

## CTC-106, Conexión de módulos SIMCOM con soporte MQTT a Amazon Web Services IoT Core



Comentario técnico: CTC-106

Componente: **Conexión de módulos SIMCOM con soporte MQTT a Amazon Web Services IoT Core**

Autor: Sergio R. Caprile, Senior R&D Engineer

| Revisiones | Fecha    | Comentarios |
|------------|----------|-------------|
| 0          | 14/09/20 |             |
|            |          |             |
|            |          |             |

En el [CTC-104](#) analizamos los Amazon Web Services (AWS) y desarrollamos la utilización de AWS IoT Core, el servicio de conectividad, utilizando MQTT. En el [CTC-102](#) vimos la forma de conectar los módulos SIMCOM como el SIM7600 a un broker MQTT. En este Comentario Técnico analizaremos la forma de conectarnos a dicha plataforma con dichos módulos.

### Credenciales y AWS IoT Core

Antes de proseguir, es fundamental que hayamos leído el [CTC-104](#) y que hayamos realizado el *quickstart* de AWS IoT Core.

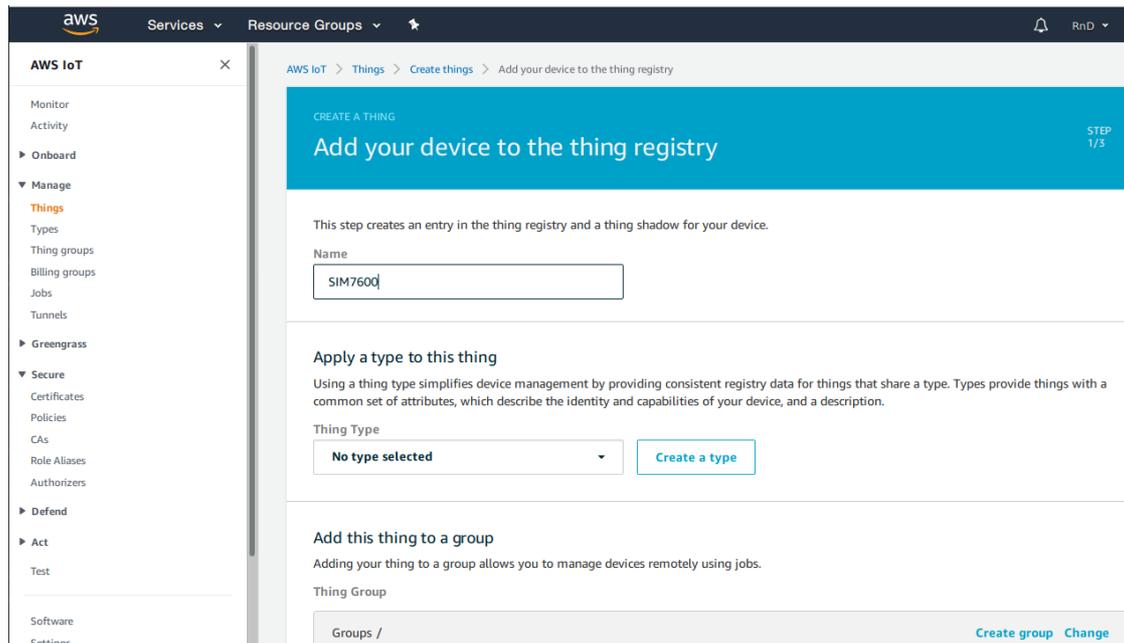
Las acciones a realizar son:

- cargar el dispositivo en la *registry*
- generar en AWS la clave privada y el certificado de esta clave y obtenerlos.
- obtener el certificado de la CA de Amazon
- generar una política con los permisos de conexión deseados
- asociar la política al certificado y éste al dispositivo
- obtener la dirección del broker MQTT que nos corresponde

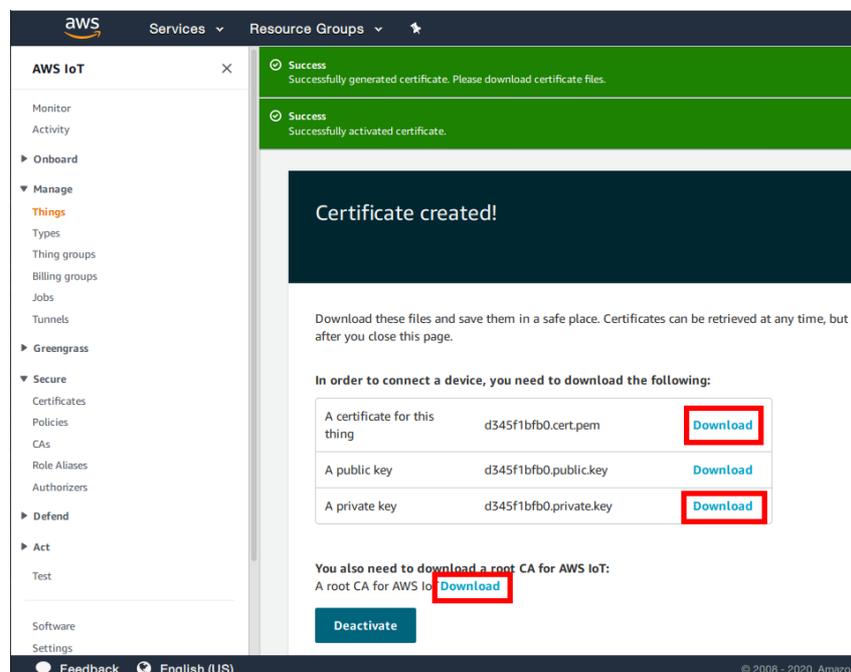
Comenzamos seleccionando *Manage* → *Things*, luego *Create* y luego *Create a single thing*. Aparece un esquema de tres pasos:

Paso 1: Creación de la *Thing*, ingresamos el nombre y no debemos hacer nada más; seleccionamos *Next*

## CTC-106, Conexión de módulos SIMCOM con soporte MQTT a Amazon Web Services IoT Core



Paso 2: Generación de claves y certificados, seleccionamos *Create a certificate*, se abre una nueva ventana con el certificado creado. Debemos primero activar el certificado haciendo click en *Activar*, bajar nuestra clave privada y certificado, y además el certificado de la CA. Nuestra clave pública no nos sirve para esto. Si ya seguimos el [CTC-105](#), o en el *quickstart* modificamos la policy, es decir, disponemos de una política de seguridad que podemos asociar a este certificado, seleccionaremos *Attach a policy* y pasaremos al paso 3. Caso contrario, seleccionaremos *Done* y saltamos el paso 3.



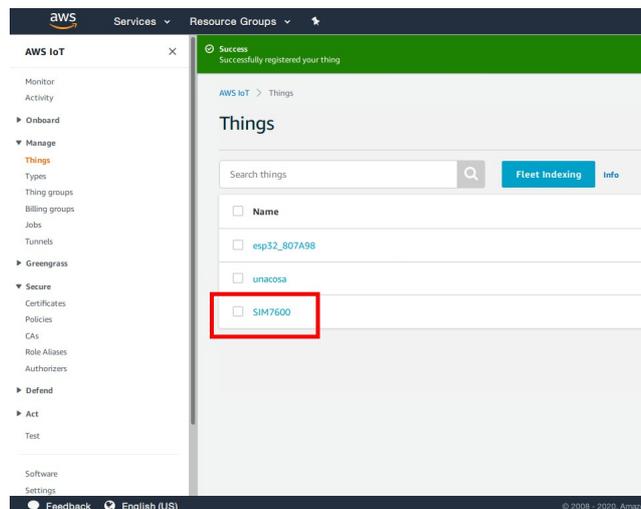
Paso 3: Policy, elegimos una de las disponibles y la asociamos al certificado. Salteamos el párrafo siguiente.

## CTC-106, Conexión de módulos SIMCOM con soporte MQTT a Amazon Web Services IoT Core

Sólo si no ejecutamos el paso 3, que es lo más probable, debemos generar una política de seguridad. La que podemos apreciar en la siguiente captura es bastante permisiva, para una aplicación real deberemos modificarla, de igual modo que tal vez deseemos crear un grupo de dispositivos o aplicar nuestra propia estrategia de despliegue de la red. Seleccionamos *Secure* → *Policies*, luego *Create*, ingresamos como se ve en la captura siguiente *Action = iot:\**, *Resource ARN = \** y *Effect = Allow*. Finalmente, vamos a *Secure* → *Certificates*, hacemos click sobre la clave del certificado y se abre una ventana con los datos. Allí seleccionamos *Policies* y luego *Actions* → *Attach Policy*.

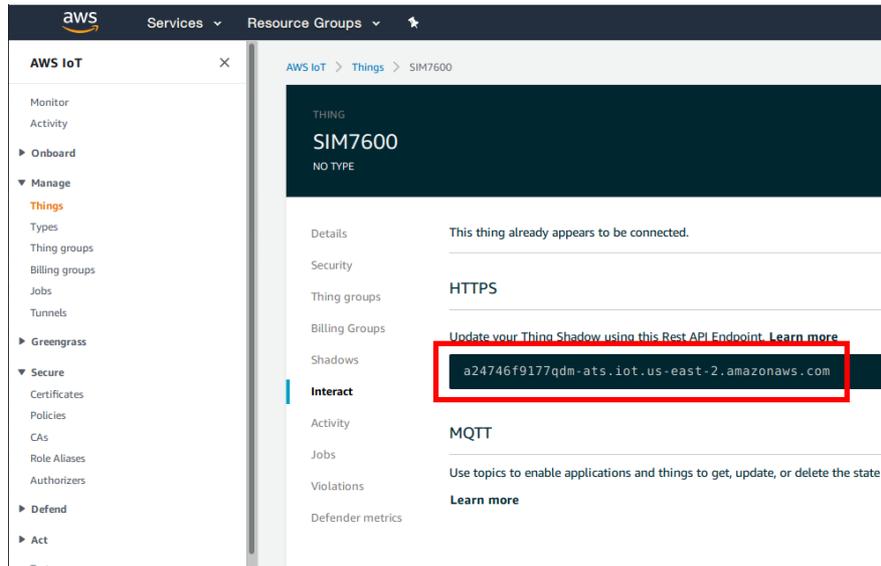
The screenshot shows the AWS IoT console interface for creating a policy. The left sidebar contains navigation options like Monitor, Activity, Onboard, Manage, Greengrass, Secure, Certificates, Policies, CAs, Role Aliases, Authorizers, Defend, Act, and Test. The main content area is titled 'Create a policy' and includes a text input for the policy name 'myPolicy'. Below this, there is a section for 'Add statements' with a table for defining policy statements. The first statement has 'Action' set to 'iot:\*', 'Resource ARN' set to '\*', and 'Effect' set to 'Allow'. A 'Create' button is located at the bottom right of the form.

Podemos detenemos a observar nuestra creación:



## CTC-106, Conexión de módulos SIMCOM con soporte MQTT a Amazon Web Services IoT Core

Finalmente obtenemos la dirección del broker MQTT como observamos en la captura siguiente:



### Operación del módulo

Las acciones a realizar son:

- cargar clave privada y certificados (nuestro y CA de Amazon) en el módulo
- conectarse por MQTT al broker

Remitimos aquí a lo explicado en el [CTC-102](#), y recomendamos utilizar además los scripts que entregamos en los [archivos provistos](#) con el mismo.

El proceso de operación es para conexión TLS con autenticación mutua (doble, dual). Debemos cargar en el módulo nuestra clave privada y certificado, y el certificado de la CA de Amazon. A tal fin podemos emplear los scripts mencionados, teniendo cuidado de modificar los nombres de archivo, y colocando el valor correcto para la longitud de cada archivo en las secuencias que lo envían.<sup>1</sup> Esto, salvando las distancias, no es muy diferente de lo que deberemos hacer en nuestro microcontrolador en un dispositivo real.

Elegido un tópico en qué publicar, podemos hacerlo. Por ejemplo, podemos utilizar un tópico del tipo `<device_id>/telemetry` como el que utilizamos en el [CTC-105](#) para publicar con el ESP32 y Mongoose-OS; o simplemente repetir el “Hola” del [CTC-102](#) para comprobar que funciona.

Con esto simplemente hemos cubierto las posibilidades de enviar y recibir datos, para poder utilizar la *shadow* podemos basarnos en estas operaciones elementales, suscribirnos a los tópicos correspondientes<sup>2</sup>, y realizar el código. Como hemos comentado en el [CTC-104](#), existen SDK<sup>3</sup> que podemos aprovechar, aunque en general deberemos realizar modificaciones dado lo particular del caso.

Para corroborar el funcionamiento, los datos de telemetría los obtenemos del broker con cualquier cliente MQTT que se conecte (y tenga los permisos adecuados). También podemos observarlos en el cliente MQTT que se provee en la consola web, como vemos en la captura a continuación:

1 Son tres secuencias, una para cada archivo: “CA cert download”, “client cert download”, “client key download”

2 <https://docs.aws.amazon.com/iot/latest/developerguide/iot-device-shadows.html>

3 <https://docs.aws.amazon.com/iot/latest/developerguide/iot-sdks.html>

# CTC-106, Conexión de módulos SIMCOM con soporte MQTT a Amazon Web Services IoT Core

