# Chapter 7b: Cloud Connectivity using MQTT + Amazon Web Services

## Objective

At this end of Chapter 7b you will understand:

* How Message Queue Telemetry Transport (MQTT) works:
  + How MQTT fits into the TCP/IP Networking Stack
  + The purpose of a **Topic**
  + The role of the **Message Broker**
  + The role of a **Publisher**
  + The role of a **Subscriber**
* How to use the JavaScript Object Notation (JSON) language.
* How the Amazon [AWS MQTT Cloud works](https://docs.aws.amazon.com/iot/latest/developerguide/aws-iot-how-it-works.html) including:
  + How to provision “things” (which for semantic reasons, will be notated *thing***,** a.k.a. your IoT device, in this chapter) in the Amazon AWS IoT Cloud by creating a *thing*, policies and certificates.
  + AWS MQTT and Security
  + Understand the *thing* shadow
  + How to use the AWS IoT MQTT Client to subscribe and publish to topics
  + Understand the scope of systems that can be implemented in the AWS Cloud (SNS, Database etc.)
* Understand in **DETAIL** how to write WICED firmware to interact with the AWS IOT Cloud

## Time: 4 Hours

## Fundamentals

### Amazon Web Services (AWS)

[AWS](https://aws.amazon.com/what-is-aws/) is a secure cloud services platform, offering compute power, database storage, content delivery and other functionality (which makes more money for Amazon than their retail operations). AWS is built from a vast array of both virtual and actual servers and networks as well as a boatload of webserver software and administrative tools including (partial list):

* [AWS IoT](https://aws.amazon.com/iot/): A cloud platform that provides Cloud services for IoT devices (the subject of this chapter).
* Amazon Elastic Cloud ([EC2](https://aws.amazon.com/ec2/)/[EC3](https://aws.amazon.com/ec3/)): A virtualized compute capability, basically Linux, Windows etc. servers that you can rent.
* [Amazon Lambda](https://aws.amazon.com/lambda/): A Cloud service that enables you to send event driven tasks to be executed.
* Storage: Large fast file systems called [Amazon S3](https://aws.amazon.com/s3/?sc_channel=PS&sc_campaign=acquisition_US&sc_publisher=google&sc_medium=s3_b&sc_content=s3_e&sc_detail=amazon%20s3&sc_category=s3&sc_segment=105589469922&sc_matchtype=e&sc_country=US&s_kwcid=AL!4422!3!105589469922!e!!g!!a) & [AWS Elastic File System](https://aws.amazon.com/efs/).
* Databases: Large fast databases called [Dynamo DB](https://aws.amazon.com/dynamodb/), [Amazon Relational Database (RDS)](https://aws.amazon.com/rds/?sc_channel=PS&sc_campaign=acquisition_US&sc_publisher=google&sc_medium=rds_b&sc_content=rds_e&sc_detail=amazon%20rds&sc_category=rds&sc_segment=145495376109&sc_matchtype=e&sc_country=US&s_kwcid=AL!4422!3!145495376109!e!), [Amazon Aurora](https://aws.amazon.com/rds/aurora/?sc_channel=PS&sc_campaign=acquisition_US&sc_publisher=google&sc_medium=aurora_rds_b&sc_content=aurora_e&sc_detail=amazon%20aurora&sc_category=aurora&sc_segment=145509396189&sc_matchtype=e&sc_country=US&s_kwcid=AL).
* Networking: Fast, fault tolerant, load balanced networks with entry points all over the world.
* Developer tools: A unified programming API supporting the AWS platform supporting a bunch of different languages.
* [Amazon Simple Notification System (SNS)](https://aws.amazon.com/sns/): A platform to send messages including SMS and Email.
* [Amazon Simple Queueing Services(SQS)](https://aws.amazon.com/sqs/): A platform to send messages between servers (NOT the same thing a MQTT messages).
* [Amazon Kinesis](https://aws.amazon.com/kinesis/): A platform to stream and analyze “massive” amounts of data. This is the plumbing for AWS IoT.

### Amazon AWS IoT Introduction

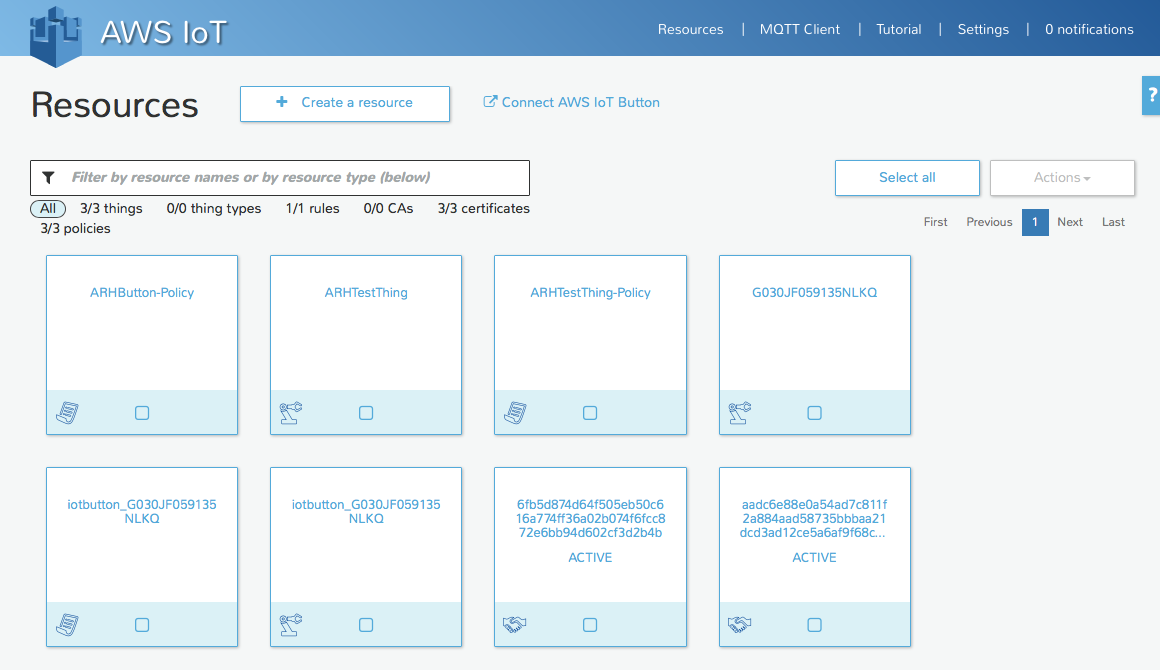
The Amazon AWS IoT Cloud service is an MQTT Message Broker **plus** a bunch of server side functionality that provides:

* Message Broker: An MQTT Message Broker.
* Thing Registry: A web interface to manage the access to your *things*.
* Security and identity: A web interface to manage the certificates and rules about *things*. You can create encryption keys and manage access privileges.
* A “shadow”: An online cache of the most recent state of your *thing***.**
* Rules Engine: An application that runs in the cloud that can subscribe to Topics and take programmatic actions based on messages – for example, you could configure it to subscribe to an “Alert” topic, and if a *thing* publishes a warning message to the alert topic, it uses Amazon SNS to send a SMS Text Message to your cell phone
* IoT Applications: An SDK to build Web pages and cell phone Apps.



### Amazon AWS IoT Resources

When you enter the [AWS IoT Console](https://console.aws.amazon.com/) (console.aws.amazon.com) you will see the Registry which shows all of the resources you have defined. There are three types of resources: *Things*, Certificates, and *Policies*. The second exercise will take you step by step through the process to create each of them.



**Thing**

A *thing* is a representation of a device or logical entity. It can be a physical device or sensor (for example, a light bulb or a switch on a wall). It can also be a logical entity like an instance of an application or a physical entity that does not connect to AWS IoT but can be related to other devices that do (for example, a car that has engine sensors or a control panel).

**Certificate**

AWS IoT provides mutual authentication and encryption at all points of connection so that data is never exchanged between *things* and AWS IoT without a proven identity. AWS IoT supports X.509 certificate-based authentication. Connections using MQTT use certificate-based authentication. You can attach policies to a certificate to allow or deny access to AWS IoT resources. A root CA certificate is used by your device to ensure it is communicating with the actual Amazon Web Services site. You can only connect your *thing* to the AWS IoT Cloud via TLS.

**Policy**

After creating a certificate for your internet-connected *thing*, you must create and attach an AWS IoT policy that will determine what AWS IoT operations the *thing* may perform. AWS IoT policies are JSON documents and they follow the same conventions as AWS Identity and Access Management policies.

You can also specify permissions for specific resources such as topics and shadows. Here is an example of the default Policy created for a new *thing*.

{

"Version": "2012-10-17",

"Statement": [

{

"Action": [ "iot:\*" ],

"Resource": ["\*"],

"Effect": "Allow"

}

]

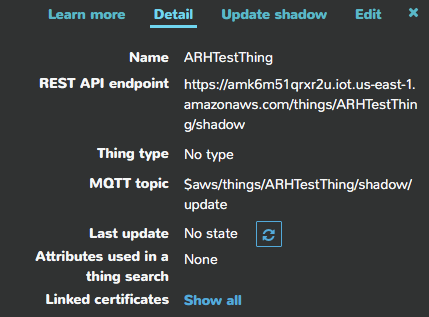
}

For the purposes of this class, when you create a *thing*, you will get a policy attached to your *thing* that will allow you to do everything you need.

### Amazon AWS MQTT

#### Internet Access

When you create an AWS IoT account, Amazon will create a new (virtual) server for you in the Cloud and will turn on an MQTT Message Broker on that server. In order to connect your WICED device to that server you will need to know the IP Address of the Message Broker (to program it into your firmware). You find the address by clicking on your *thing* in the console which will open up a window on the right of the browser which contains the DNS name and other information about your *thing*. (In this case the IP address of your message broker is: *amk6m51qrxr2u.iot.us-east-1.amazonaws.com*.)



#### [Thing Shadow](http://docs.aws.amazon.com/iot/latest/developerguide/iot-thing-shadows.html)

A *thing* shadow (sometimes referred to as a device shadow) is a JSON document that is used to store and retrieve current state information for a *thing* (device, app, and so on). The *Thing* Shadows service maintains a *thing* shadow for each *thing* you connect to AWS IoT. You can use *thing* shadows to get and set the state of a *thing* over MQTT or HTTP, regardless of whether the *thing* is currently connected to the Internet. Each *thing* shadow is uniquely identified by its name.

The JSON Shadow document representing the device has the following properties:

* state:
  + desired: The desired state of the *thing*. Applications can write to this portion of the document to update the state of a *thing* without having to directly connect to a *thing*.
  + reported: The reported state of the *thing*. *Things* write to this portion of the document to report their new state. Applications read this portion of the document to determine the state of a *thing*.
* metadata: Information about the data stored in the state section of the document. This includes timestamps, in Epoch time, for each attribute in the state section, which enables you to determine when they were updated.
* timestamp: Indicates when the message was transmitted by AWS IoT. By using the timestamp in the message and the timestamps for individual attributes in the desired or reported section, a *thing* can determine how old an updated item is, even if it doesn't feature an internal clock.
* clientToken: A string unique to the device that enables you to associate responses with requests in an MQTT environment.
* version: The document version. Every time the document is updated, this version number is incremented. Used to ensure the version of the document being updated is the most recent.

An example of the document looks like this:



If you want to update the Shadow, you can publish a JSON document with just the information you want to change to the correct topic. For example, you could do:

{

"reported" : { "color": “BLUE” }

}

#### MQTT Topics

The AWS Message Broker will allow you to create Topics with almost any name, with one exception: Topics named “$aws/…” are reserved by AWS IoT for specific functions.

As the system designer you are responsible for defining what the topics mean and do in your system. Some [best practices](http://www.hivemq.com/blog/mqtt-essentials-part-5-mqtt-topics-best-practices) include:

1. Don’t use a leading forward slash
2. Don’t use spaces
3. Keep the topic short and concise
4. Use only ASCII characters
5. Embed a unique identifier e.g. the name of the *thing*

For example, a good topic name for a temperature sensing device might be: myDevice/temperature.

[Device Shadow MQTT Topics](https://docs.aws.amazon.com/iot/latest/developerguide/thing-shadow-mqtt.html)

Each *thing* that you have will have a group of topics of the form “$aws/things/thingName/shadow/…” which allow you to publish and subscribe for topics relating to the shadow. The specific shadow topics that exist are:

|  |  |
| --- | --- |
| **MQTT Topic Suffix** | **Function** |
| /update | The JSON message that you publish to this topic will become the new state of the shadow. |
| /update/accepted | AWS will publish a message to this topic in response to a message to /update indicating a successful update of the shadow. |
| /update/documents | When a document is updated via a publish to /update, the complete new document is published to this topic. |
| /update/rejected | AWS will publish a message to this topic in response to a message to /update indicating a rejected update of the shadow. |
| /update/delta | After a message is sent to /update, the AWS will send a JSON message if the desired state and the reported state are not equal. The message contains all attributes that don’t match. |
| /get | If a *thing* publishes a message to this topic, AWS will respond with a message to either /get/accepted or /get/rejected with the current state of the shadow. |
| /get/accepted |
| /get/rejected |
| /delete | If a *thing* publishes a message to this topic, AWS will delete the shadow document. |
| /delete/accepted | AWS will publish to this topic when a successful /delete occurs. |
| /delete/reject | AWS will publish to this topic when a rejected /delete occurs. |

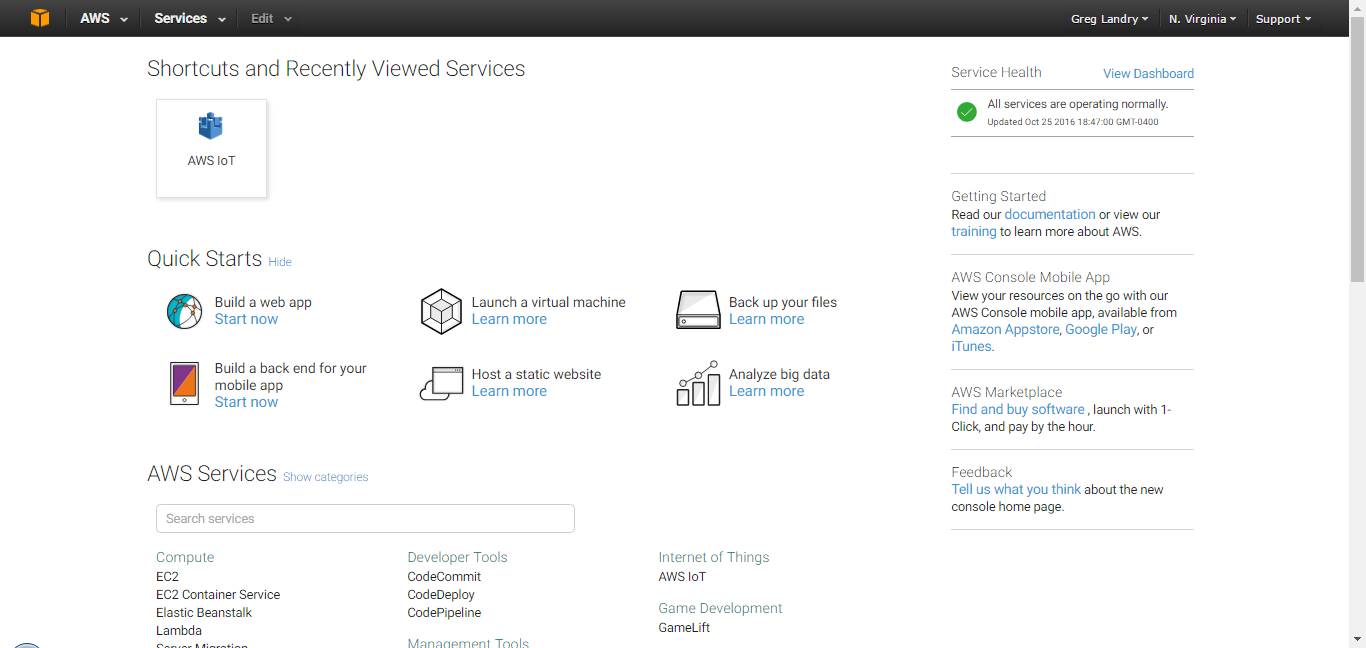
You can use “#” as a wildcard to access multiple shadow topics. For example, you can use “$aws/things/thingName/shadow/#” to subscribe to all shadow topics for the *thing* called “theThing”.

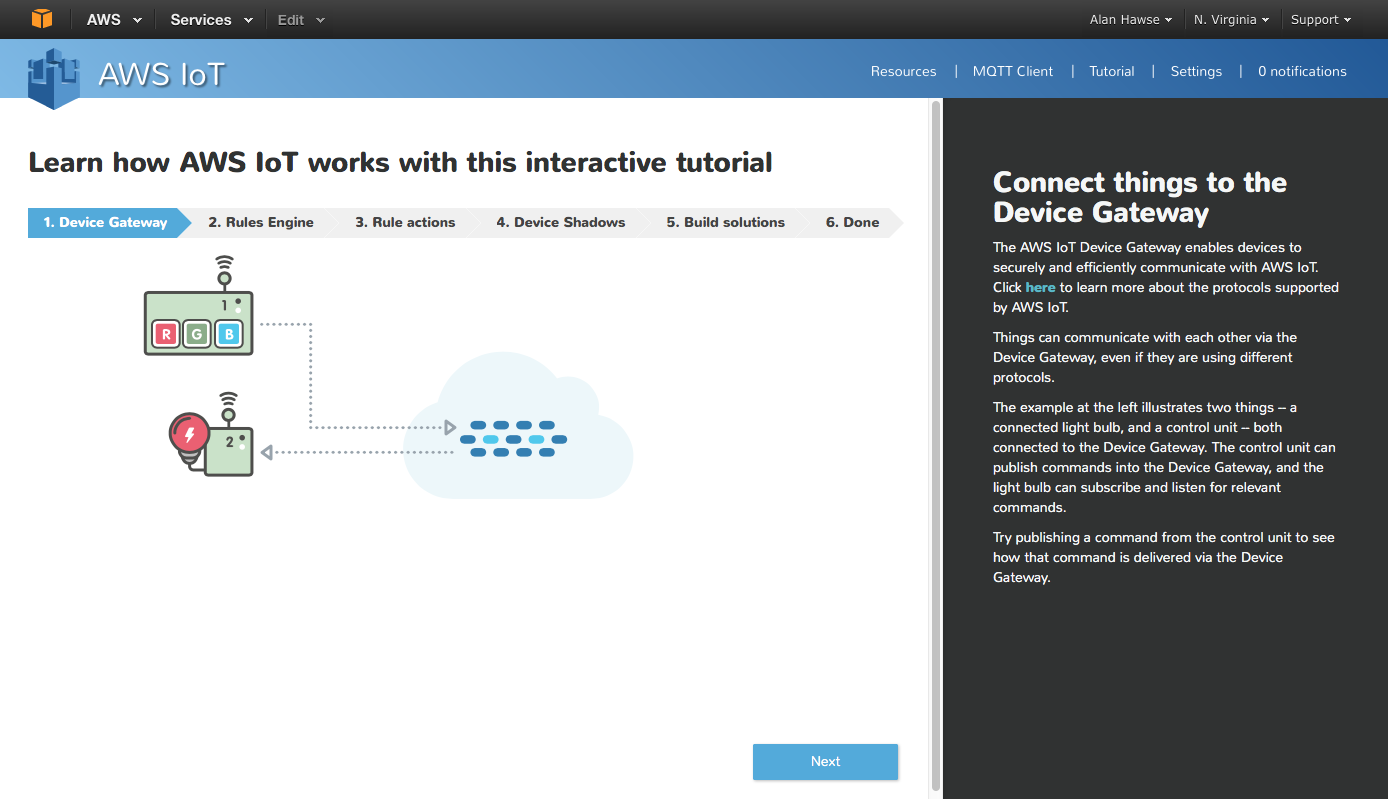
## Exercise(s)

### 00 Run the MQTT tutorial on the Amazon IoT Console (console.aws.amazon.com)

If you do not already have one, you will need to sign up for an Amazon AWS account. The minimal account is free for a year but you must provide a credit card to open the account. Be sure to delete the account before the free year period expires or you will be charged for it.

If you start out in a page that looks like the following, click on the link for the AWS IoT and then click the button that says “Start interactive tutorial”.





### 01 Provision a new *thing* in the AWS IOT Cloud, establish its policy and credentials, and test using the AWS MQTT Client

To Provision follow the “Procedure to Provision an AWS IoT Thing” section at the end of this chapter.

Note the message broker address. You can find this in the right hand window when you click on the *thing* that you create listed as ”REST API endpoint”. It is the part of the name after “https://” and before “/things…”

To test your Message Broker, follow the “Procedure to use the AWS MQTT Client” at the end of this chapter.

### 02 Build and test the demo.aws\_iot.pub\_sub.publisher App

1. Copy the WICED apps/demo/aws\_iot/pub\_sub/publisher project to your own directory (i.e. wa101/07b/02\_publisher) and update all of the files.
   1. Hint: Make sure you add your platform to the valid platforms in the make file.
2. Modify the DCT for your network.
3. Copy the certificates that you generated in (01) into the resources/apps/aws\_iot directory. Rename the files as follows:
   1. The file rootca.cer is the public key that your application will use to encrypt data to send to Amazon. That is a known-good key for AWS that is built into the SDK. This does not need to be downloaded since it never changes.
   2. The file client.cer is the certificate for your *thing*. This is how AWS knows that it is your *thing* that is trying to talk to it. This certificate was created by AWS as a file called <name>-certificate.pem.crt.txt when you set up your *thing*. Therefore, you must rename the certificate you downloaded to client.cer to replace the existing client.cer file.
   3. The file privkey.cer is the private key that your application will use to decrypt data that it gets back from AWS. This was created by AWS as a file called <name>-private.pem.key when you set up your thing. Therefore, you must rename the private key you downloaded to privkey.cer to replace the existing privkey.cer file.
   4. The other file created by AWS is called <name>-public.pem.key. This is the public key that matches the private key that your application uses when getting data back from AWS. Your application does not need this key since it is used by AWS to encrypt the data that it sends you. Since it was initially generated by AWS, it already knows what the key is!
4. Create the Make target for your project.
5. Modify the #defines for WICED\_TOPIC and MQTT\_BROKER\_ADDRESS. Use the topic and broker address from (01).
6. Build and program your project.
7. Open the serial port and watch your terminal session.
8. Subscribe to the topic using the AWS MQTT client (and test publishing). When you press the button you should see updates to the topic.

### 03 Explain in detail the firmware flow for the publisher app by answering the following questions:

1. How do the MQTT library functions (e.g. wiced\_mqtt\_publish) get into your project?
2. What function is called when the button is pressed?
3. How does the button callback unlock the main thread?
4. What WICED-SDK RTOS mechanism does the “wait\_for\_response” function use to “wait”?
5. Why did the firmware author create a function called “wait\_for\_response”?
6. Are all messages sent to the AWS IOT MQTT Message Broker required to be in JSON format?
7. What are the 7 WICED MQTT events? What file are they defined in?
8. Do you have to name the client certificate client.cer? How would you change the name?
9. What is the naming convention used to differentiate WICED MQTT library functions versus wrappers around those functions in the publisher app?
10. What steps are required to get an MQTT connection established?
11. What prevents a hung connection from deadlocking the publisher app?
12. What is the name of the flag that prevents the firmware from sending multiple button presses before the publish is finished?

### 04 Build and test the demo.aws\_iot.pub\_sub.subscriber App

1. Copy the WICED application from apps/demo/aws\_iot/pub\_sub/subscriber to your directory (i.e. wa101/07b/05\_subscriber) and modify the DCT and Makefile.
2. Update the topic and broker #defines to the same one you chose for (03).
3. We will use the same *thing* that we did for (02) so the certificate and keys will be the same.
4. Publish messages using the AWS MQTT Client.
   1. Determine what string needs to be sent to turn the light on or off.
      1. Hint: Look in the source code to find the string that is being looked for when a message is received.
      2. Hint: If you are successful, the Green LED on the baseboard should turn on/off.

### 05 (Advanced) Implement the subscriber and publisher in two different kits and test

1. In a real world application you would typically have one or more devices publishing data to a broker and one or more devices reading data from that same broker. So, let’s try that out with two different kits. You should team up with another student for this lab.
   1. Make a new *thing* in the AWS console for the subscriber so that the subscriber and publisher can be identified as different.
   2. Save the new subscriber credential files but use different names for *client.cer* and *privkey.cer* so that the subscriber and publisher can be identified as two different *things*.
   3. Update the make file so that the subscriber points to the new credentials.
      1. Hint: The rootca.cer will not need to change since it is the Amazon AWS public key which is always the same.
   4. Update the lines in subscriber.c that point to the hard-code credential files.
      1. Hint: the credentials are listed as *resources\_apps\_DIR\_aws\_iot\_DIR\_client\_cer* and *resources\_apps\_DIR\_aws\_iot\_DIR\_privkey\_cer*. These names are the path in the resources folder where folder names are separated by the keyword “\_DIR\_” and the period before cer is replaced with “\_”. You could move the credentials to another location in the resources folder by following the naming convention or just change the names of the files and put them in the same folder.
   5. Program the updated subscriber firmware.
   6. Power up both kits.
   7. Subscribe to the topic that you chose using the AWS MQTT Client.
   8. Press the button on the provider and watch it change the state of the LED on the subscriber. Also watch the messages in the MQTT Client window.

### 06 (Advanced) Build and test the Shadow App

1. This example uses a configuration Access Point serving a web browser so that the *thing* name, credentials, keys, and settings for the network to connect to can be configured from a web browser on a device attached to the configuration AP.
2. Copy the WICED application from *apps/demo/aws\_iot/shadow* to your directory and update the Makefile.
3. Update the DCT to have a Soft AP for configuration with an SSID name that is unique (so as not to collide with others in your class).
4. Update the message broker address to match what you created in the previous exercises.
   1. Hint: The message broker address goes in *aws\_common.h* for this project.
5. Program the kit.
6. Attach to the Soft AP on your board from your computer’s Wi-Fi.
   1. Connect to the SSID that you programmed into the board.
   2. Go to the webserver (The IP address is printed on the terminal when the device boots and starts the AP).
      1. Hint: Don’t use Firefox for this step – it sometimes gives strange results.
   3. Update the *thing* name to match what you created in previous exercises.
      1. Hint: The default name that shows up is in *aws\_config.h* so you could also change it there before programming the board.
   4. Follow the instructions to upload the client certificate and private key.
   5. Click on “Wi-Fi Setup >” and connect to the Wi-Fi network.
   6. The board will reboot. Once it has done that it will connect as a station to the Wi-Fi network that you configured in the previous step.
7. Attach to a Wi-Fi access point from your computer.
8. Go to console.aws.amazon.com and start an MQTT Client.
9. Subscribe to the device’s shadow topics.
   1. Hint: *$aws/things/<YourThingName>/shadow/#* will subscribe to all shadow topics for your *thing*. The # is a wildcard.
10. Press the button on the board and see the messages.
11. Answer the question: What is the sequence of events that changes the LED from On to Off?

## References

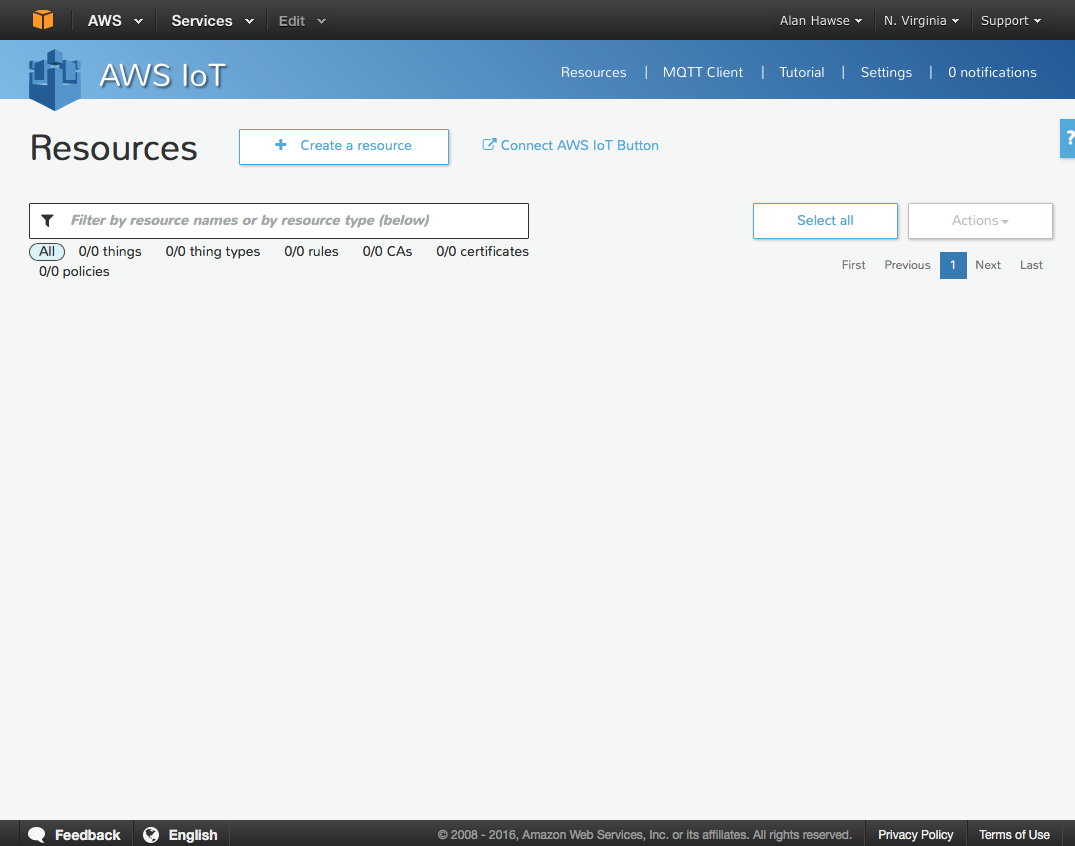
|  |  |
| --- | --- |
| **Resources** | **Link** |
| [AWS Developers Guide](http://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html) | <http://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html> |
| [AWS IOT Getting Started](https://aws.amazon.com/iot/getting-started/) | https://aws.amazon.com/iot/getting-started/ |
| [A nice powerpoint about MQTT](http://www.slideshare.net/PeterREgli/mq-telemetry-transport) | http://www.slideshare.net/PeterREgli/mq-telemetry-transport |
| [MQTT Topic Naming Best Practices](http://www.hivemq.com/blog/mqtt-essentials-part-5-mqtt-topics-best-practices) | http://www.hivemq.com/blog/mqtt-essentials-part-5-mqtt-topics-best-practices |
| [Avnet Getting Started](http://cloudconnectkits.org/system/files/GSG-BCM4343W%20IoT%20Starter%20Kit%20-%20Getting%20Started%20%28v1.1%29.pdf) | http://cloudconnectkits.org/system/files/GSG-BCM4343W%20IoT%20Starter%20Kit%20-%20Getting%20Started%20%28v1.1%29.pdf |
| Avnet User Guide [Part1](http://cloudconnectkits.org/system/files/Tutorial%20Part1%20-%20Tool%20Install%2C%20USB%20drivers%20and%20AWS%20Shadow%20%28v1.1%29.pdf) and [Part2](http://cloudconnectkits.org/system/files/Tutorial%20Part2-App%20Development%20using%20WICED%20SDK-v1.1.pdf) |  |
| [AWS Forum](https://forums.aws.amazon.com/forum.jspa?forumID=210) | https://forums.aws.amazon.com/forum.jspa?forumID=210 |
|  |  |
|  |  |
|  |  |
|  |  |

## Related Example “Apps”

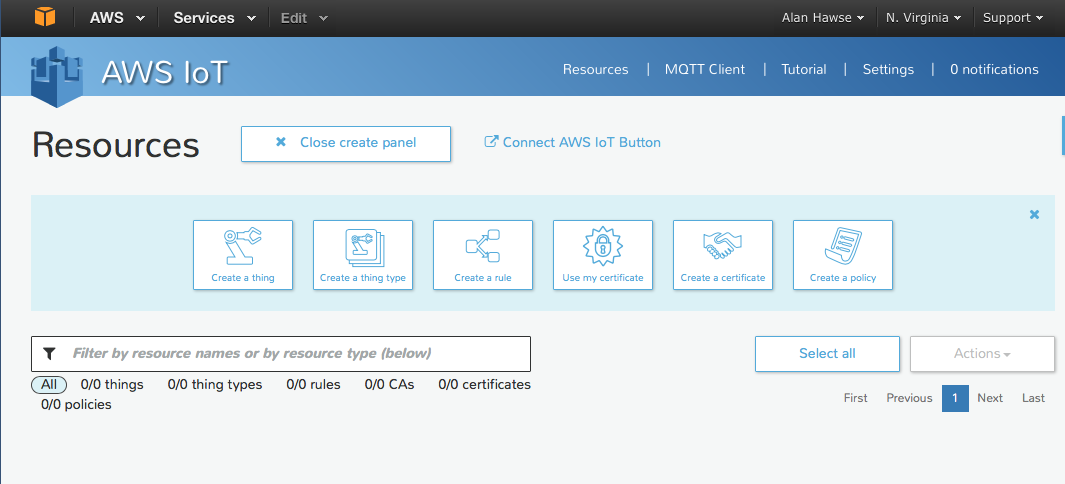
|  |  |
| --- | --- |
| **App Name** | **Function** |
| demo.aws\_iot\_pub\_sub/publisher | Demonstrates publishing information to the AWS cloud. |
| demo.aws\_iot\_pub\_sub/subscriber | Demonstrates subscribing to a topic in the AWS cloud. |
| demo.aws\_iot\_shaddow | Demonstrates using a shadow device with AWS. |

## Procedure to Provision an AWS IoT *Thing*

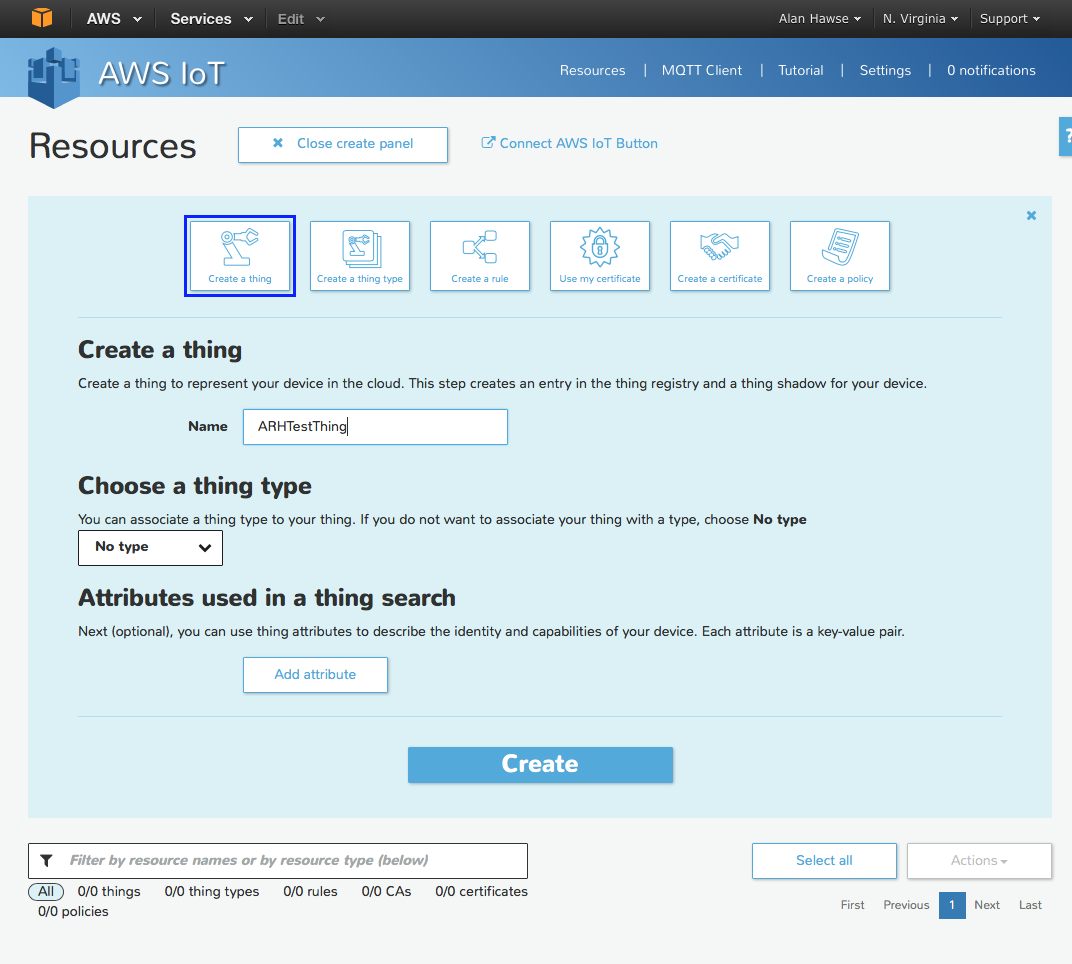
1. Start by going to the AWS IoT Console ([www.console.aws.amazon.com](http://www.console.aws.amazon.com)) which will start blank. Press “Create a resource”.
   1. Hint: Currently only the US East time zone works properly so be sure to pick a location in that time zone before setting up a new thing. In the example shown below, the selection is N. Virginia.



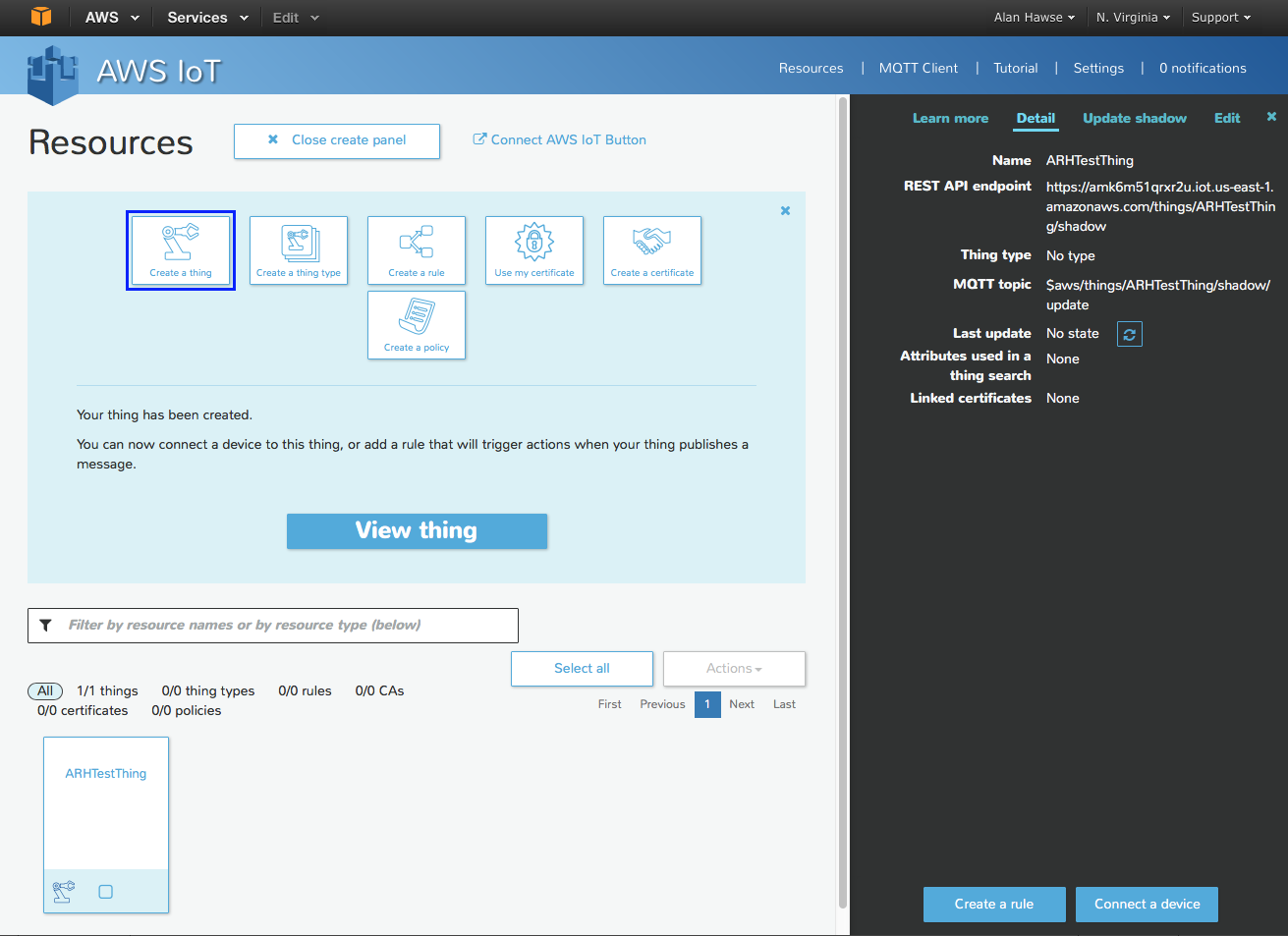
1. Press “Create a *thing*”.



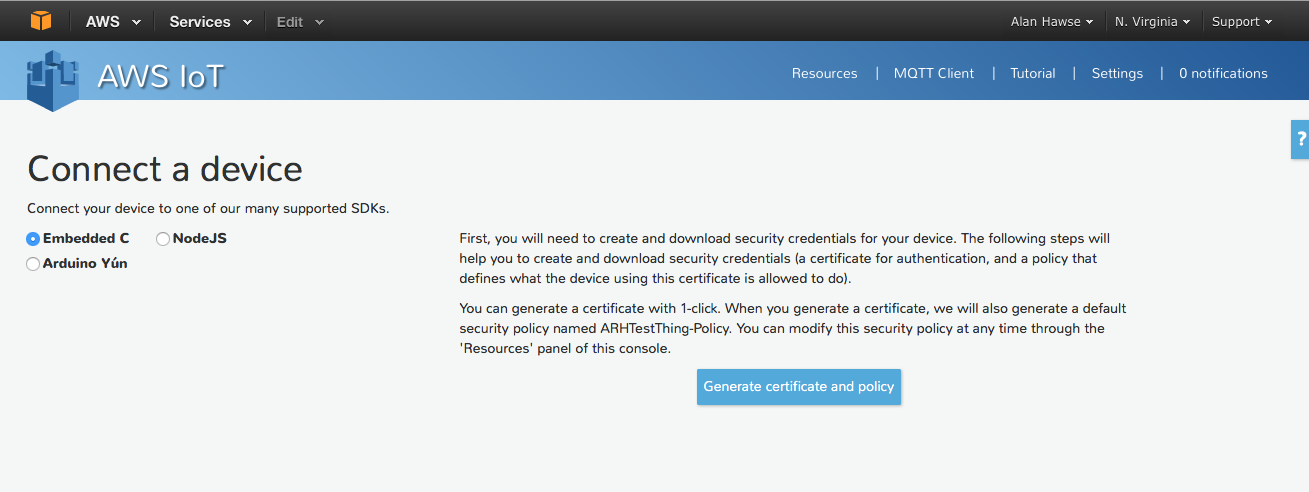
1. Name it “<YourInitials>TestThing” (or whatever) and press “Create”.



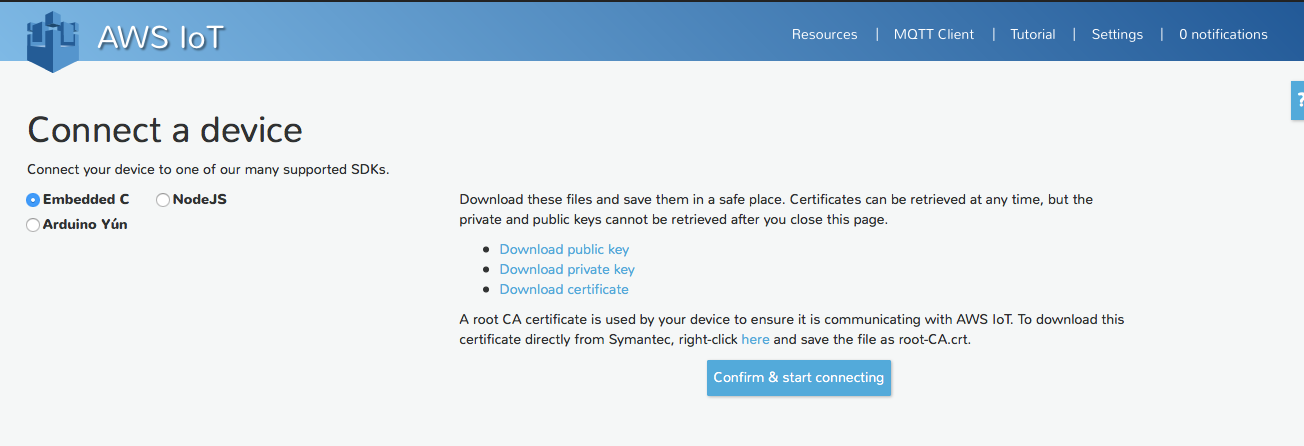
1. Click on your *thing* and it will open a window up to the right. Before you can do anything with the *thing* you need to create the encryption keys that enable you to identify yourself as that *thing*, and then update the data. To do this, click on “Connect a Device” (in the lower right hand corner).



1. Pick “Embedded C” and then click “Generate certificate and policy”.

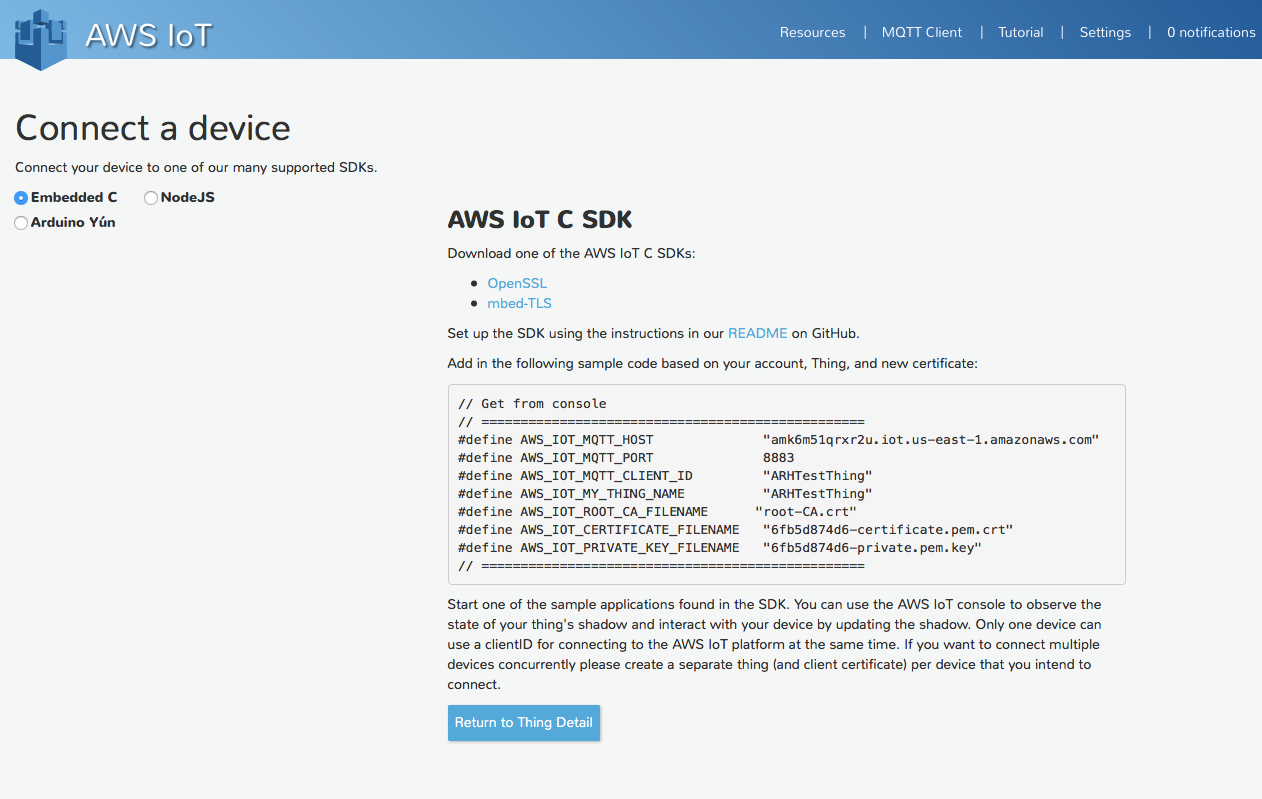


1. **Now you need to download the “public key”, “private key” and “certificate”. If you forget this step you cannot come back…so really you must download those files now to make the TLS work! Once you have downloaded the keys, then click on “Confirm and start connecting”.**



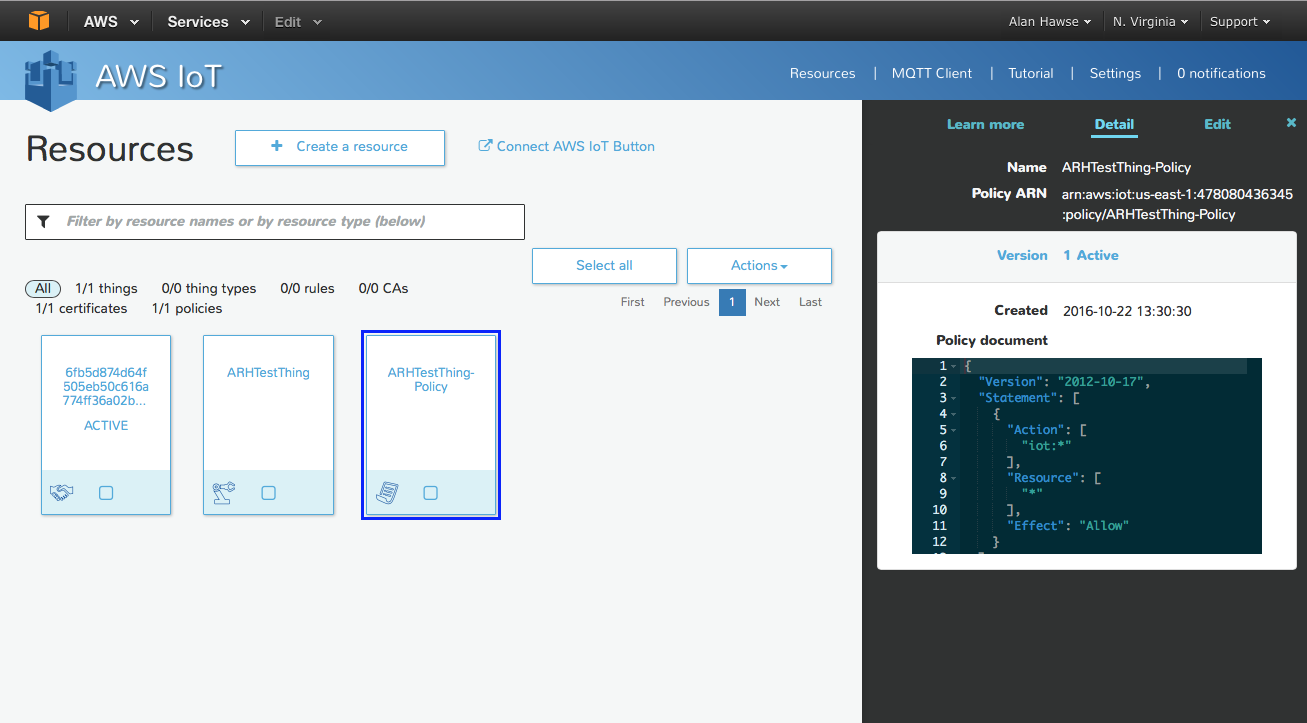
**Do this first!**

1. Press “Return to Thing Detail”.



1. Click on the Certificate which will show you that the certificate, policy and *thing* are all linked.

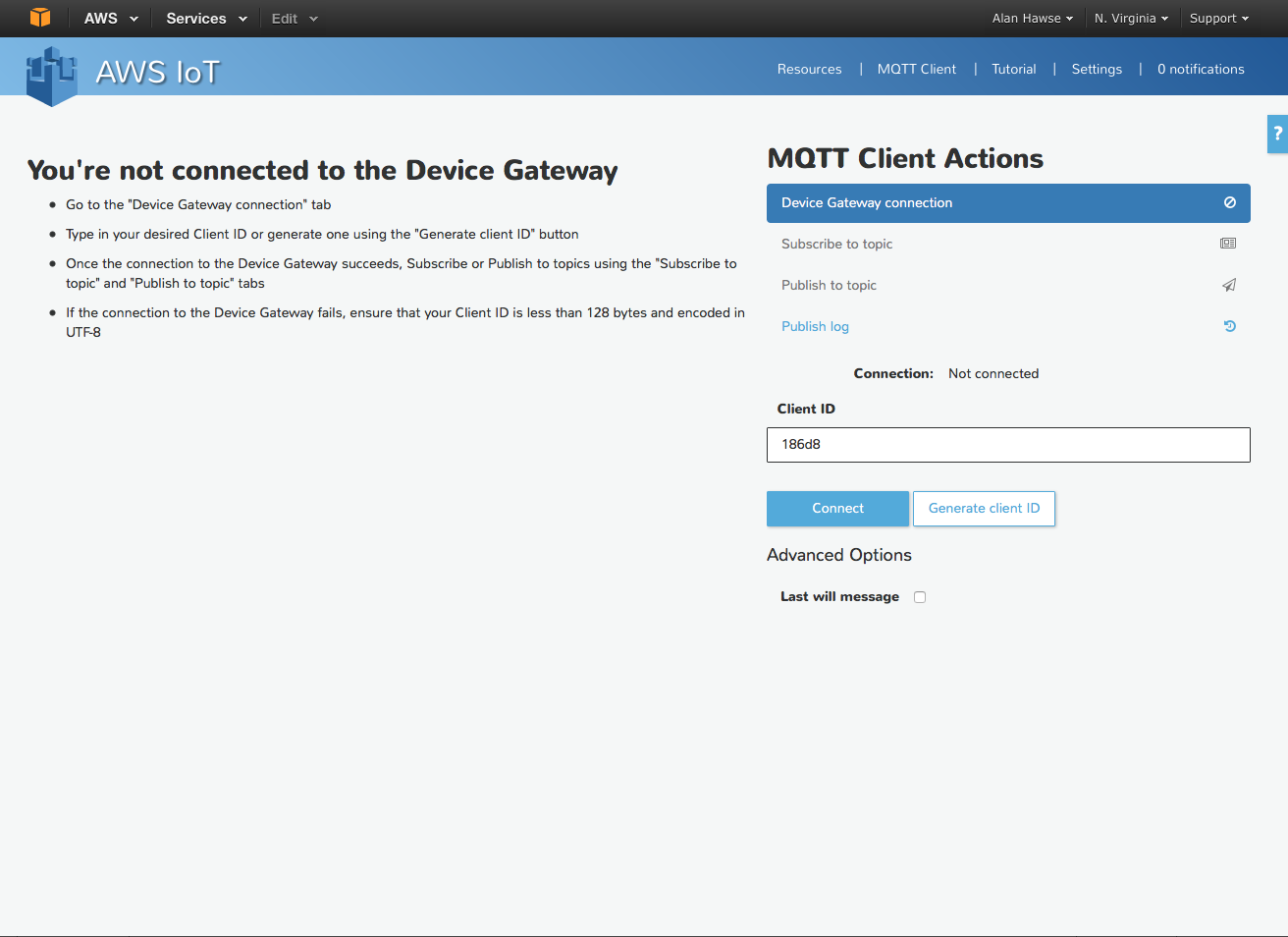


1. Click on your *thing* policy. You can see the Actions you are allowed to take on which resources. In this case the *thing* is allowed to do an “iot:” action. 

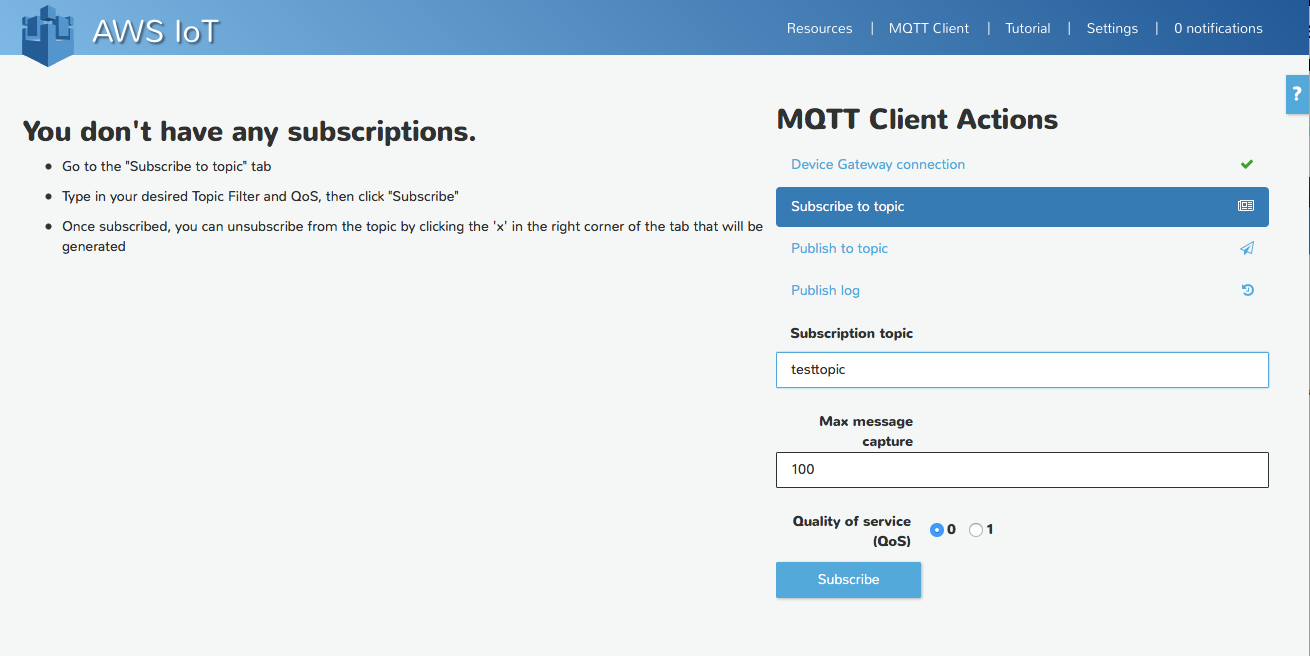
## Procedure to use the AWS MQTT Client

The AWS MQTT Client is a Web Browser based client that you can connect to “your” message broker. Then, you can publish and subscribe to topics. You can think of it as an IoT *thing* that can publish and subscribe. To use it to test you can:

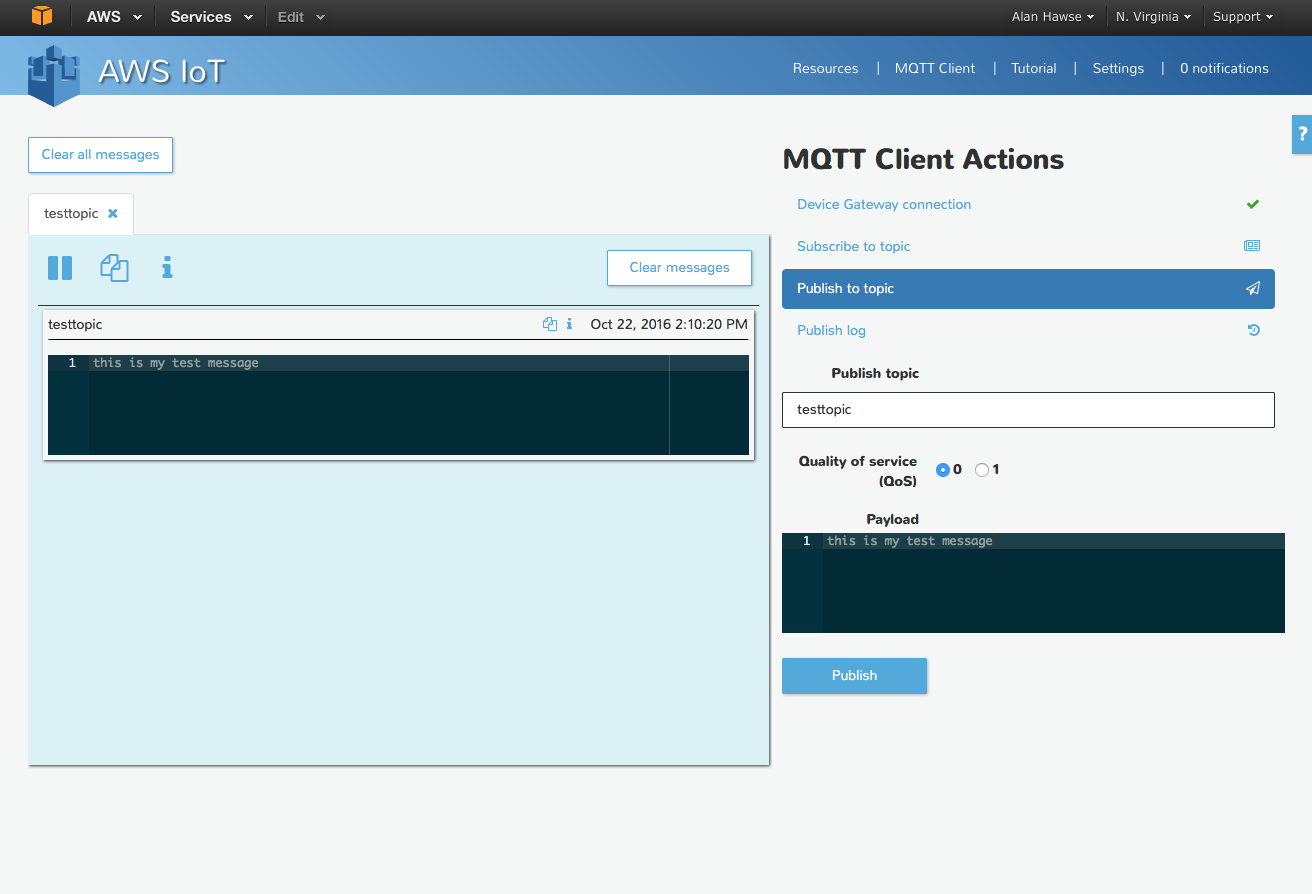
1. Click on “MQTT Client”. Then give your client a unique ID (you can use any name that isn’t already assigned) or you can click “Generate client ID” and AWS will think up a random-ish ID (which is what I did in the screen shot below). Once you have a name click “Connect” which will hook you up to the message broker.



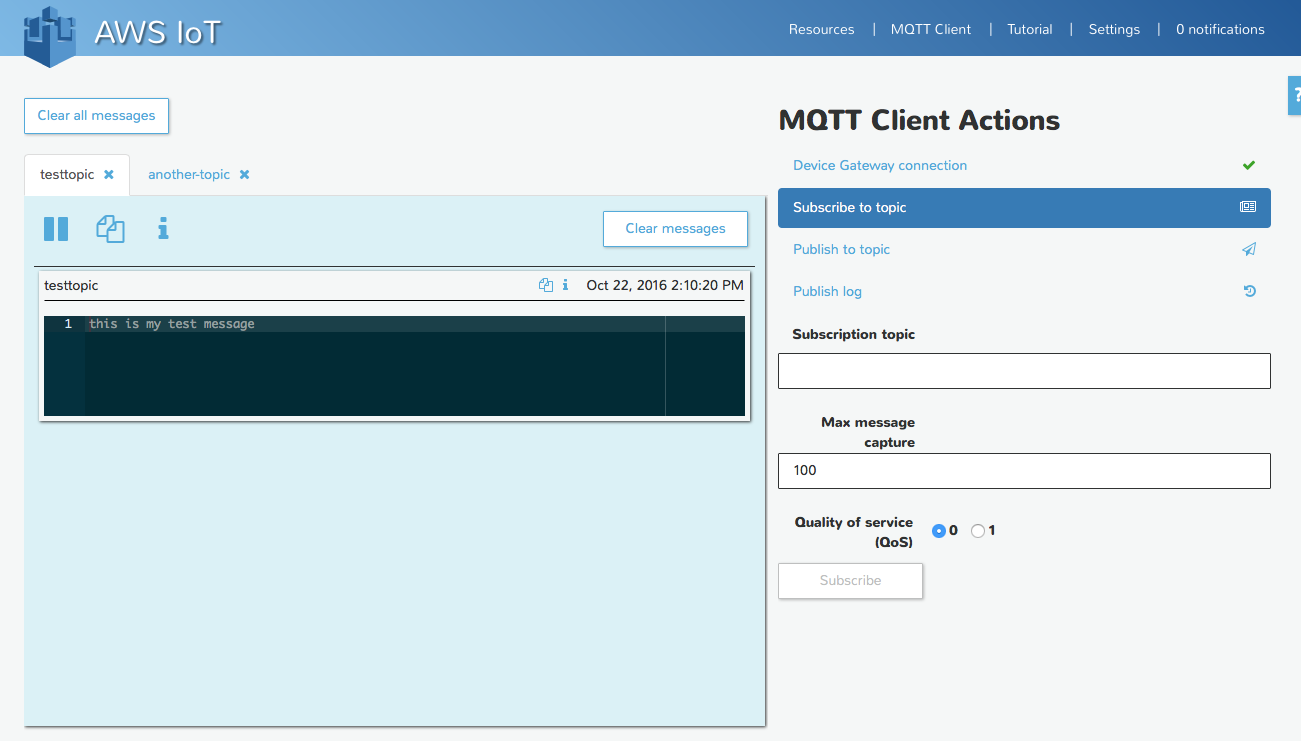
1. Now that you have a connection, the first thing to do is Subscribe to a topic. Remember that there is nothing particularly special about the topic name. Let’s choose the topic “testtopic”



1. Now that I am subscribed to a topic I can publish messages to that topic. To do this press “Publish to topic”. Then fill in the name of the topic, in the previous step we called the topic “testtopic”. Then type in your “Payload” and press “Publish”. You can see in the box below I sent the message “this is my test message”.



1. If I were to publish to the topic “testtopic” from my IoT device I would see the message appear in the window on the left side of the screen. The message viewer is cool because you can subscribe to multiple topics at the same time. You can see I did just that by subscribing to “another-topic”



1. In the screen shot below you can see that I create a WICED App that connected to the Message Broker and published “LIGHT ON” to “testtopic” (Exercise 02).

