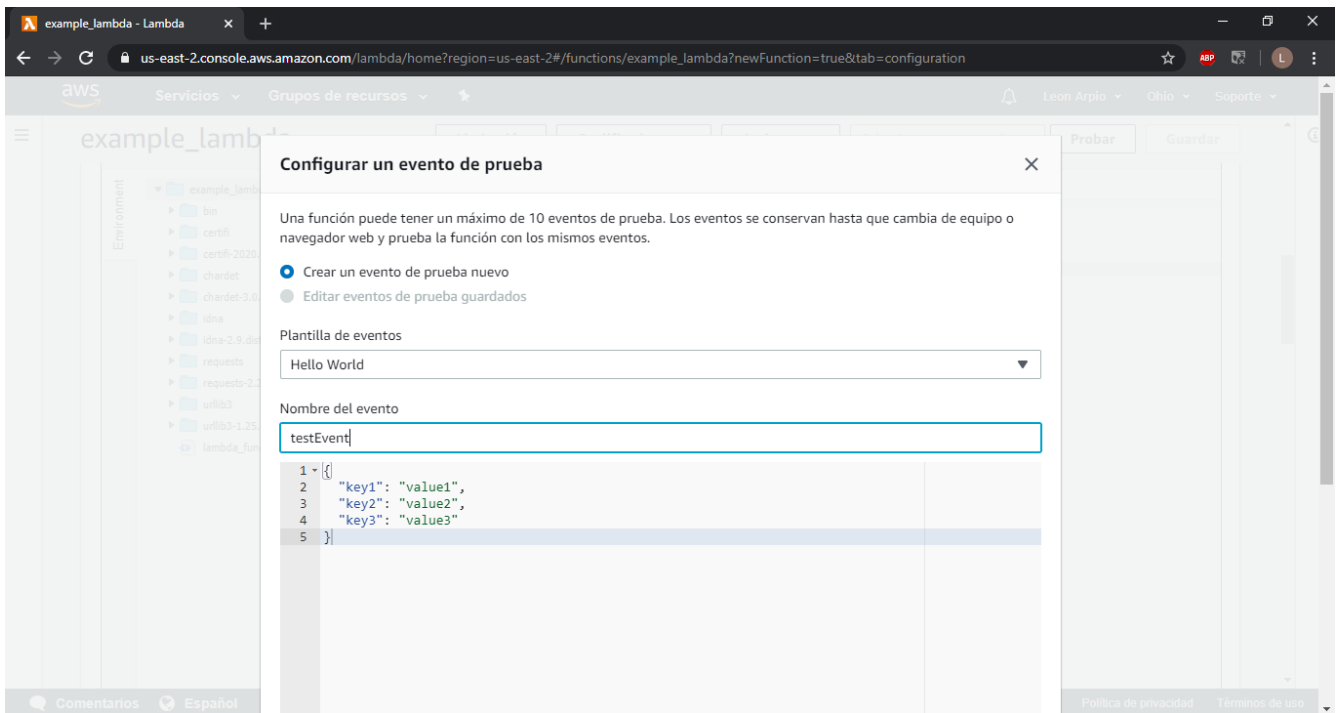
Presionar *Cargar* y seleccionar el archivo .zip que se generó. Cuando finalice la carga del archivo, presionar *Guardar*.



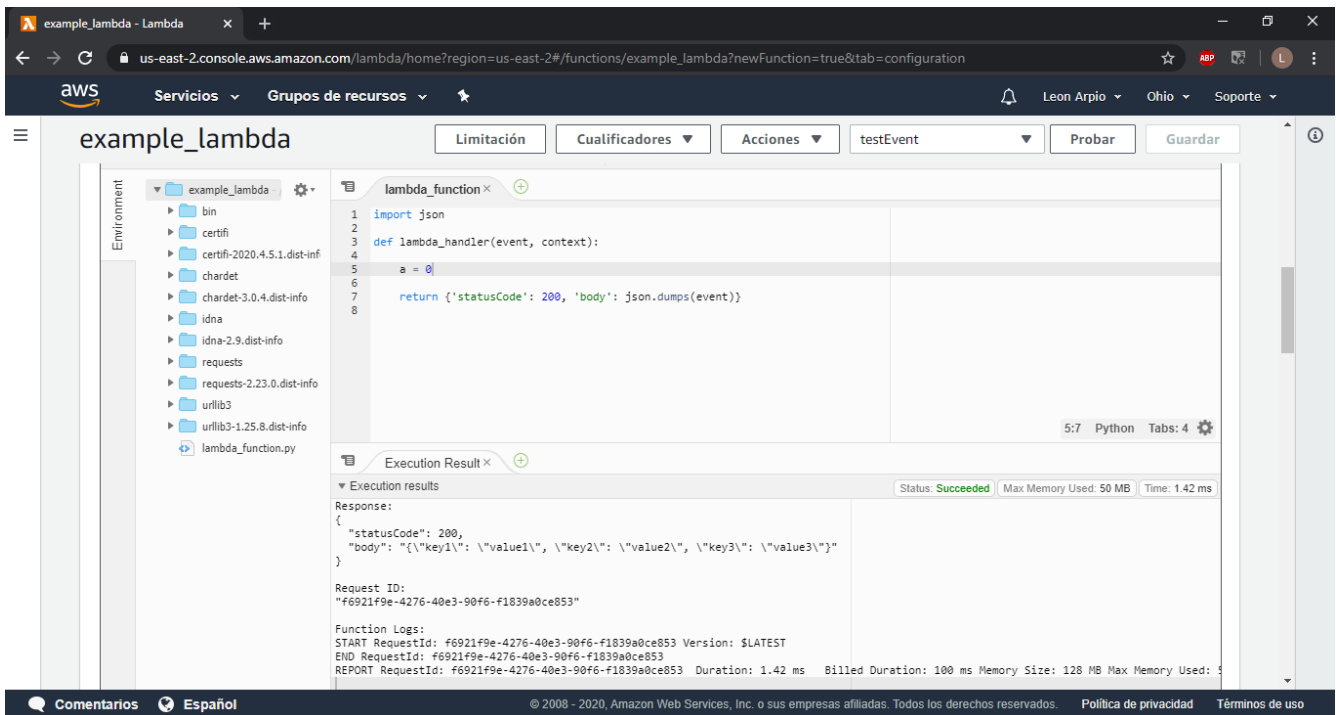
Ahora puedes seguir editando el código en línea, y hacer pruebas. Lambda recibe como argumento *event* el cual contiene el mensaje que fue recibido por MQTT en la forma de un diccionario.

**Nota:** Toda la información recibida por Lambda debe ser en formato JSON válido.

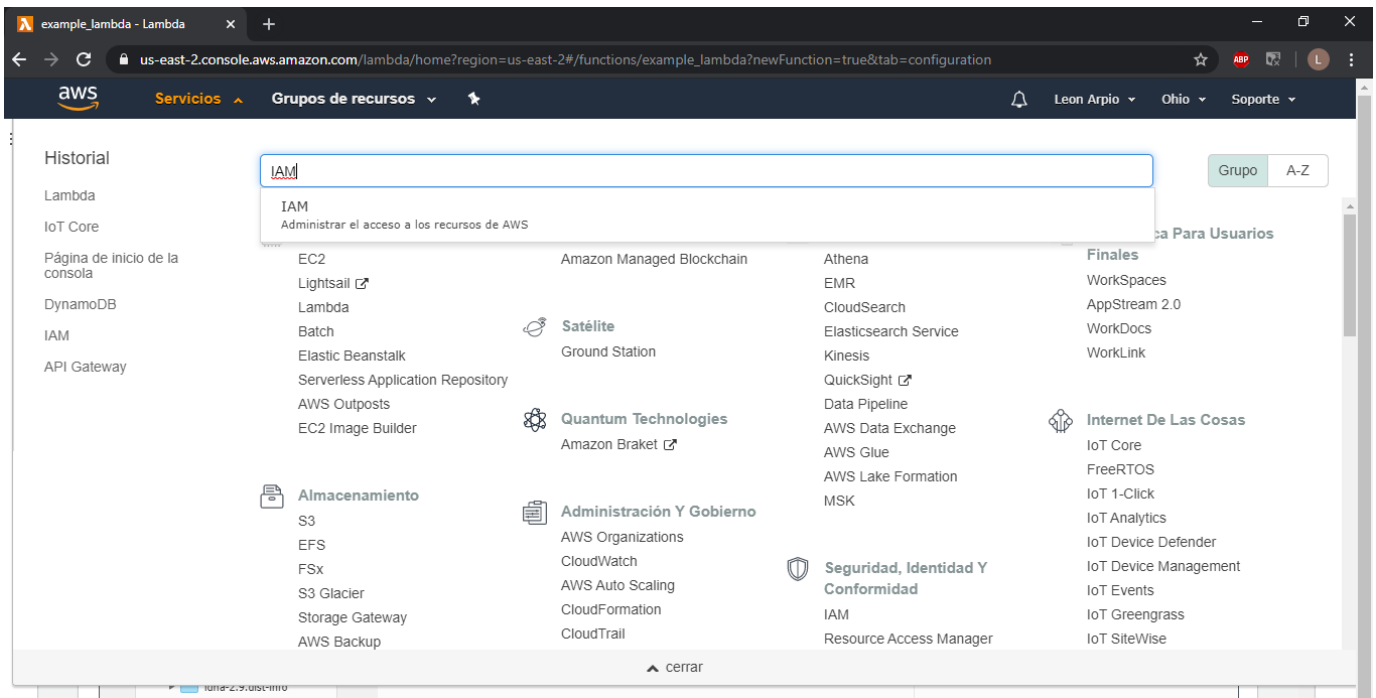
Para probar la función, seleccionar *Probar*, y se abrirá una ventana en la cual podrás configurar el diccionario que llegará a *event*. Dar un nombre y los valores deseados, y presionar *Crear*.



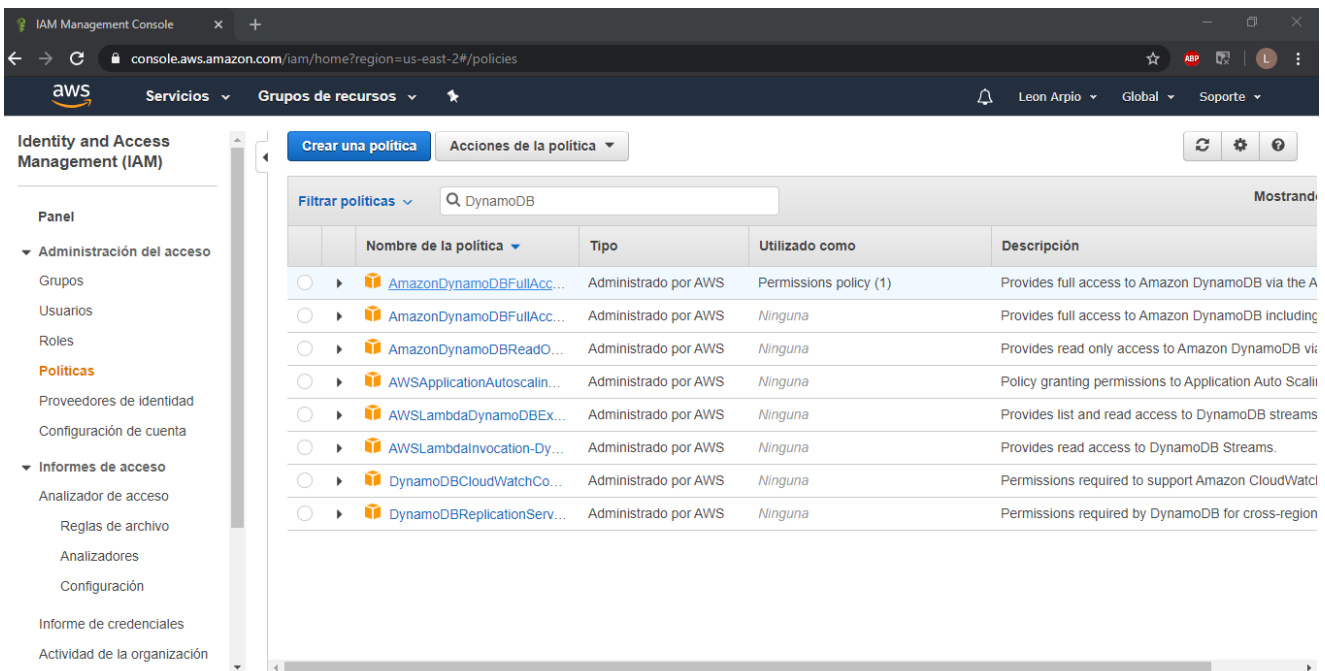
Una vez creado el evento, presionar *Probar*, y si la función se ejecuta sin errores, el valor de retorno aparecerá en pantalla, como en el siguiente ejemplo, de lo contrario, se mostrará un mensaje indicando el error.



Para dar permisos a Lambda para que publique en Dynamo DB, en *Servicios*, buscar *IAM*.

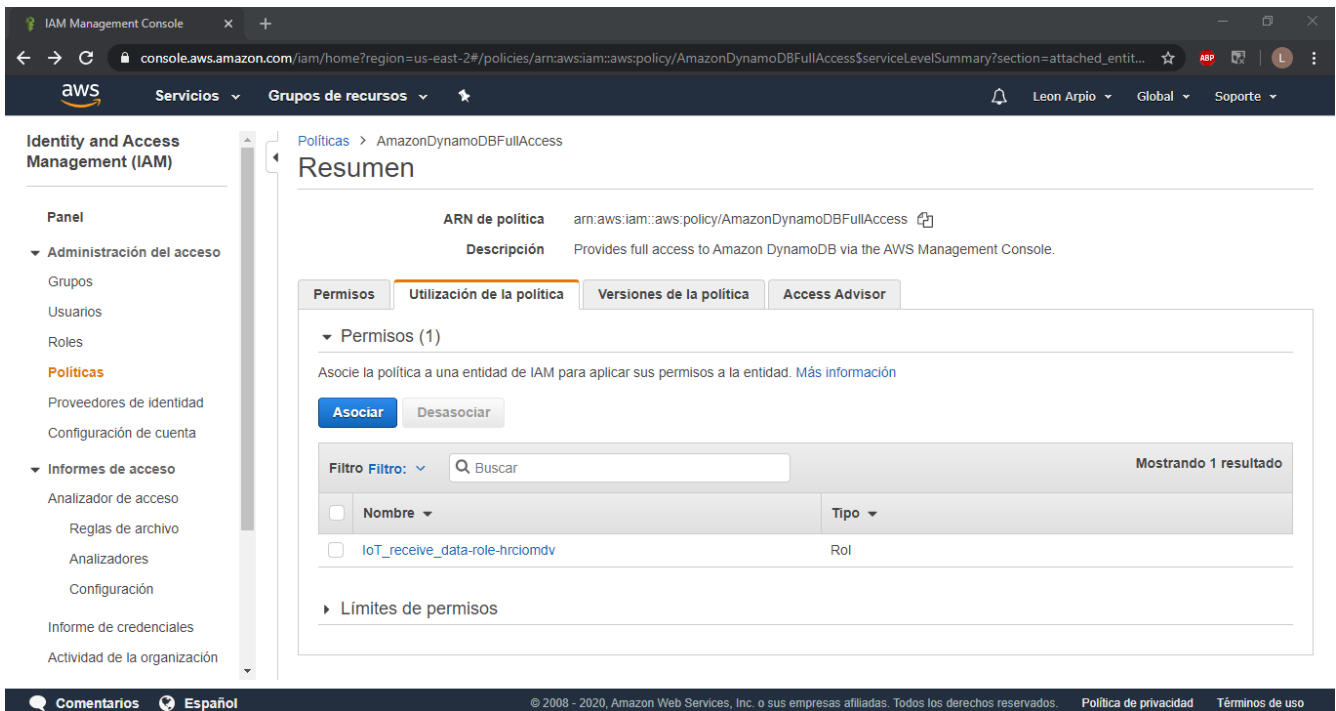


Ir a la pestaña *Políticas* y en el filtro escribir *DynamoDB*, seleccionar la política *AmazonDynamoDBFullAccess*.



En la nueva ventana, seleccionar la pestaña *Utilización de la política*, y seleccionar *Asociar*.





**Identity and Access Management (IAM)**

**Panel**

- Administración del acceso
  - Grupos
  - Usuarios
  - Roles
  - Políticas**
  - Proveedores de identidad
  - Configuración de cuenta
- Informes de acceso
  - Analizador de acceso
  - Reglas de archivo
  - Analizadores
  - Configuración
  - Informe de credenciales
  - Actividad de la organización

**Políticas** > AmazonDynamoDBFullAccess

## Resumen

**ARN de política** `arn:aws:iam::aws:policy/AmazonDynamoDBFullAccess`

**Descripción** Provides full access to Amazon DynamoDB via the AWS Management Console.

**Permisos** | **Utilización de la política** | **Versiones de la política** | **Access Advisor**

**Permisos (1)**

Asocie la política a una entidad de IAM para aplicar sus permisos a la entidad. [Más información](#)

**Asociar** **Desasociar**

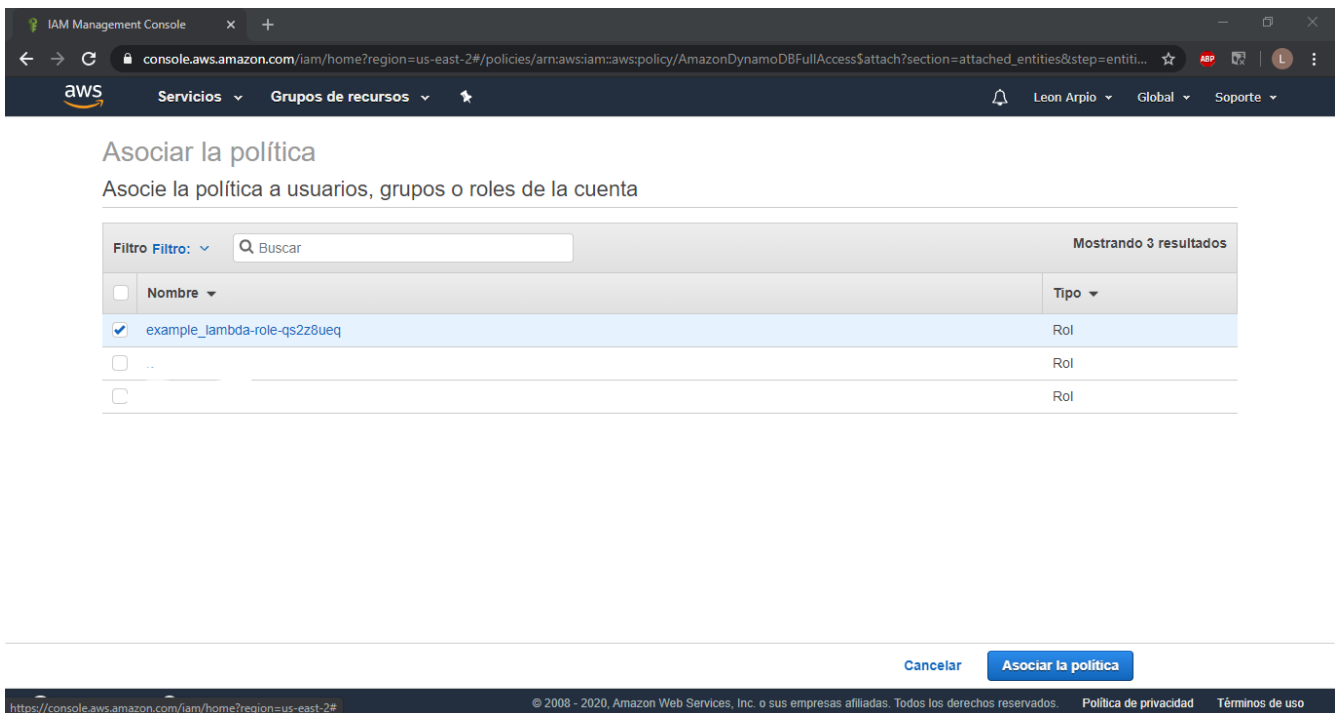
**Filtro Filtro:**  **Mostrando 1 resultado**

<input type="checkbox"/>	Nombre	Tipo
<input type="checkbox"/>	IoT_receive_data-role-hrciomdv	Rol

**Límites de permisos**

Comentarios | Español | © 2008 - 2020, Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados. | Política de privacidad | Términos de uso

Seleccionar el rol deseado para asociar a esta política, y presionar *Asociar la política*. En caso de que no haya ningún rol, o que no aparezca el deseado, seguir los pasos de IoT Core, y luego repetir este último paso.



**Asociar la política**

Asocie la política a usuarios, grupos o roles de la cuenta

**Filtro Filtro:**  **Mostrando 3 resultados**

<input type="checkbox"/>	Nombre	Tipo
<input checked="" type="checkbox"/>	example_lambda-role-qs2z8ueq	Rol
<input type="checkbox"/>	..	Rol
<input type="checkbox"/>		Rol

**Cancelar** **Asociar la política**

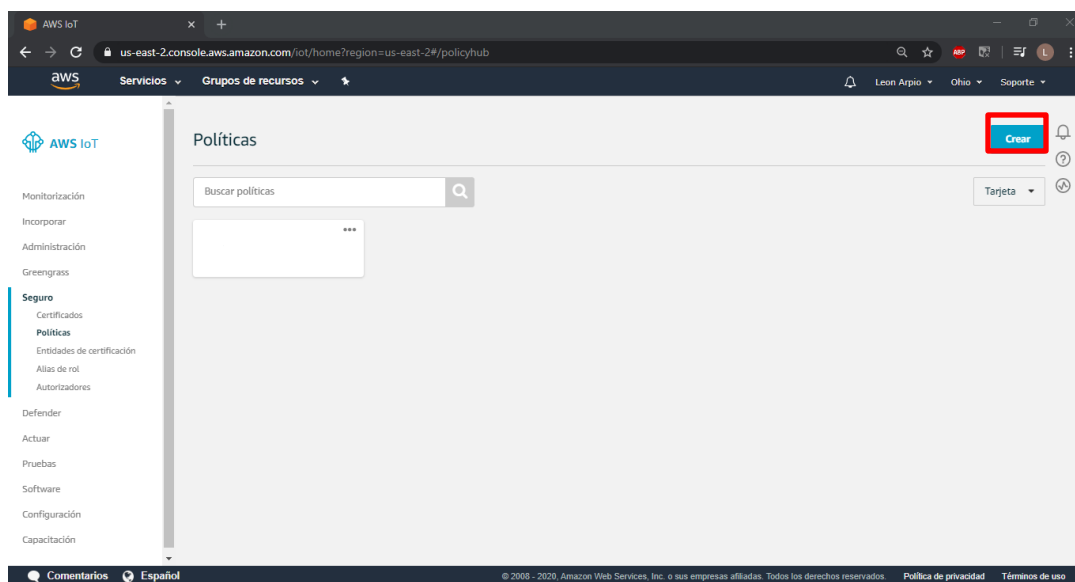
<https://console.aws.amazon.com/iam/home?region=us-east-2#> | © 2008 - 2020, Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados. | Política de privacidad | Términos de uso

## IoT Core

En la pestaña de *Servicios*, buscar *IoT Core*.

### Crear una política

Las políticas permiten o prohíben a los dispositivos conectarse, publicar, suscribirse, recibir mensajes de un tópico, y otras acciones. Ir a *Seguro>Políticas*, en la ventana del lado izquierdo de AWS, y elegir *Crear*.



En esta ventana se solicitará un nombre para la política, y se deberá añadir declaraciones. Una declaración es una configuración en la que se definirá si permitir o denegar una acción. Por ejemplo, si permitir que un dispositivo se conecte, o permitir que este se suscriba y reciba de un tópico, o denegar que publique en algún tópico. Se deberá de añadir cada una de estas acciones, con su respectivo efecto por separado. Para agregar varios dispositivos o tópicos a una sola declaración, utilizar una coma para cada ARN (Amazon Resource Number). Al finalizar de definir las declaraciones, presionar *Crear*.

←

→

↺

us-east-2.console.aws.amazon.com/iot/home?region=us-east-2#/create/policy

☆

ABP

🔍

L

⋮

aws

Servicios ▾

Grupos de recursos ▾

📌

🔔

Leon Arpio ▾

Ohio ▾

Soporte ▾

←

Crear una política

Cree una política para definir un conjunto de acciones permitidas. Puede permitir acciones en uno o varios recursos (objetos, temas o filtros de temas). Para obtener más información sobre las políticas de IoT, consulte la [página de documentación de políticas de AWS IoT](#).

Nombre

ejemplo\_politica

Añadir declaraciones

Las declaraciones de política definen los tipos de acciones que puede realizar un recurso.

Modo avanzado

Acción

iot:Connect

ARN de recurso

arn:aws:iot:us-east-2:::root/client/replaceWithAClientId1,arn:aws:iot:us-east-2:::root/client/replaceWithAClientId1

Comentarios

🌐 Español

© 2008 - 2020, Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados. [Política de privacidad](#) [Términos de uso](#)

The screenshot shows the AWS IAM console interface for creating IoT policies. The browser address bar indicates the URL: `us-east-2.console.aws.amazon.com/iot/home?region=us-east-2#/create/policy`. The navigation bar includes the AWS logo, 'Servicios', 'Grupos de recursos', and a user profile 'Leon Arpio' from 'Ohio'.

On the left sidebar, there is a back arrow button. The main content area displays two policy creation forms:

- Policy 1:**
  - Permissions: ☒ Permitir, ☐ Denegar
  - Action: `iot:Publish`
  - ARN de recurso: `arn:aws:iot:us-east-2:::topic/replaceWithATopic1`
  - Effect: ☐ Permitir, ☒ Denegar
  - Action: `iot:Subscribe`
  - ARN de recurso: `arn:aws:iot:us-east-2:::topic/replaceWithATopic2`
  - Effect: ☒ Permitir, ☐ Denegar
- Policy 2:**
  - Permissions: ☒ Permitir, ☐ Denegar
  - Action: `iot:Subscribe`
  - ARN de recurso: `arn:aws:iot:us-east-2:::topic/replaceWithATopic2`
  - Effect: ☒ Permitir, ☐ Denegar

Each policy configuration has an 'Eliminar' (Delete) button in the top right corner. The footer of the console shows 'Comentarios', 'Español', and copyright information for Amazon Web Services, Inc. (2008 - 2020).

us-east-2.console.aws.amazon.com/iot/home?region=us-east-2#/create/policy

Servicios Grupos de recursos

Leon Arpio Ohio Soporte

Efecto

☒ Permitir ☐ Denegar Eliminar

Acción

iot:Receive

ARN de recurso

arn:aws:iot:us-east-2:topic/replaceWithATopic2

Efecto

☒ Permitir ☐ Denegar Eliminar

Añadir declaración

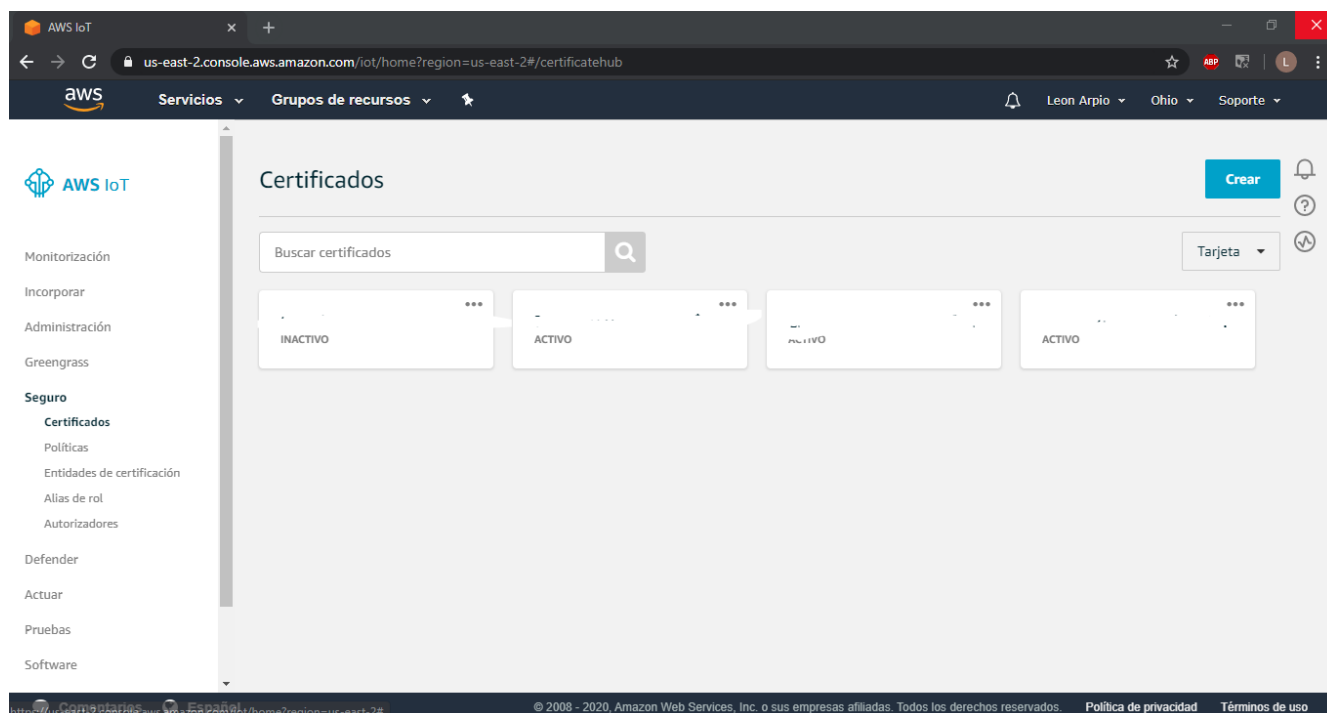
Crear

Comentarios Español © 2008 - 2020, Amazon Web Services, Inc. o sus empresas afiliadas. Todos los derechos reservados. Política de privacidad Términos de uso

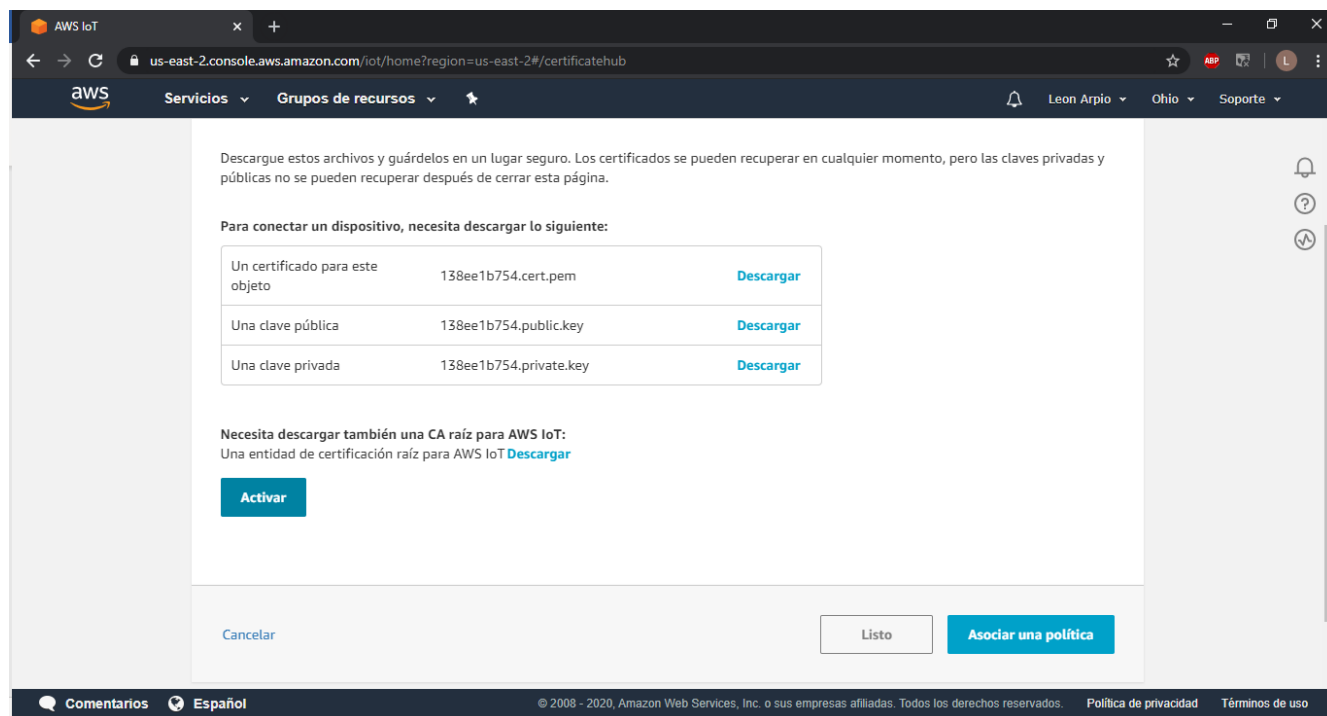
La política generada, permitirá a los dispositivos con ID de cliente *replaceWithAClientId1* y *replaceWithAClientId2* que se conecten por MQTT, y que se suscriban y reciban información del tópico *replaceWithATopic2*, pero no permitirá que publique en *replaceWithATopic1* (Una vez generado el certificado). Se puede utilizar "\*" como *wildcard*, por ejemplo, aprobar que se publique a */example/\** permitirá que pueden llegar mensajes a cualquier tópico que empiece con */example/*.

## Generar certificados

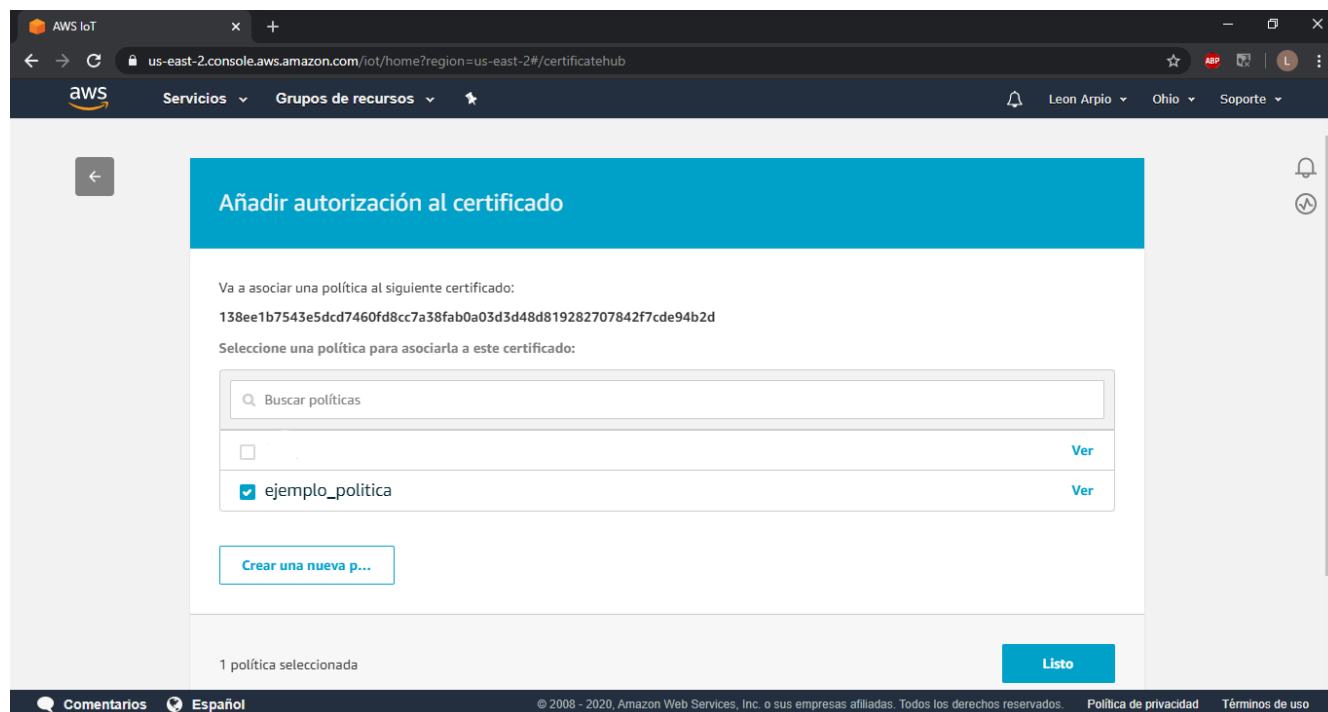
Ir a *Seguir>Certificados* para generar uno, y asignarlo a la política.



Presionar *Crear*, y luego *Crear un certificado*, en el apartado *Creación de un certificado con un clic*. Automáticamente se generarán los certificados, descargarlos y guardarlos, ya que, si se pierden, se tendrán que generar otra vez. Presionar *Activar* dentro de esta pestaña, y seguidamente, presionar *Asociar una política*.



En la siguiente pestaña, aparecerán las políticas configuradas, y se deberá seleccionar la o las políticas que se deseen asociar a este certificado. Al finalizar, presionar *Listo*.

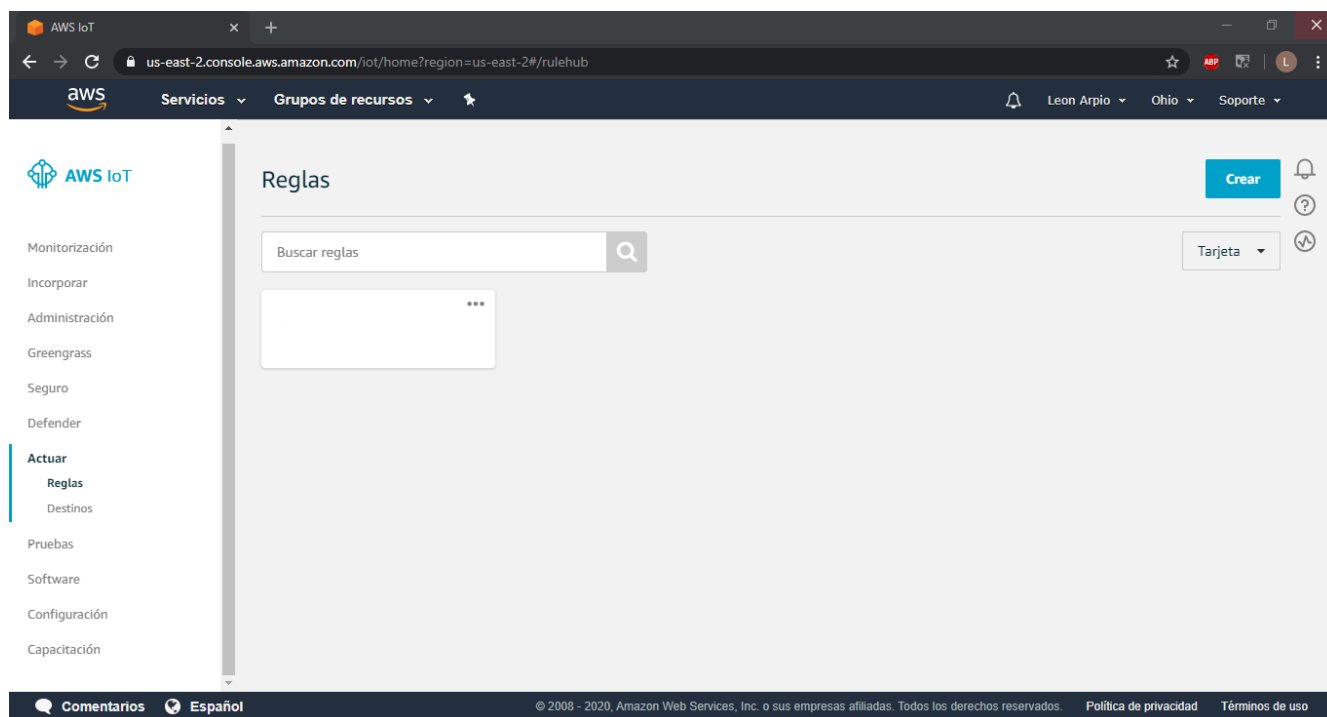


Esto implica que a partir de ahora los dispositivos *replaceWithAClientId1* y *replaceWithAClientId2* podrán conectarse a AWS, utilizando los certificados que se generaron en este paso. Al salir de esta pestaña, volverán a aparecer los certificados, pero el último que generamos aparecerá como inactivo.

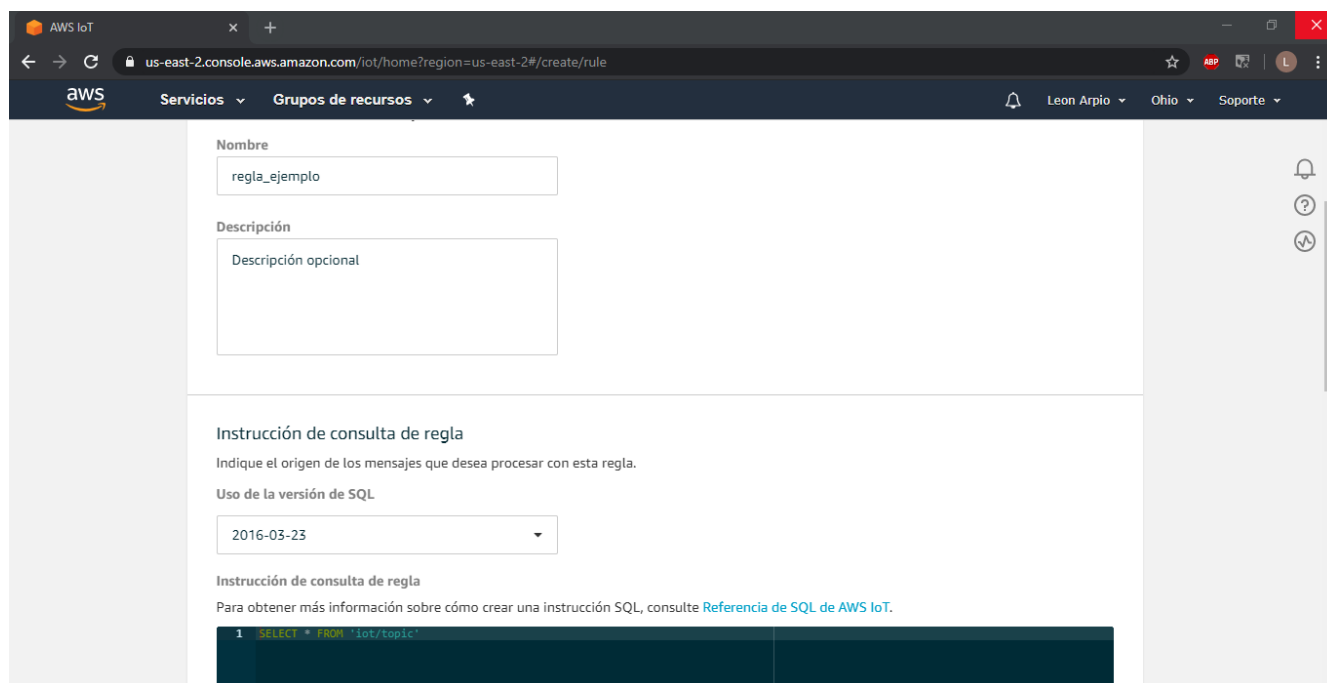
**Nota:** Ningún dispositivo se puede conectar a AWS sin una política que lo permita y los certificados correspondientes.

## Reglas

Las reglas permiten redireccionar los mensajes que llegan a AWS a los diferentes servicios de este. Ir a la pestaña *Actuar>Reglas* y presionar *Crear*.

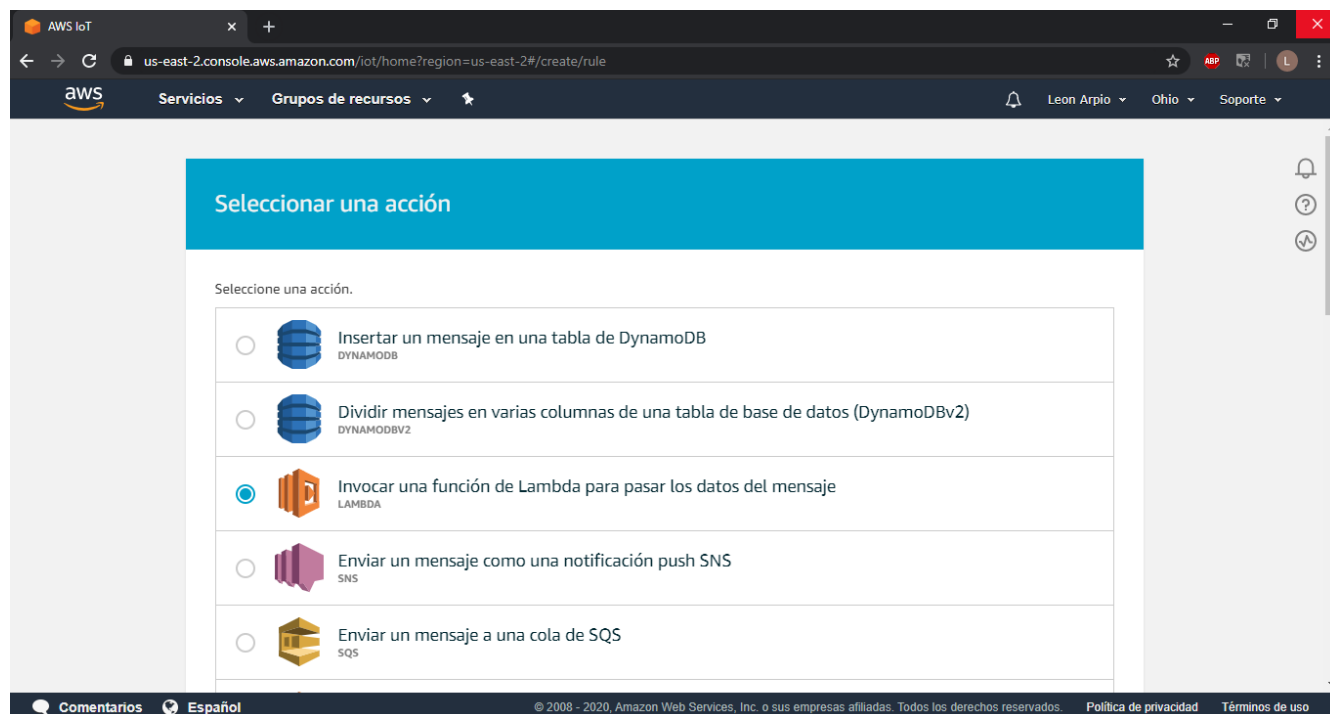


En la pestaña que se abre solicitará que se le de un nombre a la regla, y una descripción opcional. Después, se deberá configurar la instrucción de la regla, que, en otras palabras, indicará el tópico que, cuando lleguen mensajes, activará la regla.

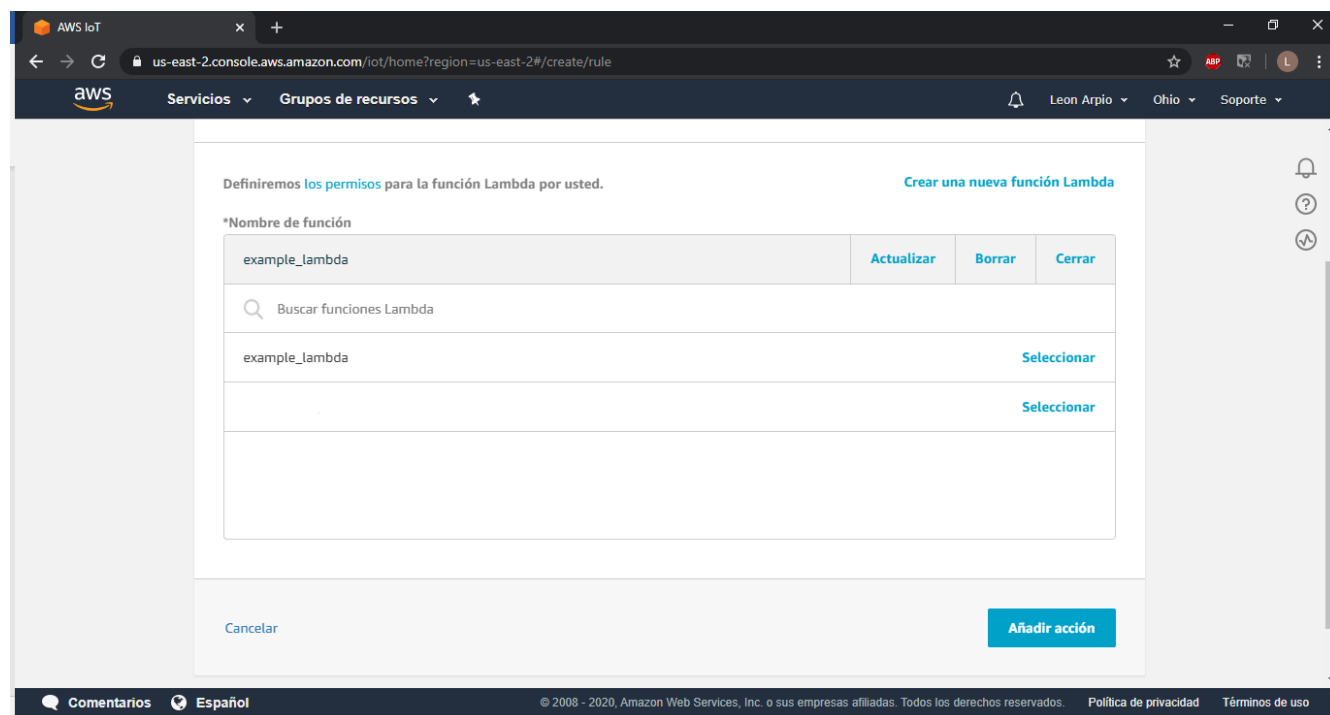


En este ejemplo, cualquier mensaje que llegue a *iot/topic* activará la regla que se está configurando. Más abajo, presionar *Añadir acción*, en el apartado *Definir una o varias acciones*.

En la siguiente pestaña, elegir *Invocar una función de Lambda para pasar los datos del Mensaje* y presionar *Configurar acción*.

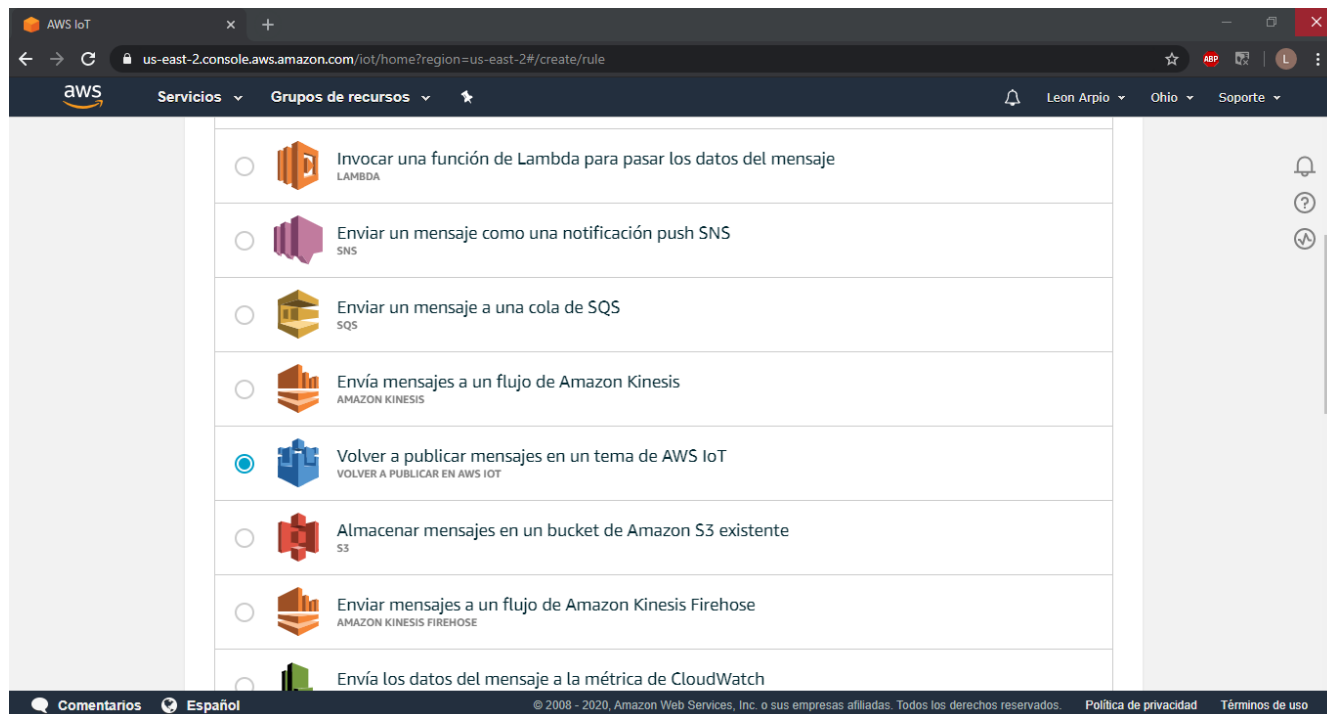


Presionar la función Lambda deseada, presionar *Seleccionar*, y luego *Añadir acción*.

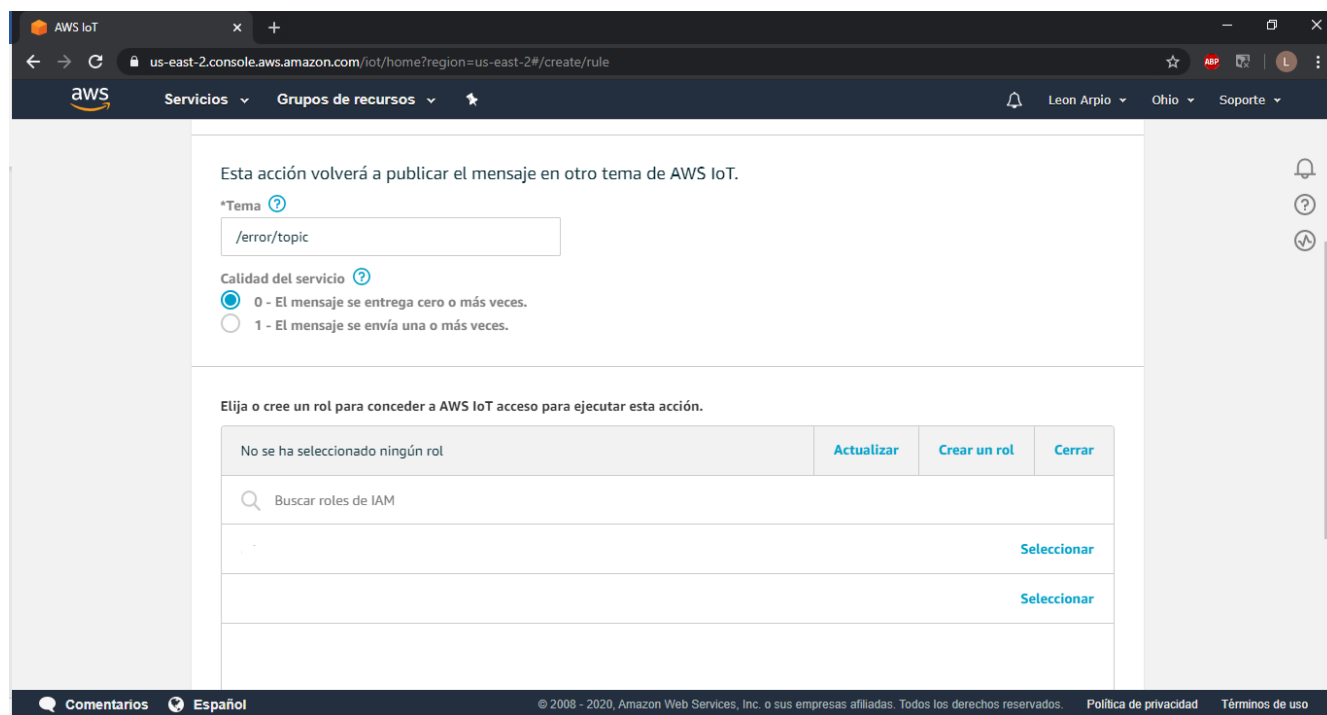




Regresaremos a la ventana anterior, en la cual debemos de elegir una acción de error, esta se ejecutará en caso de que la función Lambda produzca algún error, por ejemplo, si el mensaje que llega no está en formato JSON. Para esta acción se recomienda elegir la opción *Volver a publicar mensajes en un tema de AWS IoT* para redirigir el mensaje erróneo a otro tópico. Presionar configurar acción.



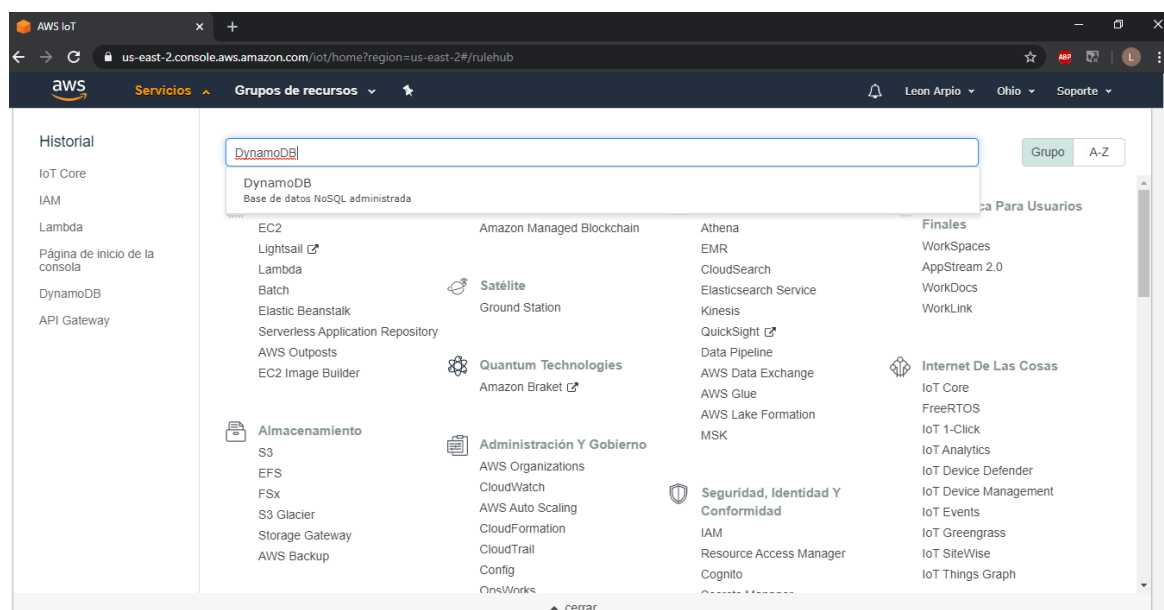
Después, elegir el tema al cual se publicará el mensaje, también, se deberá de elegir un rol para dar a AWS IoT acceso a la acción. Presionar *Crear un rol*.



En el recuadro que aparezca, elegir el nombre que tendrá el rol, y después presionar *Crear un rol*, y luego *Añadir acción*. Regresaremos otra vez a la ventana de configuración de la regla, presionar *Crear una regla*. A partir de ahora, cualquier mensaje que llegue a *iot/topic* será enviado a la función Lambda, como argumento *event*.

## Dynamo DB

En la pestaña de *Servicios*, buscar *DynamoDB*.



Cuando se abra la nueva ventana, presionar *Crear tabla*.

**Crear tabla**

Amazon DynamoDB es un servicio de base de datos no relacional totalmente administrado que ofrece un desempeño rápido y predecible, así como una escalabilidad perfecta.

[Crear tabla](#)

**Alertas recientes**

No se han activado alarmas de CloudWatch. [Ver todo en CloudWatch](#)

**Capacidad total para US East (Ohio)**

Capacidad	Límite	Reservada	Reservada
Cap. de lectura aprovisionada	5 (Máx.: 80000)	Cap. de lectura reservada	0
Cap. de escritura aprovisionada	5 (Máx.: 80000)	Cap. de escritura reservada	0

**Utilización de los límites de la capacidad de la cuenta para US East (Ohio)**

Intervalo de tiempo: Últimas 24 horas

Utilización del límite de la capacidad de lectura aprovisionada (%)

100

75

**Característica destacada**

- CloudWatch Contributor Insights para DynamoDB **NUEVO**
- NoSQL Workbench
- DynamoDB bajo demanda
- Transacciones
- Tablas globales
- Amazon DynamoDB Accelerator (DAX)
- Recuperación a un momento dado

**Recursos adicionales**

- Informar de un problema
- Guía de introducción
- Introducción al laboratorio práctico
- Guía para desarrolladores
- Preguntas frecuentes
- Guías de migración de DynamoDB

En la siguiente ventana, se deberá de dar un nombre a la tabla, y elegir una clave de partición, la cual será un identificador que permita diferenciar entre los dispositivos que publican en la tabla, por ejemplo, IMEI. Después se deberá de elegir la clave de ordenación, que es un identificador que permite diferenciar entre los mensajes publicados por un solo dispositivo, por ejemplo, timestamp. Dado que IMEI es una cadena de caracteres, y timestamp es un valor numérico, es importante seleccionar cadena y número respectivamente. Al final presionar *Crear*.

**Crear una tabla de DynamoDB**

DynamoDB es una base de datos sin esquema que solo necesita un nombre de tabla y una clave principal. La clave principal de la tabla está compuesta de uno o dos atributos que identifican de manera inequívoca cada elemento, efectúan la partición de datos y ordenan los datos dentro de cada partición.

**Nombre de la tabla\***

**Clave principal\*** Clave de partición

☒ Añadir clave de ordenación

**Configuración de la tabla**

La configuración predeterminada proporciona la forma más rápida de comenzar con la tabla. Puede modificar esta configuración predeterminada ahora o después de crear la tabla.

☒ Usar la configuración predeterminada

- No hay índices secundarios.
- Capacidad aprovisionada establecida en 5 lecturas y 5 escrituras.
- Alarmas básicas con umbral superior al 80% que usan el tema de SNS "dynamodb".
- Cifrado en reposo con el tipo de cifrado PREDETERMINADO.

A partir de ahora la tabla está lista para recibir mensajes. Se puede elegir *Elementos* en la pestaña de *Tablas* para ver los mensajes almacenados en la base de datos.

**tabla\_ejemplo** Cerrar

Información general **Elementos** Métricas Alarmas Capacidad Índices Tablas globales Más

**Crear elemento** Acciones

Examen: [Tabla] tabla\_ejemplo: IMEI, timestamp

Mostrando 0 de 0 elementos

Examen [Tabla] tabla\_ejemplo: IMEI, timestamp

+ Añadir filtro

Iniciar búsqueda

IMEI timestamp

Un elemento consta de uno o varios atributos. Cada atributo consta de un nombre, un tipo de datos y un valor. Cuando lea o escriba un elemento, los únicos atributos obligatorios son los que forman la clave principal. [Más información](#)

Ahora AWS está configurado para que se pueda usar con el proyecto de este repositorio.