## Amazon ElastiCache Setup

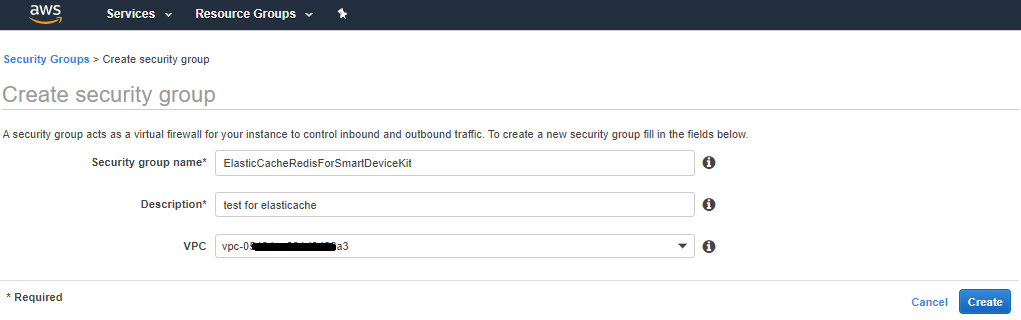
The use of ElastiCache Redis is added in the latest release.

In the latest release, ElastiCache Redis is used to store sensor data from the Smart Device Enablement Kit. The kit sends the sensor data to the MQTT topic “<THING ID>/datareport”, then, IoT Rule Engine transfer the topic message to a Lambda function and the Lambda function (named as ““wifismartdevicekit-store-data-to-elasticache-func”) extract the sensor value from the MQTT message and store the sensor value to ElastiCache Redis. Alexa Lambda Function (“WiFi-Smart-Device-Kit-Custom-Skill”) read the sensor value from the ElastiCache Redis when it receive command from the Alexa Cloud.

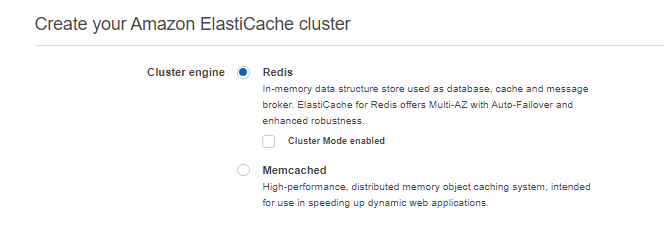
Below are the steps to create ElastiCache Redis, IoT Rule Engine and Lambda functions

**ElastiCache Setup Steps:**

1. Go to VPC Console, make sure there is at least one VPC
2. Open Security Group, create a new Security Group

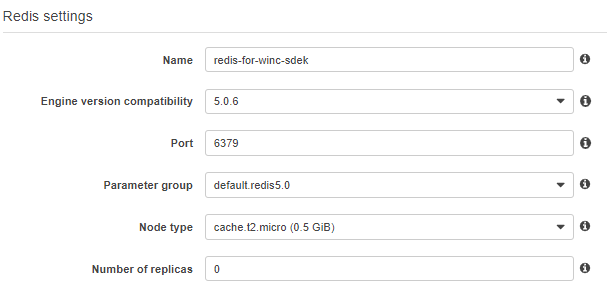


1. Go to ElastiCache Console
2. Create Cluster
3. Choose Redis as cluster engine



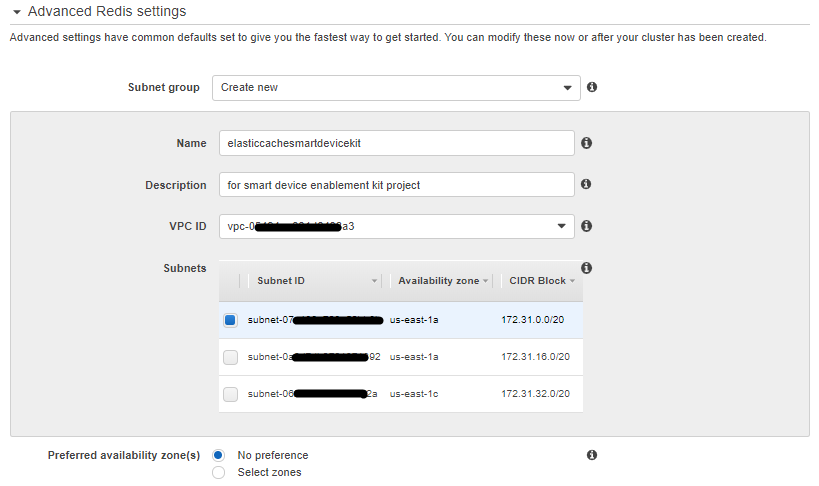
1. Fill in the Redis Setting like below:

(Select the latest Engine version )

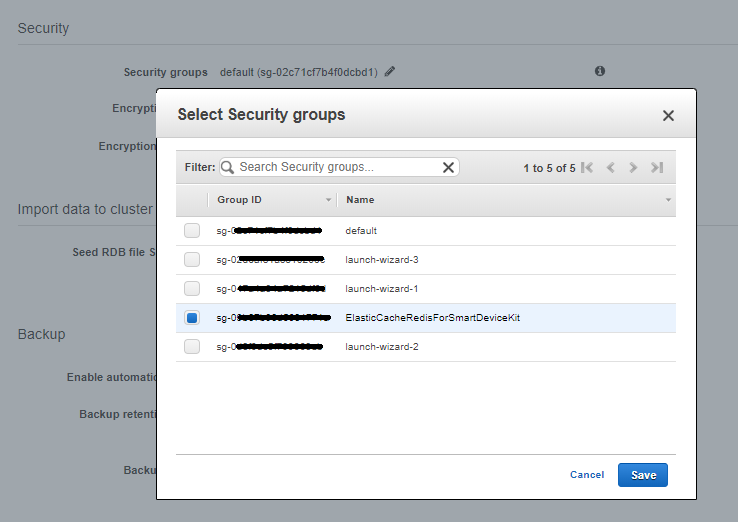


1. Fill in the Advanced Redis Settings like below:

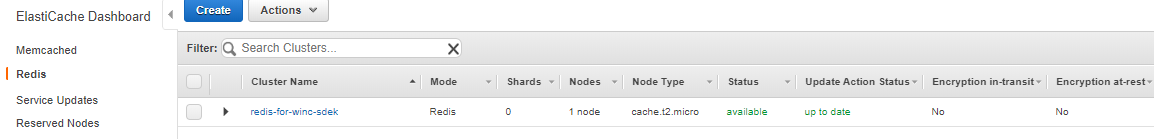
**Note:** Keep VPC ID same as the VPC configuration, and remember the Subnets



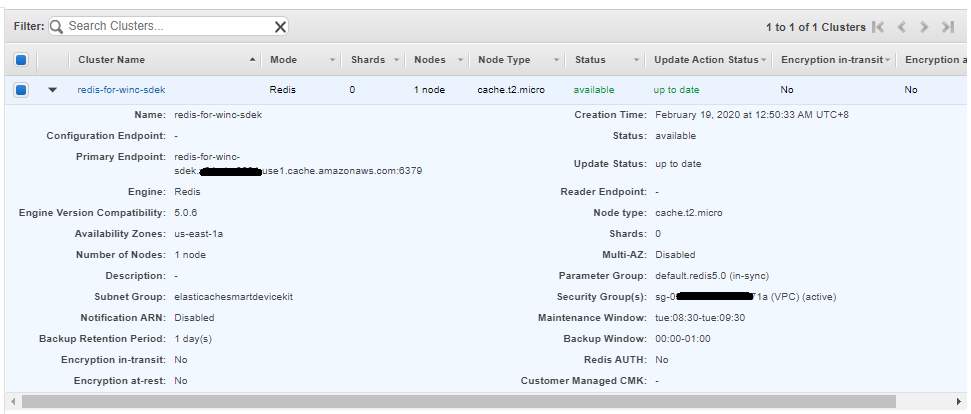
1. Select the Security Group



1. Click **Create** button
2. After create success, the cluster is shown in the console



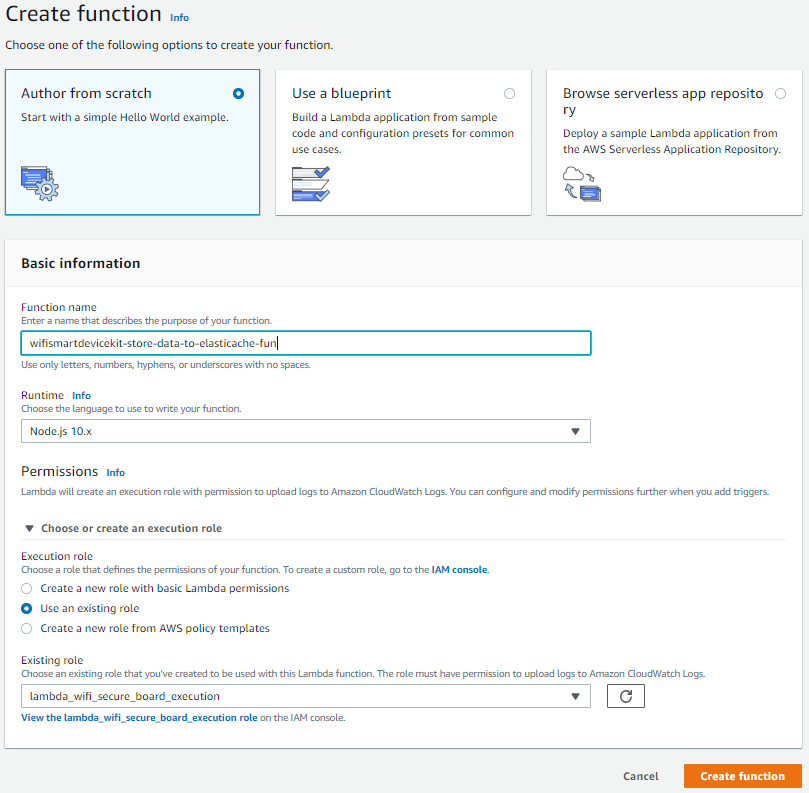
1. Details are shown when you select the cluster.



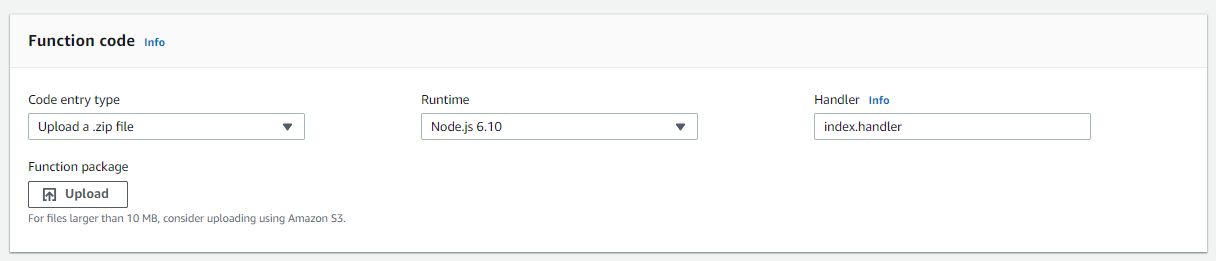
**Lambda Setup Steps: (The Lambda that saving sensor data to ElastiCache)**

1. Go to Lambda Console
2. Click on "Create Function"
3. Select "Author from scratch" and fill in a name for the Lambda function. The name can be “wifismartdevicekit-store-data-to-elasticache-func”. Select "Node.js 10.x" for "Runtime"
4. Select a Role for the Lambda function (user can create a Role in IAM Console, the role is needed to have policy " AWSLambdaVPCAccessExecutionRole, AWSLambdaFullAccess" and "CloudWatchLogsFullAccess")

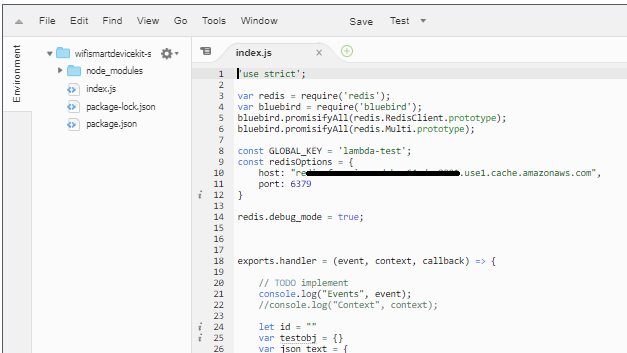
In below picture, “lambda\_wifi\_secure\_board\_execution” role is created, user can go to IAM console, select “Roles”, select , “lambda\_wifi\_secure\_board\_execution” role and attach policy “AWSLambdaVPCAccessExecutionRole”, "AWSLambdaFullAccess" and "CloudWatchLogsFullAccess" to this role



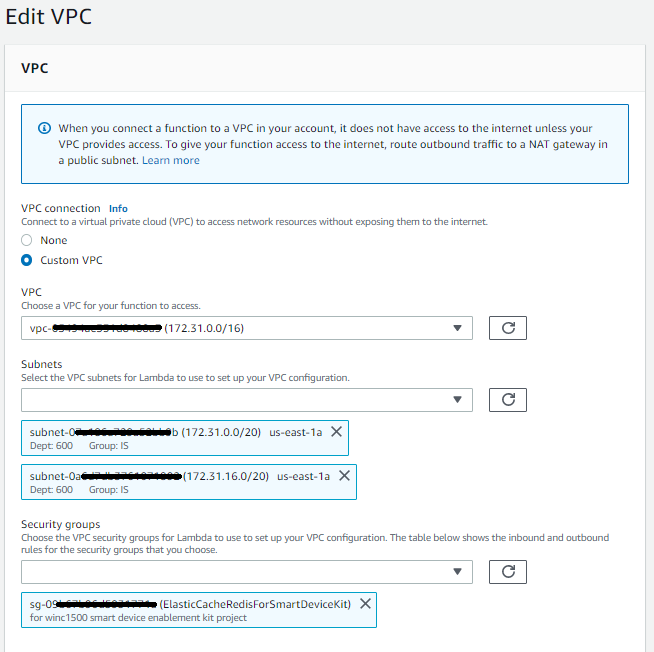
1. After creating the Lambda function, user can upload the function code to the Lambda function. As the function code include a number of files, user can upload the code as a zip file
   1. Select "Upload a .ZIP file" at "Code entry type"
   2. Select \lambda-function\ store-data-to-elasticache-func \ store-data-to-elasticache-func.zip and click on “Save”



1. In “Function code”. Edit index.js to input the ElastiCache Redis host ID.



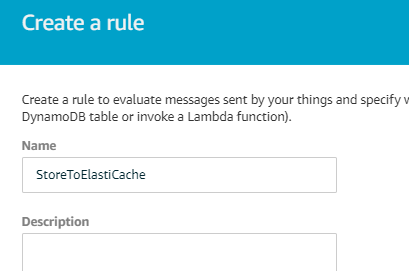
1. Edit “VPC”. Select the VPC, Subnet and the Security Group that you created in the ElastiCache configuration.



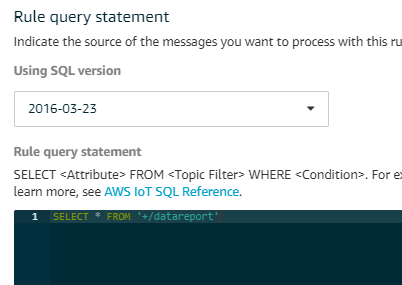
1. Click on **Save**

**AWS IoT Rule Setup Steps:**

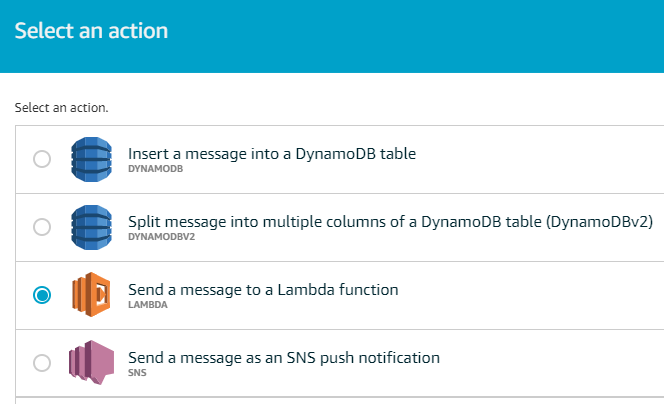
1. Go to **IoT Core** Console
2. Select **Act** in the left panel, create Rule
3. Input the name of the Rule



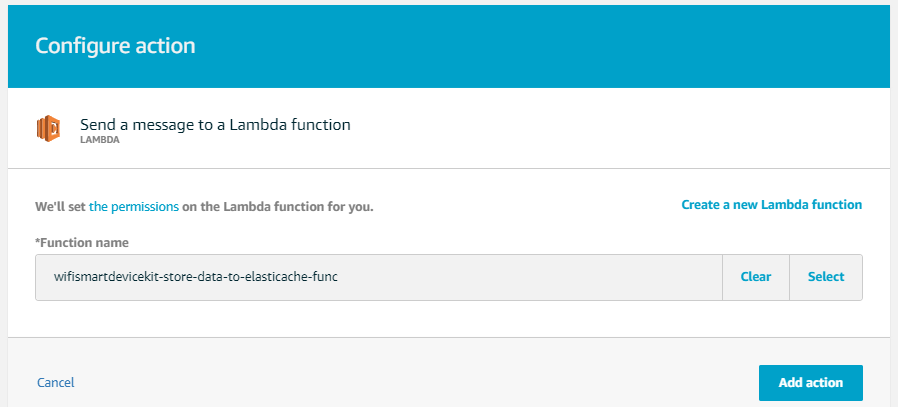
1. Input Rule query statement as below:



1. Click “Add Action” button,
2. Select “Send a message to a Lambda function ”, click **Configure action**

****

1. Select the lambda function “wifismartdevicekit-store-data-to-elasticache-func” that created in the previous section. Click **Add action**



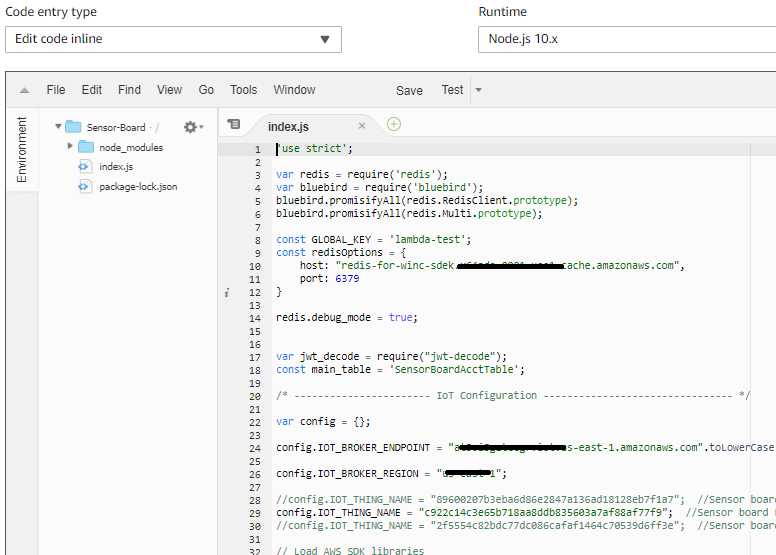
1. Click **Create rule**

**Other Lambda function update**

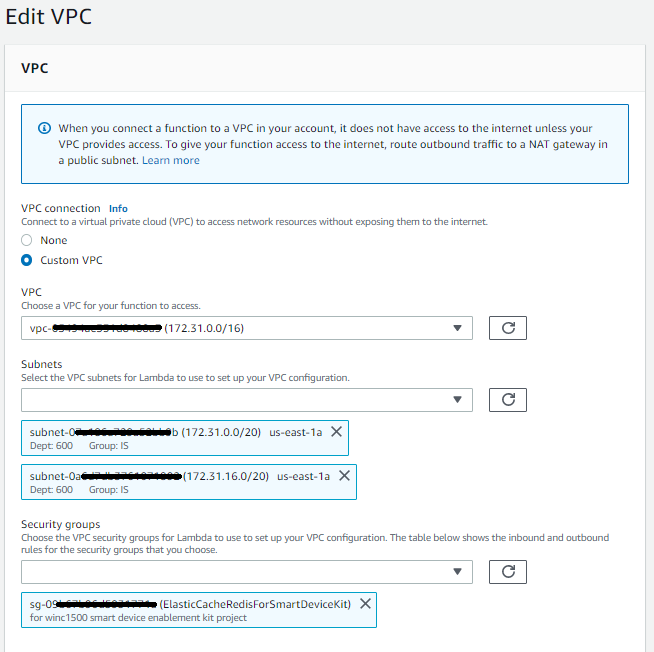
The Lambda function setting for the Microchip Wi-Fi Sensor Board Skill (WiFi-Smart-Device-Kit-Custom-Skill) need to be updated to work with ElastiCache.

Below are the highlights:

1. Upload the alexa-custom-skill.zip from the latest release to the Lambda function
2. In “Function code”. Edit index.js to input the Redis Host ID, AWS IoT Endpoint and the Region. The Redis Host ID can be found from the ElastiCache console. The AWS IoT Endpoint can be found from the Settings page of AWS IoT Console



1. Keep the previous setting of the lambda function
2. Edit “VPC”. Select the VPC, Subnet and the Security Group that you created in the ElastiCache configuration.



1. Attach the Policy “AWSLambdaVPCAccessExecutionRole” to the Role for this Lambda function
2. As the VPC cannot access to the public net, the Lambda function assign to the VPC cannot access the DynamoDB and AWS Shadow. To solve this issue, the VPC need to be configured to route outbound traffic to a NAT gateway in a public subnet.

Below link show the steps to configure VPC to route outbound traffic to public subnet:

<https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html>