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 <u>CTC-104</u> analizamos los Amazon Web Services (AWS) y desarrollamos la utilización de AWS IoT Core, el servicio de conectividad, utilizando MQTT. En el <u>CTC-102</u> 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 <u>CTC-104</u> 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* \rightarrow *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

aws	Services 🗸	Resource Groups 🗸 🏠 RnD 🗸
AWS IOT	×	AWS IoT > Things > Create things > Add your device to the thing registry
Monitor Activity • Onboard		CREATE A THING Add your device to the thing registry
 Manage Things Types Thing groups Billing groups Jobs Tunnels 		This step creates an entry in the thing registry and a thing shadow for your device. Name SIM7600
 Greengrass Secure Certificates Policies CAs Role Aliases Authorizers 		Apply a type to this thing Using a thing type simplifies device management by providing consistent registry data for things that share a type. Types provide things with a common set of attributes, which describe the identity and capabilities of your device, and a description. Thing Type No type selected Create a type
Defend Act Test Software Settings		Add this thing to a group Adding your thing to a group allows you to manage devices remotely using jobs. Thing Group Groups / Create group Change

Paso 2: Generación de claves y certificados, seleccionamos *Create a certificate*, se abre una nueva ventana con el certificado creado. Deberemos 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 <u>CTC-105</u>, 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 salteamos el paso 3.

aws	Services 🗸	Resource Groups 👻 🛠			
AWS IOT	×	Success Successfully generated certificate. Please download certificate files.			
Monitor		⊘ Success			
Activity		Successfully activated certificate.			
Onboard					
Manage					
Things		Certificate cre	ated!		
Types					
Thing groups					
Billing groups					
Jobs					
Tunnels		Download these files an	d save them in a safe place. Certific	ates can be retrieved at an	ıy time, but
Greengrass		after you close this page	2.		
▼ Secure		In order to connect a d	device, you need to download the	a following:	
Certificates					
Policies		A certificate for this	d345f1bfb0.cert.pem	Download	
CAs		uning			
Role Aliases		A public key	d345f1bfb0.public.key	Download	
Authorizers					
Defend		A private key	d345f1bfb0.private.key	Download	
▶ Act					
Test		You also need to down A root CA for AWS Io	lload a root CA for AWS loT:		
Software		Deactivate			
Settings					
Reedback	😵 English (US)				

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

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* \rightarrow *Policies*, luego *Create*, ingresamos como se ve en la captura siguiente *Action* = *iot:**, *Resource ARN* = * y *Effect* = *Allow*. Finalmente, vamos a *Secure* \rightarrow *Certificates*, hacemos click sobre la clave del certificado y se abre una ventana con los datos. Allí seleccionamos *Policies* y luego *Actions* \rightarrow *Attach Policy*.

AWS INT X	
Monitor Activity	
Onboard Create a policy to define a set of authorized actions. You can authorize actions on one or more resources (things, topics, topic filters). To lipse to the NUS IsT policies documentation approximately actions are activity to the NUS IsT policies.	earn more
Anage abdut to porces go to the ways for Policies documentation page. Arrespondences and the second s	
▼ Secure myPolicy	
Policies CAs Add statements	
Role Aliases Policy statements define the types of actions that can be performed by a resource. Advant Authorizers Advant Advant Advant	ed mode
► Defend Action	
Act iot* Test	
Software	
Settings Leam Effect	
Documentation 🖸 🔹 🛃 Allow 🗌 Deny	ove
Add statement	
Cr	eate

Podemos detenernos a observar nuestra creación:

aws	Services 🗸 F	Resource Groups 👻 🖈
AWS IOT	×	Success Successfully registered your thing
Monitor		
Activity		AWS IoT > Things
Onboard		Things
▼ Manage		3
Things		
Types		Search things Q Fleet Indexing Info
Thing groups		
Billing groups		Name
Jobs		
Tunnels		esp32_807A98
Greengrass		
▼ Secure		unacosa
Certificates		
Policies		SIM7600
CAs		
Role Aliases		
Authorizers		
Defend		
▶ Act		
Test		
Software		
Settings		
Feedback	🔮 English (US)	

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

aws	Services 🗸	Resource Groups 🗸	*
AWS IoT	×	AWS IoT > Things >	SIM7600
Monitor Activity > Onboard < Manage		THING SIM7600 NO TYPE	
Things Types Thing groups		Details Security	This thing already appears to be connected.
Jobs Tunnels		Thing groups	нттря
Greengrass		Billing Groups Update vour Thino Shado Shadows a24746f9177qdm-a	Update your Thing Shadow using this Rest API Endpoint. Learn more
Secure Certificates			a24746f9177qdm-ats.iot.us-east-2.amazonaws.com
CAs Role Aliases		Activity Jobs	MQTT
Authorizers		Violations	Use topics to enable applications and things to get, update, or delete the state in Learn more
Act Test		Defender metrics	

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 <u>CTC-102</u>, y recomendamos utilizar además los scripts que entregamos en los <u>archivos provistos</u> con el mismo.

El proceso de operación es para conexión TLS con autenticación mutua (doble, dual). Deberemos 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.¹ 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 <u>CTC-105</u> 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 correspondientes², y realizar el código. Como hemos comentado en el <u>CTC-104</u>, existen SDK³ 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

