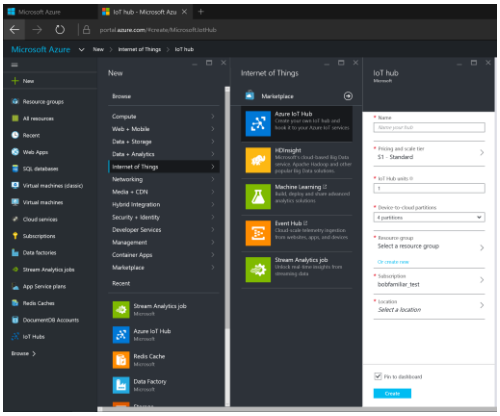
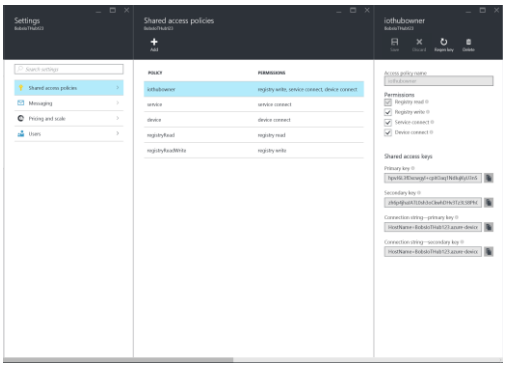
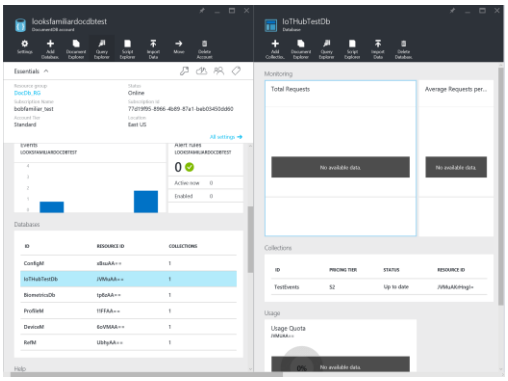
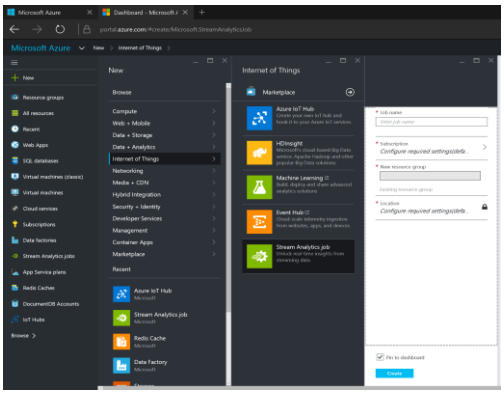
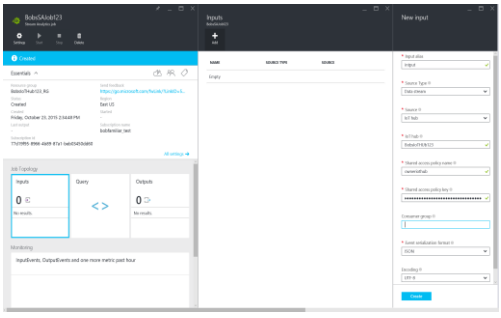
Lab 2

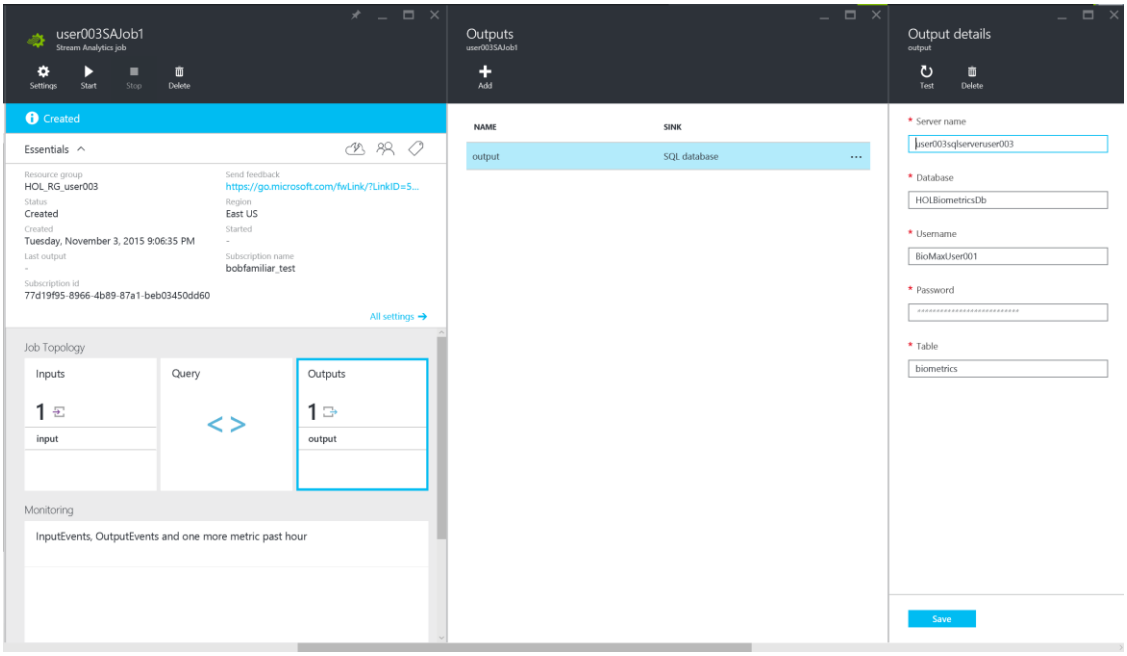
SUBJECT	TEACHER	DATE
IoT Hands-On Lab	Bob Familiar	November 19, 2015

OVERVIEW

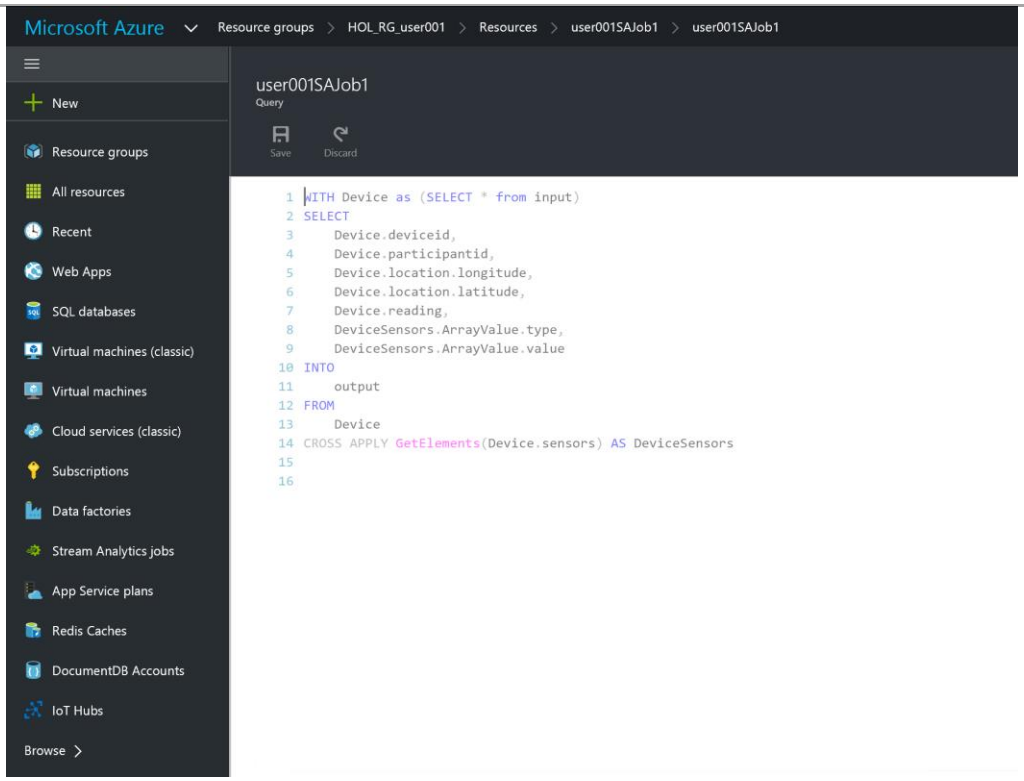
This lab involves provisioning IoT Hub and creating a Stream Analytics Jobs that reads incoming device telemetry and output to DocumentDb. These steps are done manually so that you can get firsthand experience with the configuration settings of these services. As demonstrated in Lab 1, all of these steps can be automated through PowerShell.

LAB 2		
STEP 1	• Navigate to http://portal.azure.com. • Select '+ New', 'Internet of Things', 'Azure IoT Hub'. • Create a unique name for your IoT Hub using your user tag such as user023IoTHub • Select your resource group • Select East US for the location • Click 'Create' • Wait for your IoT Hub to be provisioned before moving to Step 2	

STEP 2	• Once the IoT Hub is provisioned, you will be able to gather the connection information for your end point. • Click 'Shared Access Policies', then 'IoTHubOwner' to reveal the private key and the connection string. • Open up Notepad and copy the private key and connection string into a text file for later reference.	
STEP 3	• Navigate to your DocumentDb instance and add a database called 'Biometrics' • Select that database and add a collection called 'Alarms'	
STEP 4	• Go back to the top level of the portal blade navigation and click '+ New', 'Internet of Things', 'Stream Analytics Job'. • Create a unique name for your job using your user tag, for example: user023SAJob1 • Select the subscription • Click 'Existing Resource Group' and select your resource group • Select East US for the location • Click 'Create' • Wait for the Stream Analytics Job to complete provisioning before moving on to Step 4	
STEP 5	• Once the Stream Analytics Job has been provisioned, you can define the Input, Output and Query. Click 'input', 'add', and fill out the form. • Enter 'input' for alias • Enter the name of your IoT Hub • Set the shared access policy name to 'iothubowner' • Paste the IoT Hub private key into the shared access policy key field • Click create • Check to make sure the test connection passes before continuing	

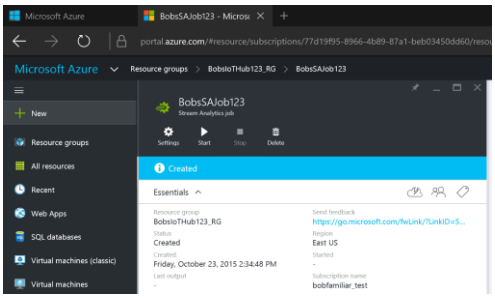
STEP 6	• Click 'output', 'add' and fill out the form • Enter 'output' as the alias • Select SQL Database as the Sink • Enter the server name; it has the format userNNNsqlserveruserNNN • Enter the database name; BiometricsDb • Enter the username: BioMaxUser001 • Enter the password: BioMaxPass001 • Enter the table name: biometrics 

STEP 7	• Click 'query' and enter the following SQL statement into the editor:
	
	`WITH Device as (SELECT * from input)`
	`SELECT`
	`  Device.deviceid,`
	`  Device.participantid,`
	`  Device.location.longitude,`
	`  Device.location.latitude,`
	`  Device.reading,`
	`  DeviceSensors.ArrayValue.type,`
	`  DeviceSensors.ArrayValue.value`
	`INTO`
	`  output`
	`FROM`
	`  Device`
	`CROSS APPLY GetElements(Device.sensors) AS DeviceSensors`
	
	• Click 'Save'



STEP 8

- On the Essentials Blade, click the 'Start' button.



STEP 9

- Create a second Stream Analytics job using the same IoT Hub settings for input and select DocumentDb as the sink.
- Enter the DocumentDB connection settings;
  - Account Id is the URI and Key
  - Database is Biometrics
  - Collection name is Alarms
  - Partition Key and Document Id is *id*
- Enter the following for the query:

```
WITH Device as (SELECT * from input)
SELECT
    Device.id,
    Device.deviceid,
    Device.participantid,
      Device.location.longitude,
    Device.location.latitude,
    Device.reading,
    DeviceSensors.ArrayValue.type,
    DeviceSensors.ArrayValue.value
INTO
    output
FROM
    Device
CROSS APPLY GetElements(Device.sensors) AS DeviceSensors
WHERE
```

	((DeviceSensors.ArrayValue.type = 1) AND (DeviceSensors.ArrayValue.value > 180)) • On the Essentials Blade, click ‘Start’