

# Microsoft

## Exam Questions AZ-220

Microsoft Azure IoT Developer



### NEW QUESTION 1

- (Exam Topic 1)

How should you complete the GROUP BY clause to meet the Streaming Analytics requirements?

- A. GROUP BY HoppingWindow(Second, 60, 30)
- B. GROUP BY TumblingWindow(Second, 30)
- C. GROUP BY SlidingWindow(Second, 30)
- D. GROUP BY SessionWindow(Second, 30, 60)

**Answer:** B

#### 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>

### NEW QUESTION 2

- (Exam Topic 1)

You plan to deploy Azure Time Series Insights.

What should you create on iothub1 before you deploy Time Series Insights?

- A. a new message route
- B. a new consumer group
- C. a new shared access policy
- D. an IP filter rule

**Answer:** B

#### Explanation:

Create a dedicated consumer group in the IoT hub for the Time Series Insights environment to consume from. Each Time Series Insights event source must have its own dedicated consumer group that isn't shared with any other consumer. If multiple readers consume events from the same consumer group, all readers are likely to exhibit failures.

Reference:

<https://docs.microsoft.com/en-us/azure/time-series-insights/time-series-insights-how-to-add-an-event-source- iothub>

### NEW QUESTION 3

- (Exam Topic 1)

You need to use message enrichment to add additional device information to messages sent from the IoT gateway devices when the reported temperature exceeds a critical threshold.

How should you configure the enrich message values? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

#### Answer Area

<input type="checkbox"/> \$iothubname	<input type="checkbox"/> desired.pressure
<input type="checkbox"/> \$twin	<input type="checkbox"/> fanSpeed.reported
<input type="checkbox"/> \$twin.properties	<input type="checkbox"/> reported.fanSpeed
<input type="checkbox"/> \$twin.results	<input type="checkbox"/> temperature
<input type="checkbox"/> \$twin.tags	<input type="checkbox"/> temperature.reported

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

Reference:

<https://docs.microsoft.com/bs-cyrl-ba/azure/iot-hub/iot-hub-message-enrichments-overview>

### NEW QUESTION 4

- (Exam Topic 1)

You create a new IoT device named device1 on iothub1. Device1 has a primary key of Uihuih76hbHb. How should you complete the device connection string? To answer, select the appropriate options in the

answer area.  
 NOTE: Each correct selection is worth one point.

HostName=

azure-devices.net

criticalep

device1

iothub1

tracestate

.

azure-devices.net

criticalep

device1

iothub1

tracestate

;DeviceId=

azure-devices.net

criticalep

device1

iothub1

tracestate

:SharedAccessKey=Uihuih76hbHb

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

Box 1: iothub1  
 The Azure IoT hub is named iothub1.  
 Box 2: azure-devices.net  
 The format of the device connection string looks like:  
 HostName={YourIoTHubName}.azure-devices.net;DeviceId=MyNodeDevice;SharedAccessKey={YourShared Box 1: device1  
 Device1 has a primary key of Uihuih76hbHb. Reference:  
<https://docs.microsoft.com/en-us/azure/iot-hub/quickstart-control-device-dotnet>

**NEW QUESTION 5**

- (Exam Topic 3)  
 You have 20 devices that connect to an Azure IoT hub.  
 You open Azure Monitor as shown in the exhibit. (Click the Exhibit tab.)



You discover that telemetry is not being received from five IoT devices.  
 You need to identify the names of the devices that are not generating telemetry and visualize the data. What should you do first?

- A. Add the Number of throttling errors metric and archive the logs to an Azure storage account.
- B. Configure diagnostics for Routes and stream the logs to Azure Event Hubs.
- C. Add the Telemetry messages sent metric and archieve the logs to an Azure Storage account.
- D. Configure diagnostics for Connections and send the logs to Azure Log Analytics.

Answer: D

**Explanation:**

To log device connection events and errors, turn on diagnostics for IoT Hub. We recommend turning on these logs as early as possible, because if diagnostic logs aren't enabled, when device disconnects occur, you won't have any information to troubleshoot the problem with.

- Sign in to the Azure portal.
- Browse to your IoT hub.
- Select Diagnostics settings.
- Select Turn on diagnostics.
- Enable Connections logs to be collected.
- For easier analysis, turn on Send to Log Analytics

Diagnostics settings

Save

Discard

Delete

Name

log-connection-errors-events-to-log-analytics

Archive to a storage account

Stream to an event hub

Send to Log Analytics

Log Analytics

iot-log-everything-workspace

LOG

Connections

Reference:

<https://docs.microsoft.com/bs-cyrl-ba/azure/lot-hub/iot-hub-troubleshoot-connectivity>

#### NEW QUESTION 6

- (Exam Topic 3)

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 \$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

**Answer:** ADF

#### 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>

#### NEW QUESTION 7

- (Exam Topic 3)

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.

**Answer:** B

#### Explanation:

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/>

#### NEW QUESTION 8

- (Exam Topic 3)

You have an Azure IoT hub.

You plan to attach three types of IoT devices as shown in the following table.

Name	Specification	Note
Transparent Field Gateway Device	High-power device with a fast processor and 4 GB of RAM	Will connect to multiple devices, each with its own credentials, by using the same TLS connection.
Low Resource Device	Low resource specifications, battery-operated, and 512 KB of RAM	Will connect directly to an IoT hub and will <b>NOT</b> connect to any other devices. Will use cloud-to-device messages.
Limited Sensor Device	Extremely low-power device with a limited microcontroller (MCU) and 256 KB of RAM	Will <b>NOT</b> support the Azure SDK. Messages must be as small as possible.

You need to select the appropriate communication protocol for each device.

What should you select? To answer, drag the appropriate protocols to the correct devices. Each protocol may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

### Protocols

AMQP

HTTPS

MQTT

### Answer Area

Device	Protocol
Transparent Field Gateway Device:	Protocol
Low Resource Device:	Protocol
Limited Sensor Device:	Protocol

- A. Mastered  
B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: AMQP

Use AMQP on field and cloud gateways to take advantage of connection multiplexing across devices. Box 2: MQTT

MQTT is used on all devices that do not require to connect multiple devices (each with its own per-device credentials) over the same TLS connection.

Box 3: HTTPS

Use HTTPS for devices that cannot support other protocols.

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

**NEW QUESTION 9**

- (Exam Topic 3)

You have an Azure IoT Central application.

You need to connect an IoT device to the application.

Which two settings do you require in IoT Central to configure the device? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Group SAS Primary Key  
B. the IoT hub name  
C. Scope ID  
D. Application Name  
E. Device ID

**Answer:** CE

**Explanation:**

In your Azure IoT Central application, add a real device to the device template

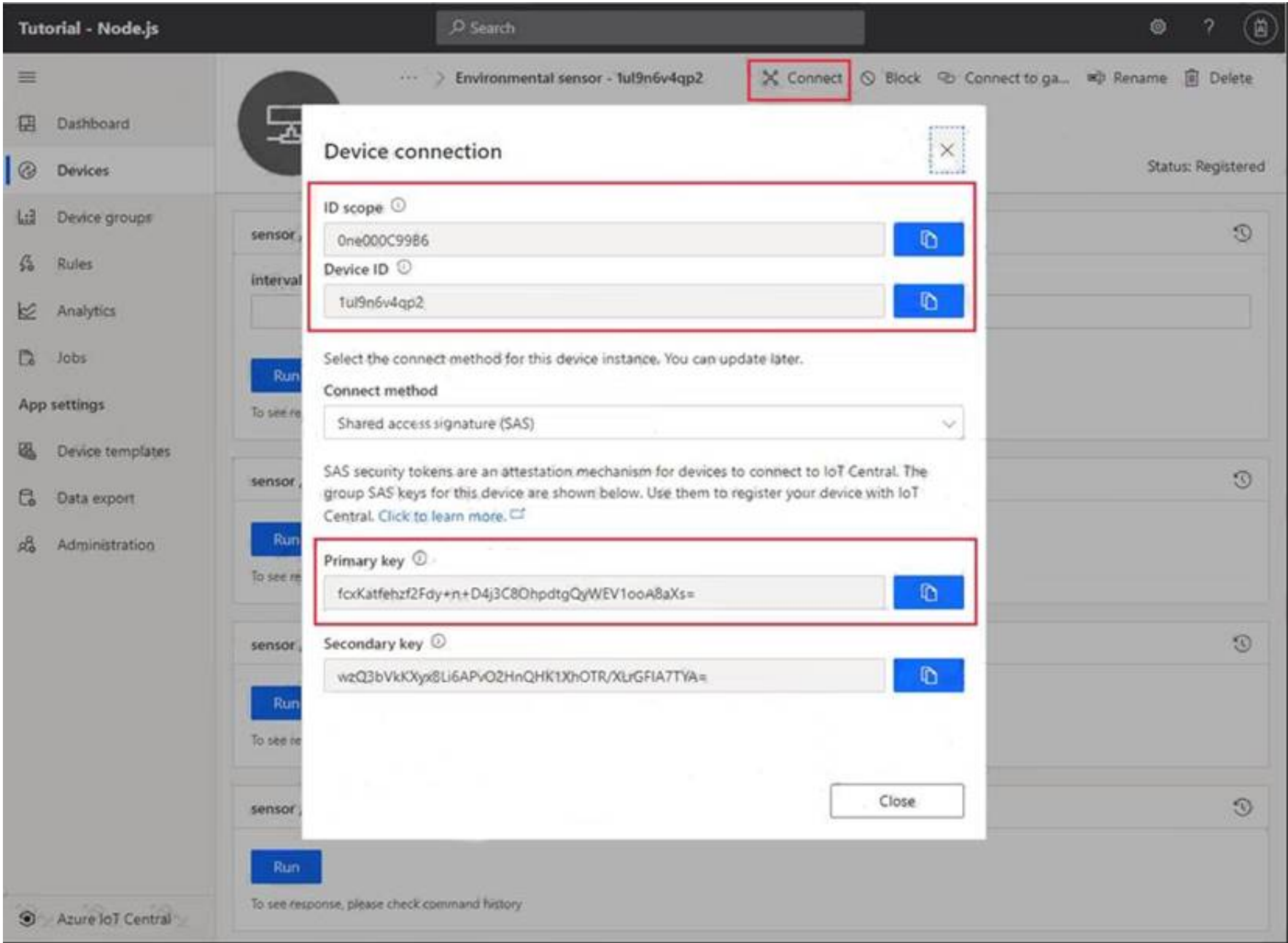
\*1. On the Devices page, select the Environmental sensor device template.

\*2. Select + New.

\*3. Make sure that Simulated is Off. Then select Create.

Click on the device name, and then select Connect. Make a note of the device connection information on the Device Connection page - ID scope, Device ID, and Primary key. You need these values when you create your device code:






Reference:  
<https://docs.microsoft.com/bs-cyrl-ba/azure/iot-central/core/tutorial-connect-device-python>




**NEW QUESTION 10**

- (Exam Topic 3)


From the Device Provisioning Service, you create an enrollment as shown in the exhibit. (Click the Exhibit tab.)





**enrollment1**  
 Enrollment Group Details



 Save
  Refresh
  Regenerate keys


**Settings**
Registration Records

 You can view and update attestation information, set how you want to assign devices to hubs, define the re-provisioning policy and set the initial twin state of provisioning devices.

**Attestation Type**  
 Symmetric Key

**Primary Key**  
 \*\*\*\*\*
 



**Secondary Key**  
 \*\*\*\*\*
 



**IoT Edge device** 


True

False


Select how you want to assign devices to hubs
 


Evenly weighted distribution
 


Select the IoT hubs this group can be assigned to: 

iothub-contoso.azure-devices.net
 

Link a new IoT hub

Select how you want device data to be handled on re-provisioning \* 

Re-provision and migrate data
 

**Enable entry** 

Enable

Disable

You need to deploy a new IoT device.

What should you use as the device identity during attestation?

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

**Answer: C**

**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>

**NEW QUESTION 10**

- (Exam Topic 3)

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

You have devices that connect to an Azure IoT hub. Each device has a fixed GPS location that includes latitude and longitude.

You discover that a device entry in the identity registry of the IoT hub is missing the GPS location.

You need to configure the GPS location for the device entry. The solution must prevent the changes from being propagated to the physical device.

Solution: You add tags to the device twin. Does the solution meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

Instead add the desired properties to the device twin.

Note: Device Twins are used to synchronize state between an IoT solution's cloud service and its devices. Each device's twin exposes a set of desired properties

and reported properties. The cloud service populates the desired properties with values it wishes to send to the device. When a device connects it requests and/or subscribes for its desired properties and acts on them.  
Reference:  
<https://azure.microsoft.com/sv-se/blog/deep-dive-into-azure-iot-hub-notifications-and-device-twin/>

#### NEW QUESTION 14

- (Exam Topic 3)

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 question, 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 the connecting to the IoT hub.

Solution: From the IoT hub, you change the credentials for the shared access policy of the IoT devices. Does the solution meet the goal?

- A. Yes
- B. No

**Answer: B**

#### Explanation:

Reference:

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

#### NEW QUESTION 16

- (Exam Topic 3)

You have an Azure IoT hub that uses a Device Provisioning Service instance.

You have 1,000 legacy IoT devices that only support MAC address or serial number identities. The device do NOT have a security feature that can be used to securely identify the device or a hardware security module (HSM).

You plan to deploy the devices to a secure environment.

You need to configure the Device Provisioning Service instance to ensure that all the devices are identified securely before they receive updates.

Which attestation mechanism should you choose?

- A. Trusted Platform Module (TPM) 1.2 attestation
- B. symmetric key attestation
- C. X.509 certificates

**Answer: B**

#### Explanation:

A common problem with many legacy devices is that they often have an identity that is composed of a single piece of information. This identity information is usually a MAC address or a serial number. Legacy devices may not have a certificate, TPM, or any other security feature that can be used to securely identify the device. The Device Provisioning Service for IoT hub includes symmetric key attestation. Symmetric key attestation can be used to identify a device based off information like the MAC address or a serial number.

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/iot-dps/how-to-legacy-device-symm-key>

#### NEW QUESTION 17

- (Exam Topic 3)

You deploy an Azure IoT hub.

You need to demonstrate that the IoT hub can receive messages from a 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.

Actions	Answer Area
Get a service primary key for the IoT hub.	
Configure the Device Provisioning Service on the IoT hub.	
Configure the device connection string on a device client.	⬅️ ⬆️
Register a device in IoT Hub.	
Trigger a new send event from a device client.	

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:



Step 1: Register a device in IoT Hub

Before you can use your IoT devices with Azure IoT Edge, you must register them with your IoT hub. Once a device is registered, you can retrieve a connection string to set up your device for IoT Edge workloads.

Step 2: Configure the device connection string on a device client.

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.

Step 3: Trigger a new send event from a device client. Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/how-to-register-device>

### NEW QUESTION 19

- (Exam Topic 3)

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.

Actions	Answer Area
Create a custom alert rule.	
Enable Azure Security Center for IoT.	
Configure the Diagnostics settings of the IoT hub.	⬅️ ⬆️
Create a shared access policy.	➡️ ⬇️
Select a device security group.	
Create a message route.	

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

Step 1: Enable Azure Security Center for IoT

Security alerts, such as failed local IoT hub logins, are stored in AzureSecurityOfThings.SecurityAlert table in the Log Analytics workspace configured for the Azure Security Center for IoT solution.

Step 2: Select a device security group Update a device security group..

Step 3: Create a custom alert rule by creating 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>

### NEW QUESTION 22

- (Exam Topic 3)

You have an Azure IoT hub that uses a Device Provisioning Service instance to automate the deployment of Azure IoT Edge devices.

The IoT Edge devices have a Trusted Platform Module (TPM) 2.0 chip.

From the Azure portal, you plan to add an individual enrollment to the Device Provisioning Service that will use the TPM of the IoT Edge devices as the attestation mechanism.

Which detail should you obtain before you can create the enrollment.

- A. the scope ID and the Device Provisioning Service endpoint
- B. the primary key of the Device Provisioning Service shared access policy and the global device endpoint
- C. the X.509 device certificate and the certificate chain
- D. the endorsement key and the registration ID

**Answer: D**

#### Explanation:

The TPM simulator's Registration ID and the Endorsement key, are used when you create an individual enrollment for your device.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/how-to-auto-provision-simulated-device-linux>

### NEW QUESTION 26

- (Exam Topic 3)

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. Upload Sensors.csv by using the IoT Hub REST API.
- B. From the Azure subscription, select the IoT hub, select Message routing, and then configure a route to storage.

- C. From the Azure subscription, select the IoT hub, select File upload, and then configure a storage container.
- D. Configure the device to use a GET request to ContosoHub.azure-devices.net/devices/ContosoDevice1/ files/notifications.

**Answer:** AC

**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}"
}
```

Reference:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/iot-hub/iot-hub-configure-file-upload.md>

**NEW QUESTION 31**

- (Exam Topic 3)

You have 10,000 IoT devices that connect to an Azure IoT hub. The devices do not support over-the-air (OTA) updates.

You need to decommission 1,000 devices. The solution must prevent connections and autoenrollment for the decommissioned devices.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Update the connectionState device twin property on all the devices.
- B. Blacklist the X.509 root certification authority (CA) certificate for the enrollment group.
- C. Delete the enrollment entry for the devices.
- D. Remove the identity certificate from the hardware security module (HSM) of the devices.
- E. Delete the device identity from the device registry of the IoT hub.

**Answer:** BC

**Explanation:**

B: X.509 certificates are typically arranged in a certificate chain of trust. If a certificate at any stage in a chain becomes compromised, trust is broken. The certificate must be blacklisted to prevent Device Provisioning Service from provisioning devices downstream in any chain that contains that certificate.

C: Individual enrollments apply to a single device and can use either X.509 certificates or SAS tokens (in a real or virtual TPM) as the attestation mechanism. (Devices that use SAS tokens as their attestation mechanism can be provisioned only through an individual enrollment.) To blacklist a device that has an individual enrollment, you can either disable or delete its enrollment entry.

To blacklist a device that has an individual enrollment, you can either disable or delete its enrollment entry. Reference:

<https://docs.microsoft.com/en-us/azure/iot-dps/how-to-revoke-device-access-portal>

**NEW QUESTION 36**

- (Exam Topic 3)

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. From the Azure portal, navigate to Hub1 and select IoT Edg
- B. Select Edge1, and then select Manage Child Device
- C. From a Bash prompt, run the following command:az iot edge set-modules -device-id Edge1 -hub-name Hub1 -content C:\deploymentMan1.json
- D. Create an IoT Edge deployment manifest that specifies the temperature module and the route to\$upstrea
- E. From a Bush prompt, run the following command: az iot hub monitor-events-device-id Edge1 -hub-name Hub1
- F. From the Azure portal, navigate to Hub1 and select IoT Edg
- G. Select Edge1, select Device Twin, and then set the deployment manifest as a desired propert
- H. From a Bash prompt, run the following commandaz iot hub monitor-events-device-id Edge1 -hub-name Hub1
- I. Create an IoT Edge deployment manifest that specifies the temperature module and the route to\$upstrea
- J. From a Bush prompt, run the following command:az iot edge set-modules -device-id Edge1 -hub-name Hub1 -content C:\deploymentMan1.json

**Answer:** D

**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>

**NEW QUESTION 38**

- (Exam Topic 3)

You have an Azure Stream Analytics job that connects to an Azure IoT hub named Hub1445 as a streaming data source. Hub1445 is configured as shown in the exhibit. (Click the Exhibit tab.)

Hub1445 - Message routing

IoT Hub

Search (Ctrl+ /)

Failover

Properties

Locks

Export template

Explorers

Query explorer

IoT devices

Automatic Device Management

IoT Edge

IoT device configuration

Send data from your devices to endpoints that you choose.

Routes

Custom endpoints

Enrich messages - preview

Create an endpoint, and then add a route (you can add up to 100 routes from each IoT hub). Since routing is based on a matching query, a message can be sent to multiple endpoints. Messages that don't match a query are automatically sent to messages/events if you've enabled the fallback route. [Learn more](#)

Enable fallback route

+ Add

Test all routes

Delete

<input type="checkbox"/>	Name	Data Source	Routing Query	Endpoint	Enabled
<input type="checkbox"/>	Route3	DeviceMessages	true	events	false
<input type="checkbox"/>	Route2	DeviceMessages	true	BlobStorage	true
<input type="checkbox"/>	Route1	DeviceMessages	false	Telemetry	true

The Stream Analytics job fails to receive any messages from the IoT hub. What should you do to resolve the issue?

- A. Change the Route1 route query to true.
- B. Enable the Route3 route.
- C. Disable the Route2 route.
- D. Enable the fallback route.

Answer: A

Explanation:

The device telemetry is usually passed as JSON from the device through the IoT Hub - this is handled nicely by Azure Streaming Analytics queries. The IoT Hub message routing should be configured as follows: Data source: Device Telemetry Messages Routing query: true (as the routing query is an expression that evaluates to true or false for each received message, the simplest way to send all messages to the endpoint is to just supply true as the query). Reference: <https://darenmay.com/blog/azure-iot-streaming-analytics-data-lake-analytics-and-json/>

NEW QUESTION 42

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### AZ-220 Practice Exam Features:

- \* AZ-220 Questions and Answers Updated Frequently
- \* AZ-220 Practice Questions Verified by Expert Senior Certified Staff
- \* AZ-220 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* AZ-220 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The AZ-220 Practice Test Here](#)**