

Microsoft

Exam Questions AZ-220

Microsoft Azure IoT Developer



NEW QUESTION 1

- (Exam Topic 1)

What should you do to identify the cause of the connectivity issues?

- A. Send cloud-to-device messages to the IoT devices.
- B. Use the heartbeat pattern to send messages from the IoT devices to iotHub1.
- C. Monitor the connection status of the device twin by using an Azure function.
- D. Enable the collection of the Connections diagnostics logs and set up alerts for the connected devices count metric.

Answer: D

Explanation:

Scenario: You discover connectivity issues between the IoT gateway devices and iotHub1, which cause IoT devices to lose connectivity and messages.

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.

Step 1:

- *1. Sign in to the Azure portal.
- *2. Browse to your IoT hub.
- *3. Select Diagnostics settings.
- *4. Select Turn on diagnostics.
- *5. Enable Connections logs to be collected.
- *6. For easier analysis, turn on Send to Log Analytics (see pricing).

Step 2:

Set up alerts for device disconnect at scale

To get alerts when devices disconnect, configure alerts on the Connected devices (preview) metric. Reference:

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

NEW QUESTION 2

- (Exam Topic 3)

You have the devices shown in the following table.

Name	Type	Hardware configuration
Device1	Azure Sphere microcontroller unit (MCU)	4 MB of RAM ARM processor
Device2	Raspberry Pi single board computer (SBC)	1 GB of RAM ARM processor
Device3	Desktop computer	8 GB of RAM x64 processor
Device4	Apple iPhone	4 GB of RAM ARM processor

You are implementing a proof of concept (POC) for an Azure IoT solution. You need to deploy an Azure IoT Edge device as part of the POC.

On which two devices can you deploy IoT Edge? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Device1
- B. Device2
- C. Device3
- D. Device4

Answer: BC

Explanation:

Azure IoT Edge runs great on devices as small as a Raspberry Pi3 to server grade hardware. Tier 1.

The systems listed in the following table are supported by Microsoft, either generally available or in public preview, and are tested with each new release.

Operating System	AMD64	ARM32v7	ARM64
Raspbian Stretch		✓	
Ubuntu Server 16.04	✓		Public preview
Ubuntu Server 18.04	✓		Public preview
Windows 10 IoT Core, build 17763	✓		
Windows 10 IoT Enterprise, build 17763	✓		
Windows Server 2019, build 17763	✓		
Windows Server IoT 2019, build 17763	✓		

Reference:
<https://docs.microsoft.com/en-us/azure/iot-edge/support>

NEW QUESTION 3

- (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 4

- (Exam Topic 3)

You have an Azure IoT solution that includes several Azure IoT hubs.
 A new alerting feature was recently added to the IoT devices. The feature uses a new device twin reported property named alertCondition.
 You need to send alerts to an Azure Service Bus queue named MessageAlerts. The alerts must include alertCondition and the name of the IoT hub.
 Which two actions should you perform? Each Answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Configure File upload for each IoT hu
- B. Configure the device to send a file to an Azure Storage container that contains the device name and status message.
- C. Add the following message enrichments: Name = iotHubNameValue = \$twin.tag.location Endpoint = MessageAlert
- D. Create an IoT Hub routing rule that has a data source of Device Twin Change Events and select the endpoint for MessageAlerts.
- E. Add the following message enrichments: Name = iotHubName Value = \$iothubnameEndpoint = MessageAlert
- F. Create an IoT Hub routing rule that has a data source of Device Telemetry Messages and select the endpoint for MessageAlerts.

Answer: BD

Explanation:

B: Message enrichments is the ability of the IoT Hub to stamp messages with additional information before the messages are sent to the designated endpoint. One reason to use message enrichments is to include data that can be used to simplify downstream processing. For example, enriching device telemetry messages with

a device twin tag can reduce load on customers to make device twin API calls for this information. D: Applying enrichments

The messages can come from any data source supported by IoT Hub message routing, including the following examples:

-->device twin change notifications -- changes in the device twin device telemetry, such as temperature or pressure

device life-cycle events, such as when the device is created or deleted Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-message-enrichments-overview>

NEW QUESTION 5

- (Exam Topic 3)

You have an existing Azure IoT hub.

You need to connect physical IoT devices to the IoT hub.

You are connecting the devices through a firewall that allows only port 443 and port 80.

Which three communication protocols can you use? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. MQTT over WebSocket
- B. AMQP
- C. AMQP over WebSocket
- D. MQTT
- E. HTTPS

Answer: ACE

Explanation:

MQTT over WebSockets, AMQP over WebSocket, and HTTPS use port 443. Reference:

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

NEW QUESTION 6

- (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 NOT 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 NOT 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	Answer Area								
<div>AMQP</div>									
<div>HTTPS</div>									
<div>MQTT</div>									
	<table><thead><tr><th>Device</th><th>Protocol</th></tr></thead><tbody><tr><td>Transparent Field Gateway Device:</td><td><div>Protocol</div></td></tr><tr><td>Low Resource Device:</td><td><div>Protocol</div></td></tr><tr><td>Limited Sensor Device:</td><td><div>Protocol</div></td></tr></tbody></table>	Device	Protocol	Transparent Field Gateway Device:	<div>Protocol</div>	Low Resource Device:	<div>Protocol</div>	Limited Sensor Device:	<div>Protocol</div>
Device	Protocol								
Transparent Field Gateway Device:	<div>Protocol</div>								
Low Resource Device:	<div>Protocol</div>								
Limited Sensor Device:	<div>Protocol</div>								

- 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 7

- (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:

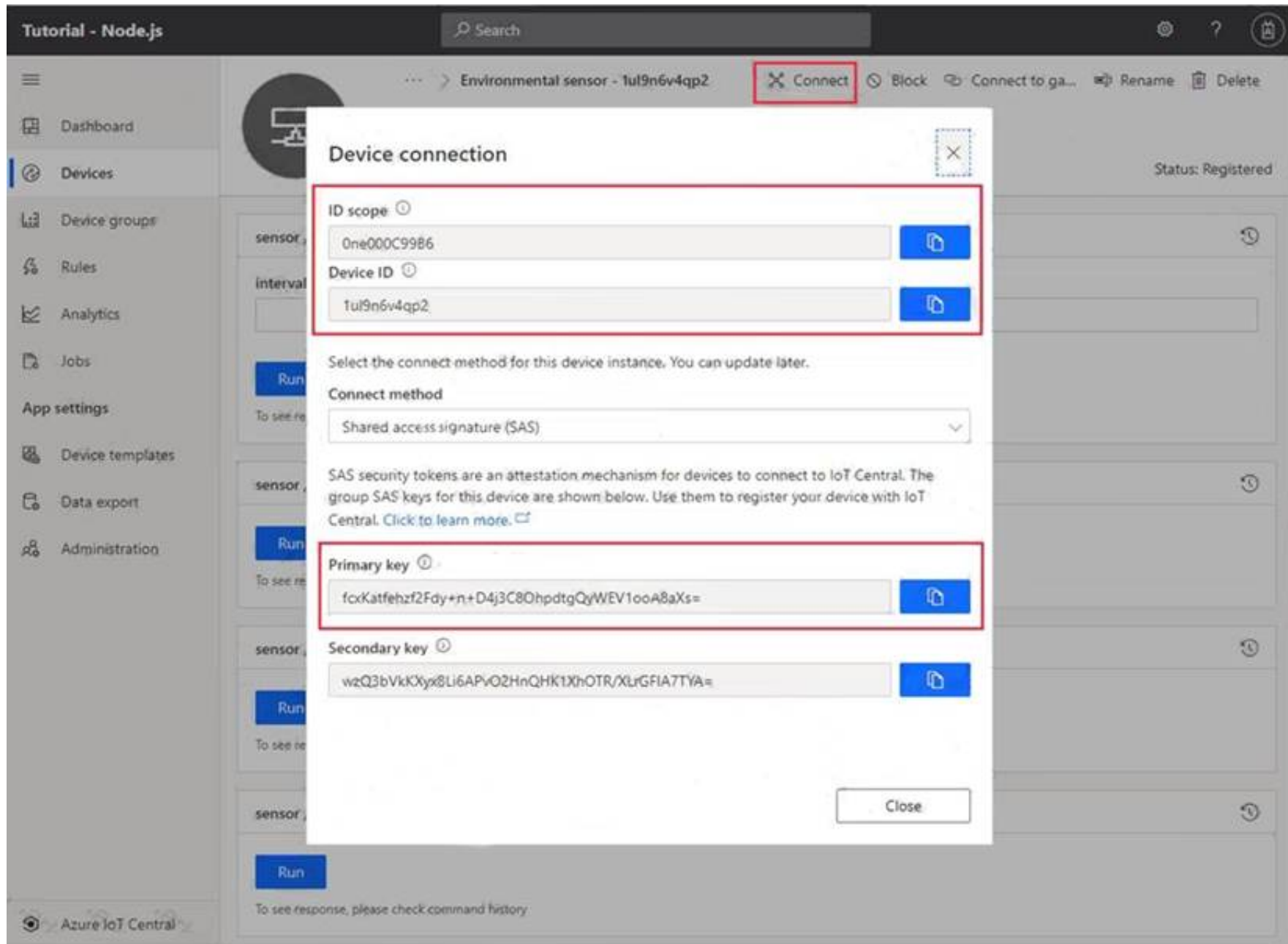
In your Azure IoT Central application, add a real device to the device template

*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 8

- (Exam Topic 3)

You have three Azure IoT hubs named Hub1, Hub2, and Hub3, a Device Provisioning Service instance, and an IoT device named Device1. Each IoT hub is deployed to a separate Azure region. Device enrollment uses the Lowest latency allocation policy. The Device Provisioning Service uses the Lowest latency allocation policy. Device1 is auto-provisioned to Hub1 by using the Device Provisioning Service. Device1 regularly moves between regions. You need to ensure that Device1 always connects to the IoT hub that has the lowest latency. What should you do?

- A. Configure device attestation that uses X.509 certificates.
- B. Implement device certificate rolling.
- C. Disenroll and reenroll Device1.
- D. Configure the re-provisioning policy.

Answer: D

Explanation:

Automated re-provisioning support.

Microsoft added first-class support for device re-provisioning which allows devices to be reassigned to a different IoT solution sometime after the initial solution assignment. Re-provisioning support is available in two options:

Factory reset, in which the device twin data for the new IoT hub is populated from the enrollment list instead of the old IoT hub. This is common for factory reset scenarios as well as leased device scenarios. Migration, in which device twin data is moved from the old IoT hub to the new IoT hub. This is common for scenarios in which a device is moving between geographies.

Reference:

<https://azure.microsoft.com/en-us/blog/new-year-newly-available-iot-hub-device-provisioning-service-features/>

NEW QUESTION 9

- (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 10

- (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.	<div>⬅️⬆️</div>
Create a shared access policy.	<div>⬆️⬇️</div>
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 10

- (Exam Topic 3)
You have an instance of Azure Time Series Insights and an Azure IoT hub that receives streaming telemetry from IoT devices.
You need to configure Time Series Insights to receive telemetry from 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
Configure the Time Series Insights event source to connect to an existing IOT hub.	
Create an Azure event hub.	
Add a new Time Series Insights event source.	<div>⬅️⬆️</div>
Increase the events retention to seven days for the built-in endpoints of the IoT hub.	<div>⬆️⬇️</div>
Create a dedicated consumer group in the built-in events endpoints of the IoT hub.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Create a dedicated consumer group.. Add a consumer group to your IoT hub.

Applications use consumer groups to pull data from Azure IoT Hub. To reliably read data from your IoT hub, provide a dedicated consumer group that's used only by this Time Series Insights environment.

Step 2: Add a new Time Series Insights event source. Add a new event source

- Sign in to the Azure portal.
- In the left menu, select All resources. Select your Time Series Insights environment.
- Under Settings, select Event Sources, and then select Add.
- In the New event source pane, for Event source name, enter a name that's unique to this Time Series Insights environment. For example, enter event-stream.

Step 3: Configure the Time Series event source to connect to an existing IOT hub Step 4: For Source, select IoT Hub.

Step 5: Select a value for Import option:

If you already have an IoT hub in one of your subscriptions, select Use IoT Hub from available subscriptions. This option is the easiest approach.

Reference:

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

NEW QUESTION 13

- (Exam Topic 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 IoT Edge module
- C. the \$edgeAgent module twin
- D. the Azure IoT Hub device twin

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>

NEW QUESTION 18

- (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: You delete the enrollment group from the Device Provisioning Service. Does the solution meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

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>

NEW QUESTION 20

- (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 23

- (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 26

.....

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](#)