

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 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"/> Siothubname	<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 3

- (Exam Topic 3)

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

Answer: D

Explanation:

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/>

NEW QUESTION 4

- (Exam Topic 3)

You have an Azure IoT Central application that has a custom device template. You need to configure the device template to support the following activities:

- Return the reported power consumption.
- Configure the desired fan speed.
- Run the device reset routine.
- Read the fan serial number.

Which option should you use for each activity? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

Return the reported power consumption:

Command

Measurement

Properties

Settings

Configure the desired fan speed:

Command

Measurement

Properties

Settings

Read the fan serial number:

Command

Measurement

Properties

Settings

Run the device reset routine:

Command

Measurement

Properties

Settings

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Measurement

Telemetry/measurement is a stream of values sent from the device, typically from a sensor. For example, a sensor might report the ambient temperature.

Box 2: Property

The template can provide a writeable fan speed property

Properties represent point-in-time values. For example, a device can use a property to report the target temperature it's trying to reach. You can set writeable properties from IoT Central.

Box 3: Settings

Box 4: Command

You can call device commands from IoT Central. Commands optionally pass parameters to the device and receive a response from the device. For example, you can call a command to reboot a device in 10 seconds.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-central/core/howto-set-up-template>

NEW QUESTION 5

- (Exam Topic 3)

You need to install the Azure IoT Edge runtime on a new device that runs Windows 10 IoT Enterprise. Which four 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
<div>From an elevated PowerShell prompt, run the following command. <code>.(Invoke-WebRequest -useb https://aka.ms/iotedge-win) Invoke-Expression; Initialize-IoTEdge</code></div>	
<div>From Azure IoT Hub, create an IoT Edge device.</div>	
<div>From a Bash prompt, run the following commands. <code>curl https://packages.microsoft.com/keys/microsoft.asc gpg --dearmor > microsoft.gpg sudo cp ./microsoft.gpg /etc/apt/trusted.gpg.d/</code></div>	<div>⏪ ⏩</div>
<div>From an elevated PowerShell prompt, run the following command. <code>.(Invoke-WebRequest -useb https://aka.ms/iotedge-win) Invoke-Expression; Deploy-IoTEdge</code></div>	<div>⏪ ⏩</div>
<div>Enter the IoT Edge device connection string.</div>	
<div>From a Bash prompt, run the following commands. <code>sudo apt-get install moby-engine</code></div>	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: From Azure IoT Hub, create an IoT Edge Device
Step 2: Deploy-IoTEdge
The Deploy-IoTEdge command checks that your Windows machine is on a supported version, turns on the containers feature, and then downloads the moby runtime and the IoT Edge runtime. The command defaults to using Windows containers.
{Invoke-WebRequest -useb https://aka.ms/iotedge-win} | Invoke-Expression; ` Deploy-IoTEdge
Step 3: Initialize-IoTEdge
The Initialize-IoTEdge command configures the IoT Edge runtime on your machine. The command defaults to manual provisioning with Windows containers.
{Invoke-WebRequest -useb https://aka.ms/iotedge Step 4: Enter the IoT Edge device connection string.
When prompted, provide the device connection string that you retrieved in step 1. The device connection string associates the physical device with a device ID in IoT Hub.
Reference:
<https://docs.microsoft.com/en-us/azure/iot-edge/module-composition>

NEW QUESTION 6

- (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 archive 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/iot-hub/iot-hub-troubleshoot-connectivity>

NEW QUESTION 7

- (Exam Topic 3)

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. Configure the devices for extended offline operations.
- B. Configure the upstream protocol of the devices to use MQTT over WebSocket.
- C. Connect the external networks to the IoT solution by using ExpressRoute.
- D. Configure the devices to use an HTTPS proxy.

Answer: B

Explanation:

MQTT over WebSockets uses port 443. Reference:
<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-protocols>

NEW QUESTION 8

- (Exam Topic 3)

You have an Azure IoT hub that is being taken from prototype to production. You plan to connect IoT devices to the IoT hub. The devices have hardware security modules (HSMs). You need to use the most secure authentication method between the devices and the IoT hub. Company policy prohibits the use of internally generated certificates. Which authentication method should you use?

- A. an X.509 self-signed certificate
- B. a certificate thumbprint
- C. a symmetric key
- D. An X.509 certificate signed by a root certification authority (CA).

Answer: D

Explanation:

Purchase X.509 certificates from a root certificate authority (CA). This method is recommended for production environments. The hardware security module, or HSM, is used for secure, hardware-based storage of device secrets, and is the most secure form of secret storage. Both X.509 certificates and SAS tokens can be stored in the HSM
Reference:
<https://docs.microsoft.com/en-us/azure/iot-dps/concepts-security>

NEW QUESTION 9

- (Exam Topic 3)

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.

Actions

Answer Area

Create an individual device enrollment by using the Device Provisioning Service.

Run the following commands.

```
sudo apt-get install moby-engine  
sudo apt-get install moby-cli  
sudo apt-get install iotedge
```

Add the connection string to the /etc/iotedge/config.yaml file, and then run the following command.

```
sudo systemctl restart iotedge
```

Install the IoT edge repository for Ubuntu Server 18.04 on the physical device. From IoT Hub, create a new IoT Edge device.

From IoT Hub, create an IoT Edge device registry entry.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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>

NEW QUESTION 10

- (Exam Topic 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

Answer: B

Explanation:

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/>

NEW QUESTION 10

- (Exam Topic 3)

You have an Azure IoT solution that includes an Azure IoT hub.

You receive a root certification authority (CA) certificate from the security department at your company. You need to configure the IoT hub to use the root CA certificate.

Which four 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

Generate a verification code.

Upload the verification certificate.

Upload the root CA certificate to the IoT hub.

Copy the thumbprint from root CA certificate.

Generate a verification certificate.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/bs-latn-ba/azure/iot-hub/iot-hub-security-x509-get-started>

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 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

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.

Answer Area

⏪

⏩

⏴

⏵

- 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)
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 use an Azure policy to apply tags to a resource group. 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 20

- (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 21

- (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 the desired properties to the device twin. Does the solution meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

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 22

- (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 25

- (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 30

- (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.

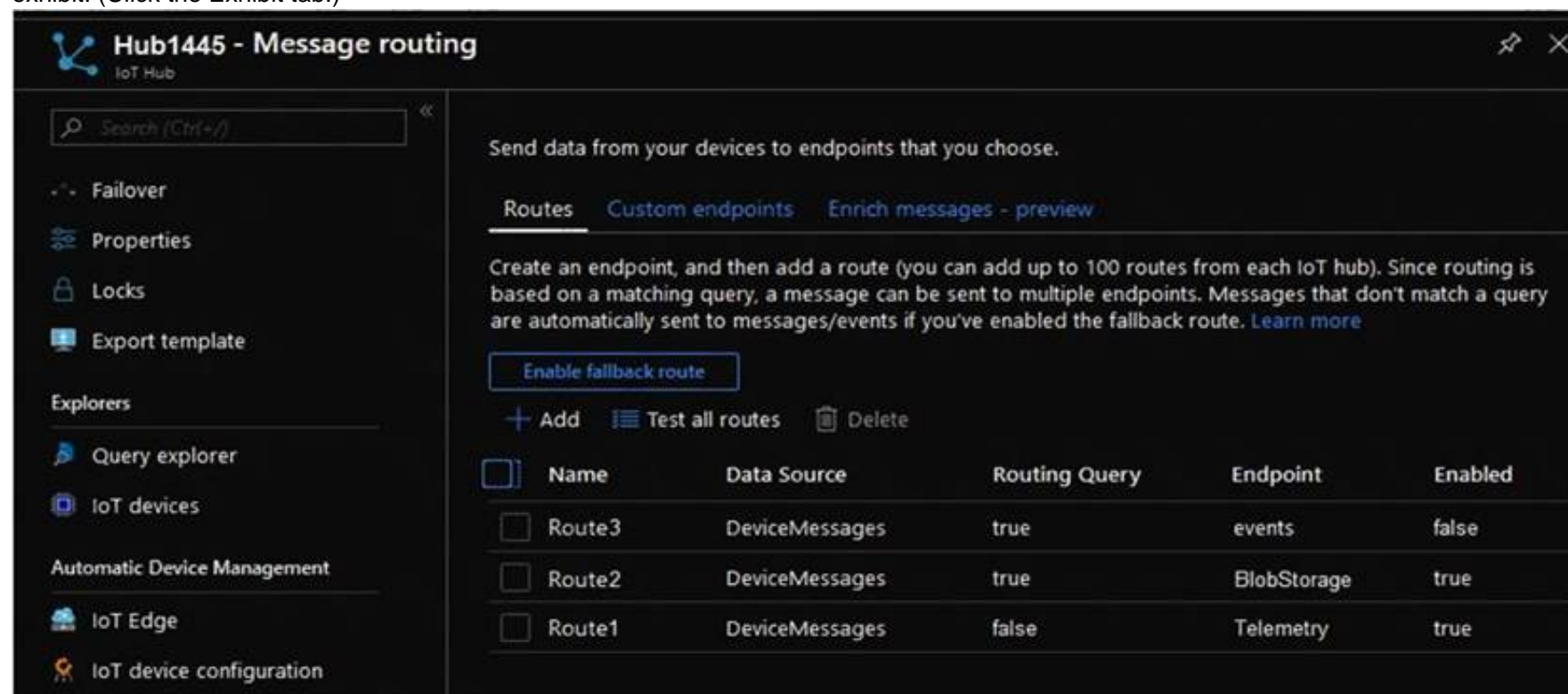
Use the following command to apply the configuration to an IoT Edge device:

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 35

- (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.)



Name	Data Source	Routing Query	Endpoint	Enabled
Route3	DeviceMessages	true	events	false
Route2	DeviceMessages	true	BlobStorage	true
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 36

- (Exam Topic 3)

You use Azure Security Center in an Azure IoT solution.

You need to exclude some security events. The solution must minimize development effort. What should you do?

- A. Create an Azure function to filter security messages.
- B. Add a configuration to the code of the physical IoT device.
- C. Add configuration details to the device twin object.
- D. Create an azureiotsecurity module twin and add configuration details to the module twin object.

Answer: D

Explanation:

Properties related to every Azure Security Center for IoT security agent are located in the agent configuration object, within the desired properties section, of the azureiotsecurity module.

To modify the configuration, create and modify this object inside the azureiotsecurity module twin identity. Note: Azure Security Center for IoT's security agent twin configuration object is a JSON format object. The configuration object is a set of controllable properties that you can define to control the behavior of the agent. These configurations help you customize the agent for each scenario required. For example, automatically excluding some events, or keeping power consumption to a minimal level are possible by configuring these properties.

Reference:

<https://docs.microsoft.com/en-us/azure/asc-for-iot/how-to-agent-configuration>

NEW QUESTION 38

.....

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](#)