Exam : **AZ-220**

Title : Microsoft Azure IoT Developer

Vendor : Microsoft

Version : DEMO

NO.1 You have an IoT device that has the following configurations:
Hardware: Raspberry Pi Operating system: Raspbian
You need to deploy Azure IoT Edge to the device.
Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Install the IoT Edge security daemon.

B. Update the IoT Edge runtime.

C. Run the Deploy-IoTEdge PowerShell cmdlet on the IoT Edge device.

D. Install the container runtime.

Answer: A,B

Explanation:
The Azure IoT Edge runtime is what turns a device into an IoT Edge device. The runtime can be deployed on devices as small as a Raspberry Pi or as large as an industrial server.
The IoT Edge security daemon provides and maintains security standards on the IoT Edge device. The daemon starts on every boot and bootstraps the device by starting the rest of the IoT Edge runtime.
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/how-to-install-iot-edge

NO.2 You have an Azure subscription named Sub1 that contains five Azure IoT hubs in the basic tier.
You assign an Azure policy named Policy! to Subl. Policy 1 ensures that when an IoT hub is deployed, a pnvate endpoint is deployed for the IoT hub.
You need to ensure that Policyl is applied to the existing IoT hubs. The solution must minimize administrative effort.
What should you do?

A. Upgrade the IoT hubs to the standard tier.

B. Perform a manual failover of each IoT hub.

C. Run a remediation task.

D. Reassign Policy1.

Answer: C

NO.3 You have an Azure IoT Edge device.
You need to modify the credentials used to access the container registry. What should you modify?

A. the @edgeHub module twin

B. the Azure IoT Hub device twin

C. the $edgeAgent module twin

D. the IoT Edge module

Answer: C

Explanation:
The module twin for the IoT Edge agent is called $edgeAgent and coordinates the communications between the IoT Edge agent running on a device and IoT Hub. The desired properties are set when applying a deployment manifest on a specific device as part of a single-device or at-scale deployment.
These properties include: runtime.settings.registryCredentials.{registryId}.username runtime.settings.registryCredentials.registryId}.password Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/module-edgeagent-edgehub

NO.4 You have an Azure subscription that contains the resources shown in the following table.

Name	Type
Hub1	Azure IoT Hub
storage1	Storage account
container1	Blob container

You need to use a REST API calls to configure Hub1 to route all messages to container1.
What should you do first?

A. Create a routing endpoint.

B. Retrieve the connection string of the storage account

C. Create a route.

D. Create an Azure Service Bus queue.

Answer: B

NO.5 You have an IoT device that gathers data in a CSV file named Sensors.csv.
You deploy an Azure IoT hub that is accessible at ContosoHub.azure-devices.net. You need to ensure that Sensors.csv is uploaded to the IoT hub.
Which two actions should you perform? Each correct answer presents part of the solution.

A. Configure the device to use a GET request to ContosoHub.azure-devices.net/devices/ContosoDevice1/ files/notifications.

B. From the Azure subscription, select the IoT hub, select Message routing, and then configure a route to storage.

C. Upload Sensors.csv by using the IoT Hub REST API.

D. From the Azure subscription, select the IoT hub, select File upload, and then configure a storage container.

Answer: C,D

Explanation:
C: To use the file upload functionality in IoT Hub, you must first associate an Azure Storage account with your hub. Select File upload to display a list of file upload properties for the IoT hub that is being modified.
For Storage container: Use the Azure portal to select a blob container in an Azure Storage account in your current Azure subscription to associate with your IoT Hub. If necessary, you can create an Azure Storage account on the Storage accounts blade and blob container on the Containers A: IoT Hub has an endpoint specifically for devices to request a SAS URI for storage to upload a file. To start the file upload process, the device sends a POST request to {iot hub}.azure-devices.net/devices/{deviceId}/ files with the following JSON body:

```
{
"blobName": "{name of the file for which a SAS URI will be generated}"
}
```

Incorrect Answers:
D: Deprecated: initialize a file upload with a GET. Use the POST method instead.
Reference:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/iot-hub/iot-hub-configure-file-

upload.md

NO.6 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. 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 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 schedule an IoT Hub job to update the twin tags and you query for job progress.
Does this meet the goal?
A. No
B. yes
Answer: A
Explanation:
Instead update the twin desired property and check the corresponding reported property.
Note: 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

NO.7 You have an Azure IoT solution that includes an Azure IoT Hub named Hub1 and an Azure IoT Edge device named Edge1. Edge1 connects to Hub1.
You need to deploy a temperature module to Edge1. What should you do?
A. Create an IoT Edge deployment manifest that specifies the temperature module and the route to $upstream. From a Bush prompt, run the following command:
az iot hub monitor-events-device-id Edge1 -hub-name Hub1
B. Create an IoT Edge deployment manifest that specifies the temperature module and the route to $upstream. From a Bush prompt, run the following command:
az iot edge set-modules -device-id Edge1 -hub-name Hub1 -content C:\deploymentMan1.json
C. From the Azure portal, navigate to Hub1 and select IoT Edge. Select Edge1, and then select Manage Child Devices. From a Bash prompt, run the following command:
az iot edge set-modules -device-id Edge1 -hub-name Hub1 -content C:\deploymentMan1.json
D. From the Azure portal, navigate to Hub1 and select IoT Edge. Select Edge1, select Device Twin, and then set the deployment manifest as a desired property. From a Bash prompt, run the following command az iot hub monitor-events-device-id Edge1 -hub-name Hub1
Answer: B
Explanation:

You deploy modules to your device by applying the deployment manifest that you configured with the module information.
Change directories into the folder where your deployment manifest is saved. If you used one of the VS Code IoT Edge templates, use the deployment.json file in the config folder of your solution directory and not the deployment.template.json file.
Use the following command to apply the configuration to an IoT Edge device:
az iot edge set-modules --device-id [device id] --hub-name [hub name] --content [file path]
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/how-to-deploy-modules-cli

NO.8 You need to visualize Azure IoT Hub telemetry data by using Microsoft Power BI.
Which service should you connect to the IoT hub?
A. SendGrid
B. Azure Stream Analytics
C. Azure Event Grid
D. Azure Notification Hubs
Answer: B
Explanation:
You can use Microsoft Power BI to visualize real-time sensor data that your Azure IoT hub receives. To do so, you configure an Azure Stream Analytics job to consume the data from IoT Hub and route it to a dataset in Power BI.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-live-data-visualization-in-power-bi

NO.9 How should you complete the GROUP BY clause to meet the Streaming Analytics requirements?
A. GROUP BY TumblingWindow(Second, 30)
B. GROUP BY HoppingWindow(Second, 60, 30)
C. GROUP BY SessionWindow(Second, 30, 60)
D. GROUP BY SlidingWindow(Second, 30)
Answer: A
Explanation:
Scenario: You plan to use a 30-second period to calculate the average temperature reading of the sensors.
Tumbling window functions are used to segment a data stream into distinct time segments and perform a function against them, such as the example below. The key differentiators of a Tumbling window are that they repeat, do not overlap, and an event cannot belong to more than one tumbling window.
InAnswers:
A: Hopping window functions hop forward in time by a fixed period. It may be easy to think of them as Tumbling windows that can overlap, so events can belong to more than one Hopping window result set.
Reference:
https://docs.microsoft.com/en-us/azure/stream-analytics/stream-analytics-window-functions

NO.10 You have an Azure IoT hub that receives messages from an IoT device. The messages are serialized as Protobuf.
You need the IoT hub to route the messages.
What should you do first?

A. From the Azure portal, configure the IoT hub to add message enrichments.

B. Configure the IoT device to add application properties to the messages.

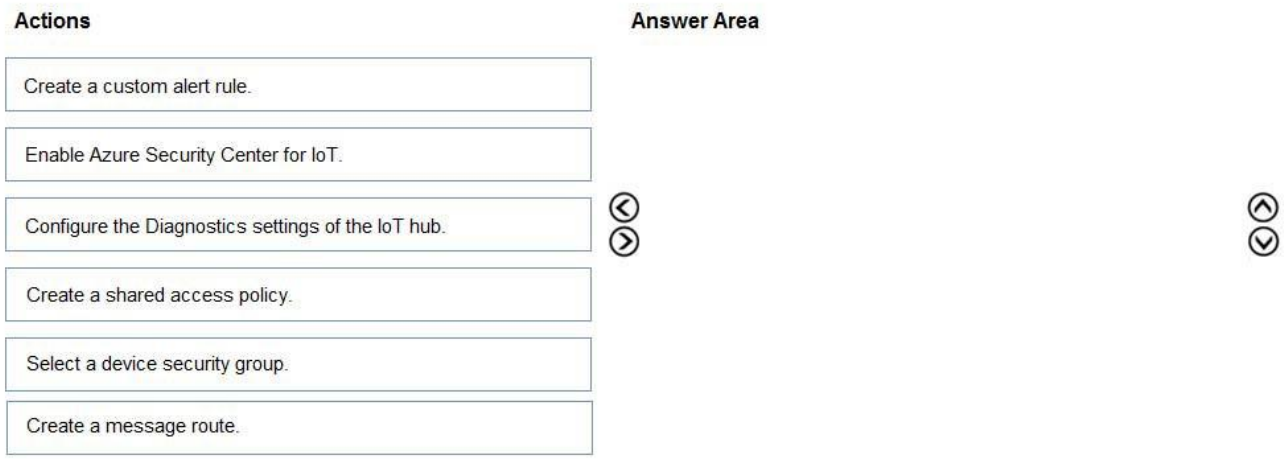
C. Configure the IoT device to add ASCII-encoded properties to the body of the messages.

D. From the Azure portal, add desired properties to the device twin.

Answer: D

Explanation:
Device twins store device-related information that:
Device and back ends can use to synchronize device conditions and configuration.
The solution back end can use to query and target long-running operations.
Desired properties. Used along with reported properties to synchronize device configuration or conditions. The solution back end can set desired properties, and the device app can read them. The device app can also receive notifications of changes in the desired properties.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-device-twins

NO.11 You have 100 devices that connect to an Azure IoT hub.
You need to be notified about failed local logins to a subnet of the devices.
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.



Answer:

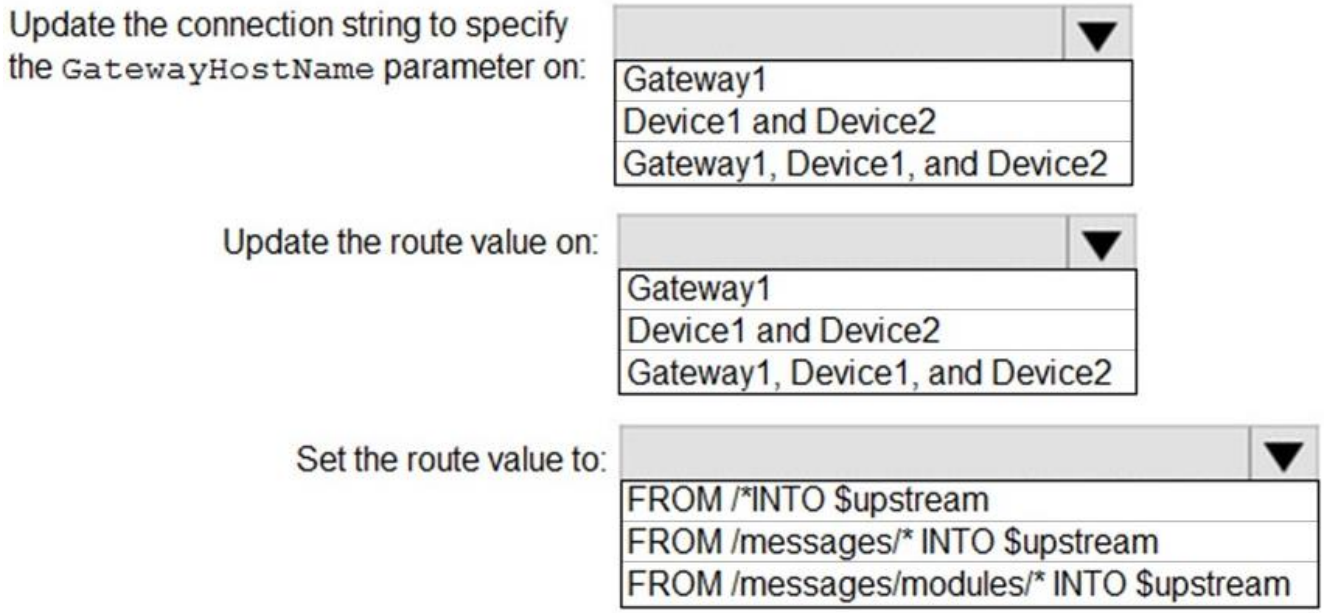
Answer Area

Enable Azure Security Center for IoT
Select a device security group
Create a custom alert rule

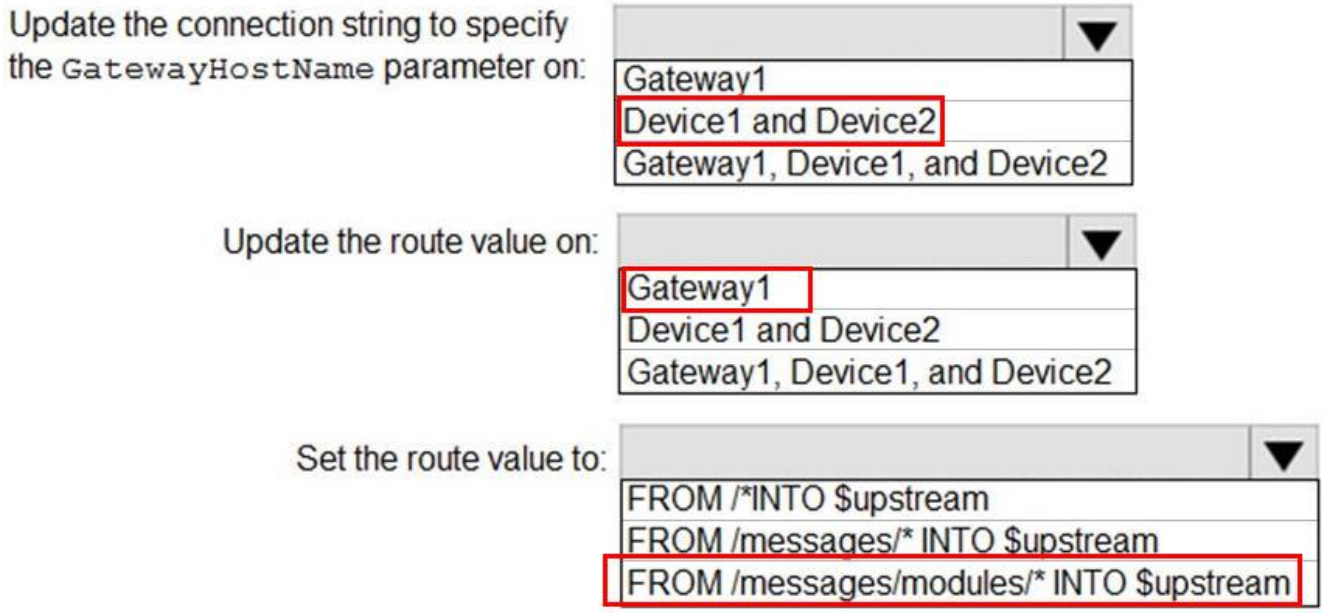
1 - Enable Azure Security Center for IoT
2 - Select a device security group
3 - Create a custom alert rule
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/asc-for-iot/how-to-security-data-access
https://docs.microsoft.com/en-us/rest/api/securitycenter/devicesecuritygroups/createorupdate

NO.12 You have an Azure IoT solution that contains an Azure IoT hub and 100 IoT devices. The devices run Windows Server 2016.
You need to deploy the Azure Defender for IoT C#-based security agent to the devices.
What should you do first?
A. From the IoT hub. create a security module for the devices.
B. From the IoT hub. create a system-assigned managed identity.
C. On the devices, set the PowerShell execution policy to Restricted.
D. On the devices, initialize Trusted Platform Module (TPM).
Answer: A
Explanation:
The IoT Edge security manager provides a safe framework for security service extensions through host-level modules. The IoT Edge security manager include Ensure safe operation of client agents for services including Device Update for IoT Hub and Azure Defender for IoT.
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/iot-edge-security-manager

NO.13 You have an Azure subscription that contains an Azure IoT hub and two IoT devices named Device1 and Device2.
You plan to deploy an Azure IoT Edge gateway device named Gateway1.
You need to ensure that all device-to-cloud messages and twin change notifications from Device1 and Device2 to the IoT hub are routed by using Gateway1.
What tasks should you perform to configure the devices? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/how-to-authenticate-downstream-device

NO.14 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. 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 and an Azure IoT Edge device.
You plan to deploy 10 Bluetooth sensors. The sensors do not support MQTT, AMQP, or HTTPS.
You need to ensure that all the sensors appear in the IoT hub as a single device.
Solution: You configure the IoT Edge device as an IoT Edge transparent gateway. You configure the sensors to connect to the device.

Does this meet the goal?

A. No

B. Yes

Answer: A

Explanation:

IoT Edge transparent gateways support only the MQTT or AMQP protocols.

Instead use a translation gateway.

IoT Hub. The translation module receives messages from downstream devices, translates them into a supported protocol, and then the IoT Edge device sends the messages on behalf of the downstream devices. All information looks like it is coming from one device, the gateway.

Reference:

https://docs.microsoft.com/en-us/azure/iot-edge/iot-edge-as-gateway

NO.15 You have an Azure IoT solution that includes an Azure IoT hub and 100 Azure IoT Edge devices.

You plan to deploy the IoT Edge devices to external networks. The firewalls of the external networks only allow traffic on port 80 and port 443.

You need to ensure that the devices can connect to the IoT hub. The solution must minimize costs.

What should you do?

A. Connect the external networks to the IoT solution by using ExpressRoute.

B. Configure the upstream protocol of the devices to use MQTT over TCP.

C. Configure the upstream protocol of the devices to use AMQP over WebSocket.

D. Integrate cellular communication hardware onto the devices and avoid the use of the external networks.

Answer: C

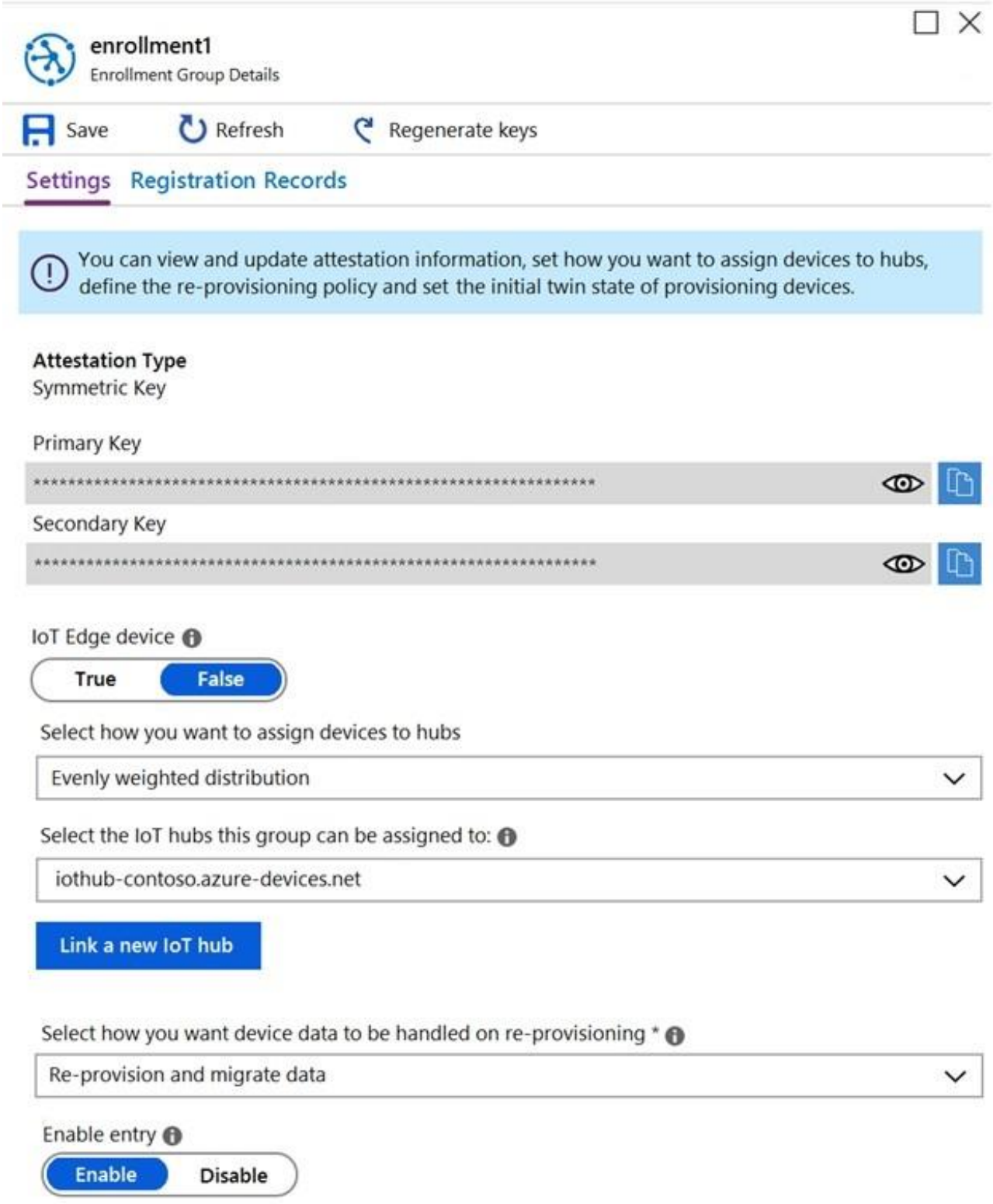
Explanation:

AMQP over WebSockets uses port 443.

Reference:

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

NO.16 From the Device Provisioning Service, you create an enrollment as shown in the exhibit. (Click the Exhibit tab.)



You need to deploy a new IoT device.
What should you use as the device identity during attestation?

A. the endorsement key of the device's Trusted Platform Module (TPM)
B. the HMACSHA256 hash of the device's registration ID
C. the random string of alphanumeric characters
D. a self-signed X.509 certificate

Answer: B

Explanation:
Each device uses its derived device key with your unique registration ID to perform symmetric key attestation with the enrollment during provisioning. To generate the device key, use the key you copied from your DPS enrollment to compute an HMAC-SHA256 of the unique registration ID for the device and convert the result into Base64 format.
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/how-to-auto-provision-symmetric-keys

NO.17 Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. 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 are developing a custom Azure IoT Edge module.
The module needs to identify the device ID of the local device.
Solution: You configure the module to read the device ID of the device twin.
Does this meet the goal?
A. No
B. Yes
Answer: B
Explanation:
Device twins are JSON documents that store device state information including metadata, configurations, and conditions. Azure IoT Hub maintains a device twin for each device that you connect to IoT Hub.
Device identity properties. The root of the device twin JSON document contains the read-only properties from the corresponding device identity stored in the identity registry.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-device-twins

NO.18 You are prototyping an IoT edge solution.
You are creating a deployment manifest for an IoT edge device that will connect to an Azure IoT hub.
Which two modules should you include in the manifest? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.
HA.
A. opc-publisher
B. iotedgeModbus
C. edgeAgent
D. zureiotsecurity
E. edgeHub
Answer: D,E

NO.19 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 Answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. the iothubowner policy credentials

B. the leaf device identities

C. the IoT Edge device identities

D. the $edgeHub module identity

E. the leaf module identities

F. the $edgeAgent module identity

Answer: B,C,D

Explanation:

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

NO.20 You have an Azure 10T hub and an I0T device.

You are developing an IoT solution that will generate an alert when the IoT device leaves a geofenced are a. The device sends telemetry in the following format.

```
{
    "location": {
        "type":"Point",
        "coordinates": [76.6, 10.1]
    }
}
```

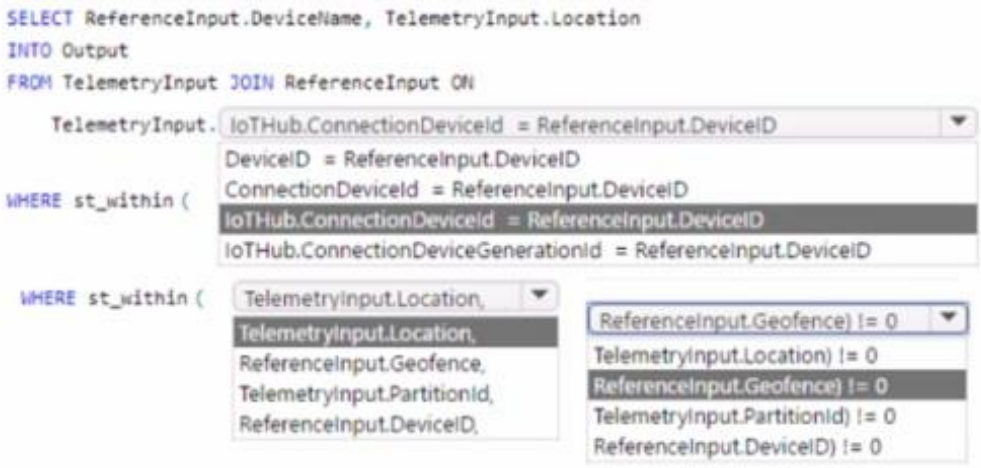
You create an Azure Stream Analytics job that uses telemetry input from the IoT hub and a reference input that contains the data shown in the following table.

DeviceID	DeviceName	Geofence
"Device1"	"Device1"	"POLYGON((-122.13301696018573 47.63764925180358,-122.13272728161212 47.63764925180358,-122.13274873928424 47.63784082716388,-122.13373579220172 47.63782998329432))"

How should you complete the Stream Analytics query? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area