AZ-220 Q&As

Microsoft Azure IoT Developer

Pass Microsoft AZ-220 Exam with 100% Guarantee

QUESTION 1

DRAG DROP

You have an Azure IoT Edge solution.

You plan to deploy an Azure Security Center for IoT security agent. You need to configure the security agent to meet the following requirements:

1.

Connection events must be reported as high priority.

2.

High priority events must be collected every seven minutes.

How should you configure the azureiotsecurity module twin? To answer, drag the appropriate values to the correct locations. Each value 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.

Select and Place:

```
"desired": {
"reported": {
"highPriorityMessageFrequency": {
"lowPriorityMessageFrequency": {
"eventPriorityConnectionCreate": {
"eventPriorityProcessCreate": {
"aggregationIntervalConnectionCreate": {
```

Answer Area

```
[                    ]
  "ms_iotn:urn_azureiot_Security_SecurityAgentConfiguration": {
      [                    ]
           "value": "PT7M"
      },
      [                    ]
           "value": "High"
      }
    }
}
```

Correct Answer:

```
"reported": {

"lowPriorityMessageFrequency": {

"eventPriorityProcessCreate": {
"aggregationIntervalConnectionCreate": {
```

Answer Area

```
"desired": {
  "ms_iotn:urn_azureiot_Security_SecurityAgentConfiguration": {
      "highPriorityMessageFrequency": {
            "value": "PT7M"
      },
      "eventPriorityConnectionCreate": {
            "value": "High"
      }
  }
}
```

Box 1: "desired": {

To configure connection events as high priority and collect high priority events every 7 minutes, use the following configuration.

"desired": { "ms_iotn:urn_azureiot_Security_SecurityAgentConfiguration": { "highPriorityMessageFrequency": {

"value": "PT7M"

},

"eventPriorityConnectionCreate": {

"value": "High"

}

Box 2: "highPriorityMessageFrequency ": { Box 3: "eventPriorityConnectionCreate": { Reference:

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

QUESTION 2

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 an Azure IoT solution that includes an Azure IoT hub and an Azure IoT Edge device.

You plan to deploy 10 Bluetooth sensors. The sensors do not support MQTT, AMQP, or HTTPS.

You need to ensure that all the sensors appear in the IoT hub as a single device.

Solution: You configure the IoT Edge device as an IoT Edge transparent gateway. You configure the sensors to connect to the device.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

IoT Edge transparent gateways support only the MQTT or AMQP protocols.

Instead use a translation gateway.

IoT Hub. The translation module receives messages from downstream devices, translates them into a supported protocol, and then the IoT Edge device sends the messages on behalf of the downstream devices. All information looks like it is

coming from one device, the gateway.

Reference:

https://docs.microsoft.com/en-us/azure/iot-edge/iot-edge-as-gateway

QUESTION 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 Edge. Select Edge1, and then select Manage Child Devices. From a Bash prompt, run the following command: az iot edge set-modules -device-id Edge1 -hub-name Hub1 -content C:\deploymentMan1.json

B. Create an IoT Edge deployment manifest that specifies the temperature module and the route to $upstream. From a Bash prompt, run the following command: az iot hub monitor-events-device-id Edge1 -hub-name Hub1

C. From the Azure portal, navigate to Hub1 and select IoT Edge. Select Edge1, select Device Twin, and then set the deployment manifest as a desired property. From a Bash prompt, run the following command: az iot hub monitor-events-device-id Edge1 -hub-name Hub1

D. Create an IoT Edge deployment manifest that specifies the temperature module and the route to $upstream. From a Bash prompt, run the following command: az iot edge set-modules -device-id Edge1 -hub-name Hub1 -content C:\deploymentMan1.json

Correct Answer: D

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

---

QUESTION 4

DRAG DROP

You have an Azure IoT hub named Hub1 and a root certification authority (CA) named CA1. Hub1 is configured to use X.509 certificate device authentication.

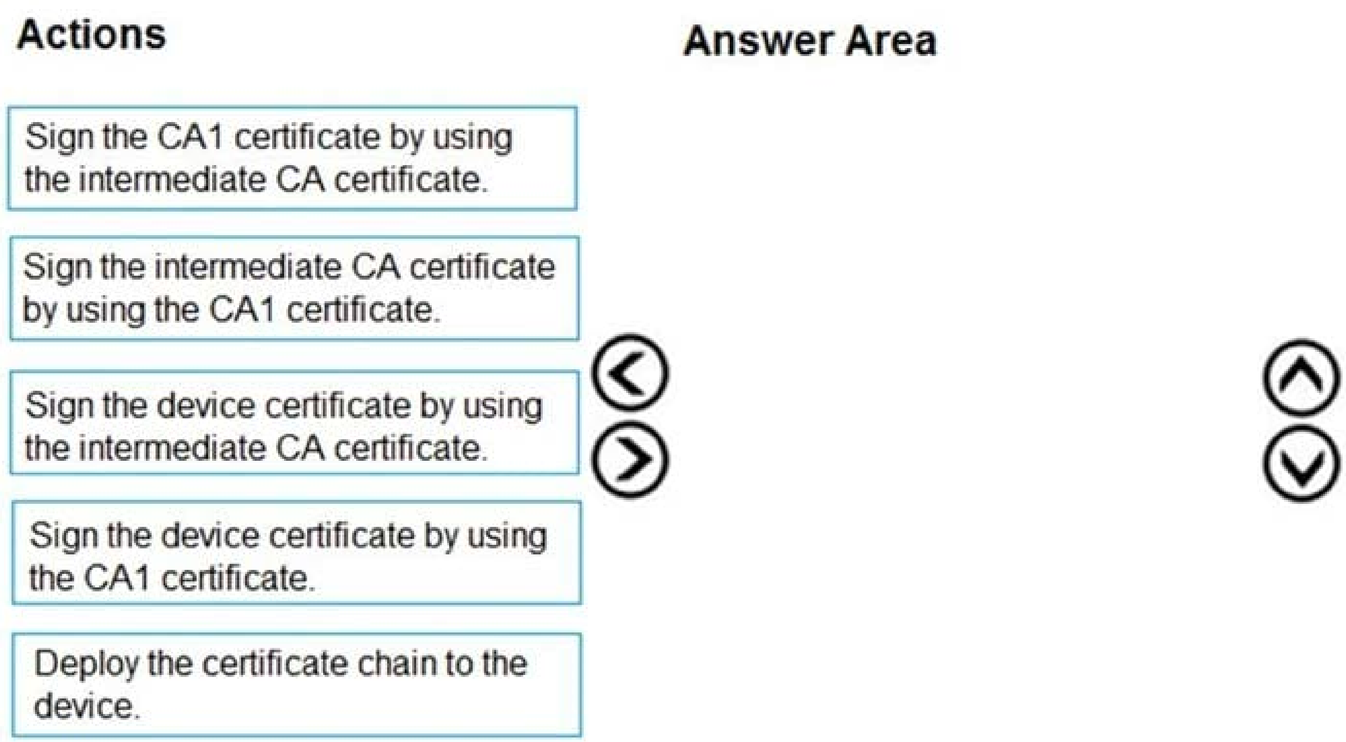
You and a custom manufacturing partner complete a proof of possession flow.

You plan to deploy IoT devices manufactured by the custom manufacturing partner. Each device will have a certificate generated by an intermediate CA. The devices will authenticate by using device certificates signed by the partner.

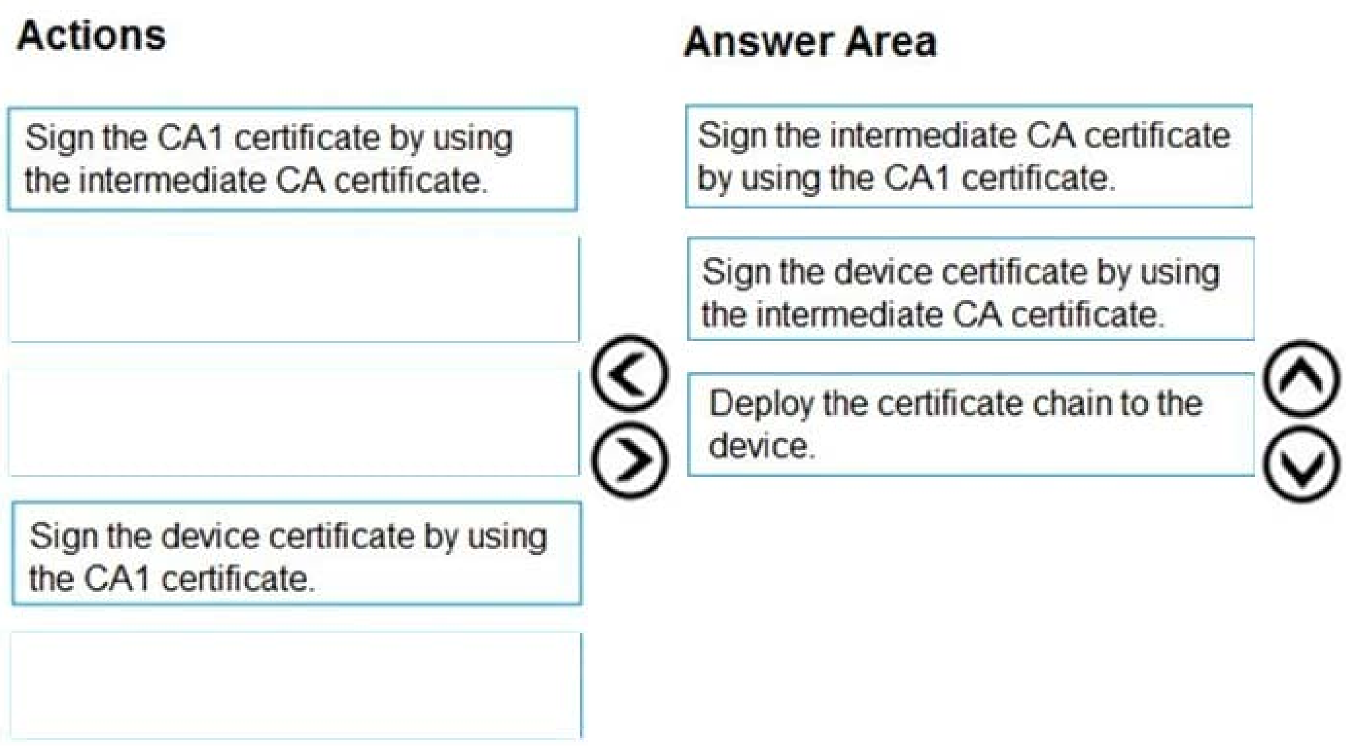
You need to ensure that the custom devices can connect successfully to Hub1.

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.

Select and Place:



Correct Answer:



Box 1: Sign the intermediate CA certificate by using the CA1 certificate.

X.509 certificates are typically arranged in a certificate chain of trust in which each certificate in the chain is signed by the private key of the next higher certificate, and so on, terminating in a self-signed root certificate. This arrangement establishes a delegated chain of trust from the root certificate generated by a trusted root certificate authority (CA) down through each intermediate CA to the end-entity "leaf" certificate installed on a device.

Box 2: Sign the device certificate by using the intermediate CA

An intermediate certificate is an X.509 certificate, which has been signed by the root certificate (or by another intermediate certificate with the root certificate in its chain). The last intermediate certificate in a chain is used to sign the leaf

certificate. An intermediate certificate can also be referred to as an intermediate CA certificate.

Box 3: Deploy the certificate chain to the device.

The leaf certificate, or end-entity certificate, identifies the certificate holder. It has the root certificate in its certificate chain as well as zero or more intermediate certificates. The leaf certificate is not used to sign any other certificates. It uniquely

identifies the device to the provisioning service and is sometimes referred to as the device certificate. During authentication, the device uses the private key associated with this certificate to respond to a proof of possession challenge from the

service.

Reference: https://docs.microsoft.com/en-us/azure/iot-dps/concepts-x509-attestation

QUESTION 5

HOTSPOT

You have an Azure subscription that contains an Azure IoT hub named Hub1 and the IoT devices shown in the following table.

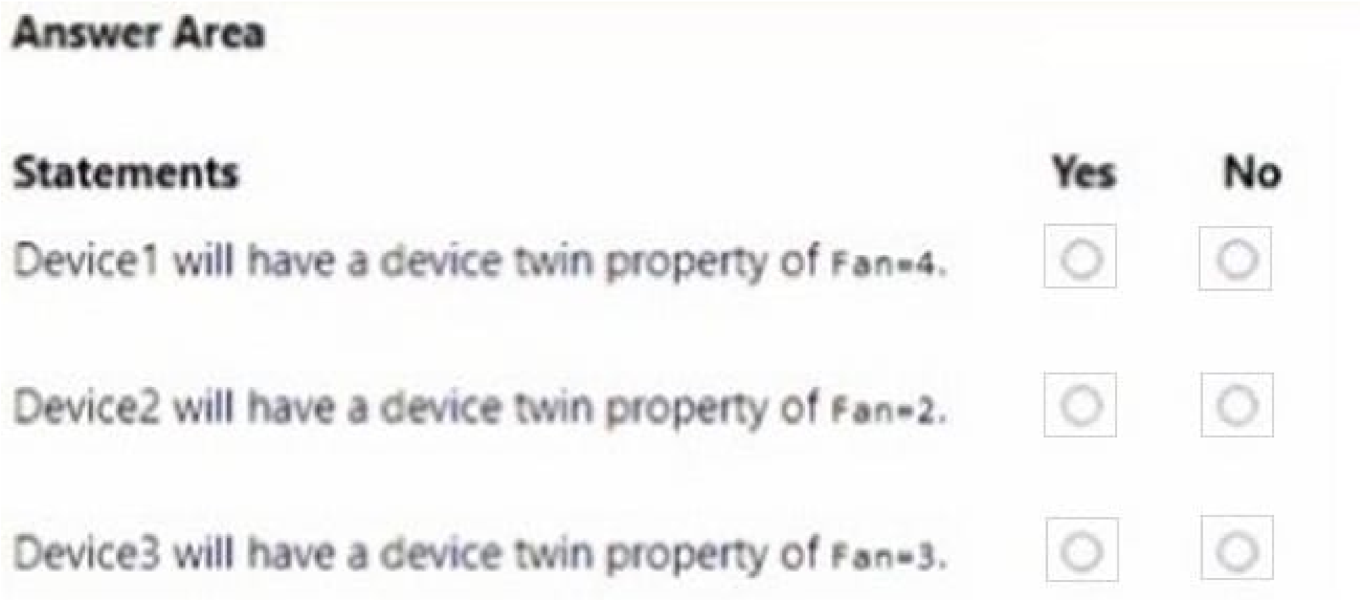
Name	Tag: "location"	Tag: "environment"	Date registered in Hub1
Device1	East	Test	January 15
Device2	East	Prod	March 12, 2022
Device3	East	Prod	April 1, 2022

You have the automatic device configure rations shown in the following table.

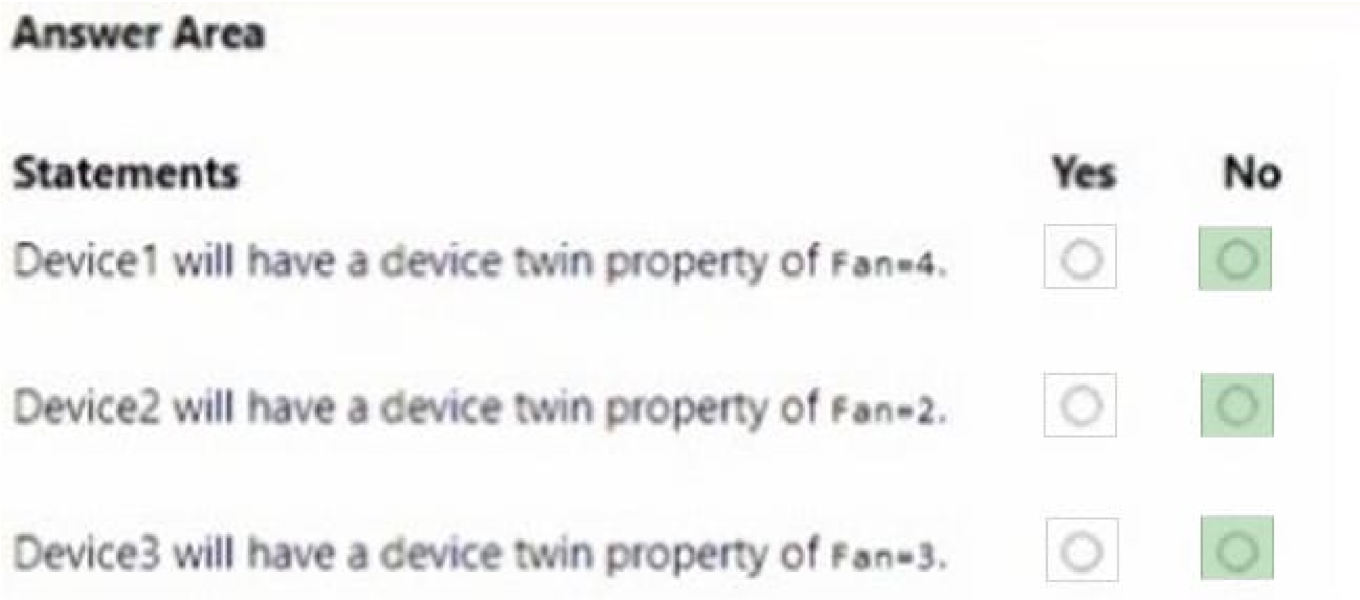
Name	Device twin property	Date configuration added	Target condition	Priority
Conf1	Fan=1	January 1, 2022	tags.location = 'East' AND tags.environment = 'Test'	10
Conf2	Fan=2	March 1, 2022	tags.location = 'East' AND tags.environment = 'Prod'	10
Conf3	Fan=3	March 15, 2022	tags.location = 'East' AND tags.environment = 'Prod'	10
Conf4	Fan=4	February 22, 2022	tags.location = 'East' AND tags.environment = 'Test'	20

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:



Correct Answer:



[Latest AZ-220 Dumps](#) [AZ-220 PDF Dumps](#) [AZ-220 Practice Test](#)