

AZ-220 Dumps

Microsoft Azure IoT Developer

<https://www.certleader.com/AZ-220-dumps.html>



NEW QUESTION 1

- (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

| | |
|-------------------|----------------------|
| \$iothubname | desired.pressure |
| \$twin | fanSpeed.reported |
| \$twin.properties | reported.fanSpeed |
| \$twin.results | temperature |
| \$twin.tags | 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 2

- (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 3

- (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:

Configure the desired fan speed:

Read the fan serial number:

Run the device reset routine:

- 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 4

- (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 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 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 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 10 IoT devices that connect to an Azure IoT hub named Hub1.

From Azure Cloud Shell, you run `az iot hub monitor-events --hub-name Hub1` and receive the following error message: "az iot hub: 'monitor-events' is not in the 'az iot hub' command group. See 'az iot hub

--help'."

You need to ensure that you can run the command successfully. What should you run first?

- A. `az iot hub monitor-feedback --hub-name Hub1`
- B. `az iot hub generate-sas-token --hub-name Hub1`
- C. `az iot hub configuration list --hub-name Hub1`
- D. `az extension add -name azure-cli-iot-ext`

Answer: D

Explanation:

Execute `az extension add --name azure-cli-iot-ext` once and try again.

In order to read the telemetry from your hub by CLI, you have to enable IoT Extension with the following commands:

Add: `az extension add --name azure-cli-iot-ext` Reference:

<https://github.com/MicrosoftDocs/azure-docs/issues/20843>

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 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 10

- (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 10

- (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. <pre>sudo apt-get install moby-engine sudo apt-get install moby-cli sudo apt-get install iotedge</pre> | |
| Add the connection string to the /etc/iotedge/config.yaml file, and then run the following command. <pre>sudo systemctl restart iotedge</pre> | <div>⏪ ⏩</div> <div>⏴ ⏵</div> |
| 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 13

- (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)

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 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.

Does the solution meet the goal?

A. Yes

B. No

Answer: A

Explanation:

You may find it necessary to deprovision devices that were previously auto-provisioned through the Device Provisioning Service.

In general, deprovisioning a device involves two steps:

*1. Disenroll the device from your provisioning service, to prevent future auto-provisioning. Depending on whether you want to revoke access temporarily or permanently, you may want to either disable or delete an enrollment entry.

*2. Deregister the device from your IoT Hub, to prevent future communications and data transfer. Again, you can temporarily disable or permanently delete the device's entry in the identity registry for the IoT Hub where it was provisioned.

Reference:

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

NEW QUESTION 20

- (Exam Topic 3)

You have 1,000 devices that connect to a standard tier Azure IoT hub.

All the devices are commissioned and send telemetry events to the built-in IoT Hub endpoint. You configure message enrichment on the events endpoint and set the enrichment value to \$twin.tags.ipV4.

When you inspect messages on the events endpoint, you discover that all the messages are stamped with a string of "\$twin.tags.ipV4".

What are two possible causes of the issue? Each Answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. The ipV4 tag is a restricted twin property that is unavailable for message enrichment.

B. A standard tier IoT hub does not support device twin properties in message enrichments.

C. The device sending the message has no device twin.

D. Message enrichment cannot be added to messages going to a built-in endpoint.

E. The device twin path used for the value of the enrichment does not exist.

F. The device twin property value used for message enrichment is set to "\$twin.tags.ipV4".

Answer: CE

Explanation:

In some cases, if you are applying an enrichment with a value set to a tag or property in the device twin, the value will be stamped as a string value. For example, if an enrichment value is set to \$twin.tags.field, the messages will be stamped with the string "\$twin.tags.field" rather than the value of that field from the twin.

This happens in the following cases:

(C) Your IoT Hub is in the standard tier, but the device sending the message has no device twin.

(E) Your IoT Hub is in the standard tier, but the device twin path used for the value of the enrichment does not exist. For example, if the enrichment value is set to \$twin.tags.location, and the device twin does not have a location property under tags, the message is stamped with the string "\$twin.tags.location".

Your IoT Hub is in the basic tier. Basic tier IoT hubs do not support device twins. Reference:

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

NEW QUESTION 22

- (Exam Topic 3)

You have 100 devices that connect to an Azure IoT hub.

You plan to use Azure functions to process all the telemetry messages from the devices before storing the messages.

You need to configure the functions binding for the IoT hub.

Which two configuration details should you use to configure the binding? Each Answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. the name of the resource group that contains the IoT hub
- B. the IoT hub's connection string shared access key that has Service connect permissions
- C. the connection string of the Azure Event Hub-compatible endpoint from the IoT Hub built-in endpoints
- D. the Azure Event-Hub compatible name

Answer: CD

Explanation:

EventHubName: Functions 2.x and higher. The name of the event hub. When the event hub name is also present in the connection string, that value overrides this property at runtime.

Connection: The name of an app setting that contains the connection string to the event hub's namespace. Copy this connection string by clicking the Connection Information button for the namespace, not the event hub itself. This connection string must have send permissions to send the message to the event stream.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-event-iot-output>

NEW QUESTION 23

- (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 26

- (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 28

- (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 31

- (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. | ⬅️ ⬆️ |
| Increase the events retention to seven days for the built-in endpoints of the IoT hub. | ➡️ ⬇️ |
| 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 34

- (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 39

- (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 41

- (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 45

• • • • •

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your AZ-220 Exam with Our Prep Materials Via below:

<https://www.certleader.com/AZ-220-dumps.html>