AZ-220 Q&As

Microsoft Azure IoT Developer

Pass Microsoft AZ-220 Exam with 100% Guarantee

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

QUESTION 1

You have an Azure IoT Central application.

You add an IoT device named Oven1 to the application. Oven1 uses an IoT Central template for industrial ovens.

You need to send an email to the managers group at your company as soon as the oven temperature falls below 400 degrees.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create a SendGrid account in the same resource group as the IoT Central application.

B. Add a condition that has Time Aggregation set to Off.

C. Add a condition that has Aggregation set to Minimum.

D. Add the Manager role to the IoT Central application.

E. From IoT Central, create a telemetry rule for the template.

Correct Answer: BE

Devices use telemetry to send numerical data from the device. A rule triggers when the selected telemetry crosses a specified threshold.

E: To create a telemetry rule, the device template must include at least one telemetry value. The rule monitors the temperature reported by the device and sends an email when it falls below 400 degrees.

B: Configure the rule conditions.

Conditions define the criteria that the rule monitors. In this tutorial, you configure the rule to fire when the temperature exceeds 70?F.

1.

Select Temperature in the Telemetry dropdown.

2.

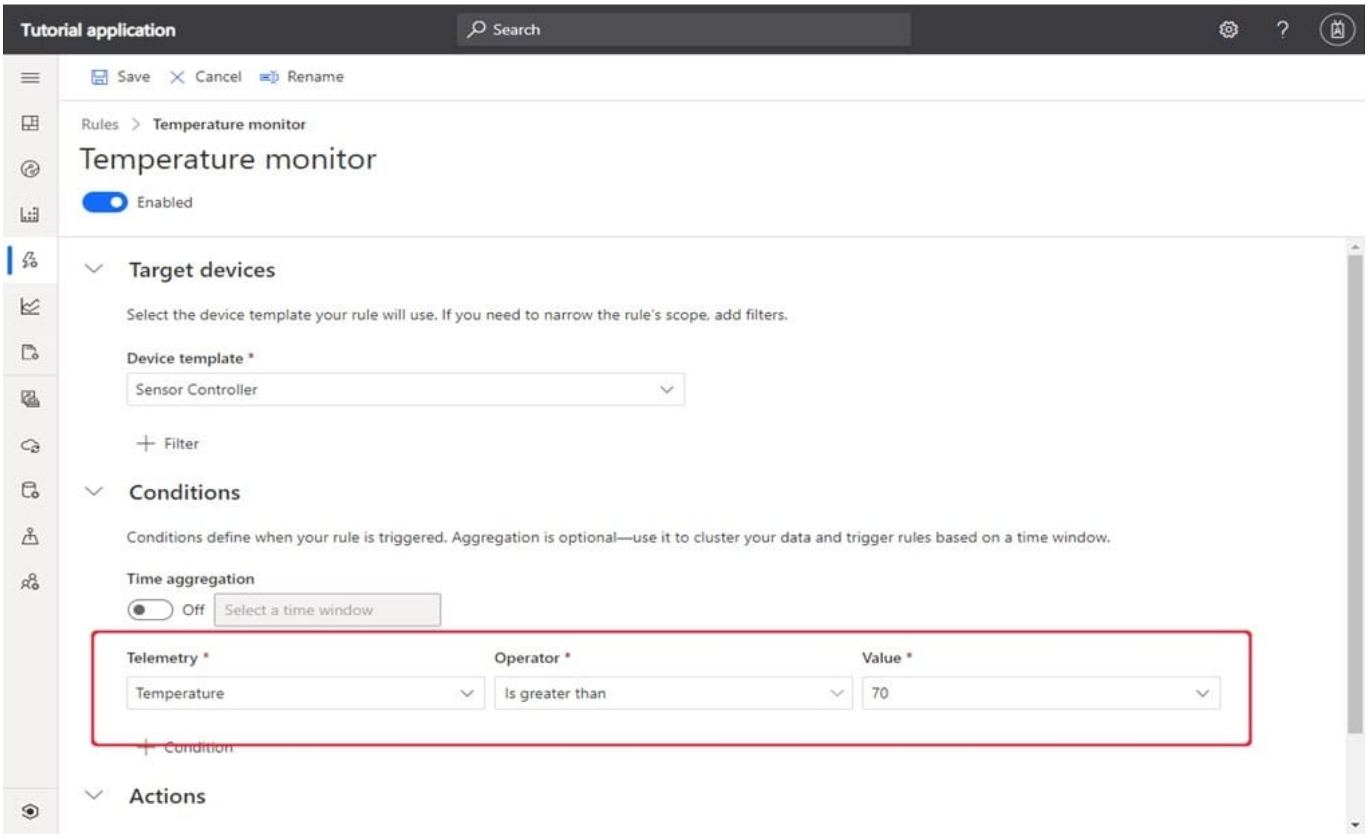
Next, choose Is less than as the Operator and enter 400 as the Value.

3.

Optionally, you can set a Time aggregation. When you select a time aggregation, you must also select an aggregation type, such as average or sum from the aggregation drop-down.

Without aggregation, the rule triggers for each telemetry data point that meets the condition.

With aggregation, the rule triggers if the aggregate value of the telemetry data points in the time window meets the condition.



Temperature monitor

Enabled

Target devices

Select the device template your rule will use. If you need to narrow the rule's scope, add filters.

Device template *: Sensor Controller

Conditions

Conditions define when your rule is triggered. Aggregation is optional—use it to cluster your data and trigger rules based on a time window.

Time aggregation: Off, Select a time window

Telemetry *: Temperature

Operator *: Is greater than

Value *: 70

Reference: https://docs.microsoft.com/en-us/azure/iot-central/core/tutorial-create-telemetry-rules

QUESTION 2

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.

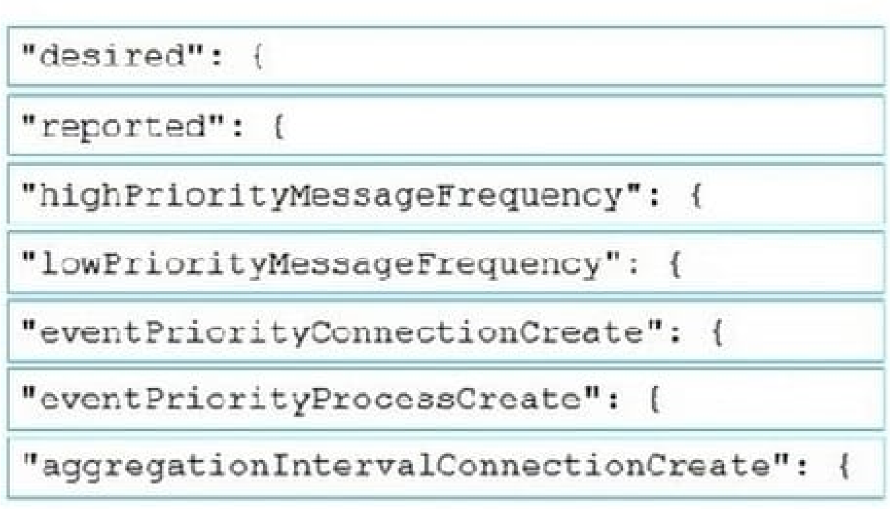
High priority events must be collected every seven minutes.

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

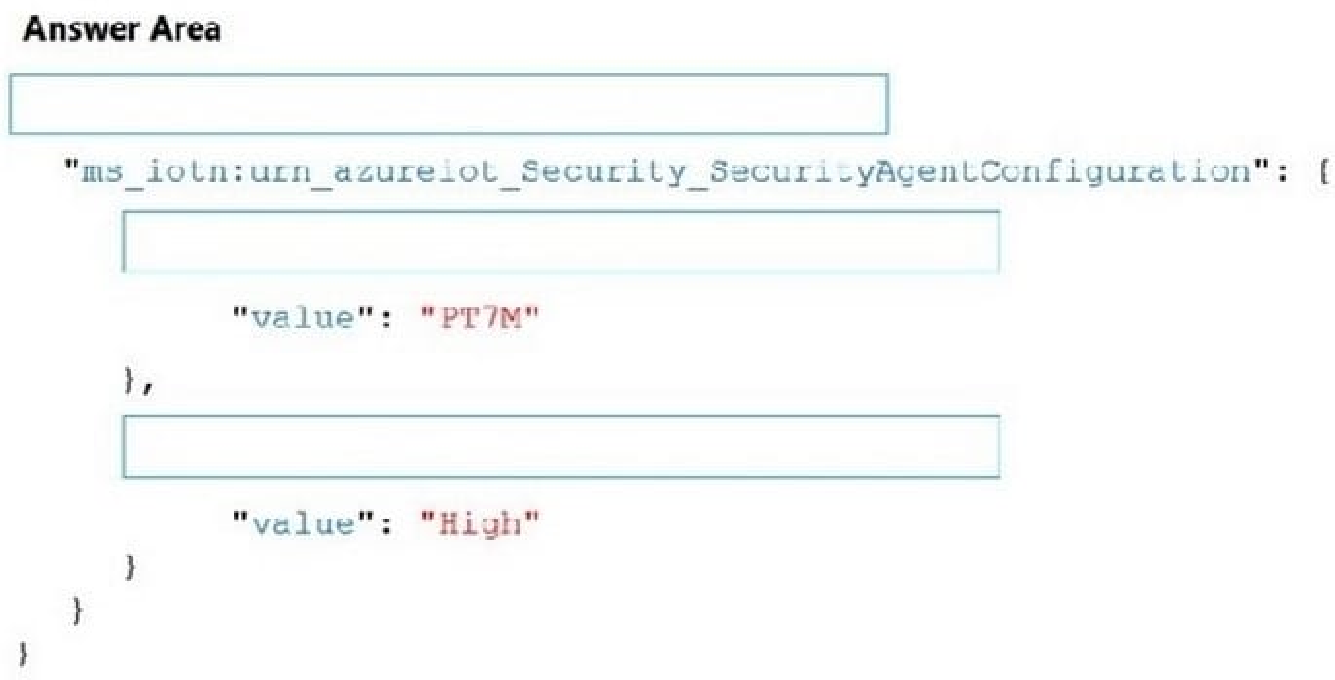
scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



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



Answer Area

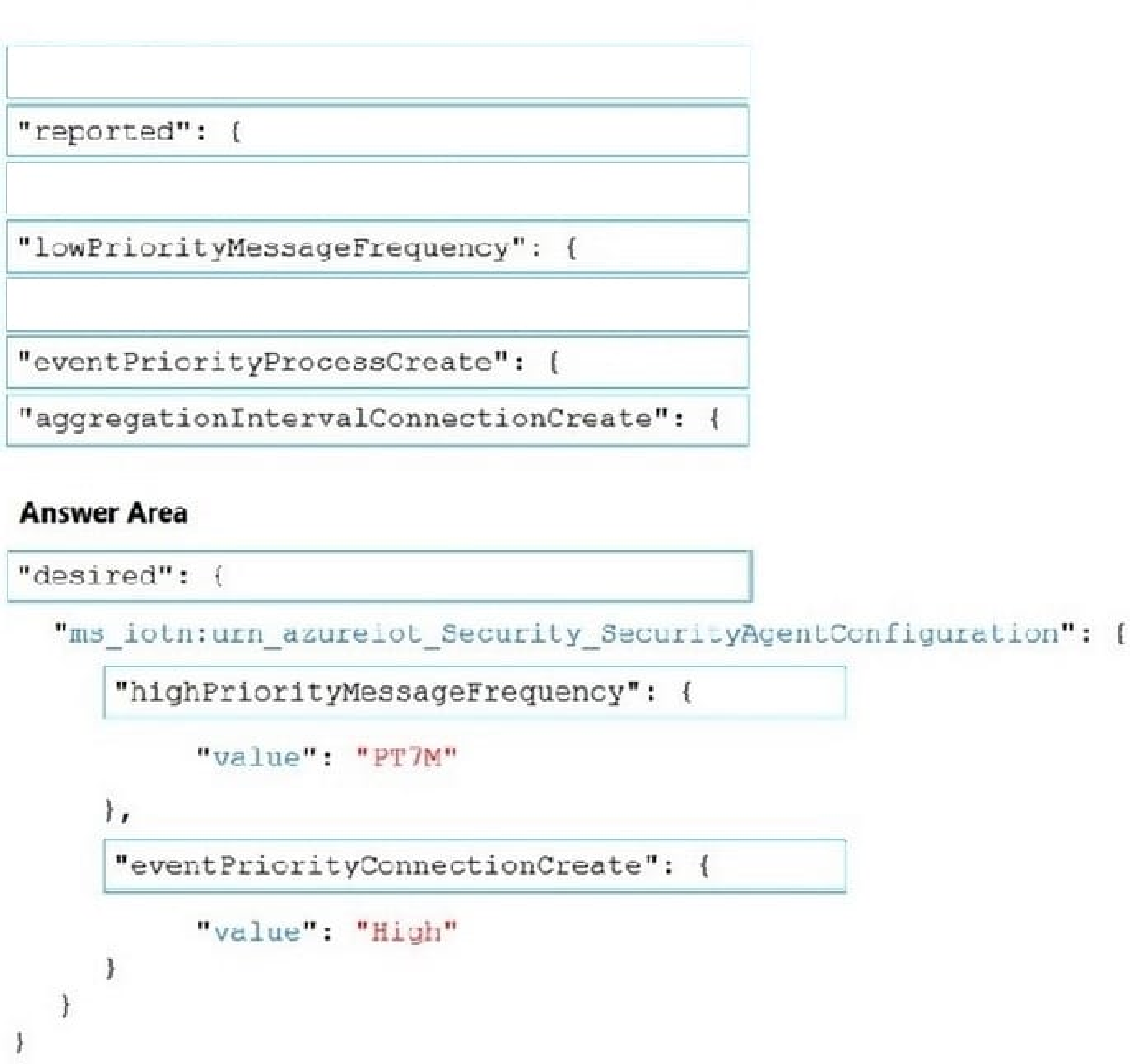
```

    "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:

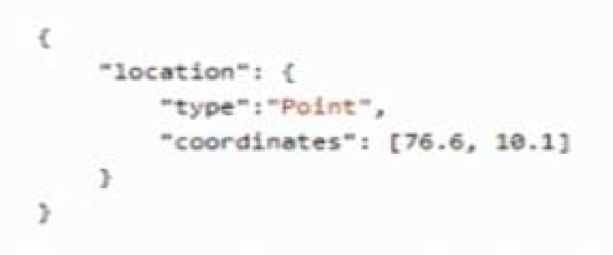
https://docs.microsoft.com/en-us/azure/defender-for-iot/how-to-agent-configuration

QUESTION 3

HOTSPOT

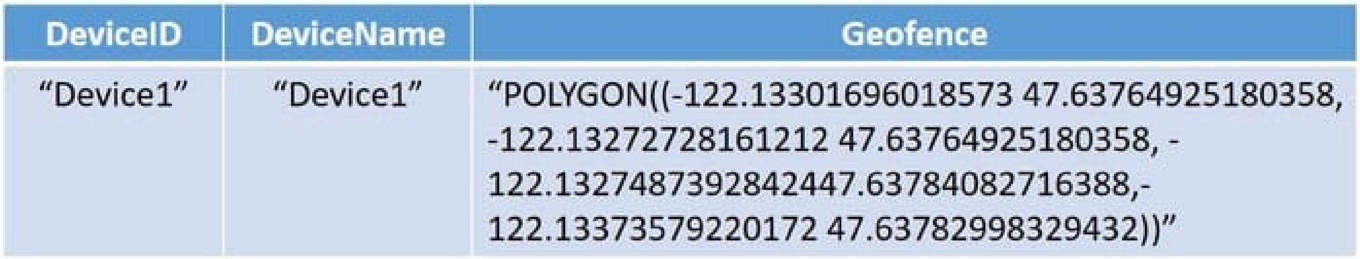
You have an Azure 10T hub and an I0T device.

You are developing an IoT solution that will generate an alert when the IoT device leaves a geofenced area. The device sends telemetry in the following format.



```
{
    "location": {
        "type":"Point",
        "coordinates": [76.6, 10.1]
    }
}
```

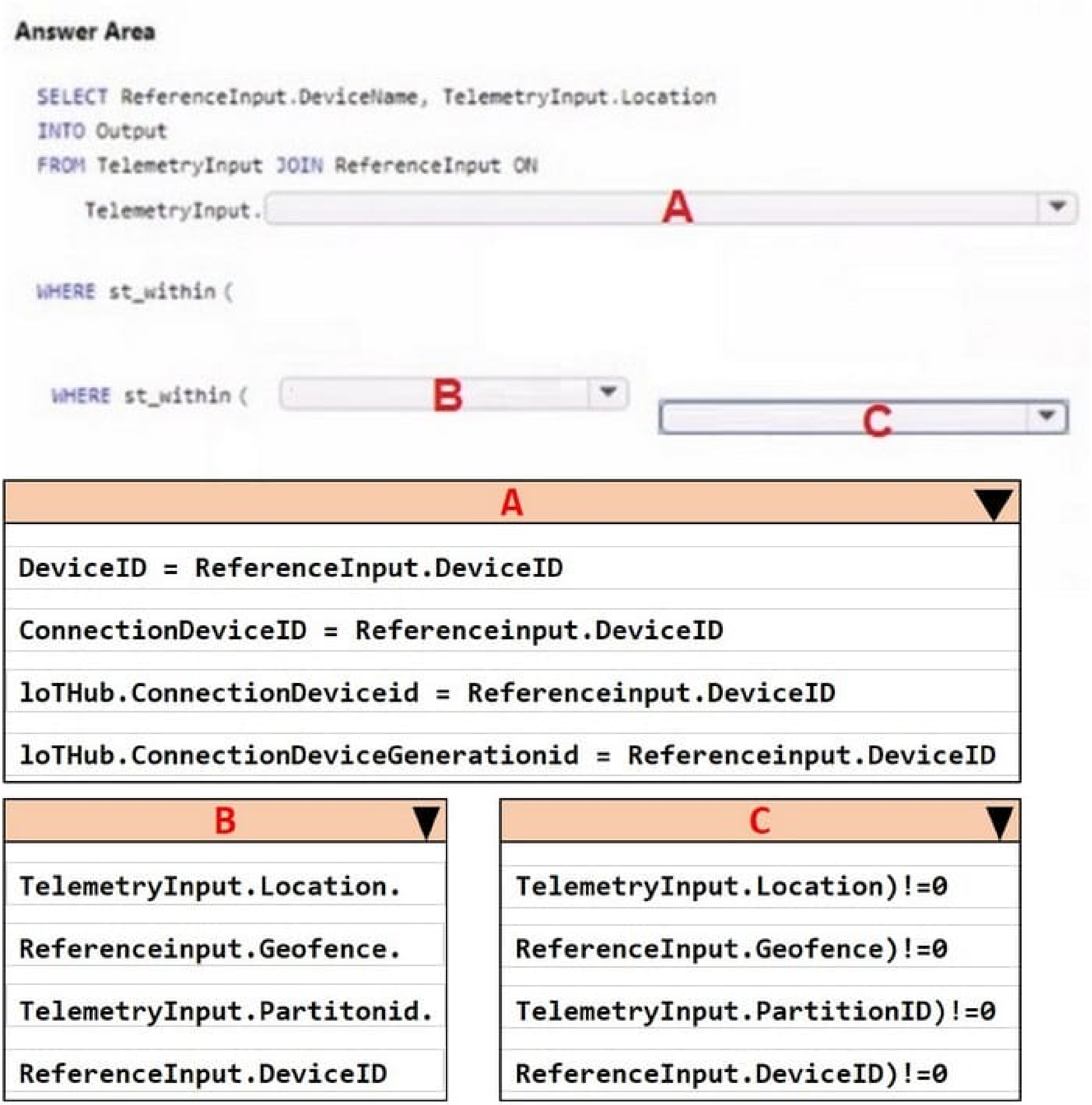
You create an Azure Stream Analytics job that uses telemetry input from the IoT hub and a reference input that contains the data shown in the following table.



DeviceID	DeviceName	Geofence
"Device1"	"Device1"	"POLYGON((-122.13301696018573 47.63764925180358, -122.13272728161212 47.63764925180358, - 122.1327487392842447.63784082716388,- 122.13373579220172 47.63782998329432))"

How should you complete the Stream Analytics query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

```
SELECT ReferenceInput.DeviceName, TelemetryInput.Location
INTO Output
FROM TelemetryInput JOIN ReferenceInput ON
     TelemetryInput. [A ▼]

WHERE st_within (

  WHERE st_within ( [B ▼]  [C ▼]
```

A ▼

- DeviceID = ReferenceInput.DeviceID
- ConnectionDeviceID = Referenceinput.DeviceID
- loTHub.ConnectionDeviceid = Referenceinput.DeviceID
- loTHub.ConnectionDeviceGenerationid = Referenceinput.DeviceID

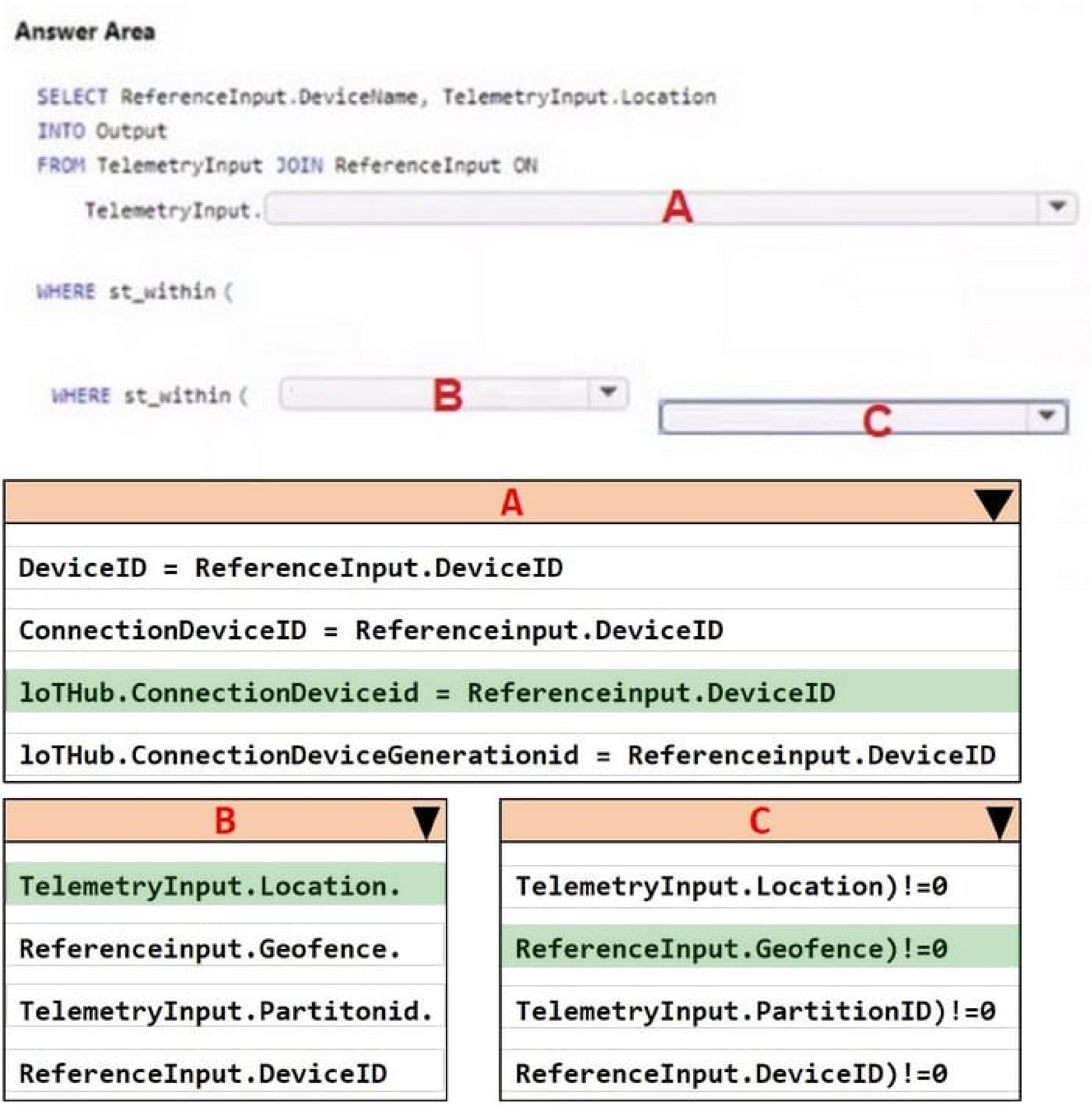
B ▼

- TelemetryInput.Location.
- Referenceinput.Geofence.
- TelemetryInput.Partitonid.
- ReferenceInput.DeviceID

C ▼

- TelemetryInput.Location)!=0
- ReferenceInput.Geofence)!=0
- TelemetryInput.PartitionID)!=0
- ReferenceInput.DeviceID)!=0

Correct Answer:



Answer Area

```
SELECT ReferenceInput.DeviceName, TelemetryInput.Location
INTO Output
FROM TelemetryInput JOIN ReferenceInput ON
     TelemetryInput. [A]

WHERE st_within (

  WHERE st_within ( [B]  [C]
```

A

- DeviceID = ReferenceInput.DeviceID
- ConnectionDeviceID = Referenceinput.DeviceID
- [✓ loTHub.ConnectionDeviceid = Referenceinput.DeviceID]
- loTHub.ConnectionDeviceGenerationid = Referenceinput.DeviceID

B

- [✓ TelemetryInput.Location.]
- Referenceinput.Geofence.
- TelemetryInput.Partitonid.
- ReferenceInput.DeviceID

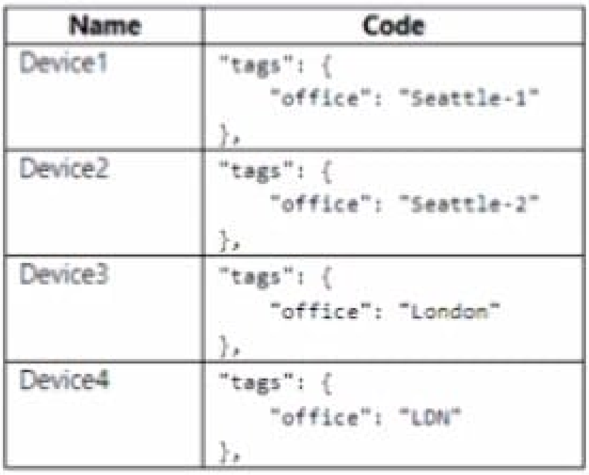
C

- TelemetryInput.Location)!=0
- [✓ ReferenceInput.Geofence)!=0]
- TelemetryInput.PartitionID)!=0
- ReferenceInput.DeviceID)!=0

QUESTION 4

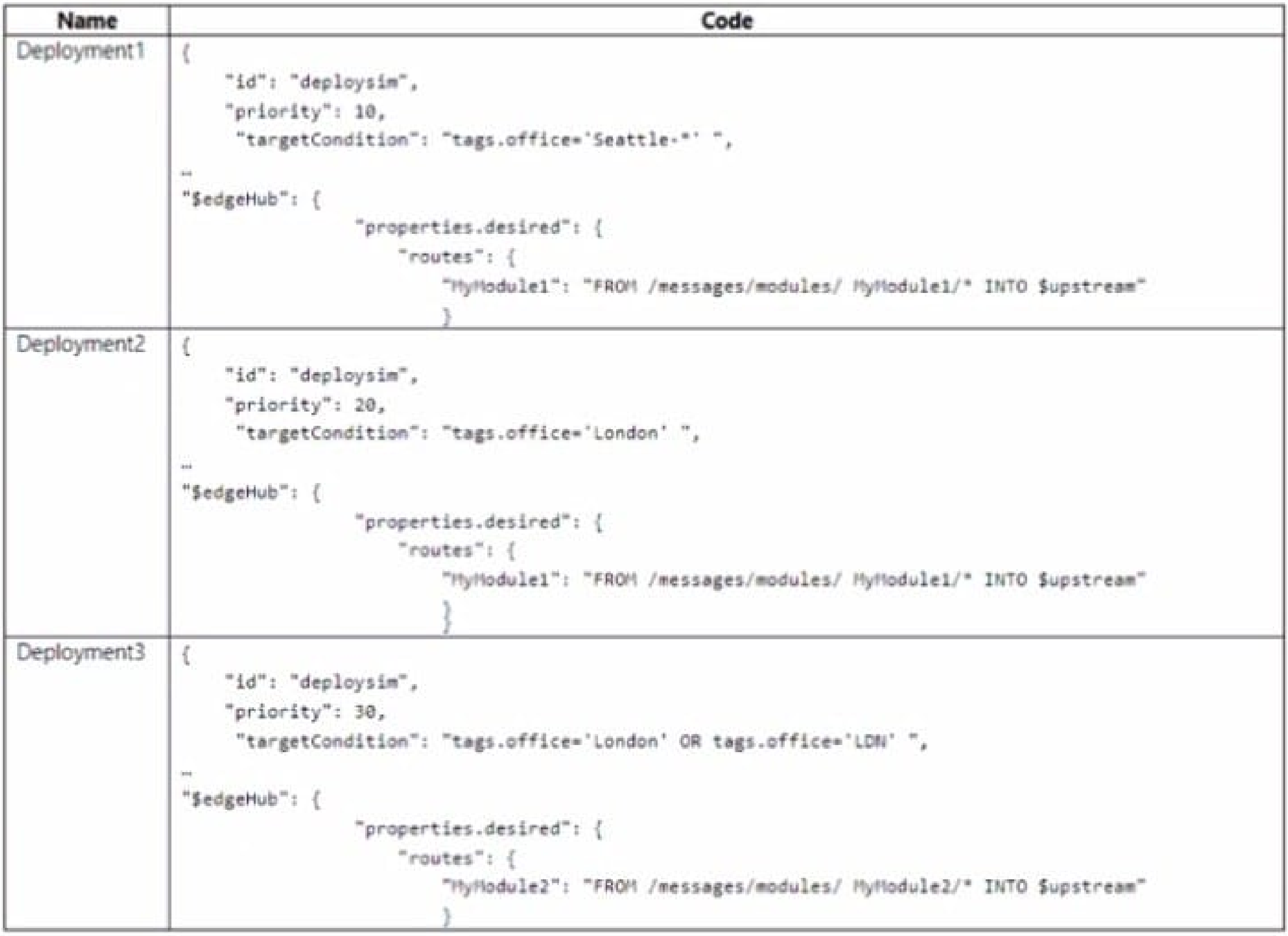
HOTSPOT

You have an Azure loT hub You have four Azure loT Edge devices and. The device twin code shown in the following table.



Name	Code
Device1	"tags": { "office": "Seattle-1" },
Device2	"tags": { "office": "Seattle-2" },
Device3	"tags": { "office": "London" },
Device4	"tags": { "office": "LDN" },

You have three deployments and the deployment code shown in the following table.



Name	Code

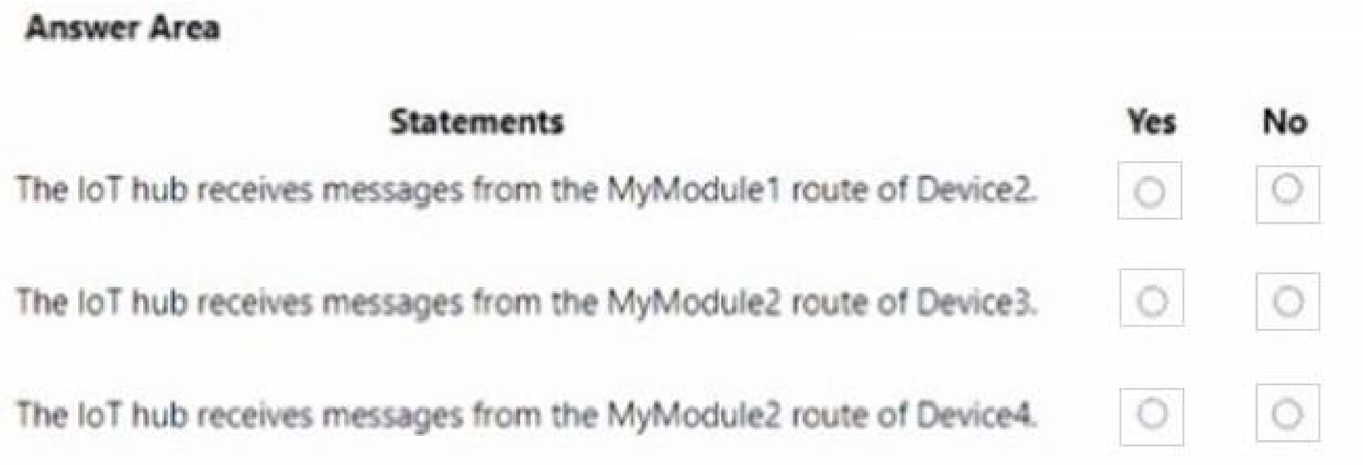
Deployment1	{
	"id": "deploysim",
	"priority": 10,
	"targetCondition": "tags.office='Seattle-*' ",
	...
	"$edgeHub": {
	"properties.desired": {
	"routes": {
	"MyModule1": "FROM /messages/modules/ MyModule1/* INTO $upstream"
	}

Deployment2	{
	"id": "deploysim",
	"priority": 20,
	"targetCondition": "tags.office='London' ",
	...
	"$edgeHub": {
	"properties.desired": {
	"routes": {
	"MyModule1": "FROM /messages/modules/ MyModule1/* INTO $upstream"
	}
	}

Deployment3	{
	"id": "deploysim",
	"priority": 30,
	"targetCondition": "tags.office='London' OR tags.office='LDN' ",
	...
	"$edgeHub": {
	"properties.desired": {
	"routes": {
	"MyModule2": "FROM /messages/modules/ MyModule2/* INTO $upstream"
	}

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

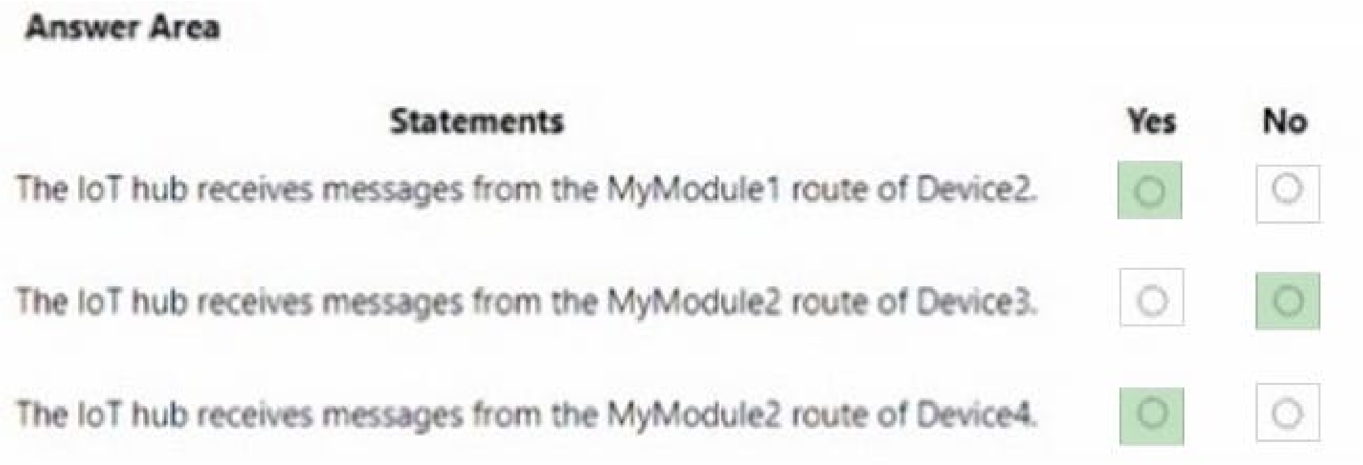
Hot Area:



Answer Area

Statements	Yes	No
The IoT hub receives messages from the MyModule1 route of Device2.	○	○
The IoT hub receives messages from the MyModule2 route of Device3.	○	○
The IoT hub receives messages from the MyModule2 route of Device4.	○	○

Correct Answer:



Answer Area

Statements	Yes	No
The IoT hub receives messages from the MyModule1 route of Device2.	[✓ ○]	○
The IoT hub receives messages from the MyModule2 route of Device3.	○	[✓ ○]
The IoT hub receives messages from the MyModule2 route of Device4.	[✓ ○]	○

QUESTION 5

You have an Azure IoT hub.

You need to enable Azure Defender for IoT on the IoT hub.

What should you do?

A. From the Security settings of the IoT hub, select Secure your IoT solution.

B. From the Diagnostics settings of the IoT hub, select Add diagnostic setting.

C. From Defender, add a security policy.

D. From Defender, configure security alerts.

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/azure/defender-for-iot/device-builders/quickstart-onboard-iot-hub