AZ-220 Q&As

Microsoft Azure IoT Developer

Pass Microsoft AZ-220 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/az-220.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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 correct 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".

Correct Answer: CE

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

QUESTION 2

You have an Azure IoT solution.

You plan to register an Azure IoT Edge device by using X.509 self-signed certificates.

You need to provide the thumbprint for the primary and secondary certificates.

Solution: You generate a 64-hex character SHA256 hash for the certificates.

Does this meet the goal?

A. Yes

B. No

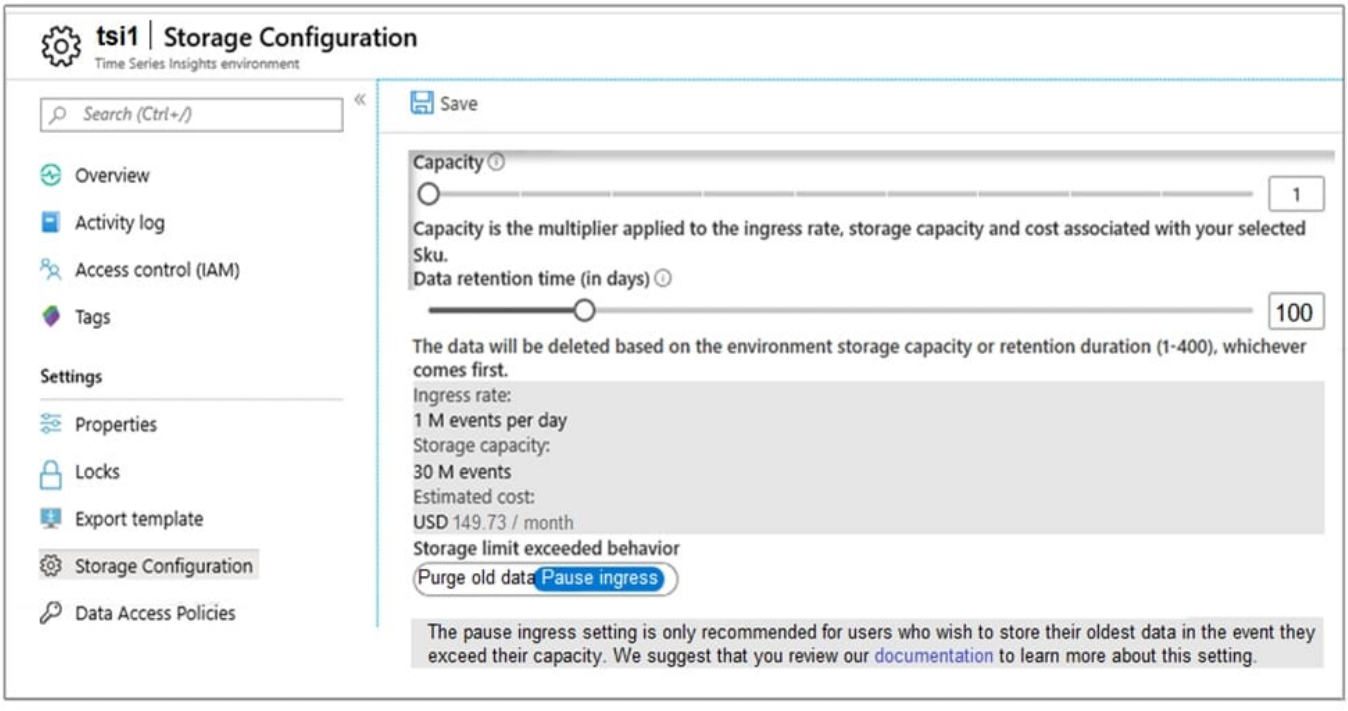
Correct Answer: B

QUESTION 3

HOTSPOT

You have an Azure IoT hub named Hub1 and an Azure Time Series Insights environment named tsi1. Tsi1 connects to Hub1. The solution has been operational for 6 months.

Tsi1 is configured as shown in the following exhibit.



Hub1 receives 1 million messages per day. Each message is up to 1 KB and is formatted as JSON.

Hub1 has seven days of retained telemetry.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:

Statement	Yes	No
Tsi1 will display 100 days of telemetry.	○	○
Tsi1 will display telemetry that arrived three months ago.	○	○
Tsi1 will display real-time data after the Time Series Insights environment has been connected to the event source of Hub1 for two days.	○	○

Correct Answer:

Statement	Yes	No
Tsi1 will display 100 days of telemetry.	○	○
Tsi1 will display telemetry that arrived three months ago.	○	○
Tsi1 will display real-time data after the Time Series Insights environment has been connected to the event source of Hub1 for two days.	○	○

Reference: https://docs.microsoft.com/en-us/azure/time-series-insights/time-series-insights-overview

QUESTION 4

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

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

You have a Standard tier Azure IoT hub and a fleet of IoT devices.

The devices connect to the IoT hub by using either Message Queuing Telemetry Transport (MQTT) or Advanced Message Queuing Protocol (AMQP).

You need to send data to the IoT devices and each device must respond. Each device will require three minutes to process the data and respond.

Solution: You use direct methods and check the response.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

IoT Hub provides three options for device apps to expose functionality to a back-end app:

Twin\\'s desired properties for long-running commands intended to put the device into a certain desired state. For example, set the telemetry send interval to 30 minutes.

Direct methods for communications that require immediate confirmation of the result. Direct methods are often used for interactive control of devices such as turning on a fan.

Cloud-to-device messages for one-way notifications to the device app.

Reference:

https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-c2d-guidance

QUESTION 5

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 devices 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

Correct Answer: B

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