- **Vendor:** **Microsoft**
- **Exam Code:** **AZ-220**
- **Exam Name:** **Planning and Administering Microsoft Azure for SAPWorkloads**
- **New Updated Questions from Braindump2go**
- **(Updated in November/2021)**

QUESTION 99
You are configuring a production environment for an Azure IoT solution.
You plan to deploy 1,000 IoT devices. Each device will send one device-to-cloud message every hour.
Each message will be 4 KB.
You need to deploy an Azure IoT hub that will support the IoT device deployment. The solution must meet the following requirements:

- Perform bulk device operations such as creating multiple device identities.
- Minimize costs

What should you deploy?

A. one unit of the B1 tier
B. one unit of the free tier
C. one unit of the S1 tier
D. one unit of the S2 tier

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-quotas-throttling

QUESTION 100
You have an Azure IoT Central solution that includes multiple IoT devices. The devices report temperature, humidity, and pressure.
You need to export the sensor data captured during a 48-hour period as a CSV file.
What should you use in IoT Central?

A. Devices
B. Jobs
C. Device groups
D. Analytics

Answer: D
Explanation:
Azure IoT Central provides rich analytics capabilities to analyze historical trends and correlate telemetry from your devices. To get started, select Analytics on the left pane.
The analytics user interface has three main components:
Data configuration panel: On the configuration panel, select the device group for which you want to analyze the data. Next, select the telemetry that you want to analyze and select the aggregation method for each telemetry. The Group

By control helps to group the data by using device properties as dimensions.
Time control: Use the time control to select the duration for which you want to analyze the data. Chart control: The chart control visualizes the data as a line chart.
Reference:
https://docs.microsoft.com/en-us/azure/iot-central/core/howto-create-analytics

QUESTION 101
You are developing an Azure IoT solution for a shipping company. The company's ships will have sensors used for predictive maintenance. Some sensor devices will be MQTT-capable, and others will use Modbus.
Each ship has an internet connection that is available only when the ship is docked.
You create an Azure IoT hub.
You need to implement an IoT solution that uses Azure IoT Edge.
What should you do?

A. Configure an IoT Edge gateway. Deploy an IoT Edge Modbus module. From the Azure portal, create IoT devices and add connection strings to the devices.
B. Add the MQTT devices to the IoT hub and configure an IoT Edge gateway. From the IoT Edge gateway device, assign the MQTT devices as child devices of the gateway. Use the File upload feature of IoT Hub when internet connectivity is available.
C. Add the MQTT devices to the IoT hub. configure an IoT Edge gateway, and set Enable connection to IoT Hub to Disable. From the IoT Edge gateway device, assign the MQTT devices as child devices of the gateway. Deploy the IoT Edge Modbus module.
D. Add the MQTT devices to the IoT hub and configure an IoT Edge gateway. From the IoT Edge gateway device, assign the MQTT devices as child devices of the gateway. Deploy an IoT Edge Modbus module.

Answer: C
Explanation:
https://docs.microsoft.com/en-us/azure/iot-edge/deploy-modbus-gateway

QUESTION 102
You have an Azure IoT Edge module named SampleModule that runs on a device named Device1.
You make changes to the code of SampleModule by using Microsoft Visual Studio Code.
You need to push the code to the container registry and then deploy the module to Device1.
Which two actions should you perform from Visual Studio Code? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Build and push the SampleModule code to the registry.
B. Create a deployment for a single device.
C. Generate a deployment manifest.
D. Build an IoT Edge solution.
E. Generate a shared access signature (SAS) token for Device 1.

Answer: BC
Explanation:
C: Configure a deployment manifest. A deployment manifest is a JSON document that describes which modules to deploy, how data flows between the modules, and desired properties of the module twins.
B: You deploy modules to your device by applying the deployment manifest that you configured with the module information.
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/how-to-deploy-modules-vscode

QUESTION 103
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 are developing a custom Azure IoT Edge module.
The module needs to identify the device ID of the local device.
Solution: You configure the module to read the IOTEDGE_DEVICEID environment variable.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
The Azure ID of the current device is available on the IOTEDGE_DEVICEID environment variable.
Instead read the device ID of the device twin.
Note: Device twins are JSON documents that store device state information including metadata, configurations, and conditions. Azure IoT Hub maintains a device twin for each device that you connect to IoT Hub.
Device identity properties. The root of the device twin JSON document contains the read-only properties from the corresponding device identity stored in the identity registry.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-device-twins

QUESTION 104
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 are developing a custom Azure IoT Edge module.
The module needs to identify the device ID of the local device.
Solution: You configure the module to read the ProductInfo property of ModuleClient.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
Instead read the device ID of the device twin.
Note: Device twins are JSON documents that store device state information including metadata, configurations, and conditions. Azure IoT Hub maintains a device twin for each device that you connect to IoT Hub.
Device identity properties. The root of the device twin JSON document contains the read-only properties from the corresponding device identity stored in the identity registry.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-device-twins

QUESTION 105
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 are developing a custom Azure IoT Edge module.
The module needs to identify the device ID of the local device.
Solution: You configure the module to read the device ID of the device twin.
Does this meet the goal?

A. Yes
B. No

Answer: A
Explanation:
Device twins are JSON documents that store device state information including metadata, configurations, and conditions. Azure IoT Hub maintains a device twin for each device that you connect to IoT Hub.
Device identity properties. The root of the device twin JSON document contains the read-only properties from the corresponding device identity stored in the identity registry.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-device-twins

QUESTION 106
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

Answer: B
Explanation:
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 107
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 sensors to connect directly to the IoT hub.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
Instead use a translation gateway.
Note: In the protocol translation gateway pattern, only the IoT Edge gateway has an identity with 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.

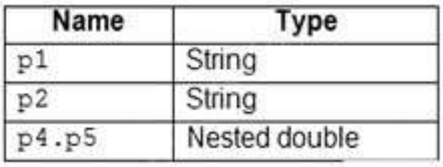
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/iot-edge-as-gateway

QUESTION 108
You need to visualize Azure IoT Hub telemetry data by using Microsoft Power BI.
Which service should you connect to the IoT hub?

A. Azure Event Grid
B. SendGrid
C. Azure Stream Analytics
D. Azure Notification Hubs

Answer: C
Explanation:
You can use Microsoft Power BI to visualize real-time sensor data that your Azure IoT hub receives. To do so, you configure an Azure Stream Analytics job to consume the data from IoT Hub and route it to a dataset in Power BI.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-live-data-visualization-in-power-bi

QUESTION 109
You have an Azure subscription that contains an Azure Time Series Insights environment. The environment has the properties shown in the following table.



Name	Type
p1	String
p2	String
p4.p5	Nested double

You need to create a D.
Which two time series expressions can be correctly used as part of the query? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. $event.p1.String = 'abc'
B. $event.p2 = 'abc'
C. $event['p1'] != NULL
D. $event.p4.p5 = 0.0

Answer: AC
Explanation:
Example: $event['p1'] != NULL
['p1'] is the only token used. Interpreted as $event['p1'].Double != NULL
Reference:
https://docs.microsoft.com/en-us/rest/api/time-series-insights/reference-time-series-expression-syntax

QUESTION 110
You have an Azure subscription that contains an Azure IoT hub, 500 IoT devices, and an Azure Time Series Insights Gen2 environment named Environment1.
You need to add calculated values to the Time Series Model.
What should you use?

A. instances
B. types
C. hierarchies

Answer: B
Explanation:

Time Series Model types help you define variables or formulas for doing computations. Types are associated with a specific instance.
A type can have one or more variables. For example, a Time Series Model instance might be of type Temperature Sensor, which consists of the variables avg temperature, min temperature, and max temperature.
Reference:
https://docs.microsoft.com/en-us/azure/time-series-insights/concepts-model-overview

QUESTION 111
You have an Azure IoT hub that has 1,000 registered devices.
You create an Azure logic app.
You need to send Device Connected and Device Disconnected events in real time to the logic app.
What should you do?

A. From the Message routing blade of the loT hub. add a route. Route DeviceLifecycleEvents to an Azure Service Bus queue.
B. From the Diagnostic settings blade of the loT hub. add a diagnostic setting. Route the connection logs to a Log Analytics workspace.
C. From the Events blade of the loThub. add an event subscription. Configure the Filter to Event Types setting and route the events to a webhook.

Answer: C
Explanation:
https://sandervandevelde.wordpress.com/2019/12/20/subscribe-your-iothub-to-eventgrid-as-event-source/

QUESTION 112
You have an Azure IoT hub.
You need to check whether the IoT hub was affected by an outage.
What should you select in the Azure portal? To answer, select the appropriate option in the answer area.
NOTE: Each correct selection is worth one point.

A. Resource health
B. Metrics
C. Alerts
D. Diagnostic settings

Answer: A
Explanation:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-azure-service-health-integration

QUESTION 113
You have an Azure IoT solution.
You need to test that the solution remains functional if IoT Hub is affected by a regional outage.
What should you do?

A. From the loT hub, set Allow public network access to Disabled.
B. From the loT hub, start a manual failover.
C. From the Device Provisioning Service (DPS), unlink the loT hub.
D. From the loT hub, select Disable fallback route.

Answer: B
Explanation:
Manual failover is a feature of the IoT Hub service that allows customers to failover their hub's operations from a primary region to the corresponding Azure geo-paired region. Manual failover can be done in the event of a regional disaster or an extended service outage. You can also perform a planned failover to test your disaster recovery capabilities, although we recommend using a test IoT hub rather than one running in production.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/tutorial-manual-failover

QUESTION 114
You have an Azure IoT hub and 15,000 IoT devices that monitor temperature. The IoT hub has four partitions. Each IoT device sends a 1-KB message every five seconds.
You plan to use Azure Stream Analytics to process the telemetry stream and generate an alert when temperatures exceed a defined threshold.
You need to recommend the minimum number of streaming units to configure for Stream Analytics.
What should you recommend?

A. 1
B. 3
C. 6
D. 12

Answer: D
Explanation:
https://docs.microsoft.com/en-us/azure/stream-analytics/stream-analytics-parallelization#calculate-the-maximum-streaming-units-of-a-job

QUESTION 115
You have an Azure IoT solution that contains an Azure IoT hub.
You need to ensure that the IoT hub configuration is compliant with the Health Insurance Portability and Accountability Act (HIPAA) audit logging requirements.
What should you use?

A. Azure Advisor recommendations
B. an Azure Policy definition
C. Azure Monitor alerts
D. an Azure Sentinel workspace

Answer: B
Explanation:
Regulatory Compliance in Azure Policy provides Microsoft created and managed initiative definitions, known as built-ins, for the compliance domains and security controls related to different compliance standards, including HIPAA auditing logging.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/security-controls-policy

QUESTION 116
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.

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

QUESTION 117
You have an Azure subscription that contains an Azure IoT hub and two Azure IoT Edge devices named Device1 and Device2.
You need to ensure that the IoT hub only accepts connections from Device1 and Device2.

What should you configure?

A. a private endpoint connection
B. Azure API Management
C. Azure Active Directory (Azure AD) Identity Protection
D. a gateway device

Answer: A
Explanation:
Ingress connectivity to IoT Hub using Azure Private Link. A private endpoint is a private IP address allocated inside a customer-owned VNet via which an Azure resource is reachable. Through Azure Private Link, you can set up a private endpoint for your IoT hub to allow services inside your VNet to reach IoT Hub without requiring traffic to be sent to IoT Hub's public endpoint. Similarly, your on-premises devices can use Virtual Private Network (VPN) or ExpressRoute peering to gain connectivity to your VNet and your IoT Hub (via its private endpoint). As a result, you can restrict or completely block off connectivity to your IoT hub's public endpoints by using IoT Hub IP filter or the public network access toggle. This approach keeps connectivity to your Hub using the private endpoint for devices.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/virtual-network-support

QUESTION 118
You have an Azure IoT solution that contains an Azure IoT hub and 100 IoT devices. The devices run Windows Server 2016.
You need to deploy the Azure Defender for IoT C#-based security agent to the devices.
What should you do first?

A. On the devices, initialize Trusted Platform Module (TPM).
B. From the loT hub. create a system-assigned managed identity.
C. From the loT hub. create a security module for the devices.
D. On the devices, set the PowerShell execution policy to Restricted.

Answer: C
Explanation:
The IoT Edge security manager provides a safe framework for security service extensions through host-level modules. The IoT Edge security manager include Ensure safe operation of client agents for services including Device Update for IoT Hub and Azure Defender for IoT.
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/iot-edge-security-manager

QUESTION 119
You deploy an Azure Digital Twins instance.
You are developing client code that will modify digital twin data.
You run the client code and receive the following response for an Azure Digital Twins API.
`403 (Forbidden)`
You need to configure access control for the Azure Digital Twins instance to ensure that the client code can modify the data.
Which role should you assign?

A. Contributor
B. Azure Digital Twins Data Owner
C. Owner
D. Managed Application Operator Role

Answer: B
Explanation:
Most often, this error indicates that your Azure role-based access control (Azure RBAC) permissions for the service aren't set up correctly. Many actions for an Azure Digital Twins instance require you to have the Azure Digital Twins

Data Owner role on the instance you are trying to manage.
Reference:
https://docs.microsoft.com/en-us/azure/digital-twins/troubleshoot-error-403

QUESTION 120
You have an Azure IoT solution.
You need to create a digital twin model.
Which language should you use?

A. XHTML
B. DTDL
C. YAML
D. XML

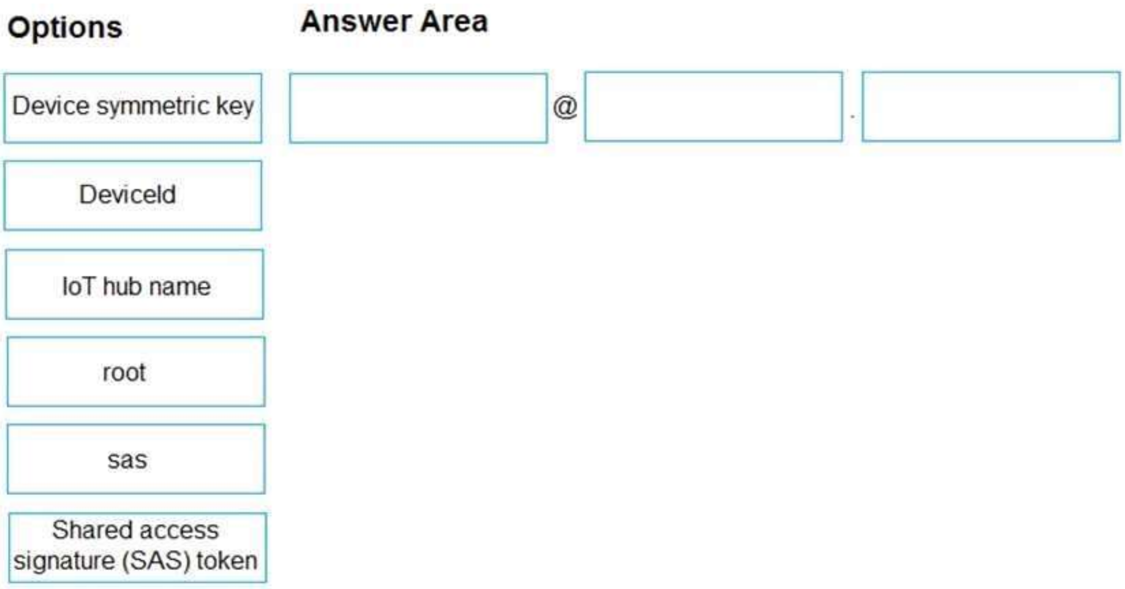
Answer: B
Explanation:
Azure Digital Twins models are represented in the JSON-LD-based Digital Twin Definition Language (DTDL).
Reference:
https://docs.microsoft.com/en-us/azure/digital-twins/concepts-models

QUESTION 121
You need to route events in Azure Digital Twins to a downstream service for additional processing.
Which type of output endpoint can you use?

A. Azure Event Hubs
B. Azure Queue storage
C. Microsoft Power BI
D. Azure Table storage

Answer: A
Explanation:
Create an endpoint for Azure Digital Twins.
These are the supported types of endpoints that you can create for your instance:
- Event Grid
- Event Hubs
- Service Bus
Note: In Azure Digital Twins, you can route event notifications to downstream services or connected compute resources. This is done by first setting up endpoints that can receive the events. You can then create event routes that specify which events generated by Azure Digital Twins are delivered to which endpoints.
Reference:
https://docs.microsoft.com/en-us/azure/digital-twins/how-to-manage-routes

QUESTION 122
Drag and Drop Question
You have an Azure subscription that contains an Azure IoT hub and 100 IoT devices.
The devices connect to the IoT hub by using the Advanced Message Queuing Protocol (AMQP) protocol and authenticate to the IoT hub by using symmetric keys.
You need to configure the SASL PLAIN username for the AMQP connection.
How should you configure the username? To answer, drag the appropriate options to the correct targets. Each option 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.



Options

Device symmetric key

DeviceId

IoT hub name

root

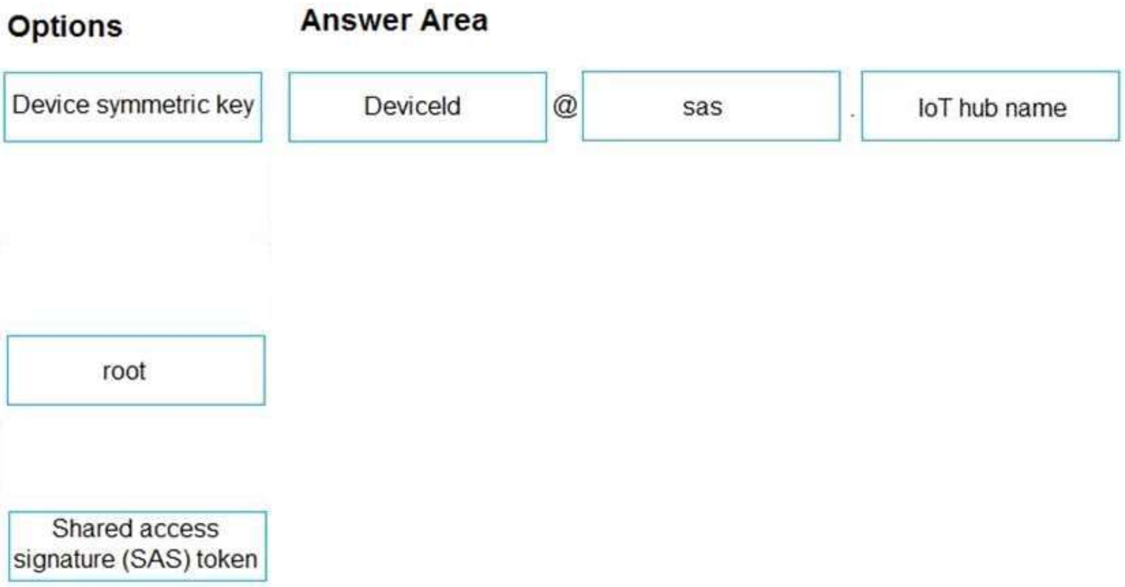
sas

Shared access signature (SAS) token

Answer Area

[ ] @ [ ] . [ ]

Answer:



Options

Device symmetric key

root

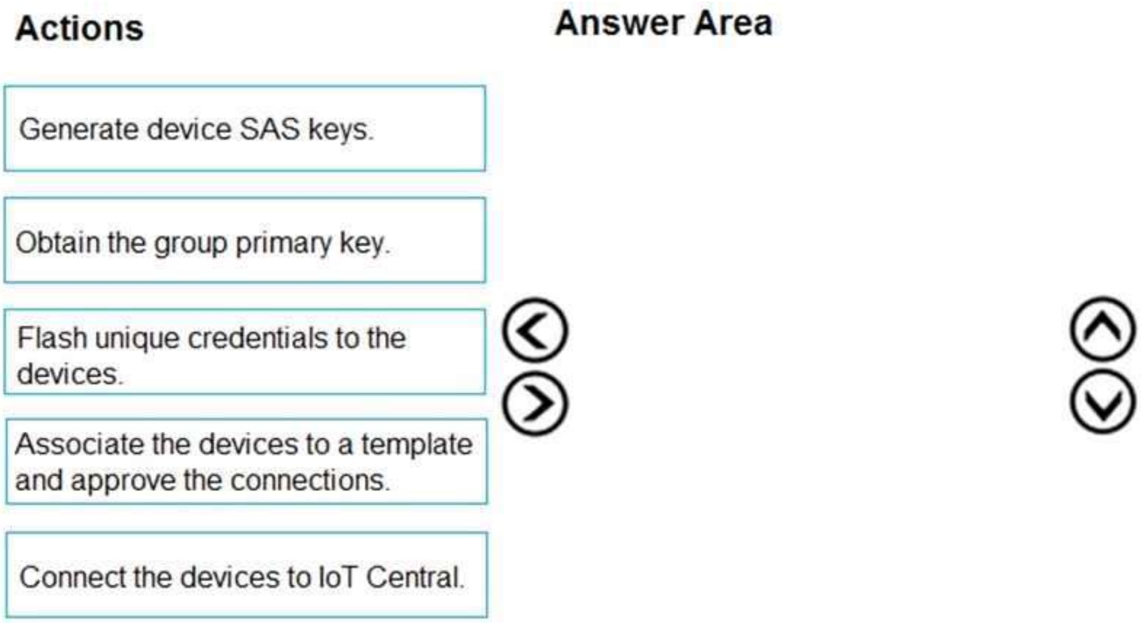
Shared access signature (SAS) token

Answer Area

DeviceId @ sas . IoT hub name

Explanation:
Box 1: DeviceID
If you use AMQP claims-based-security, the standard specifies how to transmit these tokens.
For SASL PLAIN, the username can be:
{policyName}@sas.root.{iothubName} if using IoT hub-level tokens. {deviceId}@sas.{iothubname} if using device-scoped tokens.
Box 2: sas
Box 3:IoT hub hame
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-dev-guide-sas

QUESTION 123
Drag and Drop Question
You have an Azure IoT Central application.
You need to connect IoT devices that use SAS tokens to the application without first registering the devices.
In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.



Actions

Generate device SAS keys.

Obtain the group primary key.

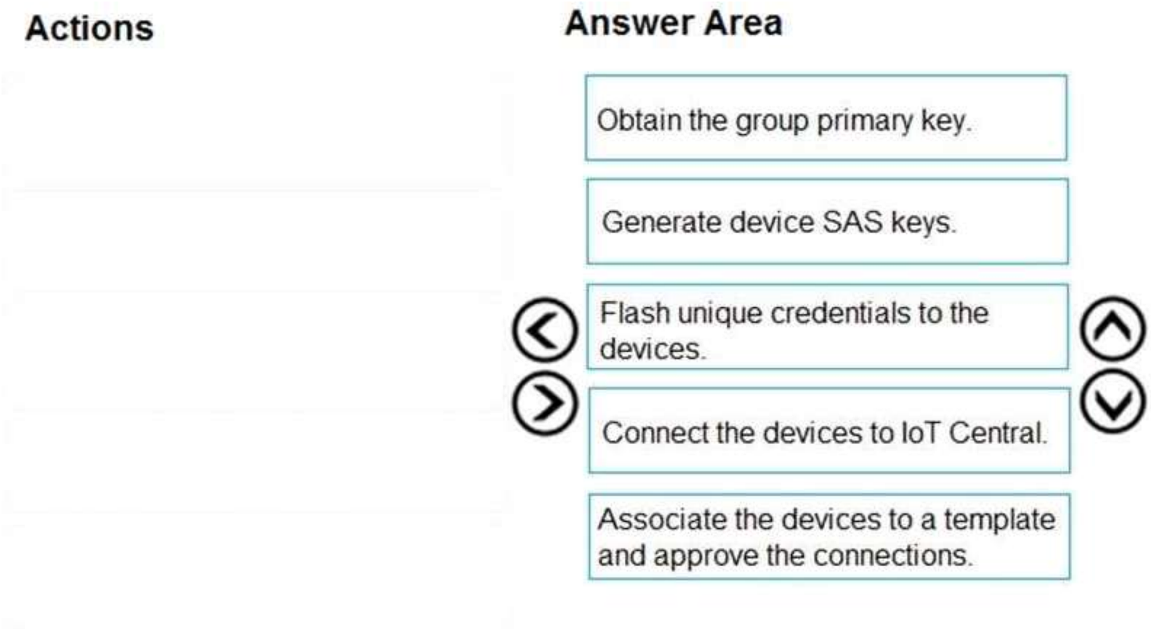
Flash unique credentials to the devices.

Associate the devices to a template and approve the connections.

Connect the devices to IoT Central.

Answer Area

Answer:



Actions

Answer Area

Obtain the group primary key.

Generate device SAS keys.

Flash unique credentials to the devices.

Connect the devices to IoT Central.

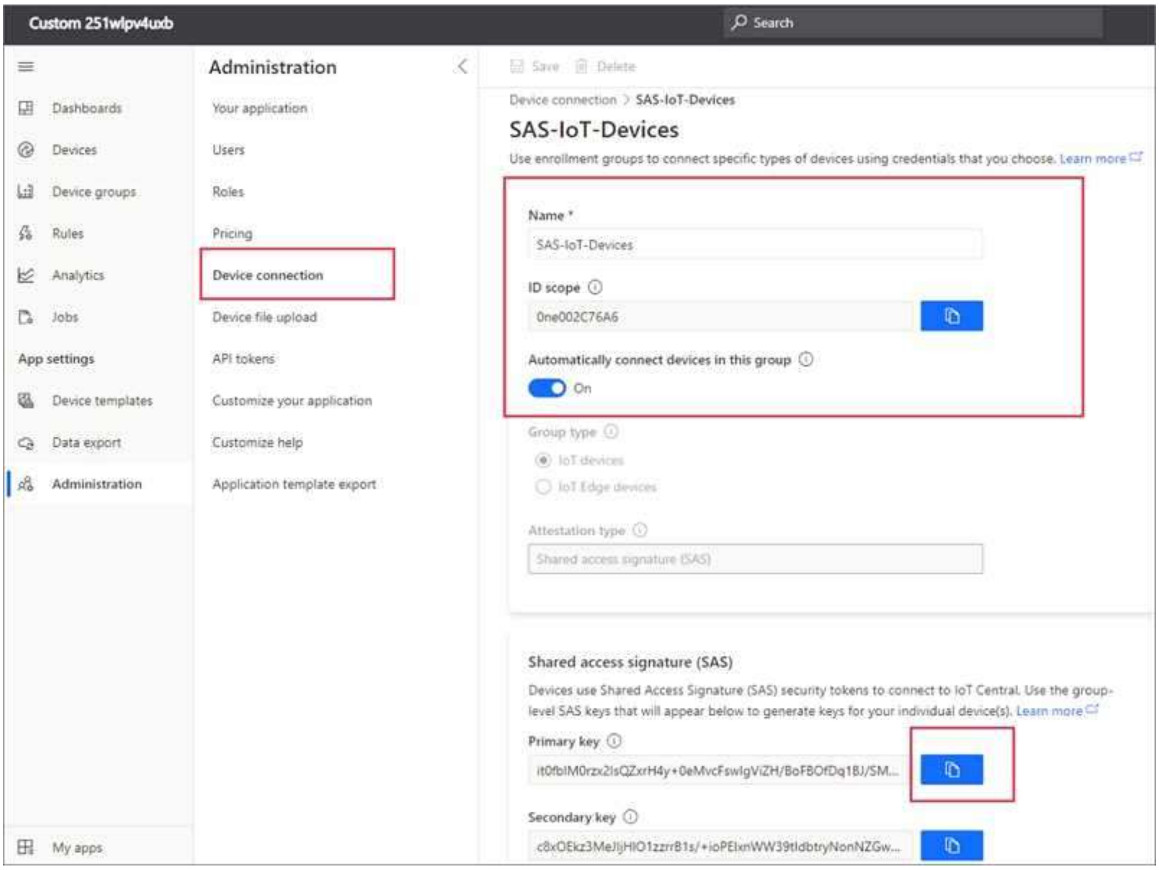
Associate the devices to a template and approve the connections.

Explanation:

Automatically register devices that use SAS tokens:

Step 1: Obtain the group primary key

1. Copy the group primary key from the SAS-IoT-Devices enrollment group:



SAS-IoT-Devices

Use enrollment groups to connect specific types of devices using credentials that you choose. Learn more

Name *: SAS-IoT-Devices

ID scope: 0ne002C76A6

Automatically connect devices in this group: On

Group type: ● IoT devices ○ IoT Edge devices

Attestation type: Shared access signature (SAS)

Shared access signature (SAS)

Devices use Shared Access Signature (SAS) security tokens to connect to IoT Central. Use the group-level SAS keys that will appear below to generate keys for your individual device(s). Learn more

Primary key: it0fbIM0rzx2IsQZxrH4y+0eMvcFswlgViZH/BoFBOfDq1BJ/SM...

Secondary key: c8xOEkz3MeJIjHIO1zzrrB1s/+ioPElxnWW39tldbtryNonNZGw...

Step 2: Generate device SAS Keys.

2. Use the az iot central device compute-device-key command to generate the device SAS keys. Use the group primary key from the previous step.

Step 3: Flash unique credentials to the devices.

3. As an OEM, flash each device with the device ID, the generated device SAS key, and the application ID scope value. The device code should also send the model ID of the device model it implements.

Step 4: Connect the devices to IoT Central

4. When you switch on a device, it first connects to DPS to retrieve its IoT Central registration information.

5. The device uses the information from DPS to connect to, and register with, your IoT Central application.

Step 5: Associate the devices to a template and approve the connections. The IoT Central application uses the model ID sent by the device to associate the registered device with a device template.

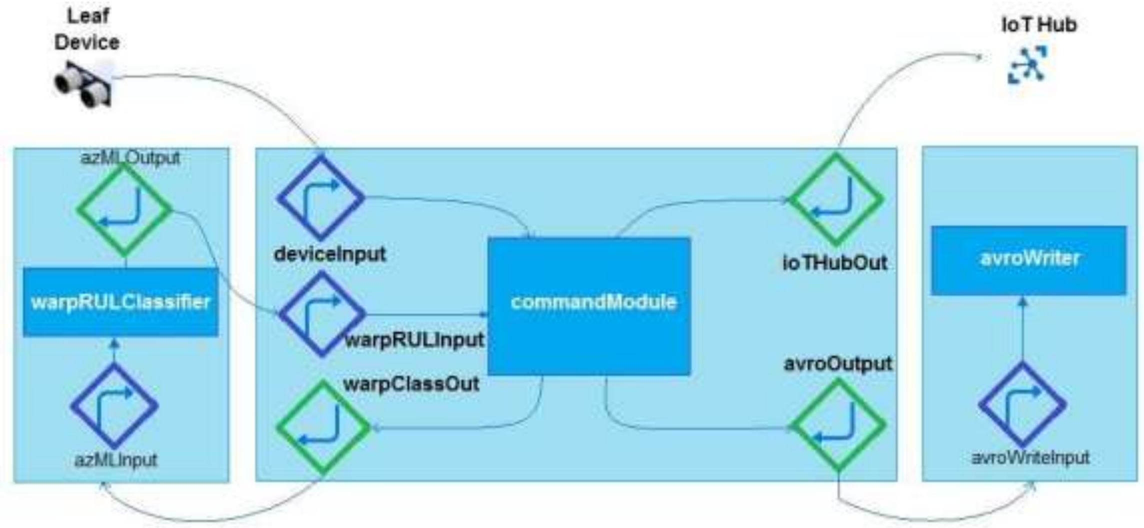
Reference:

https://docs.microsoft.com/en-us/azure/iot-central/core/concepts-get-connected

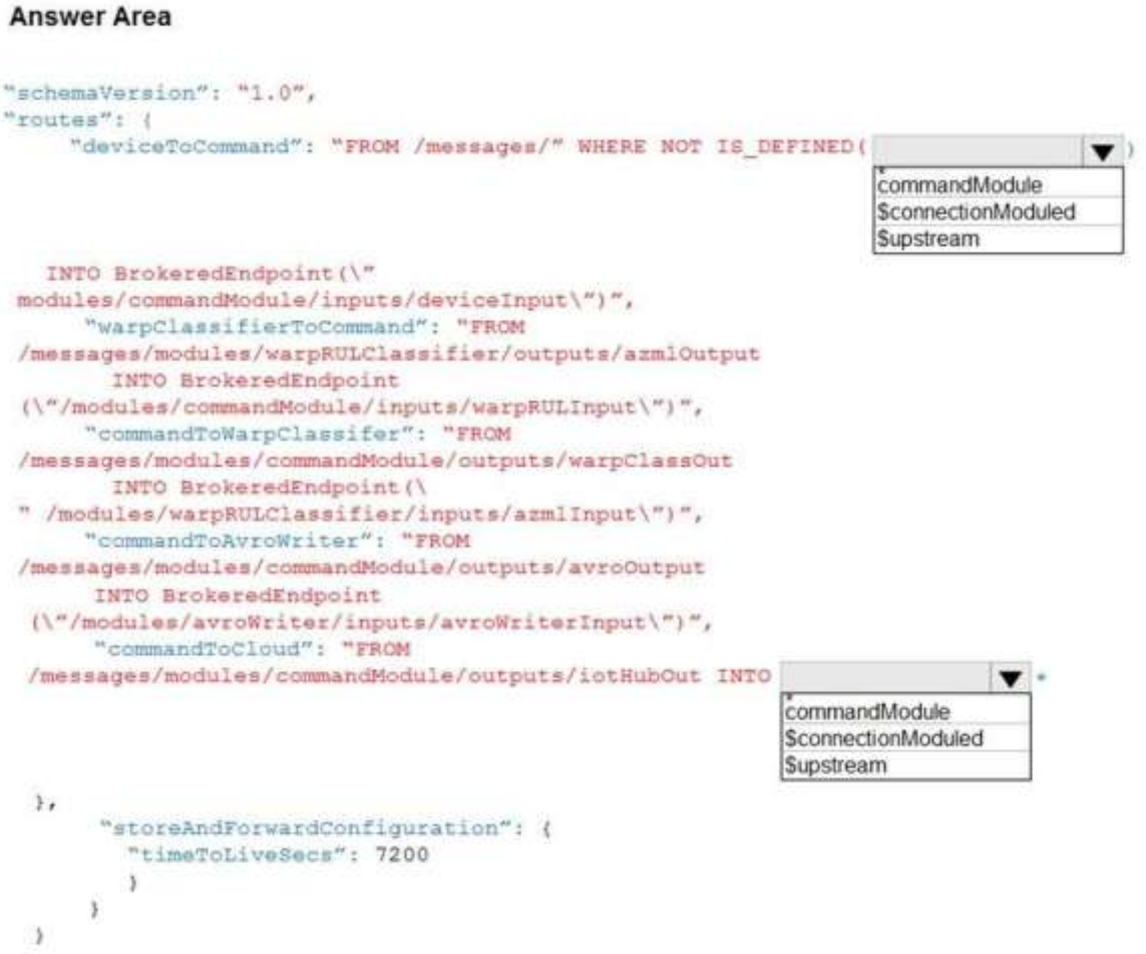
QUESTION 124

Hotspot Question

You need to configure Azure IoT Edge module routing to ensure that modules route traffic as shown in the following exhibit.



How should you complete the IoT Edge module routes? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



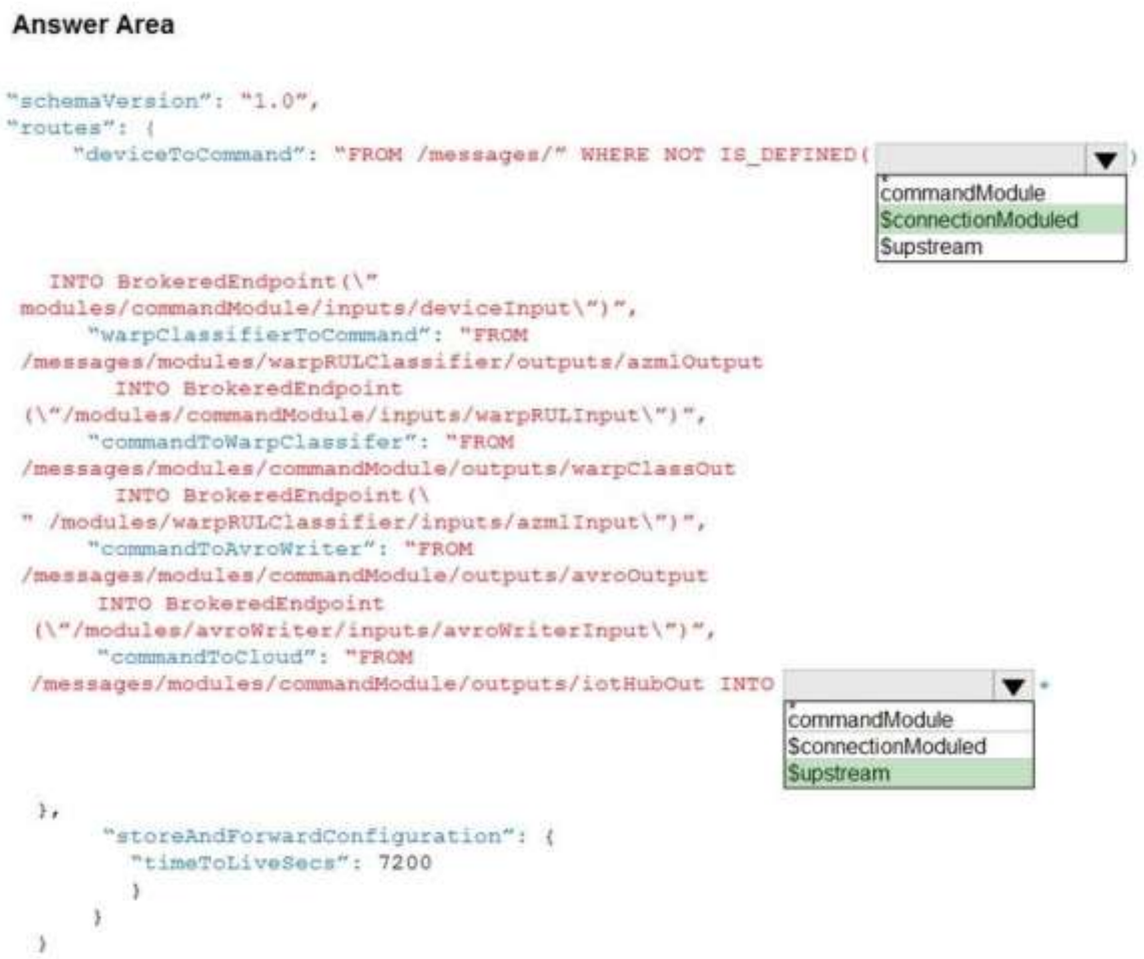
Answer Area

```
"schemaVersion": "1.0",
"routes": {
    "deviceToCommand": "FROM /messages/" WHERE NOT IS_DEFINED( [▼] )
```

```
  INTO BrokeredEndpoint(\"
 modules/commandModule/inputs/deviceInput\")",
     "warpClassifierToCommand": "FROM
 /messages/modules/warpRULClassifier/outputs/azmlOutput
        INTO BrokeredEndpoint
 (\"/modules/commandModule/inputs/warpRULInput\")",
     "commandToWarpClassifer": "FROM
 /messages/modules/commandModule/outputs/warpClassOut
        INTO BrokeredEndpoint(\
 " /modules/warpRULClassifier/inputs/azmlInput\")",
     "commandToAvroWriter": "FROM
 /messages/modules/commandModule/outputs/avroOutput
       INTO BrokeredEndpoint
  (\"/modules/avroWriter/inputs/avroWriterInput\")",
      "commandToCloud": "FROM
  /messages/modules/commandModule/outputs/iotHubOut INTO [▼] "
```

```
  },
      "storeAndForwardConfiguration": {
        "timeToLiveSecs": 7200
        }
     }
  }
```

Answer:



Answer Area

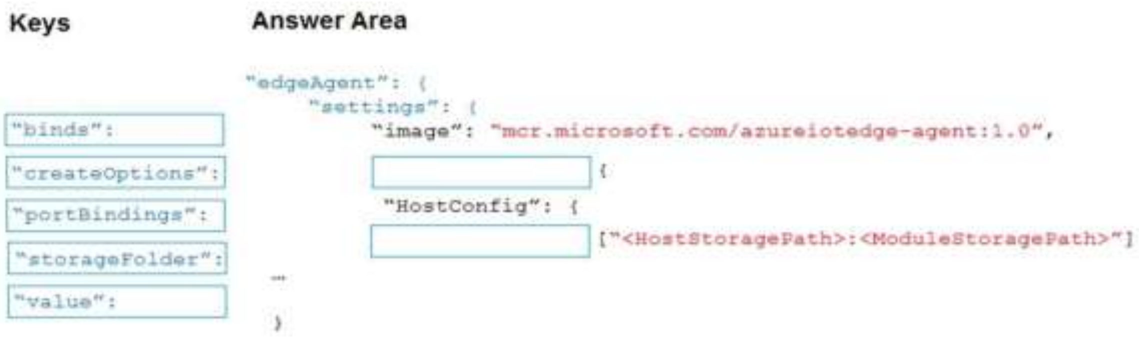
```
"schemaVersion": "1.0",
"routes": {
    "deviceToCommand": "FROM /messages/" WHERE NOT IS_DEFINED(           )
```

```
   INTO BrokeredEndpoint(\"
 modules/commandModule/inputs/deviceInput\")",
      "warpClassifierToCommand": "FROM
 /messages/modules/warpRULClassifier/outputs/azmlOutput
        INTO BrokeredEndpoint
 (\"/modules/commandModule/inputs/warpRULInput\")",
      "commandToWarpClassifer": "FROM
 /messages/modules/commandModule/outputs/warpClassOut
        INTO BrokeredEndpoint(\
 " /modules/warpRULClassifier/inputs/azmlInput\")",
      "commandToAvroWriter": "FROM
 /messages/modules/commandModule/outputs/avroOutput
       INTO BrokeredEndpoint
  (\"/modules/avroWriter/inputs/avroWriterInput\")",
       "commandToCloud": "FROM
  /messages/modules/commandModule/outputs/iotHubOut INTO           "
```

```
  },
       "storeAndForwardConfiguration": {
         "timeToLiveSecs": 7200
         }
       }
  }
```

Explanation:
Box 1: $connectionModuled
Add a route that tells the edge hub to route any message received by the IoT Edge device that was not sent by an IoT Edge module.
Box 2: $upstream
Send messages to $upstream, which passes the messages to the connected IoT Hub.
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/tutorial-machine-learning-edge-06-custom- modules

QUESTION 125
Drag and Drop Question
You have an Azure IoT Edge device named Edge1.
You need to configure the module container to link the module storage to the host storage.
How should you configure the deployment manifest? To answer, drag the appropriate keys to the correct targets. Each key 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.



Keys

"binds":

"createOptions":

"portBindings":

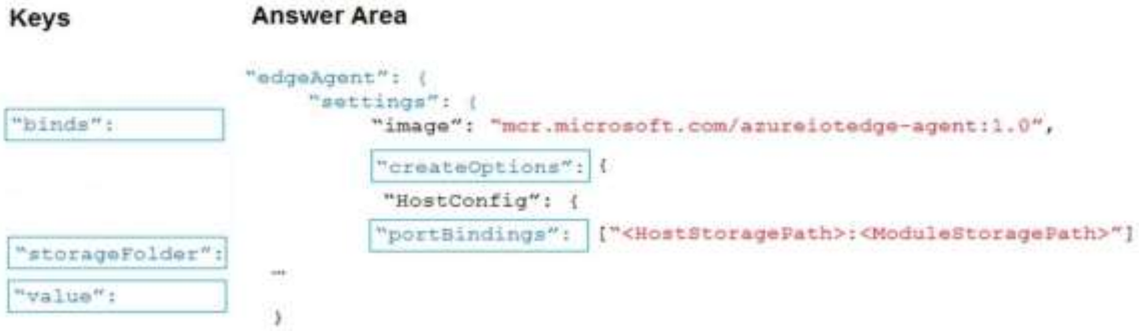
"storageFolder":

"value":

Answer Area

```
"edgeAgent": {
    "settings": {
        "image": "mcr.microsoft.com/azureiotedge-agent:1.0",
        ☐ {
         "HostConfig": {
        ☐ ["<HostStoragePath>:<ModuleStoragePath>"]
  ...
  }
```

Answer:



Keys

"binds":

"storageFolder":

"value":

Answer Area

```
"edgeAgent": {
    "settings": {
        "image": "mcr.microsoft.com/azureiotedge-agent:1.0",
        "createOptions": {
         "HostConfig": {
        "portBindings": ["<HostStoragePath>:<ModuleStoragePath>"]
  ...
  }
```

Explanation:
Box 1: createOptions
Every module has a settings property that contains the module image, an address for the container image in a container registry, and any createOptions to configure the image on startup.
Box 2: portbindings
Use the PortBindings setting in the HostConfig group of the Docker container create options to map the exposed port in the module to a port on the host device. For example, if you exposed port 8080 inside the module and want to map that to port 80 of the host device, the create options in the template.json file would look like the following example:

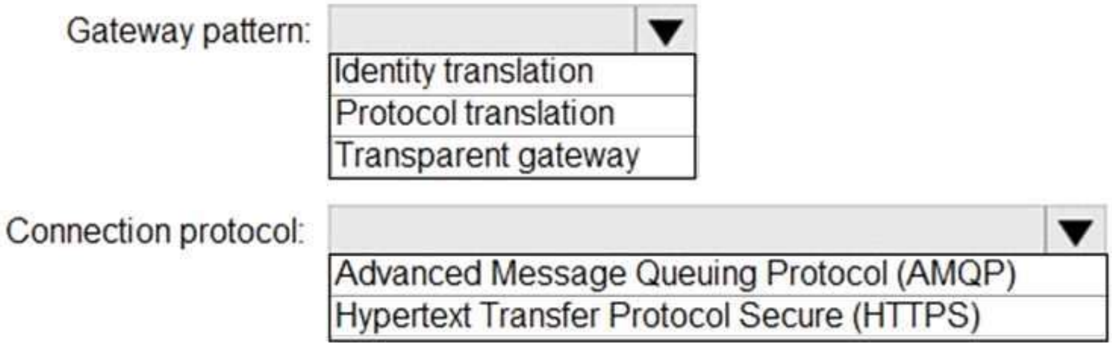
```
"createOptions": {
"HostConfig": {
"PortBindings": {
"8080/tcp": [
{
"HostPort": "80"
}
]
}
}
}
```

Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/how-to-use-create-options

QUESTION 126
Hotspot Question
You have an Azure subscription that contains an Azure IoT hub, an Azure IoT Edge gateway, and 1,000 leaf devices. The leaf devices use a custom communication protocol that is NOT supported by the IoT hub.
You need to configure the gateway to meet the following requirements:

```
- Minimize the number of connections between the gateway and the IoT hub.
- Support addressing cloud-to-device messages to individual leaf devices.
```

How should you configure the gateway? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



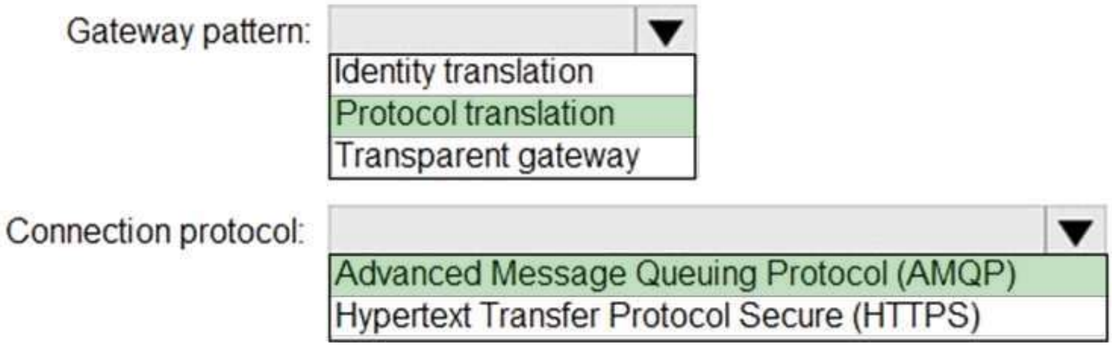
Gateway pattern:

- Identity translation
- Protocol translation
- Transparent gateway

Connection protocol:

- Advanced Message Queuing Protocol (AMQP)
- Hypertext Transfer Protocol Secure (HTTPS)

Answer:



Gateway pattern:

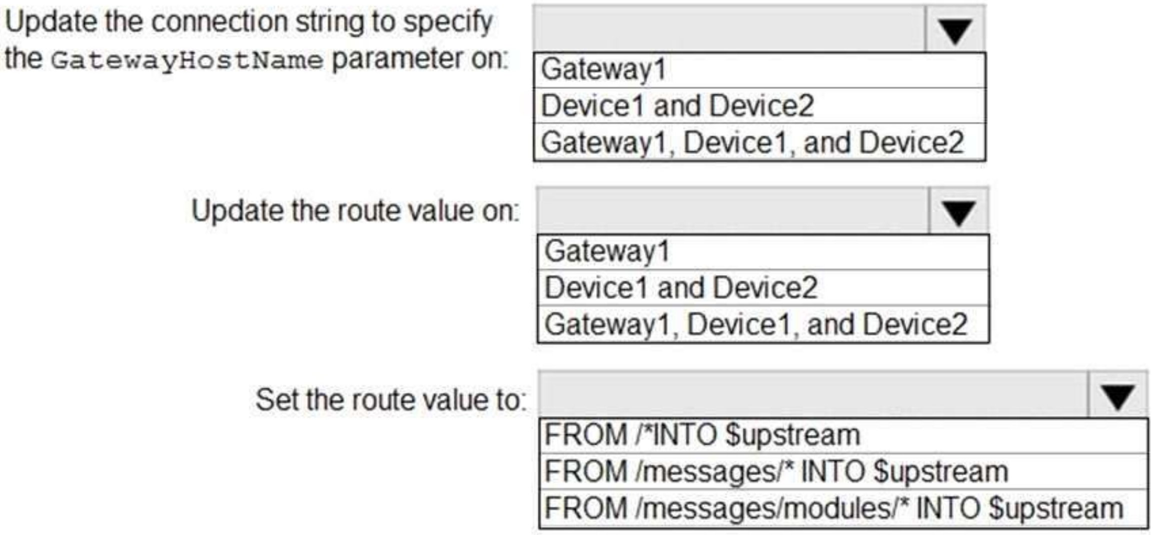
- Identity translation
- Protocol translation
- Transparent gateway

Connection protocol:

- Advanced Message Queuing Protocol (AMQP)
- Hypertext Transfer Protocol Secure (HTTPS)

Explanation:
Box 1: Protocol translation
In the protocol translation gateway pattern, only the IoT Edge gateway has an identity with 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.
Box 2: Advanced MessageQueuing Protocol (AMQP)
Connection multiplexing - All devices connecting to IoT Hub through an IoT Edge gateway can use the same underlying connection. This multiplexing capability requires that the IoT Edge gateway uses AMQP as its upstream protocol.
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/iot-edge-as-gateway

QUESTION 127
Hotspot Question
You have an Azure subscription that contains an Azure IoT hub and two IoT devices named Device1 and Device2.
You plan to deploy an Azure IoT Edge gateway device named Gateway1.
You need to ensure that all device-to-cloud messages and twin change notifications from Device1 and Device2 to the IoT hub are routed by using Gateway1.
What tasks should you perform to configure the devices? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Update the connection string to specify the `GatewayHostName` parameter on:

- Gateway1
- Device1 and Device2
- Gateway1, Device1, and Device2

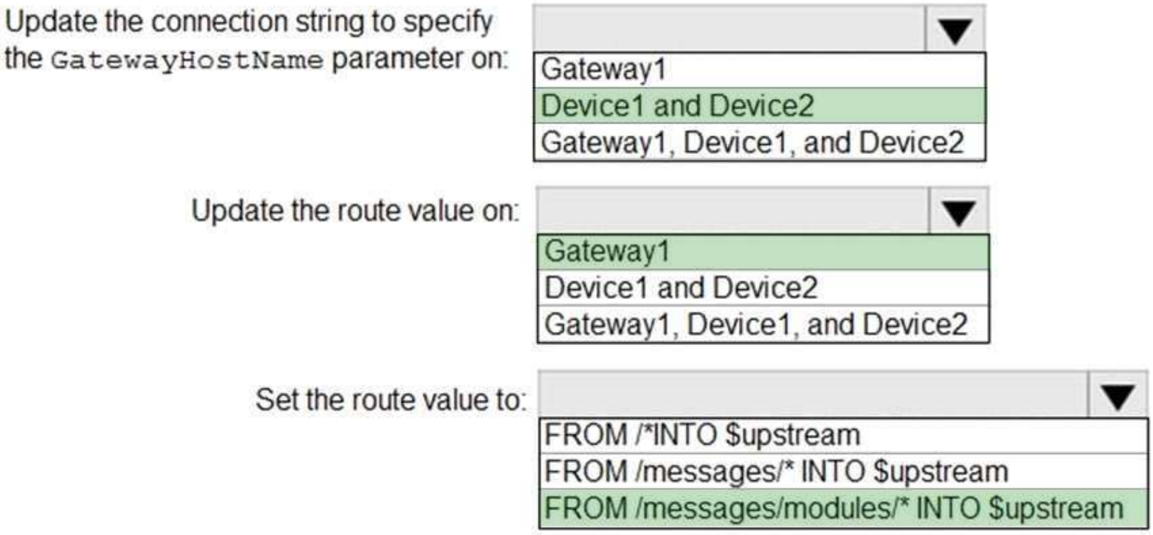
Update the route value on:

- Gateway1
- Device1 and Device2
- Gateway1, Device1, and Device2

Set the route value to:

- FROM /*INTO $upstream
- FROM /messages/* INTO $upstream
- FROM /messages/modules/* INTO $upstream

Answer:



Update the connection string to specify the `GatewayHostName` parameter on:

- Gateway1
- [✓ Device1 and Device2]
- Gateway1, Device1, and Device2

Update the route value on:

- [✓ Gateway1]
- Device1 and Device2
- Gateway1, Device1, and Device2

Set the route value to:

- FROM /*INTO $upstream
- FROM /messages/* INTO $upstream
- [✓ FROM /messages/modules/* INTO $upstream]

Explanation:
Box 1: Device1 and Device2
Connection strings for downstream devices need the following components:
The gateway device that the device connects through. Provide the hostname value from the IoT Edge gateway device's config file: GatewayHostName={gateway hostname}
Box 2: Gateway1
To deploy the IoT Edge hub module and configure it with routes to handle incoming messages from downstream devices, follow these steps:
In the Azure portal, navigate to your IoT hub.
Go to IoT Edge and select your IoT Edge device that you want to use as a gateway.
Select Set Modules.
On the Modules page, you can add any modules you want to deploy to the gateway device.
Select Next: Routes.
On the Routes page, make sure that there is a route to handle messages coming from downstream devices. For example:
A route that sends all messages, whether from a module or from a downstream device, to IoT Hub:
Name: allMessagesToHub
Value: FROM /messages/* INTO $upstream
Box 3: FROM /messages/* INTO $upstream
Reference:

https://docs.microsoft.com/en-us/azure/iot-edge/how-to-authenticate-downstream-device