Vendor: Microsoft

Exam Code:AZ-220

Exam Name: Microsoft Azure IoT Developer

Version: Demo

QUESTION 1

You have an Azure IoT hub.

You need to recommend a solution to scale the IoT hub automatically.

What should you include in the recommendation?

A. Create an SMS alert in IoT Hub for the Total number of messages used metric.

B. Create an Azure function that retrieves the quota metrics of the IoT hub.

C. Configure autoscaling in Azure Monitor.

D. Emit custom metrics from the IoT device code and create an Azure Automation runbook alert.

Correct Answer: B

Note: IoT Hub is scaled and priced based on an allowed number of messages per day across all devices connected to that IoT Hub. If you exceed the allowed message threshold for your chosen tier and number of units, IoT Hub will begin rejecting new messages. To date, there is no built-in mechanism for automatically scaling an IoT Hub to the next level of capacity if you approach or exceed that threshold.

Reference: https://docs.microsoft.com/en-us/samples/azure-samples/iot-hub-dotnet-autoscale/iot-hub-dotnet-autoscale/

QUESTION 2

DRAG DROP

You have an Azure IoT Central application that includes a Device Provisioning Service instance.

You need to connect IoT devices to the application without first registering the devices.

In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Actions

- Flash unique credentials to the devices.
- Obtain the credential.
- Generate device credentials.
- Associate the devices to a template and approve the connections.
- Connect the devices to IoT Central.

Answer Area

Correct Answer:

Actions

Answer Area

- Generate device credentials.
- Flash unique credentials to the devices.
- Connect the devices to IoT Central.
- Associate the devices to a template and approve the connections.
- Obtain the credential.

Step: With DPS (Device Provisioning Service) you can generate device credentials and configure the devices offline without registering the devices through IoT Central UI. Connect devices that use SAS tokens without registering

1.

Copy the IoT Central application\\'s group primary key

2.

Use the dps-keygen tool to generate the device SAS keys. Use the group primary key from the previous step. The device IDs must be lower-case: dps-keygen -mk: -di:

3.

The OEM flashes each device with a device ID, a generated device SAS key, and the application ID scope value.

4.

When you switch on a device, it first connects to DPS to retrieve its IoT Central registration information.

The device initially has a device status Unassociated on the Devices page and isn\\'t assigned to a device template. On the Devices page, Migrate the device to the appropriate device template. Device provisioning is now complete, the device

status is now Provisioned, and the device can start sending data.

On the Administration > Device connection page, the Auto approve option controls whether you need to manually approve the device before it can start sending data.

Reference:

https://docs.microsoft.com/en-us/azure/iot-central/core/concepts-get-connected

---

QUESTION 3

You have an Azure IoT solution that includes a standard tier Azure IoT hub and an IoT device.

The device sends one 100-KB device-to-cloud message every hour.

You need to calculate the total daily message consumption of the device.

What is the total daily message consumption of the device?

A. 24

B. 600

C. 2,400

D. 4,800

Correct Answer: B

100 KB * 24 is around 2,400 bytes.

The 100 KB message is divided into 4 KB blocks, and it is billed for 25 messages. 25 times 24 is 600

Note: The maximum message size for messages sent from a device to the cloud is 256 KB. These messages are metered in 4 KB blocks for the paid tiers so for instance if the device sends a 16 KB message via the paid tiers it will be billed

as 4 messages.

Reference:

https://azure.microsoft.com/en-us/pricing/details/iot-hub/

QUESTION 4

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure IoT solution that includes an Azure IoT hub, a Device Provisioning Service instance, and 1,000 connected IoT devices.

All the IoT devices are provisioned automatically by using one enrollment group.

You need to temporarily disable the IoT devices from connecting to the IoT hub.

Solution: You disconnect the Device Provisioning Service from the IoT hub.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead, from the Device Provisioning Service, you disable the enrollment group, and you disable device entries in the identity registry of the IoT hub to which the IoT devices are provisioned.

Reference: https://docs.microsoft.com/bs-latn-ba/azure/iot-dps/how-to-unprovision-devices

---

QUESTION 5

You have 1,000 devices that connect to an Azure IoT hub.

You discover that some of the devices fail to send data to the IoT hub.

You need to ensure that you can use Azure Monitor to troubleshoot the device connectivity issues.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From the Diagnostics settings of the IoT hub, select Archive to a storage account.

B. Collect the DeviceTelemetry, Connections, and Routes logs.

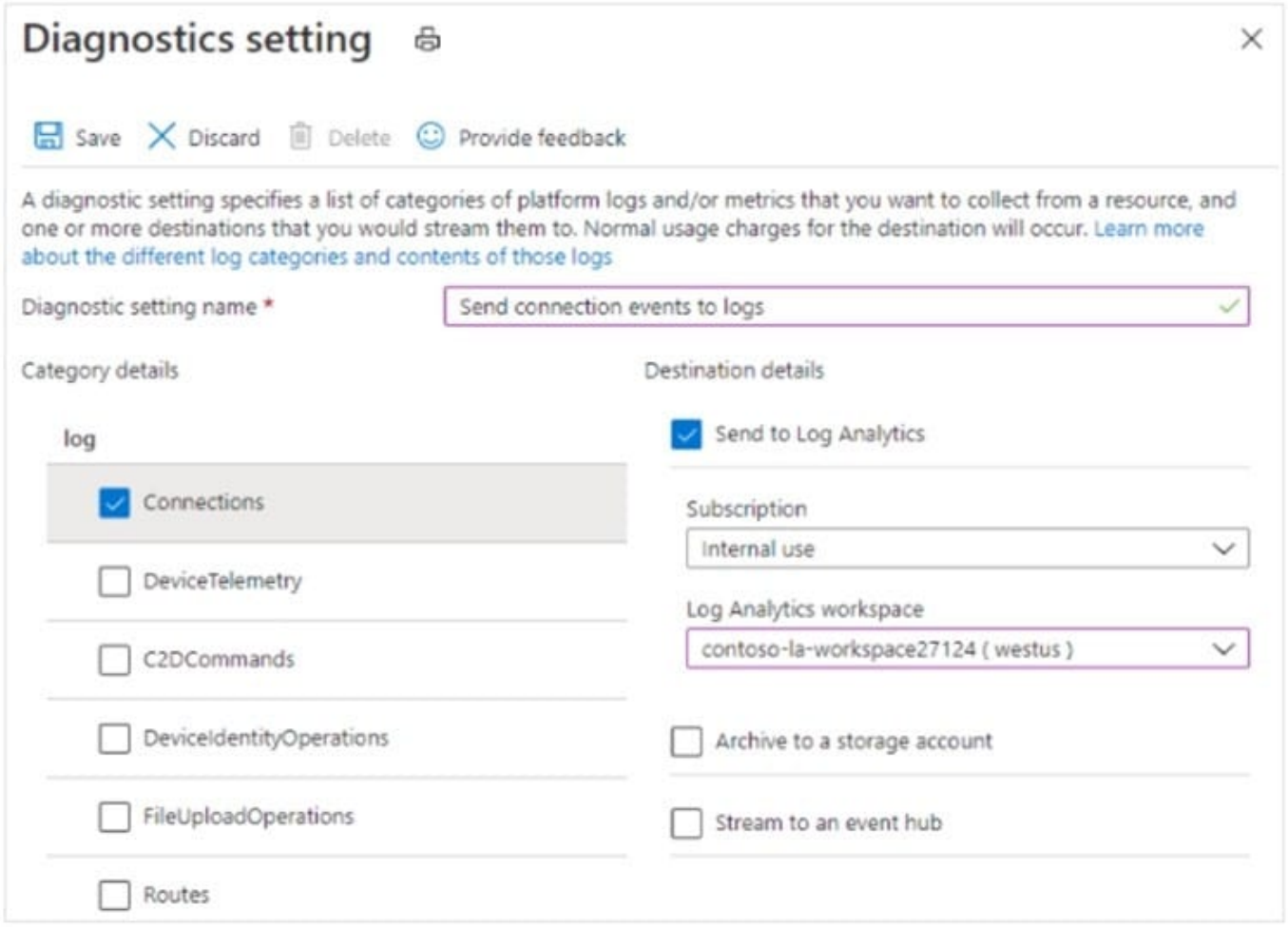
C. Collect all metrics.

D. From the Diagnostics settings of the IoT hub, select Send to Log Analytic.

E. Collect the JobsOperations, DeviceStreams, and FileUploadOperations logs.

Correct Answer: BD

The IoT Hub resource logs connections category emits operations and errors having to do with device connections. The following screenshot shows a diagnostic setting to route these logs to a Log Analytics workspace:



Note: Azure Monitor: Route connection events to logs:

IoT hub continuously emits resource logs for several categories of operations. To collect this log data, though, you need to create a diagnostic setting to route it to a destination where it can be analyzed or archived. One such destination is

Azure Monitor Logs via a Log Analytics workspace, where you can analyze the data using Kusto queries.

Reference:

https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-troubleshoot-connectivity

---

QUESTION 6

You have an Azure IoT solution that includes multiple Azure IoT hubs in different geographic locations and a single Device Provision Service instance. You need to configure device enrollment to assign devices to the appropriate IoT hub based on the following requirements:

1.

The registration ID of the device

2.

The geographic location of the device

The load between the IoT hubs in the same geographic location must be balanced.

What should you use to assign the devices to the IoT hubs?

A. Static configuration (via enrollment list only)

B. Lowest latency

C. Evenly weighted distribution

D. Custom (Use Azure Function)

Correct Answer: A

Set the Device Provisioning Service allocation policy

The allocation policy is a Device Provisioning Service setting that determines how devices are assigned to an IoT hub. There are three supported allocation policies:

Lowest latency: Devices are provisioned to an IoT hub based on the hub with the lowest latency to the device.

Evenly weighted distribution (default): Linked IoT hubs are equally likely to have devices provisioned to them. This is the default setting. If you are provisioning devices to only one IoT hub, you can keep this setting.

Static configuration via the enrollment list: Specification of the desired IoT hub in the enrollment list takes priority over the Device Provisioning Service-level allocation policy.

Reference:

https://docs.microsoft.com/en-us/azure/iot-dps/tutorial-provision-multiple-hubs

---

QUESTION 7

You need to store the real-time alerts generated by Stream Analytics to meet the technical requirements. Which type of Stream Analytics output should you configure?

A. Azure Blob storage

B. Microsoft Power BI

C. Azure Cosmos DB

D. Azure SQL Database

Correct Answer: A

When you create a Time Series Insights Preview pay-as-you-go (PAYG) SKU environment, you create two Azure resources:

An Azure Storage general-purpose V1 blob account for cold data storage.

An Azure Time Series Insights Preview environment that can be configured for warm data storage.

Reference:

https://docs.microsoft.com/en-us/azure/time-series-insights/time-series-insights-update-storage-ingress

---

QUESTION 8

DRAG DROP

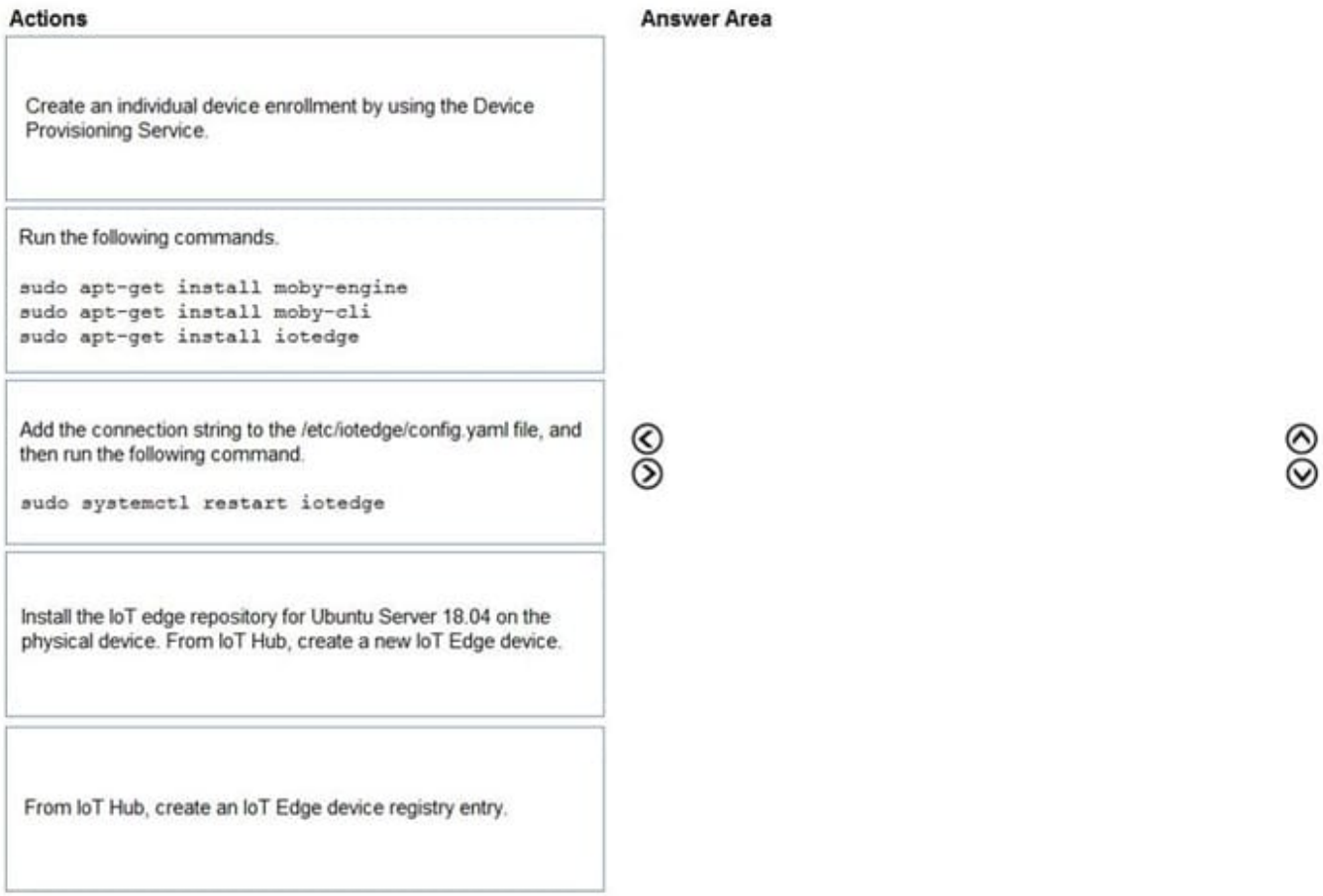
Your company is creating a new camera security system that will use Azure IoT Hub.

You plan to use an Azure IoT Edge device that will run Ubuntu Server 18.04.

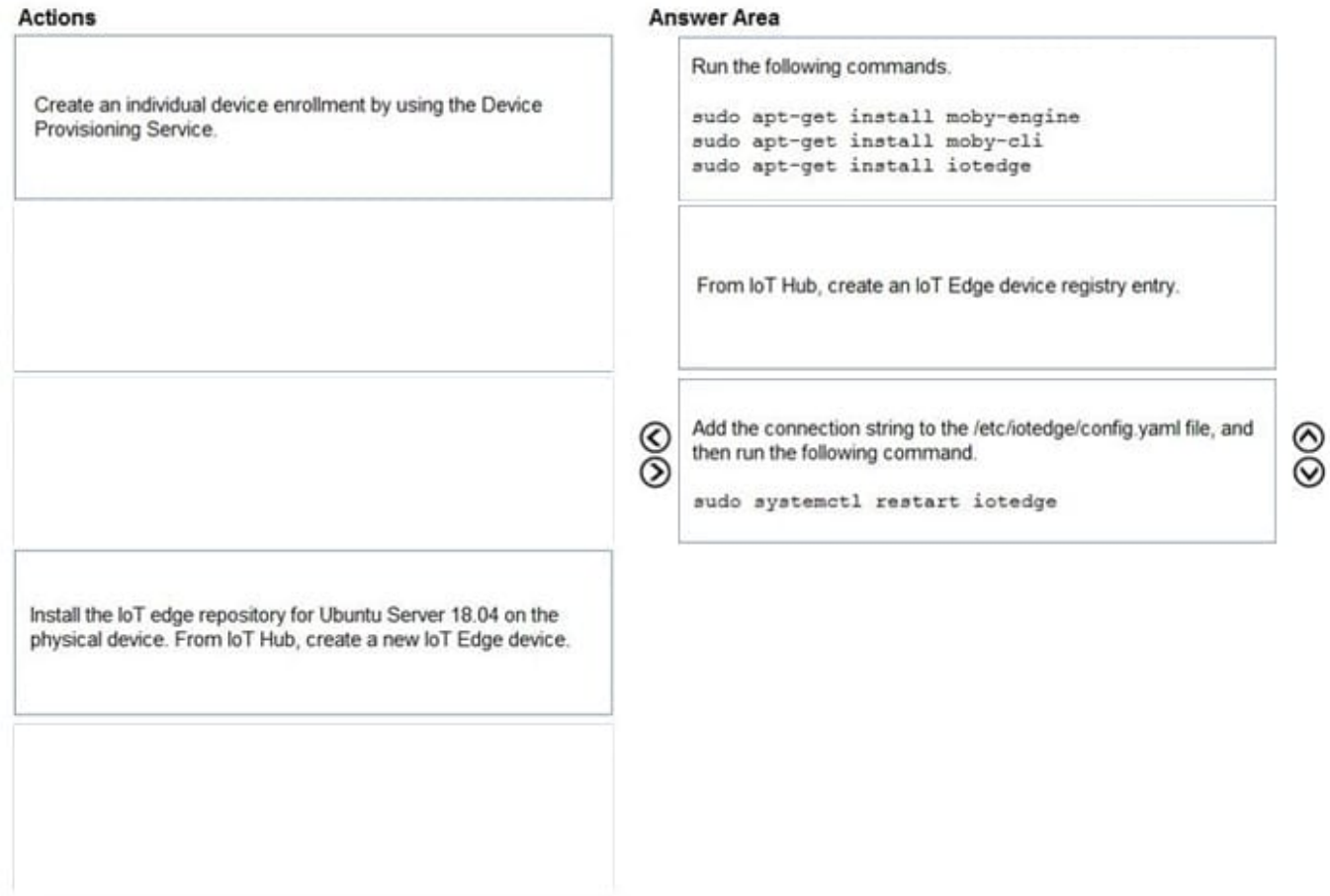
You need to configure the IoT Edge device.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:



Correct Answer:



Step 1: Run the following commands

Install the container runtime.

Azure IoT Edge relies on an OCI-compatible container runtime. For production scenarios, we recommended that you use the Moby-based engine provided below. The Moby engine is the only container engine officially supported with Azure

IoT Edge. Docker CE/EE container images are compatible with the Moby runtime.

Install the Moby engine.

sudo apt-get install moby-engine

Install the Moby command-line interface (CLI). The CLI is useful for development but optional for production deployments.

sudo apt-get install moby-cli

Install the security daemon. The package is installed at /etc/iotedge/.

sudo apt-get install iotedge

Step 2: From Iot Hub,create an IoT Edge device registry entry.

Note: In your IoT Hub in the Azure portal, IoT Edge devices are created and managed separately from IOT devices that are not edge enabled.

Sign in to the Azure portal and navigate to your IoT hub.

In the left pane, select IoT Edge from the menu.

Select Add an IoT Edge device.

Provide a descriptive device ID. Use the default settings to auto-generate authentication keys and connect the new device to your hub.

Select Save.

Retrieve the connection string in the Azure portal

1.

When you\\'re ready to set up your device, you need the connection string that links your physical device with its identity in the IoT hub.

2.

From the IoT Edge page in the portal, click on the device ID from the list of IoT Edge devices.

3.

Copy the value of either Primary Connection String or Secondary Connection String.

Step 3: Add the connection string to..

To manually provision a device, you need to provide it with a device connection string that you can create by registering a new device in your IoT hub.

Open the configuration file.

sudo nano /etc/iotedge/config.yaml

Find the provisioning configurations of the file and uncomment the Manual provisioning configuration section. Update the value of device_connection_string with the connection string from your IoT Edge device.

Save and close the file.

After entering the provisioning information in the configuration file, restart the daemon:

sudo systemctl restart iotedge

Reference: https://docs.microsoft.com/en-us/azure/iot-edge/how-to-install-iot-edge-linux

---

QUESTION 9

You need to recommend a solution to keep device properties synced to IoT Hub. The solution must minimize data loss caused by the connectivity issues.

What should you include in the recommendation?

A. Azure Event Grid

B. a cloud-to-device message

C. IoT Hub device twins

D. the IoT Hub direct method

Correct Answer: C

Scenario: You discover connectivity issues between the IoT gateway devices and iothub1, which cause IoT devices to lose connectivity and messages.

To synchronize state information between a device and an IoT hub, you use device twins. A device twin is a JSON document, associated with a specific device, and stored by IoT Hub in the cloud where you can query them. A device twin contains desired properties, reported properties, and tags.

Reference: https://docs.microsoft.com/en-us/azure/iot-hub/tutorial-device-twins

---

QUESTION 10

You have an Azure IoT solution that includes an Azure IoT hub, 100 Azure IoT Edge devices, and 500 leaf devices.

You need to perform a key rotation across the devices.

Which three types of entities should you update? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. the $edgeHub module identity

B. the $edgeAgent module identity

C. the leaf module identities

D. the IoT Edge device identities

E. the iothubowner policy credentials

F. the leaf device identities

Correct Answer: ADF

To get authorization to connect to IoT Hub, devices and services must send security tokens signed with either a shared access or symmetric key. These keys are stored with a device identity in the identity registry.

An IoT Hub identity registry can be accessed like a dictionary, by using the deviceId or moduleId as the key.

Reference:

https://docs.microsoft.com/bs-latn-ba/azure/iot-dps/how-to-control-access

https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-identity-registry

---

QUESTION 11

You plan to deploy a standard tier Azure IoT hub.

You need to perform an over-the-air (OTA) update on devices that will connect to the IoT hub by using scheduled jobs.

What should you use?

A. a device-to-cloud message

B. the device twin reported properties

C. a cloud-to-device message

D. a direct method

Correct Answer: D

Releases via the REST API.

All of the operations that can be performed from the Console can also be automated using the REST API. You might do this to automate your build and release process, for example.

You can build firmware using the Particle CLI or directly using the compile source code API.

Note: Over-the-air (OTA) firmware updates are a vital component of any IoT system. Over-the-air firmware updates refers to the practice of remotely updating the code on an embedded device.

Reference:

https://docs.particle.io/tutorials/device-cloud/ota-updates/

QUESTION 12

You have a Standard tier Azure IoT hub and a fleet of IoT devices.

The devices connect to the IoT hub by using either Message Queuing Telemetry Transport (MQTT) or Advanced Message Queuing Protocol (AMQP).

You need to send data to the IoT devices and each device must respond. Each device will require three minutes to process the data and respond.

Solution: You use cloud-to-device messages and watch the cloud-to-device feedback endpoint for successful acknowledgement.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

IoT Hub provides three options for device apps to expose functionality to a back-end app:

Twin\\'s desired properties for long-running commands intended to put the device into a certain desired state. For example, set the telemetry send interval to 30 minutes.

Direct methods for communications that require immediate confirmation of the result. Direct methods are often used for interactive control of devices such as turning on a fan.

Cloud-to-device messages for one-way notifications to the device app.

Reference:

https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-c2d-guidance