

Microsoft.AZ-220.v2023-05-24.q110

| | |
|---|-------------------------------|
| Exam Code: | AZ-220 |
| Exam Name: | Microsoft Azure IoT Developer |
| Certification Provider: | Microsoft |
| Free Question Number: | 110 |
| Version: | v2023-05-24 |
| # of views: | 1083 |
| # of Questions views: | 1100 |
| https://www.exam-tests.com/AZ-220-exam/Microsoft.AZ-220.v2023-05-24.q110.html | |

NEW QUESTION: 1

You have an Azure IoT hub and an Azure virtual network.

You configure a private endpoint for the IoT hub.

You need to ensure that the IoT hub can send data to downstream services. What should you create first?

- A. a message route
- B. a managed identity
- C. an IP filter rule
- D. a consumer group

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 2

You are planning a proof of concept (POC) that will use an Azure IoT hub.

You have two self-signed client authentication certificates named Cert1 and Cert2. Cert1 has a basic constraint that contains Subject Type=C. You need to identify which certificates to use.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Certificate you can use to authenticate a leaf device to IoT Hub during testing:

| | |
|----------------------|---|
| | ▼ |
| Cert1 only | |
| Cert2 only | |
| Both Cert1 and Cert2 | |
| Neither certificate | |

Certificate that you can upload to IoT Hub as a verified certificate:



| | |
|----------------------|---|
| | ▼ |
| Cert1 only | |
| Cert2 only | |
| Both Cert1 and Cert2 | |
| Neither certificate | |

Answer:

Certificate you can use to authenticate a leaf device to IoT Hub during testing:

| | |
|----------------------|---|
| | ▼ |
| Cert1 only | |
| Cert2 only | |
| Both Cert1 and Cert2 | |
| Neither certificate | |

Certificate that you can upload to IoT Hub as a verified certificate:

| | |
|----------------------|---|
| | ▼ |
| Cert1 only | |
| Cert2 only | |
| Both Cert1 and Cert2 | |
| Neither certificate | |

Reference:

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

NEW QUESTION: 3

You have an Azure IoT hub named hub1 and five IoT devices. The IoT devices connect to hub1 and send data that is formatted by using a proprietary binary format. You need to convert the data to JSON before the data is sent to a downstream service. The solution must minimize administrative effort. What should you use?

A. an Azure Service Bus trigger

- B. an Azure IoT Central application
- C. an Azure function
- D. a message enrichment

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 4

You create an Azure IoT hub as shown in the following exhibit.

The screenshot shows the 'Management' tab of an Azure IoT Hub. The 'Scale tier and units' section is set to 'S1: Standard tier' with 1 unit. 'Defender for IoT' is turned on. A table lists the following features and their status:

| Feature | Status |
|--------------------------|--------------------------------------|
| Pricing and scale tier | S1 |
| Messages per day | 400,000 |
| Cost per month | 18.63 GBP |
| Defender for IoT | 0.000745309 GBP per device per month |
| Device-to-cloud-messages | Enabled |
| Message routing | Enabled |
| Cloud-to-device commands | Enabled |
| IoT Edge | Enabled |
| Device management | Enabled |

Advanced settings show 'Scale' is set to 2 device-to-cloud partitions.

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

| Statements | Yes | No |
|---|-----------------------|-----------------------|
| To support 1,200,000 messages per day and have Cloud-to-device commands enabled, the tier must be set to S3: Standard tier . | <input type="radio"/> | <input type="radio"/> |
| Defender for IoT can be enabled if the tier is set to B3: Basic tier . | <input type="radio"/> | <input type="radio"/> |
| Increasing Device-to-cloud partitions will increase the number of possible concurrent readers. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements | Yes | No |
|---|----------------------------------|----------------------------------|
| To support 1,200,000 messages per day and have Cloud-to-device commands enabled, the tier must be set to S3: Standard tier . | <input type="radio"/> | <input checked="" type="radio"/> |
| Defender for IoT can be enabled if the tier is set to B3: Basic tier . | <input type="radio"/> | <input checked="" type="radio"/> |
| Increasing Device-to-cloud partitions will increase the number of possible concurrent readers. | <input checked="" type="radio"/> | <input type="radio"/> |

Explanation

The screenshot shows a Microsoft exam question interface. It features a header with the Microsoft logo and the word 'Microsoft'. Below the header, there is a table with three rows of statements and two columns for 'Yes' and 'No' answers. The 'Yes' column has radio buttons, and the 'No' column has radio buttons. The statements are:

| Statements | Yes | No |
|---|----------------------------------|----------------------------------|
| To support 1,200,000 messages per day and have Cloud-to-device commands enabled, the tier must be set to S3: Standard tier . | <input type="radio"/> | <input checked="" type="radio"/> |
| Defender for IoT can be enabled if the tier is set to B3: Basic tier . | <input type="radio"/> | <input checked="" type="radio"/> |
| Increasing Device-to-cloud partitions will increase the number of possible concurrent readers. | <input checked="" type="radio"/> | <input type="radio"/> |

NEW QUESTION: 5

You have an Azure IoT hub.

You plan to implement IoT Hub events by using Azure Event Grid.

You need to send an email when the following events occur:

- * Device Created
- * Device Deleted
- * Device Connected
- * Device Disconnected

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

NOTE: Each correct selection is worth one point.

- A. From the IoT hub, configure an event subscription that has API management as the Endpoint Type.
- B. From the IoT hub, configure an event subscription that has Web Hook as the Endpoint Type.
- C. Create an Azure logic app that has a Request trigger.
- D. From the IoT hub, configure an event subscription that has Service Bus Queue as the Endpoint Type.

Answer: B,C (LEAVE A REPLY)

For non-telemetry events like DeviceConnected, DeviceDisconnected, DeviceCreated and DeviceDeleted, the Event Grid filtering can be used when creating the subscription.

C: Azure Event Grid enables you to react to events in IoT Hub by triggering actions in your downstream business applications.

A trigger, such as a Request trigger, is a specific event that starts your logic app.

Reference:

<https://docs.microsoft.com/en-us/azure/event-grid/publish-iot-hub-events-to-logic-apps>

NEW QUESTION: 6

You need to install the Azure IoT Edge runtime on a new device that runs Windows 10 IoT Enterprise.

Which four 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

From an elevated PowerShell prompt, run the following command.

```
•(Invoke-WebRequest -useb https://aka.ms/  
iotedge-win) |  
Invoke-Expression; Initialize-IoTEdge
```

From Azure IoT Hub, create an IoT Edge device.

From a Bash prompt, run the following commands.

```
curl https://packages.  
microsoft.com/keys/microsoft.asc |  
gpg --dearmor > microsoft.gpg  
sudo cp ./microsoft.gpg /etc/apt/trusted.gpg.d/
```

From an elevated PowerShell prompt, run the following command.

```
•(Invoke-WebRequest -useb https://aka.ms/  
iotedge-win) |  
Invoke-Expression; Deploy-IoTEdge
```

Enter the IoT Edge device connection string.

From a Bash prompt, run the following commands.

```
sudo apt-get install moby-engine
```



Answer:

Answer Area

From Azure IoT Hub, create an IoT Edge Device

From an elevated PowerShell prompt, run the following command.

From the relevant PowerShell Prompt, run the following command.

Enter the IoT Edge device connection string.

- 1 - From Azure IoT Hub, create an IoT Edge Device
- 2 - From an elevated PowerShell prompt, run the following command.
- 3 - From the relevant PowerShell Prompt, run the following command.
- 4 - Enter the IoT Edge device connection string.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/module-composition>

NEW QUESTION: 7

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: (SHOW ANSWER)

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: 8

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 Stream Analytics job that receives input from an Azure IoT hub and sends the outputs to Azure Blob storage. The job has compatibility level 1.1 and six streaming units.

You have the following query for the job.

```
SELECT COUNT(*) AS Count, TollBoothID
INTO BlobOutput
FROM IotHubInput
GROUP BY TumblingWindow(minute, 3), TollBoothID
```

You plan to increase the streaming unit count to 12.

You need to optimize the job to take advantage of the additional streaming units and increase the throughput.

Solution: You change the compatibility level of the job to 1.2.

Does this meet the goal?

- A. Yes
- B. No

Answer: B (LEAVE A REPLY)

Explanation

Max number of Streaming Units with one step and with no partitions is 6.

Reference:

<https://docs.microsoft.com/en-us/azure/stream-analytics/stream-analytics-parallelization>

NEW QUESTION: 9

You create an Azure Stream Analytics job that has the following query.

```
SELECT
    Count(*) AS dailyCount,
    System.Timestamp() AS time
INTO FunctionOutput
FROM IotHubInput TIMESTAMP BY deviceTime
GROUP BY TumblingWindow(hour, 24)
```

The job is configured to have an Azure IoT Hub input and an output to an Azure function.

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

NOTE: Each correct selection is worth one point.

| Statements | Yes | No |
|---|-----------------------|-----------------------|
| The function will be invoked at midnight UTC. | <input type="radio"/> | <input type="radio"/> |
| The function will be invoked only when the IoT hub receives telemetry. | <input type="radio"/> | <input type="radio"/> |
| When the Stream Analytics job is restarted, the function can be invoked more than once in a 24-hour period. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements | Yes | No |
|---|----------------------------------|----------------------------------|
| The function will be invoked at midnight UTC. | <input checked="" type="radio"/> | <input type="radio"/> |
| The function will be invoked only when the IoT hub receives telemetry. | <input type="radio"/> | <input checked="" type="radio"/> |
| When the Stream Analytics job is restarted, the function can be invoked more than once in a 24-hour period. | <input checked="" type="radio"/> | <input type="radio"/> |

Explanation

| Statements | Yes | No |
|---|----------------------------------|----------------------------------|
| The function will be invoked at midnight UTC. | <input checked="" type="radio"/> | <input type="radio"/> |
| The function will be invoked only when the IoT hub receives telemetry. | <input type="radio"/> | <input checked="" type="radio"/> |
| When the Stream Analytics job is restarted, the function can be invoked more than once in a 24-hour period. | <input checked="" type="radio"/> | <input type="radio"/> |

Box 1: Yes

All time handling operations in Azure Stream Analytics are in UTC.

Box 2: No

Tumbling windows are a series of fixed-sized, non-overlapping and contiguous time intervals.

Box 3: Yes

Reference:

<https://docs.microsoft.com/en-us/stream-analytics-query/time-management-azure-stream-analytics>

NEW QUESTION: 10

You create an Azure IoT hub by running the following command.

```
aziot hub create --resource-group MyResourceGroup --name MylotHub --sku B1 -- location westus --partition-count 4
```

What does MylotHub support?

- A. Device Provisioning Service
- B. cloud-to-device messaging
- C. Azure IoT Edge
- D. device twins

Answer: A (LEAVE A REPLY)

The Device Provisioning Service is included in the Basic Tiers (such as B1).

Incorrect Answers:

B, C, D: The Standard tier is needed for cloud-to-device messaging, Azure IoT Edge, and device twins.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-scaling>

NEW QUESTION: 11

You have an Azure IoT hub

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

| Name | Code |
|---------|---|
| Device1 | <pre>"tags": { "office": "Seattle-1" },</pre> |
| Device2 | <pre>"tags": { "office": "Seattle-2" },</pre> |
| Device3 | <pre>"tags": { "office": "London" },</pre> |
| Device4 | <pre>"tags": { "office": "LDN" },</pre> |

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

| Name | Code |
|-------------|---|
| Deployment1 | <pre>{ "id": "deploysim", "priority": 10, "targetCondition": "tags.office='Seattle-*' ", "SedgeHub": { "properties.desired": { "routes": { "MyModule1": "FROM /messages/modules/ MyModule1/* INTO \$upstream" } } } }</pre> |
| Deployment2 | <pre>{ "id": "deploysim", "priority": 20, "targetCondition": "tags.office='London' ", "SedgeHub": { "properties.desired": { "routes": { "MyModule1": "FROM /messages/modules/ MyModule1/* INTO \$upstream" } } } }</pre> |
| Deployment3 | <pre>{ "id": "deploysim", "priority": 30, "targetCondition": "tags.office='London' OR tags.office='LDN' ", "SedgeHub": { "properties.desired": { "routes": { "MyModule2": "FROM /messages/modules/ MyModule2/* INTO \$upstream" } } } }</pre> |

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

Answer Area

| Statements | Yes | No |
|--|-----------------------|-----------------------|
| The IoT hub receives messages from the MyModule1 route of Device2. | <input type="radio"/> | <input type="radio"/> |
| The IoT hub receives messages from the MyModule2 route of Device3. | <input type="radio"/> | <input type="radio"/> |
| The IoT hub receives messages from the MyModule2 route of Device4. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

| Statement | Yes | No |
|--|----------------------------------|----------------------------------|
| The IoT hub receives messages from the MyModule1 route of Device2. | <input checked="" type="radio"/> | <input type="radio"/> |
| The IoT hub receives messages from the MyModule2 route of Device3. | <input type="radio"/> | <input checked="" type="radio"/> |
| The IoT hub receives messages from the MyModule2 route of Device4. | <input checked="" type="radio"/> | <input type="radio"/> |

Explanation

Answer Area

| Statements | Yes | No |
|--|----------------------------------|----------------------------------|
| The IoT hub receives messages from the MyModule1 route of Device2. | <input checked="" type="radio"/> | <input type="radio"/> |
| The IoT hub receives messages from the MyModule2 route of Device3. | <input type="radio"/> | <input checked="" type="radio"/> |
| The IoT hub receives messages from the MyModule2 route of Device4. | <input checked="" type="radio"/> | <input type="radio"/> |

NEW QUESTION: 12

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

You need to be notified about failed local logins to a subnet of 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

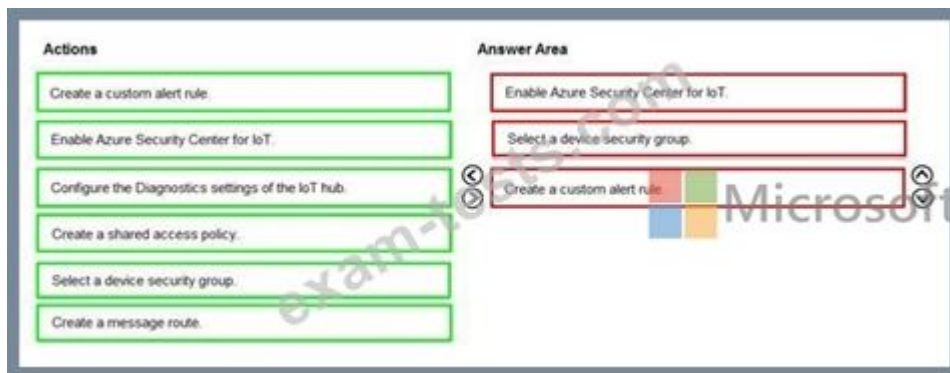
- Create a custom alert rule.
- Enable Azure Security Center for IoT.
- Configure the Diagnostics settings of the IoT hub.
- Create a shared access policy.
- Select a device security group.
- Create a message route.

Answer Area

Answer Area

Three empty boxes for moving and ordering actions.

Answer:



Explanation:

Step 1: Enable Azure Security Center for IoT

Security alerts, such as failed local IoT hub logins, are stored in AzureSecurityOfThings.SecurityAlert table in the Log Analytics workspace configured for the Azure Security Center for IoT solution.

Step 2: Select a device security group

Update a device security group..

Step 3: Create a custom alert rule

..by creating a custom alert rule

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/asc-for-iot/how-to-security-data-access>

<https://docs.microsoft.com/en-us/rest/api/securitycenter/devicesecuritygroups/createorupdate>

NEW QUESTION: 13

You have an Azure IoT hub that uses a Device Provisioning Service instance.

You create a new individual device enrollment that uses symmetric key attestation.

Which detail from the enrollment is required to auto provision the device by using the Device Provisioning Service?

- A. the registration ID of the enrollment
- B. the primary key of the enrollment
- C. the device identity of the IoT hub
- D. the hostname of the IoT hub

Answer: (SHOW ANSWER)

An enrollment is the record of devices or groups of devices that may register through auto-provisioning. The enrollment record contains information about the device or group of devices, including:

- * the attestation mechanism used by the device
- * the optional initial desired configuration
- * desired IoT hub

the desired device ID

Note: Azure IoT auto-provisioning can be broken into three phases:

1. Service configuration - a one-time configuration of the Azure IoT Hub and IoT Hub Device Provisioning Service instances, establishing them and creating linkage between them.

2. Device enrollment - the process of making the Device Provisioning Service instance aware of the devices that will attempt to register in the future. Enrollment is accomplished by configuring device identity information in the provisioning service, as either an "individual enrollment" for a single device, or a "group enrollment" for multiple devices.

3. Device registration and configuration

Reference:

<https://docs.microsoft.com/en-us/azure/iot-dps/concepts-service#enrollment>

NEW QUESTION: 14

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.)

| <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 (LEAVE A REPLY)

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: 15

You have three Azure IoT hubs named Hub1, Hub2, and Hub3, a Device Provisioning Service instance, and an IoT device named Device1.

Each IoT hub is deployed to a separate Azure region. Device enrollment uses the Lowest latency allocation policy.

The Device Provisioning Service uses the Lowest latency allocation policy. Device1 is auto-provisioned to Hub1 by using the Device Provisioning Service. Device1 regularly moves between regions.

You need to ensure that Device1 always connects to the IoT hub that has the lowest latency.

What should you do?

- A. Configure device attestation that uses X.509 certificates.
- B. Implement device certificate rolling.
- C. Disenroll and reenroll Device1.
- D. Configure the re-provisioning policy.

Answer: D (LEAVE A REPLY)

Explanation

Automated re-provisioning support.

Microsoft added first-class support for device re-provisioning which allows devices to be reassigned to a different IoT solution sometime after the initial solution assignment. Re-provisioning support is available in two options:

Factory reset, in which the device twin data for the new IoT hub is populated from the enrollment list instead of the old IoT hub. This is common for factory reset scenarios as well as leased device scenarios. Migration, in which device twin data is moved from the old IoT hub to the new IoT hub. This is common for scenarios in which a device is moving between geographies.

Reference:

<https://azure.microsoft.com/en-us/blog/new-year-newly-available-iot-hub-device-provisioning-service-features/>

NEW QUESTION: 16

You need to recommend the format of telemetry messages to meet the POV requirements.

What should you recommend?

- A. XML
- B. Avro
- C. JSON

Answer: (SHOW ANSWER)

Scenario: POV Requirements

* Ensure that all message content during this phase is human readable to simplify debugging.

Avro uses a binary format, so it is not human readable.

The more lightweight JSON (Javascript object notation) has become a popular alternative to XML for various reasons. A couple obvious ones are:

- * Less verbose- XML uses more words than necessary
- * JSON is faster- Parsing XML software is slow and cumbersome.

Reference:

<https://blog.cloud-elements.com/json-better-xml>

Process and manage data

Question Set 3

Valid AZ-220 Dumps shared by BraindumpsPass.com for Helping Passing AZ-220 Exam! BraindumpsPass.com now offer the **newest AZ-220 exam dumps**, the BraindumpsPass.com AZ-220 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com AZ-220 dumps with Test Engine here:
<https://www.braindumpspass.com/Microsoft/AZ-220-practice-exam-dumps.html> (205 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 17

You have an Azure subscription that contains an Azure IoT hub named Hub1 and an Azure IoT Edge device named Device1.

You need to configure Device1 to operate in extended offline mode and to support modifying the configuration of modules deployed to Device1 while the device is offline.

Solution: From Microsoft Visual Studio Code, you modify the deployment manifest and you configure the address of the localhost for the container registry in the runtime settings of edgeAgent. You deploy the manifest to Device1, and then you restart the device.

Does this meet the goal?

A. No

B. Yes

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 18

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 |
|--|-------------|
| <p>Create an individual device enrollment by using the Device Provisioning Service.</p> | |
| <p>Run the following commands.</p> <pre>sudo apt-get install moby-engine sudo apt-get install moby-cli sudo apt-get install iotedge</pre> | |
| <p>Add the connection string to the /etc/iotedge/config.yaml file, and then run the following command.</p> <pre>sudo systemctl restart iotedge</pre> | <p>⏪ ⏩</p> |
| <p>Install the IoT edge repository for Ubuntu Server 18.04 on the physical device. From IoT Hub, create a new IoT Edge device.</p> | |
| <p>From IoT Hub, create an IoT Edge device registry entry.</p> | |

Answer:

| Actions | Answer Area |
|--|--|
| <p>Create an individual device enrollment by using the Device Provisioning Service.</p> | <p>Run the following commands.</p> <pre>sudo apt-get install moby-engine sudo apt-get install moby-cli sudo apt-get install iotedge</pre> |
| <p>Run the following commands.</p> <pre>sudo apt-get install moby-engine sudo apt-get install moby-cli sudo apt-get install iotedge</pre> | <p>From IoT Hub, create an IoT Edge device registry entry.</p> |
| <p>Add the connection string to the /etc/iotedge/config.yaml file, and then run the following command.</p> <pre>sudo systemctl restart iotedge</pre> | <p>⏪ ⏩</p> <p>Add the connection string to the /etc/iotedge/config.yaml file, and then run the following command.</p> <pre>sudo systemctl restart iotedge</pre> <p>⏪ ⏩</p> |
| <p>Install the IoT edge repository for Ubuntu Server 18.04 on the physical device. From IoT Hub, create a new IoT Edge device.</p> | |
| <p>From IoT Hub, create an IoT Edge device registry entry.</p> | |

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 recommend 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: 19

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 Stream Analytics job that receives input from an Azure IoT hub and sends the outputs to Azure Blob storage. The job has compatibility level 1.1 and six streaming units.

You have the following query for the job.

```
SELECT COUNT(*) AS Count, TollBoothID
INTO BlobOutput
FROM IotHubInput
GROUP BY TumblingWindow(minute, 3), TollBoothID
```

You plan to increase the streaming unit count to 12.

You need to optimize the job to take advantage of the additional streaming units and increase the throughput.

Solution: You change the query to the following.

```
WITH Step1 AS (
SELECT COUNT(*) AS Count, TollBoothID, PartitionID
FROM IotHubInput PARTITION BY PartitionID
GROUP BY TumblingWindow(minute, 3), TollBoothID, PartitionID
)
SELECT SUM(Count) AS Count, TollBoothID
INTO BlobOutput
FROM Step1
GROUP BY TumblingWindow(minute, 3), TollBoothID
```

Does this meet the goal?

A. Yes

B. No

Answer: A (LEAVE A REPLY)

Max number of Streaming Units with one step and with no partitions is 6.

Reference:

<https://docs.microsoft.com/en-us/azure/stream-analytics/stream-analytics-parallelization>

NEW QUESTION: 20

You have an Azure IoT solution that includes an Azure IoT hub, a Device Provisioning Service instance, and 1,000 connected IoT devices. The IoT devices are allocated to four enrollment groups. Each enrollment group is configured to use certificate attestation.

You need to decommission all the devices in a single enrollment group and the enrollment group itself.

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

- Delete each device from the identity registry.
- Delete the IoT hub.
- Remove the X.509 root certificate.
- Disable the enrollment group.
- Delete the enrollment group.

Answer Area

Answer:

Actions

- Delete each device from the identity registry.
- Delete the IoT hub.
- Remove the X.509 root certificate.
- Disable the enrollment group.
- Delete the enrollment group.

Answer Area

- Disable the enrollment group.
- Delete each device from the identity registry.
- Delete the enrollment group.

Explanation:

To deprovision all of the devices that have been provisioned through an enrollment group:
 Disable the enrollment group to disallow its signing certificate.

Use the list of provisioned devices for that enrollment group to disable or delete each device from the identity registry of its respective IoT hub.

After disabling or deleting all devices from their respective IoT hubs, you can optionally delete the enrollment group. Be aware, though, that, if you delete the enrollment group and there is an enabled enrollment group for a signing certificate higher up in the certificate chain of one or more of the devices, those devices can re-enroll.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-dps/how-to-unprovision-devices>

NEW QUESTION: 21

You create a new IoT device named device1 on iothub1. Device1 has a primary key of Uihuih76hbHb.

How should you complete the device connection string? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

HostName= [azure-devices.net] . [azure-devices.net] ; DeviceId= [azure-devices.net] : SharedAccessKey=Uihuih76hbHb

Options for HostName: azure-devices.net, criticalep, device1, iothub1, tracestate

Options for DeviceId: azure-devices.net, criticalep, device1, iothub1, tracestate

Answer:



Explanation:

Box 1: iothub1

The Azure IoT hub is named iothub1.

Box 2: azure-devices.net

The format of the device connection string looks like:

HostName={YourIoTHubName}.azure-

devices.net;DeviceId=MyNodeDevice;SharedAccessKey={YourSharedAccessKey} Box 1:

device1 Device1 has a primary key of Uihuih76hbHb.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/quickstart-control-device-dotnet>

NEW QUESTION: 22

You have an Azure IoT hub that has a hostname of contoso-hub.azure-devices.net and an MCU-based IoT device named Device1. Device1 does You plan to connect Device1 to the IoT hub by using the Message Queuing Telemetry Transport (MQTT) protocol and to authenticate by using X.509 certificates.

You need to ensure that Device1 can authenticate to the IoT hub.

What should you do?

- A. Create an Azure key vault and enable the encryption of data at rest for the IoT hub by using a customermanaged key.
- B. Enable a hardware security module (HSM) on Device1.
- C. From the Azure portal, create an IoT Hub Device Provisioning Service (DPS) instance and add a certificate enrollment for Device1.
- D. Add the DigiCert Baltimore Root Certificate to Device1.

Answer: D (LEAVE A REPLY)

Explanation

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>

NEW QUESTION: 23

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: ([SHOW ANSWER](#))

Explanation

<https://docs.microsoft.com/en-us/azure/iot-edge/deploy-modbus-gateway>

NEW QUESTION: 24

HOTSPOT

You have an Azure IoT hub.

You plan to deploy 1,000 IoT devices by using automatic device management.

The device twin is shown below.

```

{
  "deviceId": "ContosoHyperDriveEngine1",
  "etag": "AAAAAAAAAAw=",
  "deviceEtag": "MTYyNDk20kw",
  "status": "enabled",
  "statusUpdateTime": "0001-01-01t00:00:00Z",
  "connectionTime": "Disconnected",
  "lastActivityTime": "0001-01-01T00:00:00Z",
  "cloudToDeviceMessageCount": 0,
  "authenticationType": "sas",
  "x509Thumbprint": {
    "primaryThumbprint": null,
    "secondaryThumbprint": null
  },
  "version": 13,
  "tags": {
    "engine": {
      "warpCorVersion": "1.2.65b",
      "warpDriveType": "WM105a"
    }
  },
  "properties": {
    "desired": {
      "$metadata": {
        "$lastUpdated": "2019-10-17T18:43:33.7599556Z"
      },
      "$version": 1
    },
    "reported": {
      "$metadata": {
        "$lastUpdated": "2019-10-17T18:43:33.7599556Z"
      },
      "$version": 1
    }
  }
}

```



You need to configure automatic device management for the deployment.

Which target Condition and Device Twin Path should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.


Hot Area:

Answer Area  Microsoft

Target Condition:

Device Twin Path:

Answer:

Answer Area  Microsoft

Target Condition:

Device Twin Path:

Explanation:

Box 1: tags.engine.warpDriveType='VM105a'

Use tags to target twins. Before you create a configuration, you must specify which devices or modules you want to affect. Azure IoT Hub identifies devices and using tags in the device twin, and identifies modules using tags in the module twin.

Box 2: properties.desired.warpOperating

The twin path, which is the path to the JSON section within the twin desired properties that will be set.

For example, you could set the twin path to properties.desired.chiller-water and then provide the following JSON content:

{

```
"temperature": 66,  
"pressure": 28  
}
```

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-automatic-device-management> Provision and manage devices
Testlet 1 Case Study This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided. To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Existing Environment. Current State of Development

Contoso produces a set of Bluetooth sensors that read the temperature and humidity. The sensors connect to IoT gateway devices that relay the data.

All the IoT gateway devices connect to an Azure IoT hub named iothub1.

Existing Environment. Device Twin

You plan to implement device twins by using the following JSON sample.



Microsoft

```
{
  "deviceId": "device_n",
  "etag": "AAAAAAAAAAQ=",
  "deviceEtag": "NDcwMTU4Mzk=",
  "status": "enabled",
  "statusUpdateTime": "0001-01-01T00:00:00Z",
  "connectionState": "Disconnected",
  "lastActivityTime": "0001-01-01T00:00:00Z",
  "cloudToDeviceMessageCount": 0,
  "authenticationType": "sas",
  "x509Thumbprint": {
    "primaryThumbprint": null,
    "secondaryThumbprint": null
  },
  "version": 11,
  "properties": {
    "desired": {
      "fanSpeed": 70,
      "$metadata": {
        "$lastUpdated": "2019-10-16T09:43:42.2944169Z",
        "$lastUpdatedVersion": 4,
        "fanSpeed": {
          "$lastUpdated": "2019-10-16T09:43:42.2944169Z",
          "$lastUpdatedVersion": 4
        }
      }
    },
    "$version": 4
  },
  "reported": {
    "fanSpeed": 80,
    "metadata": {
      "$lastUpdated": "2019-10-16T09:43:42.4035171Z",
      "fanSpeed": {
        "$lastUpdated": "2019-10-16T09:43:42.4035171Z"
      }
    }
  },
  "$version": 7
}
},
"capabilities": {
  "lotEdge": false
}
}
```

Existing Environment. Azure Stream Analytics

Each room will have between three to five sensors that will generate readings that are sent to a single IoT gateway device. The IoT gateway device will forward all the readings to iothub1 at intervals of between 10 and 60 seconds.

You plan to use a gateway pattern so that each IoT gateway device will have its own IoT Hub device identity.

You draft the following query, which is missing the GROUP BY clause.

```
SELECT
AVG(temperature),
System.TimeStamp() AS AsaTime
FROM
iothub
```

You plan to use a 30-second period to calculate the average temperature reading of the sensors. You plan to minimize latency between the condition reported by the sensors and the corresponding alert issued by the Stream Analytics job.

Existing Environment. Device Messages

The IoT gateway devices will send messages that contain the following JSON data whenever the temperature exceeds a specified threshold.

```
{
  "event": {
    "payload": "Temperature = 26.23 Humidity = 78.70597746416186 Button = 0",
    "properties": {
      "application": {
        "level": "critical"
      }
    }
  }
}
```



The levelproperty will be used to route the messages to an Azure Service Bus queue endpoint named criticalep.

Existing Environment. Issues

You discover connectivity issues between the IoT gateway devices and iothub1, which cause IoT devices to lose connectivity and messages.

Requirements. Planning Changes

Contoso plans to make the following changes:

- * Use Stream Analytics to process and view data.
- * Use Azure Time Series Insights to visualize data.
- * Implement a system to sync device statuses and required settings.
- * Add extra information to messages by using message enrichment.
- * Create a notification system to send an alert if a condition exceeds a specified threshold.
- * Implement a system to identify what causes the intermittent connection issues and lost messages.

Requirements. Technical Requirements

Contoso must meet the following requirements:

- * Use the built-in functions of IoT Hub whenever possible.
- * Minimize hardware and software costs whenever possible.
- * Minimize administrative effort to provision devices at scale.
- * Implement a system to trace message flow to and from iotHub1.
- * Minimize the amount of custom coding required to implement the planned changes.
- * Prevent read operations from being negatively affected when you implement additional services.

NEW QUESTION: 25

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 correct 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: C,D (LEAVE A REPLY)

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:

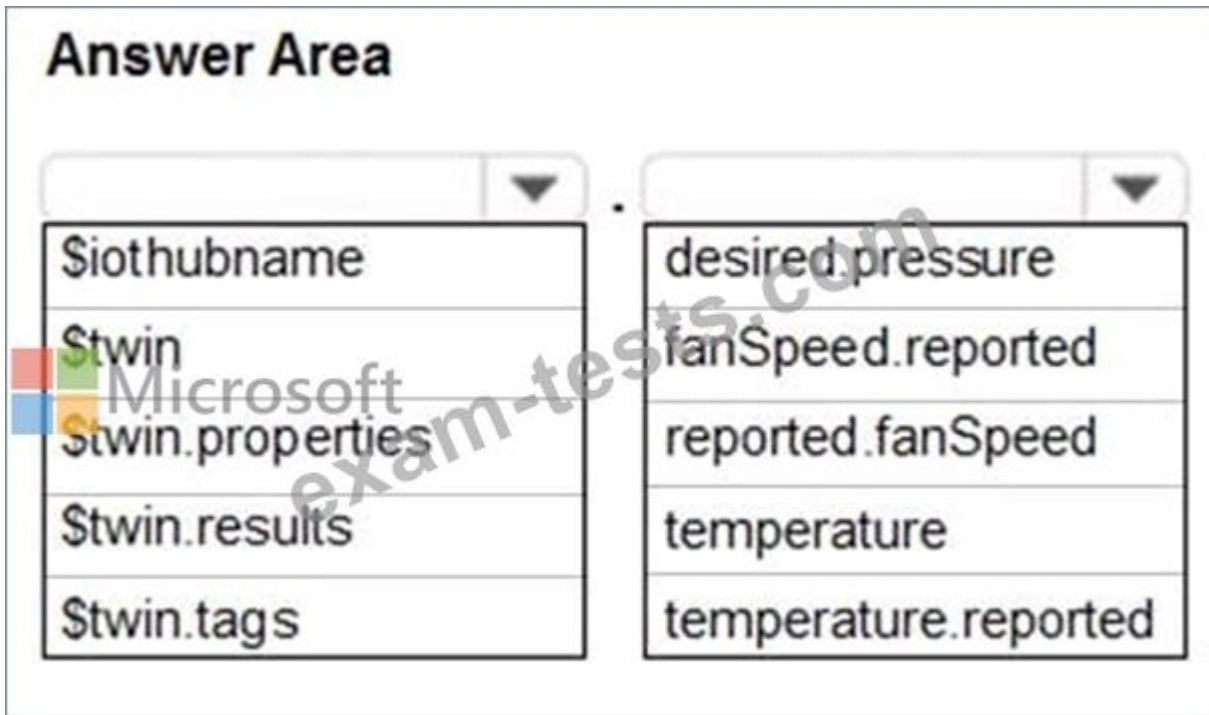
<https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-event-iot-output>

NEW QUESTION: 26

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.

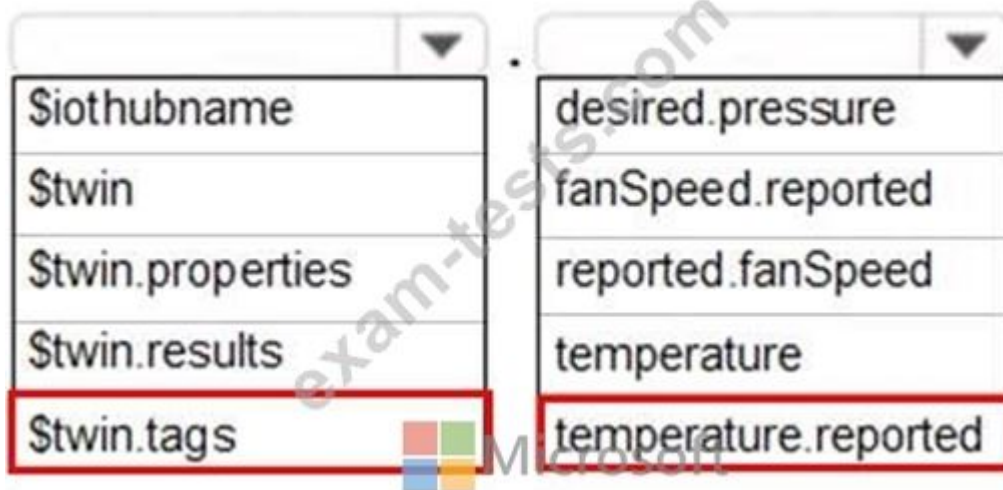
How should you configure the enrich message values? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

Answer Area



Reference:

<https://docs.microsoft.com/bs-cyrl-ba/azure/iot-hub/iot-hub-message-enrichments-overview>

NEW QUESTION: 27

You need to configure Stream Analytics to meet the POV requirements.

What are two ways to achieve the goal? Each Answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. From IoT Hub, create a custom event hub endpoint, and then configure the endpoint as an input to Stream Analytics.
- B. Create a Stream Analytics module, and then deploy the module to all IoT Edge devices in the fleet.
- C. Create an input in Stream Analytics that uses the built-in events endpoint of IoT Hub as the source.

D. Route telemetry to an Azure Blob storage custom endpoint, and then configure the Blob storage as a reference input for Stream Analytics.

Answer: A,C ([LEAVE A REPLY](#))

| Name | Data Source | Routing Query | Endpoint | Enabled | |
|--------------------------|-------------|----------------|----------|----------|------|
| <input type="checkbox"/> | cloud-route | DeviceMessages | true | coldpath | true |

NEW QUESTION: 28

You have an existing Azure IoT hub.

You use IoT Hub jobs to schedule long running tasks on connected devices.

Which two operations do the IoT Hub jobs support directly? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Trigger Azure functions.
- B. Invoke direct methods.
- C. Update desired properties.
- D. Send cloud-to-device messages.
- E. Disable IoT device registry entries.

Answer: ([SHOW ANSWER](#))

Consider using jobs when you need to schedule and track progress any of the following activities on a set of devices:

Invoke direct methods

Update desired properties

Update tags

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-jobs>

NEW QUESTION: 29

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: (SHOW ANSWER)

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.

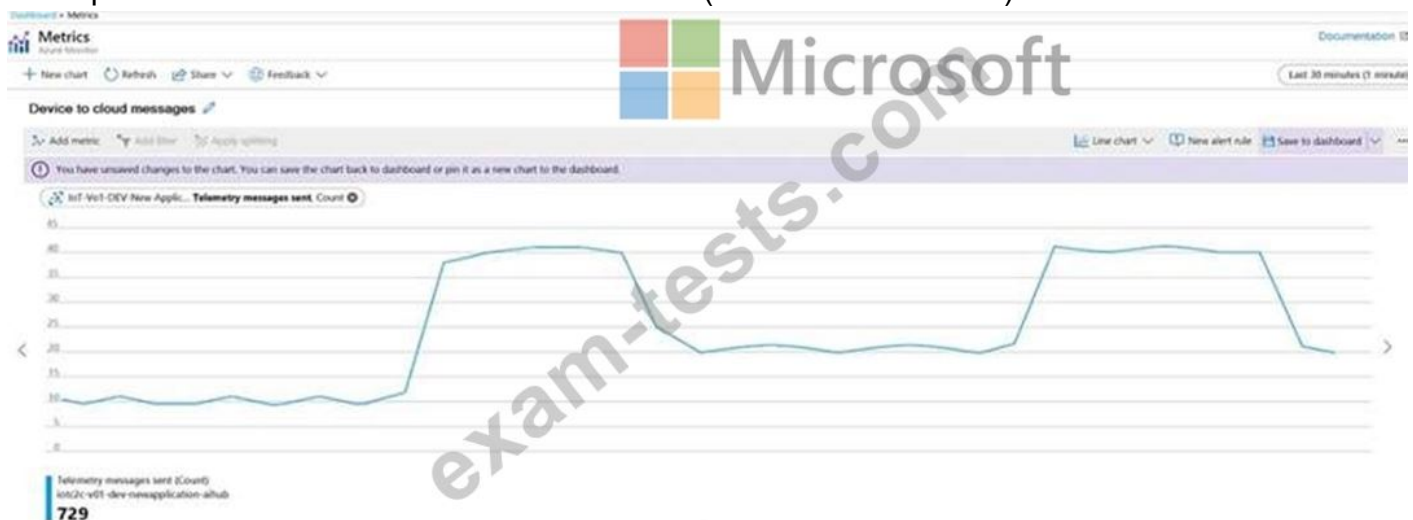
Reference:

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

NEW QUESTION: 30

You have 20 devices that connect to an Azure IoT hub.

You open Azure Monitor as shown in the exhibit. (Click the Exhibit tab.)



You discover that telemetry is not being received from five IoT devices.

You need to identify the names of the devices that are not generating telemetry and visualize the data. What should you do first?

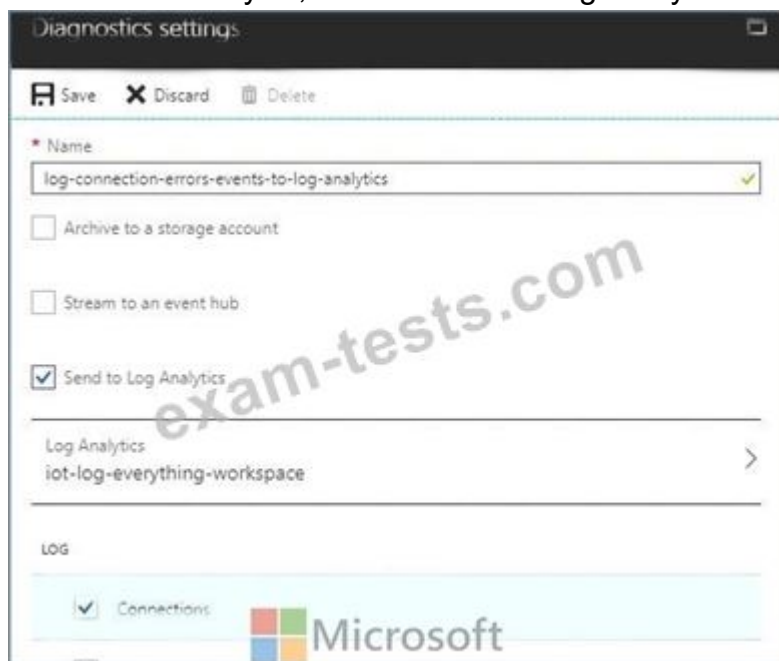
- A. Add the Number of throttling errors metric and archive the logs to an Azure storage account.
- B. Configure diagnostics for Routes and stream the logs to Azure Event Hubs.
- C. Add the Telemetry messages sent metric and archive the logs to an Azure Storage account.
- D. Configure diagnostics for Connections and send the logs to Azure Log Analytics.

Answer: D (LEAVE A REPLY)

Explanation

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.

- * Sign in to the Azure portal.
- * Browse to your IoT hub.
- * Select Diagnostics settings.
- * Select Turn on diagnostics.
- * Enable Connections logs to be collected.
- * For easier analysis, turn on Send to Log Analytics



Reference:

<https://docs.microsoft.com/bs-cyrl-ba/azure/lot-hub/iot-hub-troubleshoot-connectivity>

NEW QUESTION: 31

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

You need to be notified about failed local logins to a subnet of 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

| |
|--|
| Create a custom alert rule. |
| Enable Azure Security Center for IoT. |
| Configure the Diagnostics settings of the IoT hub. |
| Create a shared access policy. |
| Select a device security group. |
| Create a message route. |



Answer:

| |
|--------------------------------------|
| Answer Area Microsoft |
| Enable Azure Security Center for IoT |
| Select a device security group |
| Create a custom alert rule |

- 1 - Enable Azure Security Center for IoT
- 2 - Select a device security group
- 3 - Create a custom alert rule

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/asc-for-iot/how-to-security-data-access>

<https://docs.microsoft.com/en-us/rest/api/securitycenter/devicesecuritygroups/createorupdate>

Valid AZ-220 Dumps shared by BraindumpsPass.com for Helping Passing AZ-220 Exam! BraindumpsPass.com now offer the **newest AZ-220 exam dumps**, the BraindumpsPass.com AZ-220 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com AZ-220 dumps with Test Engine here:

<https://www.braindumps.com/Microsoft/AZ-220-practice-exam-dumps.html> (205 Q&As

Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 32

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 (LEAVE A REPLY)

Explanation

Azure Digital Twins models are represented in the JSON-LD-based Digital Twin Definition Language (DTDLE).

Reference:

<https://docs.microsoft.com/en-us/azure/digital-twins/concepts-models>

NEW QUESTION: 33

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: (SHOW ANSWER)

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: 34

You need to configure Stream Analytics to meet the POV requirements.

What are two ways to achieve the goal? Each Answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. From IoT Hub, create a custom event hub endpoint, and then configure the endpoint as an input to Stream Analytics.
- B. Create a Stream Analytics module, and then deploy the module to all IoT Edge devices in the fleet.

C. Create an input in Stream Analytics that uses the built-in events endpoint of IoT Hub as the source.

D. Route telemetry to an Azure Blob storage custom endpoint, and then configure the Blob storage as a reference input for Stream Analytics.

Answer: A,C (LEAVE A REPLY)

Explanation

The screenshot shows the Azure IoT Hub Message Routing configuration page for 'az220-hub'. The page title is 'az220-hub - Message routing'. The breadcrumb navigation is 'Home > Resource groups > az220 > az220-hub - Message routing'. The page content includes a search bar, a left-hand navigation menu with options like 'Failover', 'Properties', 'Locks', 'Export template', 'Explorers', 'Query explorer', 'IoT devices', 'Automatic Device Management', 'IoT Edge', 'IoT device configuration', 'Messaging', 'File upload', 'Message routing', and 'Security'. The main content area is titled 'Send data from your devices to endpoints that you choose.' and has tabs for 'Routes', 'Custom endpoints', and 'Enrich messages - preview'. Below the tabs, there is a 'Disable fallback route' button and a table of routes. The table has columns for 'Name', 'Data Source', 'Routing Query', 'Endpoint', and 'Enabled'. There is one route listed: 'cloud-route' with 'DeviceMessages' as the Data Source, 'true' as the Routing Query, 'coldpath' as the Endpoint, and 'true' as the Enabled status. The Microsoft logo is visible at the bottom of the page.

NEW QUESTION: 35

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:

```
aziot 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:

```
aziot 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 `aziot 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 Bush prompt, run the following command:

```
aziot edge set-modules -device-id Edge1 -hub-name Hub1 -content C:\deploymentMan1.json
```

Answer: D (LEAVE A REPLY)

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:

```
aziot 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>

NEW QUESTION: 36

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: (SHOW ANSWER)

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: 37

You need to install the Azure IoT Edge runtime on a new device that runs Windows 10 IoT Enterprise.

In which order should you perform the actions? 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 |
|--|-------------|
| From an elevated PowerShell prompt, run the Initialize-IoTEdge cmdlet. | |
| Enter the IoT Edge device connection string. | |
| From Azure IoT Hub, create an IoT Edge device. | |
| From an elevated PowerShell prompt, run the Deploy-IoTEdge cmdlet. | |

Answer:

| Actions | Answer Area |
|--|--|
| From an elevated PowerShell prompt, run the Initialize-IoTEdge cmdlet. | From Azure IoT Hub, create an IoT Edge device. |
| Enter the IoT Edge device connection string. | From an elevated PowerShell prompt, run the Deploy-IoTEdge cmdlet. |
| From Azure IoT Hub, create an IoT Edge device. | From an elevated PowerShell prompt, run the Initialize-IoTEdge cmdlet. |
| From an elevated PowerShell prompt, run the Deploy-IoTEdge cmdlet. | Enter the IoT Edge device connection string. |

Explanation

| |
|--|
| From Azure IoT Hub, create an IoT Edge device. |
| From an elevated PowerShell prompt, run the Deploy-IoTEdge cmdlet. |
| From an elevated PowerShell prompt, run the Initialize-IoTEdge cmdlet. |
| Enter the IoT Edge device connection string. |

Step 1: From Azure IoT hub, create an IoT Edge device

In the Azure Cloud Shell, enter the following command to create a device named myEdgeDevice in your hub.

az iot hub device-identity create --device-id myEdgeDevice --edge-enabled --hub-name {hub_name} View the connection string for your device, which links your physical device with its identity in IoT Hub.

Copy the value of the connectionString key from the JSON output and save it. This value is the device connection string. You'll use this connection string to configure the IoT Edge runtime in the step 3.

Step 2: From an elevated PowerShell prompt, run the Deploy-IoTEdge cmdlet. Install the Azure IoT Edge runtime on your IoT Edge device.

* Run PowerShell as an administrator.

* Run the Deploy-IoTEdge command, which performs the following tasks:

- Checks that your Windows machine is on a supported version.
- Turns on the containers feature.
- Downloads the moby engine and the IoT Edge runtime.

Step 3: From an elevated PowerShell prompt, run the Initialize-IoTEdge cmdlet Step 4: Enter the IoT Edge device connection string.

Configure the IoT Edge device with a device connection string.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/quickstart>

NEW QUESTION: 38

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.

The screenshot displays the 'Storage Configuration' page for the Time Series Insights environment 'tsi1'. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Settings, Properties, Locks, Export template, Storage Configuration (selected), and Data Access Policies. The main content area shows a 'Save' button and two sliders: 'Capacity' (set to 1) and 'Data retention time (in days)' (set to 100). Below the sliders, a summary table provides the following details:

| | |
|-------------------|--------------------|
| Ingress rates: | 1 M events per day |
| Storage capacity: | 30 M events |
| Estimated cost: | USD 149.73 / month |

Below the table, there is a 'Storage limit exceeded behavior' section with a 'Pause ingress' button. A warning message at the bottom states: 'The pause ingress setting is only recommended for users who wish to store their oldest data in the event they exceed their capacity. We suggest that you review our documentation to learn more about this setting.'

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.

| Statement | Yes | No |
|--|-----------------------|-----------------------|
| Tsi1 will display 100 days of telemetry. | <input type="radio"/> | <input type="radio"/> |
| Tsi1 will display telemetry that arrived three months ago. | <input type="radio"/> | <input type="radio"/> |
| Tsi1 will display real-time data after the Time Series Insights environment has been connected to the event source of Hub1 for two days. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statement | Yes | No |
|--|----------------------------------|----------------------------------|
| Tsi1 will display 100 days of telemetry. | <input checked="" type="radio"/> | <input type="radio"/> |
| Tsi1 will display telemetry that arrived three months ago. | <input type="radio"/> | <input checked="" type="radio"/> |
| Tsi1 will display real-time data after the Time Series Insights environment has been connected to the event source of Hub1 for two days. | <input type="radio"/> | <input checked="" type="radio"/> |

Reference:

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

NEW QUESTION: 39

You need to store the real-time alerts generated by Stream Analytics to meet the technical requirements.

Which type of Stream Analytics output should you configure?

- A. Azure Blob storage
- B. Microsoft Power BI
- C. Azure Cosmos DB
- D. Azure SQL Database

Answer: A (LEAVE A REPLY)

When you create a Time Series Insights Preview pay-as-you-go (PAYG) SKU environment, you create two Azure resources:

An Azure Storage general-purpose V1 blob account for cold data storage.

An Azure Time Series Insights Preview environment that can be configured for warm data storage.

Reference:

<https://docs.microsoft.com/en-us/azure/time-series-insights/time-series-insights-update-storage-ingress>

NEW QUESTION: 40

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: ▼

| |
|-------------|
| Command |
| Measurement |
| Properties |
| Settings |

Configure the desired fan speed: ▼

| |
|-------------|
| Command |
| Measurement |
| Properties |
| Settings |



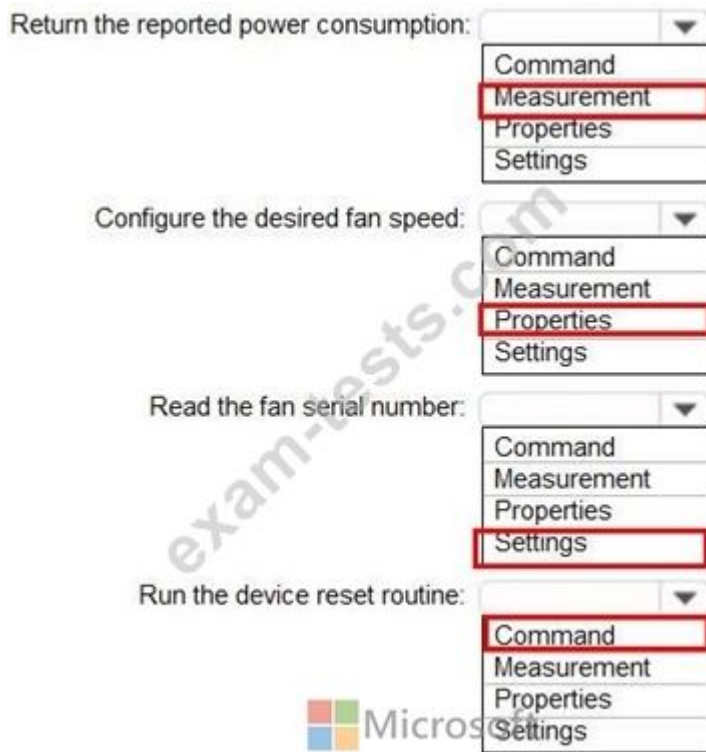
Read the fan serial number: ▼

| |
|-------------|
| Command |
| Measurement |
| Properties |
| Settings |

Run the device reset routine: ▼

| |
|-------------|
| Command |
| Measurement |
| Properties |
| Settings |

Answer:



Reference:

<https://docs.microsoft.com/en-us/azure/iot-central/core/howto-set-up-template>

NEW QUESTION: 41

You need to recommend the format of telemetry messages to meet the POV requirements.

What should you recommend?

- A. XML
- B. Avro
- C. JSON

Answer: ([SHOW ANSWER](#))

Explanation

Scenario: POV Requirements

Ensure that all message content during this phase is human readable to simplify debugging.

Avro uses a binary format, so it is not human readable.

The more lightweight JSON (Javascript object notation) has become a popular alternative to XML for various reasons. A couple obvious ones are:

Less verbose- XML uses more words than necessary

JSON is faster- Parsing XML software is slow and cumbersome.

Reference:

<https://blog.cloud-elements.com/json-better-xml>

NEW QUESTION: 42

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, 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 (LEAVE A REPLY)

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: 43

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.

The screenshot shows a configuration interface for an Azure IoT Edge deployment manifest. It is divided into two main sections: 'Keys' and 'Answer Area'.
The 'Keys' section on the left contains five input boxes, each with a label: 'binds:', 'createOptions:', 'portBindings:', 'storageFolder:', and 'value:'.
The 'Answer Area' on the right displays a JSON configuration for an 'edgeAgent' module. The configuration is as follows:

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


A blue box highlights the 'HostStoragePath' property in the 'HostConfig' object, and a red box highlights the corresponding 'storageFolder:' key in the 'Keys' section, indicating that this key should be dragged to the 'HostStoragePath' property. The Microsoft logo is visible at the bottom of the interface.

Answer:

| Keys | Answer Area |
|--|--|
| <code>"binds":</code> <input type="text"/> | <code>"edgeAgent": {</code> |
| <code>"createOptions":</code> <input type="text"/> | <code> "settings": {</code> |
| <code>"portBindings":</code> <input type="text"/> | <code> "image": "mcr.microsoft.com/azureiotedge-agent:1.0",</code> |
| <code>"storageFolder":</code> <input type="text"/> | <code> "createOptions": {</code> |
| <code>"value":</code> <input type="text"/> | <code> "HostConfig": {</code> |
| | <code> "portBindings": ["<HostStoragePath>:<ModuleStoragePath>"]</code> |
| | <code> }</code> |
| | <code> }</code> |
| | <code> }</code> |
| | <code>}</code> |



Reference:

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

NEW QUESTION: 44

You have the following device twin for the IoT device.

```
{
  "deviceId": "device1",
  "etag": "AAAAAAAAAAk=",
  "deviceEtag": "NDCwMTU4Mzk=",
  "status": "enabled",
  "statusUpdateTime": "0001-01-01T00:00:00Z",
  "connectionState": "Disconnected",
  "lastActivityTime": "2019-10-21T22:45:57.9732805Z",
  "cloudToDeviceMessageCount": 0,
  "authenticationType": "sas",
  "x509Thumbprint": {
    "primaryThumbprint": null,
    "secondaryThumbprint": null
  },
  "version": 17,
  "properties": {
    "desired": {
      "$metadata": {
        "$lastUpdated": "2019-10-24T19:40:46.4809147Z",
        "$lastUpdatedVersion": 9
      },
      "$version": 9
    },
    "reported": {
      "fanSpeed": 73,
      "$metadata": {
        "$lastUpdated": "2019-10-24T19:41:28.8839751Z",
        "fanSpeed": {
          "$lastUpdated": "2019-10-24T19:41:28.8839751Z"
        }
      },
      "$version": 8
    }
  },
  "capabilities": {
    "iotEdge": false
  }
}
```



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

NOTE: Each correct selection is worth one point.

| Statements | Yes | No |
|--|-----------------------|-----------------------|
| You can add a property that contains multiple nested values to the device twin. | <input type="radio"/> | <input type="radio"/> |
| The device twin will set <code>fanSpeed</code> for the physical IoT device to 73. | <input type="radio"/> | <input type="radio"/> |
| You can change the device identity of the physical IoT device by modifying the <code>deviceId</code> property. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements | Yes | No |
|--|----------------------------------|----------------------------------|
| You can add a property that contains multiple nested values to the device twin. | <input checked="" type="radio"/> | <input type="radio"/> |
| The device twin will set <code>fanSpeed</code> for the physical IoT device to 73. | <input checked="" type="radio"/> | <input type="radio"/> |
| You can change the device identity of the physical IoT device by modifying the <code>deviceId</code> property. | <input type="radio"/> | <input checked="" type="radio"/> |

Explanation:

Box1: Yes

Box 2: Yes

Fanspeed 73 is a reported property.

Box 3: No

The `deviceId` property is read only.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-device-twins>

NEW QUESTION: 45

You have an Azure IoT hub that has a hostname of `contoso-hub.azure-devices.net` and an MCU-based IoT device named `Device1`. `Device1` does NOT support Azure IoT SDKs.

You plan to connect `Device1` to the IoT hub by using the Message Queuing Telemetry Transport (MQTT) protocol and to authenticate by using X.509 certificates.

You need to ensure that `Device1` can authenticate to the IoT hub.

What should you do?

- A. Create an Azure key vault and enable the encryption of data at rest for the IoT hub by using a customermanaged key.
- B. Enable a hardware security module (HSM) on `Device1`.
- C. From the Azure portal, create an IoT Hub Device Provisioning Service (DPS) instance and add a certificate enrollment for `Device1`.

D. Add the DigiCert Baltimore Root Certificate to Device1.

Answer: ([SHOW ANSWER](#))

Explanation

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>

NEW QUESTION: 46

You have an Azure IoT solution that uses Azure Digital Twins. You plan to ingest telemetry from an IoT device into a digital twin.

You need to create an Azure function that will process the telemetry messages received by the Azure IoT hub and update the digital twin of the IoT device with the new values.

How should you complete the code? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



```
var cred = new DefaultAzureCredential();
var client = new DigitalTwinsClient(new Uri(adInstanceUrl), cred);
if (egEvent != null && egEvent.Data != null)
{
    JObject deviceMessage = (JObject)JsonConvert.DeserializeObject(egEvent.Data.ToString());
    string deviceId = (string)deviceMessage["systemProperties"]["iothub-connection-device-id"];
    var humidity = deviceMessage["body"]["Humidity"];
    var updateTwinData = new
    updateTwinData. PropertyMetadata
        {
            JsonPatchDocument();
            DigitalTwinMetadata();
            Message();
            TwinCollection();
        };
    updateTwinData.PropertyMetadata ("/Humidity", humidity.Value<double>());
    await client.UpdateTwin(deviceId, updateTwinData);
}
```

Answer:

Answer Area

```
var cred = new DefaultAzureCredential();
var client = new DigitalTwinsClient(new Uri(adInstanceUrl), cred);
if (egEvent != null && egEvent.Data != null)
{
    JObject deviceMessage = (JObject)JsonConvert.DeserializeObject(egEvent.Data.ToString());
    string deviceId = (string)deviceMessage["systemProperties"]["iothub-connection-device-id"];
    var humidity = deviceMessage["body"]["Humidity"];
    var updateTwinData = new
    updateTwinData. PropertyMetadata
        {
            JsonPatchDocument();
            DigitalTwinMetadata();
            Message();
            TwinCollection();
        };
    updateTwinData.PropertyMetadata ("/Humidity", humidity.Value<double>());
    await client.UpdateTwin(deviceId, updateTwinData);
}
```



AZ-220 exam questions have been updated and answers have been corrected get the newest BraindumpsPass.com AZ-220 dumps with Test Engine here:

<https://www.braindumps.com/Microsoft/AZ-220-practice-exam-dumps.html> (205 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 47

You have an Azure IoT hub.

You plan to deploy 1,000 IoT devices by using automatic device management.

The device twin is shown below.

```
{
  "deviceId": "ContosoHyperDriveEngine1",
  "etag": "AAAAAAAAAAw=",
  "deviceEtag": "MTYyNDk2Okw",
  "status": "enabled",
  "statusUpdateTime": "0001-01-01t00:00:00Z",
  "connectionTime": "Disconnected",
  "lastActivityTime": "0001-01-01T00:00:00Z",
  "cloudToDeviceMessageCount": 0,
  "authenticationType": "sas",
  "x509Thumbprint": {
    "primaryThumbprint": null,
    "secondaryThumbprint": null
  },
  "version": 13,
  "tags": {
    "engine": {
      "warpCorVersion": "1.2.65b",
      "warpDriveType": "WM105a"
    }
  },
  "properties": {
    "desired": {
      "$metadata": {
        "$lastUpdated": "2019-10-17T18:43:33.7599556Z"
      },
      "$version": 1
    },
    "reported": {
      "$metadata": {
        "$lastUpdated": "2019-10-17T18:43:33.7599556Z"
      },
      "$version": 1
    }
  }
}
```



You need to configure automatic device management for the deployment. Which target Condition and Device Twin Path should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Target Condition:

- properties.desired.warpDriveType='WM105a'
- properties.reported.warpDriveType='WM105a'
- tags.engine.warpDriveType='WM105a'

Device Twin Path:

- properties.desired.warpOperating
- properties.reported.warpOperating
- properties.warpOperating

Answer:

Answer Area

Target Condition:

- properties.desired.warpDriveType='WM105a'
- properties.reported.warpDriveType='WM105a'
- tags.engine.warpDriveType='WM105a'

Device Twin Path:

- properties.desired.warpOperating
- properties.reported.warpOperating
- properties.warpOperating

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-automatic-device-management>

NEW QUESTION: 48

You develop a custom Azure IoT Edge module named temperature-module. You publish temperature-module to a private container registry named mycr.azurecr.io. You need to build a deployment manifest for the IoT Edge device that will run temperature-module. Which three container images should you define in the manifest? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. mcr.microsoft.com/azureiotedge-simulated-temperature-sensor:1.0
- B. mcr.microsoft.com/azureiotedge-agent:1.0

C. mcr.microsoft.com/iotedge:2.0

D. mycr.azurecr.io/temperature-module:latest

E. mcr.microsoft.com/azureiotedge-hub:1.0

Answer: B,D,E (LEAVE A REPLY)

Each IoT Edge device runs at least two modules: \$edgeAgent and \$edgeHub, which are part of the IoT Edge runtime. IoT Edge device can run multiple additional modules for any number of processes. Use a deployment manifest to tell your device which modules to install and how to configure them to work together.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/module-composition>

Process and manage data

Testlet 1

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

A company named Contoso, Ltd. is creating a building monitoring system that will monitor the temperature, humidity, and light level at various points in a building's internal structure.

Contoso will test the system at a single building located in the United Kingdom. The building has 25 floors.

Each floor has 15 rooms.

Existing Environment. Current State of Development

Contoso produces a set of Bluetooth sensors that read the temperature and humidity. The sensors connect to IoT gateway devices that relay the data.

All the IoT gateway devices connect to an Azure IoT hub named iothub1.

Existing Environment. Device Twin

You plan to implement device twins by using the following JSON sample.

```
{
  "deviceId": "device_n",
  "etag": "AAAAAAAAAAQ=",
  "deviceEtag": "NDcwMTU4Mzk=",
  "status": "enabled",
  "statusUpdateTime": "0001-01-01T00:00:00Z",
  "connectionState": "Disconnected",
  "lastActivityTime": "0001-01-01T00:00:00Z",
  "cloudToDeviceMessageCount": 0,
  "authenticationType": "sas",
  "x509Thumbprint": {
    "primaryThumbprint": null,
    "secondaryThumbprint": null
  },
  "version": 11,
  "properties": {
    "desired": {
      "fanSpeed": 70,
      "$metadata": {
        "$lastUpdated": "2019-10-16T09:43:42.2944169Z",
        "$lastUpdatedVersion": 4,
        "fanSpeed": {
          "$lastUpdated": "2019-10-16T09:43:42.2944169Z",
          "$lastUpdatedVersion": 4
        }
      }
    },
    "$version": 4
  },
  "reported": {
    "fanSpeed": 80,
    "$metadata": {
      "$lastUpdated": "2019-10-16T09:43:42.4035171Z",
      "fanSpeed": {
        "$lastUpdated": "2019-10-16T09:43:42.4035171Z"
      }
    }
  },
  "$version": 7
},
"capabilities": {
  "iotEdge": false
}
}
```



Existing Environment. Azure Stream Analytics

Each room will have between three to five sensors that will generate readings that are sent to a single IoT gateway device. The IoT gateway device will forward all the readings to iotHub1 at intervals of between 10 and

60 seconds.

You plan to use a gateway pattern so that each IoT gateway device will have its own IoT Hub device identity.

You draft the following query, which is missing the GROUP BY clause.

```
SELECT
AVG(temperature),
System.TimeStamp() AS AsaTime
FROM
iothub
```

You plan to use a 30-second period to calculate the average temperature reading of the sensors. You plan to minimize latency between the condition reported by the sensors and the corresponding alert issued by the Stream Analytics job.

Existing Environment. Device Messages

The IoT gateway devices will send messages that contain the following JSON data whenever the temperature exceeds a specified threshold.

```
{
  "event": {
    "payload": "Temperature = 26.23 Humidity = 78.70597746416186 Button = 0",
    "properties": {
      "application": {
        "level": "critical"
      }
    }
  }
}
```



The level property will be used to route the messages to an Azure Service Bus queue endpoint named criticalep.

Existing Environment. Issues

You discover connectivity issues between the IoT gateway devices and iothub1, which cause IoT devices to lose connectivity and messages.

Requirements. Planned Changes

Contoso plans to make the following changes:

- * Use Stream Analytics to process and view data.
- * Use Azure Time Series Insights to visualize data.
- * Implement a system to sync device statuses and required settings.
- * Add extra information to messages by using message enrichment.
- * Create a notification system to send an alert if a condition exceeds a specified threshold.
- * Implement a system to identify what causes the intermittent connection issues and lost messages.

Requirements. Technical Requirements

Contoso must meet the following technical requirements:

- * Use the built-in functions of IoT Hub whenever possible.
- * Minimize hardware and software costs whenever possible.

- * Minimize administrative effort to provision devices at scale.
- * Implement a system to trace message flow to and from iotHub1.
- * Minimize the amount of custom coding required to implement the planned changes.
- * Prevent read operations from being negatively affected when you implement additional services.

NEW QUESTION: 49

You need to add Time Series Insights to the solution to meet the pilot requirements. 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.

The screenshot shows an exam interface with two main sections: 'Actions' and 'Answer Area'. The 'Actions' list contains five items:

- Route telemetry from IoT Hub to a custom event.
- Provision Time Series Insights.
- Add a custom event hub endpoint to IoT Hub.
- Add a new consumer group to the built-in events endpoint of IoT Hub.
- Add a data access policy to Time Series Insights for the dashboard web app.

The 'Answer Area' is currently empty. There are navigation arrows on the right side of the interface.

Answer:

The screenshot shows the 'Answer Area' with the Microsoft logo. The three actions are arranged in the following order from top to bottom:

- Provision Time Series Insights
- Route telemetry from IoT Hub to a custom event.
- Add a data access policy to Time Series Insights for the dashboard web app

- 1 - Provision Time Series Insights
 - 2 - Route telemetry from IoT Hub to a custom event.
 - 3 - Add a data access policy to Time Series Insights for the dashboard web app
- Reference: <https://docs.microsoft.com/en-us/azure/time-series-insights/time-series-insights-update-create-environment>

NEW QUESTION: 50

You need to install the Azure IoT Edge runtime on a new device that runs Windows 10 IoT Enterprise.

In which order should you perform the actions? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

From an elevated PowerShell prompt, run the Initialize-IoTEdge cmdlet.

Enter the IoT Edge device connection string.

From Azure IoT Hub, create an IoT Edge device.

From an elevated PowerShell prompt, run the Deploy-IoTEdge cmdlet.

Answer Area

Answer:

Actions

From an elevated PowerShell prompt, run the Initialize-IoTEdge cmdlet.

Enter the IoT Edge device connection string.

From Azure IoT Hub, create an IoT Edge device.

From an elevated PowerShell prompt, run the Deploy-IoTEdge cmdlet.

Answer Area

From Azure IoT Hub, create an IoT Edge device.

From an elevated PowerShell prompt, run the Deploy-IoTEdge cmdlet.

From an elevated PowerShell prompt, run the Initialize-IoTEdge cmdlet.

Enter the IoT Edge device connection string.

Explanation

From Azure IoT Hub, create an IoT Edge device.

From an elevated PowerShell prompt, run the Deploy-IoTEdge cmdlet.

From an elevated PowerShell prompt, run the Initialize-IoTEdge cmdlet.

Enter the IoT Edge device connection string.

Step 1: From Azure IoT hub, create an IoT Edge device

In the Azure Cloud Shell, enter the following command to create a device named myEdgeDevice in your hub.

az iot hub device-identity create --device-id myEdgeDevice --edge-enabled --hub-name {hub_name} View the connection string for your device, which links your physical device with its identity in IoT Hub.

Copy the value of the connectionString key from the JSON output and save it. This value is the device connection string. You'll use this connection string to configure the IoT Edge runtime in the step 3.

Step 2: From an elevated PowerShell prompt, run the Deploy-IoTEdge cmdlet.

Install the Azure IoT Edge runtime on your IoT Edge device.

* Run PowerShell as an administrator.

* Run the Deploy-IoTEdge command, which performs the following tasks:

- Checks that your Windows machine is on a supported version.
- Turns on the containers feature.
- Downloads the moby engine and the IoT Edge runtime.

Step 3: From an elevated PowerShell prompt, run the Initialize-IoTEdge cmdlet Step 4: Enter the IoT Edge device connection string.

Configure the IoT Edge device with a device connection string.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/quickstart>

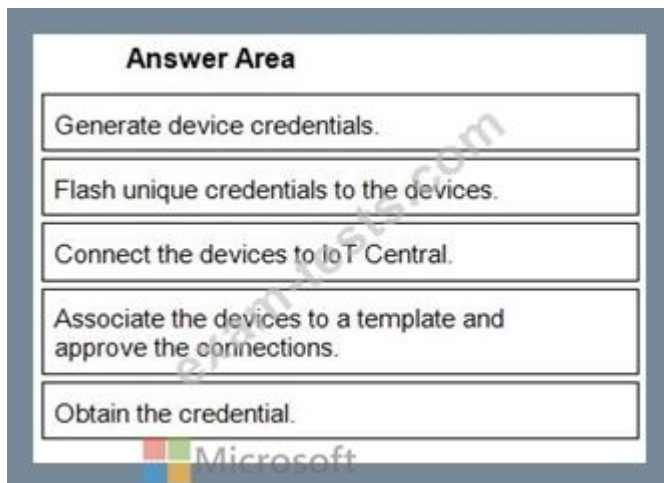
NEW QUESTION: 51

You have an Azure IoT Central application that includes a Device Provisioning Service instance. You need to connect IoT devices 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.

The screenshot shows an exam question interface. On the left, under the heading "Actions", there is a list of five actions in rectangular boxes: "Flash unique credentials to the devices.", "Obtain the credential.", "Generate device credentials.", "Associate the devices to a template and approve the connections.", and "Connect the devices to IoT Central." On the right, there is an "Answer Area" with a Microsoft logo and a watermark "exam-tips.com". The answer area contains two empty boxes for moving and ordering the actions, with up and down arrow icons on the right side of the boxes.

Answer:



- 1 - Generate device credentials.
- 2 - Flash unique credentials to the devices.
- 3 - Connect the devices to IoT Central.
- 4 - Associate the devices to a template and approve the connections.
- 5 - Obtain the credential.

Reference:

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

NEW QUESTION: 52

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 (LEAVE A REPLY)

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>

NEW QUESTION: 53

You have a digital twin model named Modell and a digital twin named Twin!. Twin! uses Modell.

You need to prevent new digital twins from using Modell. The solution must ensure that you can edit the properties of Twin!.

What should you do?

- A. Delete Modell.
- B. Update the version of Modell.

- C. Update the schema of Model 1.
- D. Decommission Modell.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 54

You have an Azure subscription named Sub1 that contains five Azure IoT hubs in the basic tier. You assign an Azure policy named Policy1 to Sub1. Policy 1 ensures that when an IoT hub is deployed, a private endpoint is deployed for the IoT hub.

You need to ensure that Policy1 is applied to the existing IoT hubs. The solution must minimize administrative effort.

What should you do?

- A. Upgrade the IoT hubs to the standard tier.
- B. Perform a manual failover of each IoT hub.
- C. Run a remediation task.
- D. Reassign Policy1.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 55

You have an IoT device that has the following configurations:

Hardware: Raspberry Pi Operating system: Raspbian

You need to deploy Azure IoT Edge to the device.

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

NOTE: Each correct selection is worth one point.

- A. Update the IoT Edge runtime.
- B. Install the IoT Edge security daemon.
- C. Run the Deploy-IoTEdge PowerShell cmdlet on the IoT Edge device.
- D. Install the container runtime.

Answer: A,B ([LEAVE A REPLY](#))

The Azure IoT Edge runtime is what turns a device into an IoT Edge device. The runtime can be deployed on devices as small as a Raspberry Pi or as large as an industrial server.

The IoT Edge security daemon provides and maintains security standards on the IoT Edge device. The daemon starts on every boot and bootstraps the device by starting the rest of the IoT Edge runtime.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/how-to-install-iot-edge>

NEW QUESTION: 56

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.)



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: B (LEAVE A REPLY)

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: 57

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 cloud-to-device messages and watch the cloud-to-device feedback endpoint for successful acknowledgement.

Does this meet the goal?

A. Yes

B. No

Answer: (SHOW ANSWER)

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>

NEW QUESTION: 58

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: B,C (LEAVE A REPLY)

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>

Process and manage data

Testlet 1

Case Study

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Existing Environment. Current State of Development

Contoso produces a set of Bluetooth sensors that read the temperature and humidity. The sensors connect to IoT gateway devices that relay the data.

All the IoT gateway devices connect to an Azure IoT hub named `iothub1`.

Existing Environment. Device Twin

You plan to implement device twins by using the following JSON sample.



Microsoft

```
{
  "deviceId": "device_n",
  "etag": "AAAAAAAAAAQ=",
  "deviceEtag": "NDcwMTU4Mzk=",
  "status": "enabled",
  "statusUpdateTime": "0001-01-01T00:00:00Z",
  "connectionState": "Disconnected",
  "lastActivityTime": "0001-01-01T00:00:00Z",
  "cloudToDeviceMessageCount": 0,
  "authenticationType": "sas",
  "x509Thumbprint": {
    "primaryThumbprint": null,
    "secondaryThumbprint": null
  },
  "version": 11,
  "properties": {
    "desired": {
      "fanSpeed": 70,
      "$metadata": {
        "$lastUpdated": "2019-10-16T09:43:42.2944169Z",
        "$lastUpdatedVersion": 4,
        "fanSpeed": {
          "$lastUpdated": "2019-10-16T09:43:42.2944169Z",
          "$lastUpdatedVersion": 4
        }
      }
    },
    "$version": 4
  },
  "reported": {
    "fanSpeed": 80,
    "metadata": {
      "$lastUpdated": "2019-10-16T09:43:42.4035171Z",
      "fanSpeed": {
        "$lastUpdated": "2019-10-16T09:43:42.4035171Z"
      }
    }
  },
  "$version": 7
}
},
"capabilities": {
  "lotEdge": false
}
}
```

Existing Environment. Azure Stream Analytics

Each room will have between three to five sensors that will generate readings that are sent to a single IoT gateway device. The IoT gateway device will forward all the readings to iothub1 at intervals of between 10 and 60 seconds.

You plan to use a gateway pattern so that each IoT gateway device will have its own IoT Hub device identity.

You draft the following query, which is missing the GROUP BY clause.

```
SELECT
AVG(temperature),
System.TimeStamp() AS AsaTime
FROM
iothub
```

You plan to use a 30-second period to calculate the average temperature reading of the sensors. You plan to minimize latency between the condition reported by the sensors and the corresponding alert issued by the Stream Analytics job.

Existing Environment. Device Messages

The IoT gateway devices will send messages that contain the following JSON data whenever the temperature exceeds a specified threshold.

```
{
  "event": {
    "payload": "Temperature = 26.23 Humidity = 78.70597746416186 Button = 0",
    "properties": {
      "application": {
        "level": "critical"
      }
    }
  }
}
```



The levelproperty will be used to route the messages to an Azure Service Bus queue endpoint named criticalep.

Existing Environment. Issues

You discover connectivity issues between the IoT gateway devices and iothub1, which cause IoT devices to lose connectivity and messages.

Requirements. Planning Changes

Contoso plans to make the following changes:

- * Use Stream Analytics to process and view data.
- * Use Azure Time Series Insights to visualize data.
- * Implement a system to sync device statuses and required settings.
- * Add extra information to messages by using message enrichment.
- * Create a notification system to send an alert if a condition exceeds a specified threshold.
- * Implement a system to identify what causes the intermittent connection issues and lost messages.

Requirements. Technical Requirements

Contoso must meet the following requirements:

- * Use the built-in functions of IoT Hub whenever possible.
- * Minimize hardware and software costs whenever possible.
- * Minimize administrative effort to provision devices at scale.
- * Implement a system to trace message flow to and from iothub1.
- * Minimize the amount of custom coding required to implement the planned changes.
- * Prevent read operations from being negatively affected when you implement additional services.

NEW QUESTION: 59

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: ([SHOW ANSWER](#))

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: 60

You create a new IoT device named device1 on iothub1. Device1 has a primary key of Uihuih76hbHb.

How should you complete the device connection string? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

HostName= azure-devices.net . azure-devices.net ;DeviceId= azure-devices.net :SharedAccessKey=Uihuih76hbHb

criticallep
device1
iothub1
tracestate

criticallep
device1
iothub1
tracestate

criticallep
device1
iothub1
tracestate

Answer:



Explanation



Box 1: iothub1

The Azure IoT hub is named iothub1.

Box 2: azure-devices.net

The format of the device connection string looks like:

HostName={YourIoTHubName}.azure-

devices.net;DeviceId=MyNodeDevice;SharedAccessKey={YourSharedA Box 1: device1 Device1

has a primary key of Uihuih76hbHb.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/quickstart-control-device-dotnet>

NEW QUESTION: 61

You have an Azure IoT hub that uses a Device Provision Service instance.

You plan to deploy 100 IoT devices.

You need to confirm the identity of the devices by using the Device Provision Service.

Which three device attestation mechanisms can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. X.509 certificates
- B. Trusted Platform Module (TPM) 2.0
- C. Trusted Platform Module (TPM) 1.2
- D. Symmetric key
- E. Device Identity Composition Engine (DICE)

Answer: A,B,D (LEAVE A REPLY)

The Device Provisioning Service supports the following forms of attestation:

X.509 certificates based on the standard X.509 certificate authentication flow.

Trusted Platform Module (TPM) based on a nonce challenge, using the TPM 2.0 standard for keys to present a signed Shared Access Signature (SAS) token.

This does not require a physical TPM on the device, but the service expects to attest using the endorsement key per the TPM spec.

Symmetric Key based on shared access signature (SAS) Security tokens, which include a hashed signature and an embedded expiration.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-dps/concepts-service#attestation-mechanism>

Valid AZ-220 Dumps shared by BraindumpsPass.com for Helping Passing AZ-220 Exam! BraindumpsPass.com now offer the **newest AZ-220 exam dumps**, the BraindumpsPass.com AZ-220 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com AZ-220 dumps with Test Engine here:

<https://www.braindumps.com/Microsoft/AZ-220-practice-exam-dumps.html> (205 Q&As

Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 62

You have an Azure IoT solution that includes an Azure IoT hub, a Device Provisioning Service instance, and

1,000 connected IoT devices. The IoT devices are allocated to four enrollment groups. Each enrollment group is configured to use certificate attestation.

You need to decommission all the devices in a single enrollment group and the enrollment group itself.

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 |
|--|-------------|
| Delete each device from the identity registry. | |
| Delete the IoT hub. | |
| Remove the X.509 root certificate. | |
| Disable the enrollment group. | |
| Delete the enrollment group. | |

Answer:

Actions

- Delete each device from the identity registry.
- Delete the IoT hub.
- Remove the X.509 root certificate.
- Disable the enrollment group.
- Delete the enrollment group.

Answer Area

| |
|--|
| Disable the enrollment group. |
| Delete each device from the identity registry. |
| Delete the enrollment group. |

Explanation

Disable the enrollment group.

Delete each device from the identity registry.

Delete the enrollment group.

To deprovision all of the devices that have been provisioned through an enrollment group:

- * Disable the enrollment group to disallow its signing certificate.
- * Use the list of provisioned devices for that enrollment group to disable or delete each device from the identity registry of its respective IoT hub.
- * After disabling or deleting all devices from their respective IoT hubs, you can optionally delete the enrollment group. Be aware, though, that, if you delete the enrollment group and there is an enabled enrollment group for a signing certificate higher up in the certificate chain of one or more of the devices, those devices can re-enroll.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-dps/how-to-unprovision-devices>

NEW QUESTION: 63

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 IoT hub, create a system-assigned managed identity.
- C. From the IoT hub, create a security module for the devices.
- D. On the devices, set the PowerShell execution policy to Restricted.

Answer: (SHOW ANSWER)

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>

NEW QUESTION: 64

You have an Azure IoT hub.

You plan to deploy 1,000 IoT devices by using automatic device management.

The device twin is shown below.

You need to configure automatic device management for the deployment.

Which target Condition and Device Twin Path should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Target Condition:

- properties.desired.warpDriveType='WM105a'
- properties.reported.warpDriveType='WM105a'
- tags.engine.warpDriveType='WM105a'

Device Twin Path:

- properties.desired.warpOperating
- properties.reported.warpOperating
- properties.warpOperating

Answer:

Answer Area

Target Condition:

- properties.desired.warpDriveType='WM105a'
- properties.reported.warpDriveType='WM105a'
- tags.engine.warpDriveType='WM105a'

Device Twin Path:

- properties.desired.warpOperating
- properties.reported.warpOperating
- properties.warpOperating

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-automatic-device-management>

NEW QUESTION: 65

You need to install the Azure IoT Edge runtime on a new device that runs Windows 10 IoT Enterprise.

Which four 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 |
|---|-------------|
| <p>From an elevated PowerShell prompt, run the following command.</p> <pre>•(Invoke-WebRequest -useb https://aka.ms/iotedge-win) Invoke-Expression; Initialize-IoTEdge</pre> | |
| <p>From Azure IoT Hub, create an IoT Edge device.</p> | |
| <p>From a Bash prompt, run the following commands.</p> <pre>curl https://packages.microsoft.com/keys/microsoft.asc gpg --dearmor > microsoft.gpg sudo cp ./microsoft.gpg /etc/apt/trusted.gpg.d/</pre> | |
| <p>From an elevated PowerShell prompt, run the following command.</p> <pre>•(Invoke-WebRequest -useb https://aka.ms/iotedge-win) Invoke-Expression; Deploy-IoTEdge</pre> | |
| <p>Enter the IoT Edge device connection string.</p> | |
| <p>From a Bash prompt, run the following commands.</p> <pre>sudo apt-get install moby-engine</pre> | |

Answer:

Answer Area Microsoft

- From Azure IoT Hub, create an IoT Edge Device
- Deploy-IoTEdge
- Initialize-IoTEdge
- Enter the IoT Edge device connection string.

- 1 - From Azure IoT Hub, create an IoT Edge Device
- 2 - Deploy-IoTEdge
- 3 - Initialize-IoTEdge
- 4 - Enter the IoT Edge device connection string.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/module-composition>

NEW QUESTION: 66

You plan to deploy an Azure IoT hub.

The IoT hub must support the following:

- * Three Azure IoT Edge devices 2,500 IoT devices
- * Each IoT device will send a 6 KB message every five seconds.

You need to size the IoT hub to support the devices. The solution must minimize costs. What should you choose?

- A. one unit of the S1 tier
- B. one unit of the B2 tier
- C. one unit of the B1 tier
- D. one unit of the S3 tier

Answer: (SHOW ANSWER)

Explanation

$2500 * 6 \text{ KB} * 12 = 180,000 \text{ KB/minute} = 180 \text{ MB/Minute}$.

B3, S3 can handle up to 814 MB/minute per unit. Incorrect Answers:

A, C: B1, S1 can only handle up to 1111 KB/minute per unit B: B2, S2 can only handle up to 16 MB/minute per unit.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-scaling>

NEW QUESTION: 67

You have 1,000 IoT devices that connect to an Azure IoT hub.

Each device has a property tag named city that is used to store the location of the device.

You need to update the properties on all the devices located at an office in the city of Seattle as quickly as possible. Any new devices in the Seattle office that are added to the IoT hub must receive the updated properties also.

What should you do?

- A. From Automatic Device Management, create an IoT device configuration.
- B. From the IoT hub, generate a query for the target devices.
- C. Create a scheduled job by using the IoT Hub service SDKs.
- D. Deploy an Azure IoT Edge transparent gateway to the Seattle office and deploy an Azure Stream Analytics edge job.

Answer: A (LEAVE A REPLY)

Explanation

Automatic device management in Azure IoT Hub automates many of the repetitive and complex tasks of managing large device fleets. With automatic device management, you can target a set of devices based on their properties, define a desired configuration, and then let IoT Hub update the devices when they come into scope. This update is done using an automatic device

configuration or automatic module configuration, which lets you summarize completion and compliance, handle merging and conflicts, and roll out configurations in a phased approach.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-automatic-device-management>

NEW QUESTION: 68

You are troubleshooting an Azure IoT hub.

You discover that some telemetry messages are dropped before they reach downstream processing. You suspect that IoT Hub throttling is the root cause.

Which log in the Diagnostics settings of the IoT hub should you use to capture the throttling error events?

- A. Routes
- B. C2DCommands
- C. DeviceTelemetry
- D. Connections

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 69

You are troubleshooting an Azure IoT hub.

You discover that some telemetry messages are dropped before they reach downstream processing. You suspect that IoT Hub throttling is the root cause.

Which log in the Diagnostics settings of the IoT hub should you use to capture the throttling error events?

- A. Routes
- B. DeviceTelemetry
- C. Connections
- D. C2DCommands

Answer: B ([LEAVE A REPLY](#))

Explanation

The device telemetry category tracks errors that occur at the IoT hub and are related to the telemetry pipeline.

This category includes errors that occur when sending telemetry events (such as throttling) and receiving telemetry events (such as unauthorized reader). This category cannot catch errors caused by code running on the device itself.

Note: The metric `d2c.telemetry.ingress.sendThrottle` is the number of throttling errors due to device throughput throttles.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-monitor-resource-health>

NEW QUESTION: 70

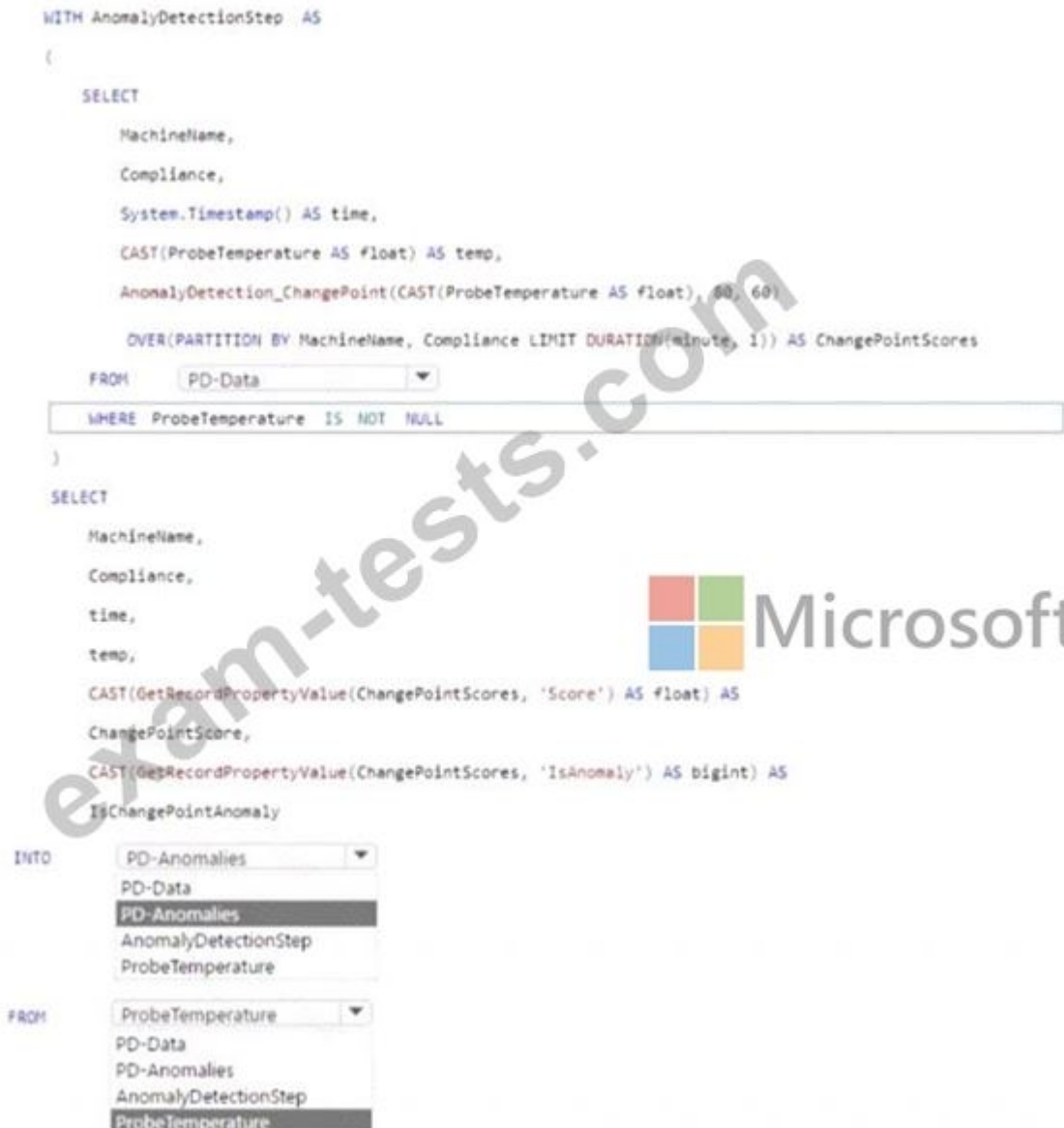
You have an Azure solution that contains an Azure IoT Edge deployment.

You are configuring an Azure Stream Analytics Edge job as shown in the following exhibit. How should you complete the query? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

ANSWER AREA

```
WITH AnomalyDetectionStep AS
(
    SELECT
        MachineName,
        Compliance,
        System.Timestamp() AS time,
        CAST(ProbeTemperature AS float) AS temp,
        AnomalyDetection_ChangePoint(CAST(ProbeTemperature AS float), 60, 60)
        OVER(PARTITION BY MachineName, Compliance LIMIT DURATION(Minute, 1)) AS ChangePointScores
    FROM PD-Data
    WHERE ProbeTemperature IS NOT NULL
)
SELECT
    MachineName,
    Compliance,
    time,
    temp,
    CAST(GetRecordPropertyValue(ChangePointScores, 'Score') AS float) AS
    ChangePointScore,
    CAST(GetRecordPropertyValue(ChangePointScores, 'IsAnomaly') AS bigint) AS
    IsChangePointAnomaly
INTO PD-Anomalies
FROM ProbeTemperature
```



Answer:

Answer Area

```
WITH AnomalyDetectionStep AS
(
    SELECT
        MachineName,
        Compliance,
        System.Timestamp() AS time,
        CAST(ProbeTemperature AS float) AS temp,
        AnomalyDetection_ChangePoint(CAST(ProbeTemperature AS float), 80, 60)
            OVER(PARTITION BY MachineName, Compliance LIMIT DURATION(minute, 1)) AS ChangePointScores
    FROM PD-Data
    WHERE ProbeTemperature IS NOT NULL
)
SELECT
    MachineName,
    Compliance,
    time,
    temp,
    CAST(GetRecordPropertyValue(ChangePointScores, 'Score') AS float) AS
    ChangePointScore,
    CAST(GetRecordPropertyValue(ChangePointScores, 'IsAnomaly') AS bigint) AS
    IsChangePointAnomaly
INTO PD-Anomalies
FROM ProbeTemperature
```

Explanation

```

WITH AnomalyDetectionStep AS
(
    SELECT
        MachineName,
        Compliance,
        System.Timestamp() AS time,
        CAST(ProbeTemperature AS float) AS temp,
        AnomalyDetection_ChangePoint(CAST(ProbeTemperature AS float), 80, 60)
        OVER(PARTITION BY MachineName, Compliance LIMIT DURATION(minute, 1)) AS ChangePointScores
    FROM PD-Data
    WHERE ProbeTemperature IS NOT NULL
)
SELECT
    MachineName,
    Compliance,
    time,
    temp,
    CAST(GetRecordPropertyValue(ChangePointScores, 'Score') AS float) AS
    ChangePointScore,
    CAST(GetRecordPropertyValue(ChangePointScores, 'IsAnomaly') AS bigint) AS
    IsChangePointAnomaly
INTO PD-Anomalies
FROM ProbeTemperature

```



NEW QUESTION: 71

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: (SHOW ANSWER)

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>

NEW QUESTION: 72

You have an Azure subscription that contains a resource group named RG1.

You need to deploy the Device Provisioning Service. The solution must ensure that the Device Provisioning Service can accept new device enrollments.

You create a Device Provisioning Service instance.

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

NOTE: Each correct selection is worth one point.

A. From the Linked IoT hubs blade of the Device Provisioning Service, link an Azure IoT hub.

B. From the Azure portal, create a new Azure IoT hub.

C. From the Manage allocation policy blade of the Device Provisioning Service, configure an allocation policy.

D. From the Certificates blade of the Device Provisioning Service, upload an X.509 certificate to the Device Provisioning Service.

Answer: D (LEAVE A REPLY)

A: The Device Provisioning Service can only provision devices to IoT hubs that have been linked to it.

C: Allocation policy. The service-level setting that determines how Device Provisioning Service assigns devices to an IoT hub. There are three supported allocation policies:

Lowest latency: devices are provisioned to an IoT hub with the lowest latency to the device.

Evenly weighted distribution Static configuration via the enrollment list Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/iot-dps/concepts-service>

NEW QUESTION: 73

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 20 IoT devices deployed across two floors of a building. The devices on the first floor must be set to 60 degrees. The devices on the second floor must be set to 80 degrees.

The device twins are configured to use a tag that identifies the floor on which the twins are located.

You create the following automatic configuration for the devices on the first floor.

```

{
  "id": "first_floor_devices",
  "schemaVersion": null,
  "labels": {
    "Version": "1"
  },
  "content": {
    "deviceContent": {
      "properties.desired.ac": {
        "temperature": 60
      }
    }
  },
  "targetCondition": "tags.floor-'first'",
  "createdTimeUtc": "2020-12-08T04:06:56.651Z",
  "lastUpdatedTimeUtc": "2020-12-08T04:06:56.651Z",
  "priority": 1,
  ...
}

```

You create the following automatic configuration for the devices on the second floor.

```

{
  "id": "second_floor_devices",
  "schemaVersion": null,
  "labels": {
    "Version": "1"
  },
  "content": {
    "deviceContent": {
      "properties.desired.ac": {
        "temperature": 80
      }
    }
  },
  "targetCondition": "*",
  "createdTimeUtc": "2020-12-08T04:11:08.561Z",
  "lastUpdatedTimeUtc": "2020-12-09T18:50:55.070Z",
  "priority": 10,
  ...
}

```

The IoT devices on the first floor report that the temperature is set to 80 degrees. You need to ensure that the first-floor devices are set to the correct temperature.

Solution: In the automatic configuration for the second-floor devices, you set targetCondition to "tags.floor='second'".

Does this meet the goal?

A. Yes

B. No

Answer: A ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/module-deployment-monitoring?view=iotedge-2020-11>

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-automatic-device-management-cli>

NEW QUESTION: 74

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

-
-
-
-
-

Answer Area

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

Answer:

Keys

-
-
-
-
-

Answer Area

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

Reference:

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

NEW QUESTION: 75

From the Device Provisioning Service, you create an enrollment as shown in the exhibit. (Click the Exhibit tab.)

The screenshot displays the 'enrollment1' configuration page in the Microsoft Device Provisioning Service. The page title is 'enrollment1 Enrollment Group Details'. At the top, there are navigation buttons for 'Save', 'Refresh', and 'Regenerate keys'. Below this, there are tabs for 'Settings' (selected) and 'Registration Records'. A blue informational banner states: 'You can view and update attestation information, set how you want to assign devices to hubs, define the re-provisioning policy and set the initial twin state of provisioning devices.'

The configuration section includes:

- Attestation Type:** Symmetric Key
- Primary Key:** A field containing a masked key (asterisks) with an eye icon and a copy icon.
- Secondary Key:** A field containing a masked key (asterisks) with an eye icon and a copy icon.
- IoT Edge device:** A toggle switch set to 'False'.
- Select how you want to assign devices to hubs:** A dropdown menu set to 'Evenly weighted distribution'.
- Select the IoT hubs this group can be assigned to:** A dropdown menu set to 'iothub-contoso.azure-devices.net'.
- Link a new IoT hub:** A blue button.
- Select how you want device data to be handled on re-provisioning *:** A dropdown menu set to 'Re-provision and migrate data'.
- Enable entry:** A toggle switch set to 'Enable'.

You need to deploy a new IoT device.

What should you use as the device identity during attestation?

- A. a self-signed X.509 certificate
- B. the random string of alphanumeric characters

- C. the HMACSHA256 hash of the device's registration ID
- D. the endorsement key of the device's Trusted Platform Module (TPM)

Answer: (SHOW ANSWER)

Each device uses its derived device key with your unique registration ID to perform symmetric key attestation with the enrollment during provisioning. To generate the device key, use the key you copied from your DPS enrollment to compute an HMAC-SHA256 of the unique registration ID for the device and convert the result into Base64 format.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/how-to-auto-provision-symmetric-keys>

NEW QUESTION: 76

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. Upload to Azure Storage.
- D. Build an IoT Edge solution.
- E. Generate a shared access signature (SAS) token for Device 1.

Answer: B,D (LEAVE A REPLY)

Explanation

D: Once you create IoT Edge modules with your business logic, you want to deploy them to your devices to operate at the edge.

B: 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.

You deploy modules to your device by applying the deployment manifest that you configured with the module information.

* In the Visual Studio Code explorer view, expand the Azure IoT Hub section, and then expand the Devices node.

* To confirm that the device you've chosen is an IoT Edge device, select it to expand the list of modules and verify the presence of \$edgeHub and \$edgeAgent. Every IoT Edge device includes these two modules.

* Select Create Deployment for Single Device.

* Navigate to the deployment manifest JSON file that you want to use, and click Select Edge Deployment Manifest.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/how-to-deploy-modules-vscode>

Valid AZ-220 Dumps shared by BraindumpsPass.com for Helping Passing AZ-220 Exam! BraindumpsPass.com now offer the **newest AZ-220 exam dumps**, the BraindumpsPass.com AZ-220 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com AZ-220 dumps with Test Engine here: <https://www.braindumps.com/Microsoft/AZ-220-practice-exam-dumps.html> (205 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 77

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, 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 connecting to the IoT hub.

Solution: You disconnect the Device Provisioning Service from the IoT hub.

Does this meet the goal?

- A. Yes
- B. No

Answer: B (LEAVE A REPLY)

Instead, 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.

Reference:

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

NEW QUESTION: 78

You plan to develop modules for an Azure IoT Edge solution.

You need to recommend a development tool that supports the following:

Node.js

Module templates

Development on Linux workstations

What should you recommend?

- A. the Azure IoT explorer
- B. Microsoft Visual Studio
- C. Microsoft Visual Studio Online

D. Microsoft Visual Studio Code

Answer: C (LEAVE A REPLY)

Use Visual Studio Code to develop Node.js code and deploy it to a device running Azure IoT Edge.

You can use IoT Edge modules with Linux containers to deploy code that implements your business logic directly to your IoT Edge devices.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/tutorial-node-module?view=iotedge-2020-11>

NEW QUESTION: 79

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 (LEAVE A REPLY)

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>

NEW QUESTION: 80

You have an Azure subscription that contains the resources shown in the following table.

| Name | Type |
|------|---|
| Hub1 | Azure IoT Hub |
| DPS1 | Azure IoT Hub Device Provisioning service (DPS) |
| CA1 | Certification authority (CA) |

You create a group enrollment in DPS1 and enroll 100 IoT devices. Each device is issued a leaf certificate from CAT. You need to deprovision a single IoT device from the group enrollment. The solution must not affect the other devices.

Solution: You create a disabled individual enrollment by using the X.509 certificate of the device.
Does this meet the goal?

- A. Yes
- B. No

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 81

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:

Connection events must be reported as high priority.

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.

The screenshot shows the configuration interface for the azureiotsecurity module twin. On the left, a list of properties is shown with a split bar between panes. On the right, the JSON configuration is displayed with some values already entered:

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

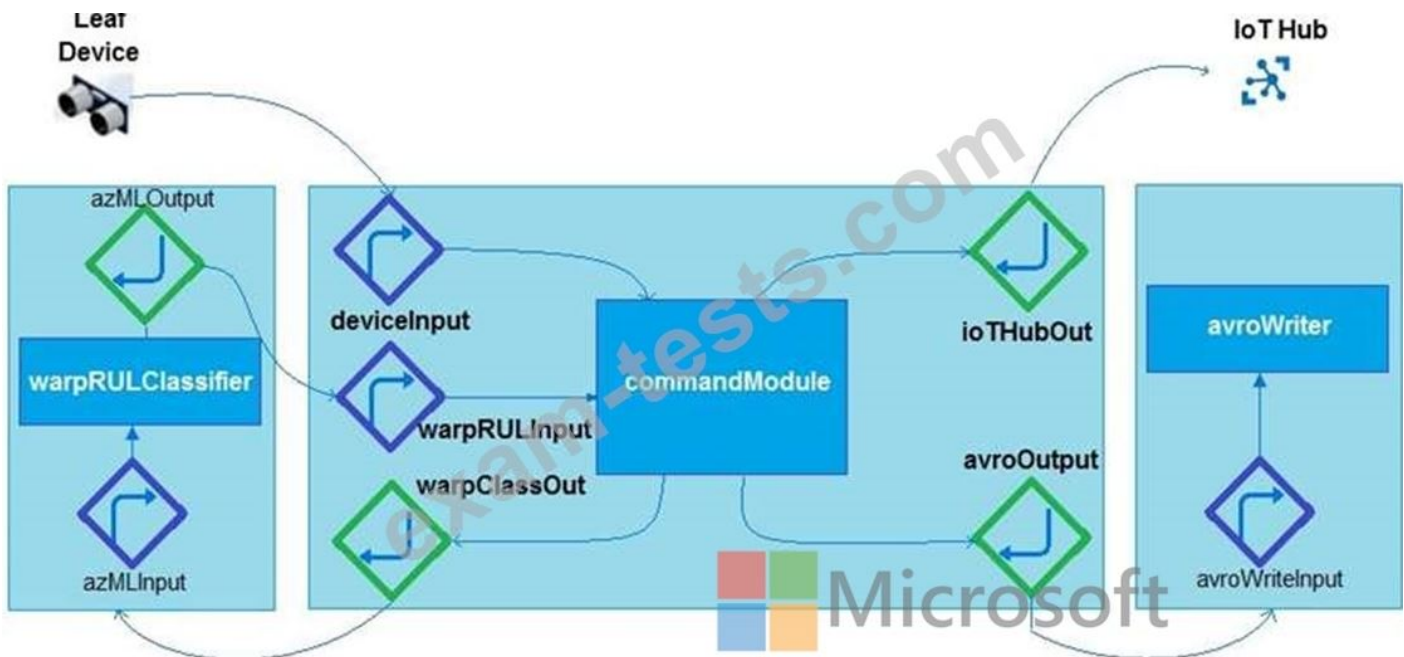
Answer:

The screenshot shows the final configuration for the azureiotsecurity module twin. The left pane shows the list of properties, and the right pane shows the JSON configuration with the correct values selected:

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

NEW QUESTION: 82

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\\)\",
  "commandToWarpClassifier": "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
  }
}

```

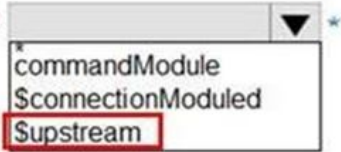
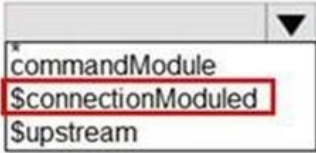
- commandModule
- \$connectionModule
- \$upstream

- commandModule
- \$connectionModule
- \$upstream



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\"),
    "commandToWarpClassifier": "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
  }
}
```



Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/tutorial-machine-learning-edge-06-custom-modules>

NEW QUESTION: 83

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 (LEAVE A REPLY)

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>

NEW QUESTION: 84







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.

| Actions | Answer Area |
|---|--|
| Sign the CA1 certificate by using the intermediate CA certificate. |       |
| Sign the intermediate CA certificate by using the CA1 certificate. | |
| Sign the device certificate by using the intermediate CA certificate. | |
| Sign the device certificate by using the CA1 certificate. | |
| Deploy the certificate chain to the device. | |

Answer:

Actions  **Answer Area**

| | |
|---|---|
| Sign the CA1 certificate by using the intermediate CA certificate. | Sign the intermediate CA certificate by using the CA1 certificate. |
| Sign the intermediate CA certificate by using the CA1 certificate. | Sign the device certificate by using the intermediate CA certificate. |
| Sign the device certificate by using the intermediate CA certificate. | Deploy the certificate chain to the device. |
| Sign the device certificate by using the CA1 certificate. | |
| Deploy the certificate chain to the device. | |

Navigation arrows: Left, Right, Up, Down

Explanation

Graphical user interface, text, application, chat or text message Description automatically generated

Sign the intermediate CA certificate by using the CA1 certificate.

Sign the device certificate by using the intermediate CA certificate.

Deploy the certificate chain to the device.

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>

NEW QUESTION: 85

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 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 the desired properties to the device twin.

Does the solution meet the goal?

A. Yes

B. No

Answer: B (LEAVE A REPLY)

Instead add tags to the device twin. Desired properties are synced, while tags are not.

Incorrect Answers:

A: 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://docs.microsoft.com/de-de/azure/iot-hub/iot-hub-devguide-device-twins>

<https://azure.microsoft.com/sv-se/blog/deep-dive-into-azure-iot-hub-notifications-and-device-twin/>

NEW QUESTION: 86

You have the following device twin for the IoT device.

```

{
  "deviceId": "device1",
  "etag": "AAAAAAAAAAk=",
  "deviceEtag": "NDCwMTU4Mzk=",
  "status": "enabled",
  "statusUpdateTime": "0001-01-01T00:00:00Z",
  "connectionState": "Disconnected",
  "lastActivityTime": "2019-10-21T22:45:57.9732805Z",
  "cloudToDeviceMessageCount": 0,
  "authenticationType": "sas",
  "x509Thumbprint": {
    "primaryThumbprint": null,
    "secondaryThumbprint": null
  },
  "version": 17,
  "properties": {
    "desired": {
      "$metadata": {
        "$lastUpdated": "2019-10-24T19:40:46.4809147Z",
        "$lastUpdatedVersion": 9
      },
      "$version": 9
    },
    "reported": {
      "fanSpeed": 73,
      "$metadata": {
        "$lastUpdated": "2019-10-24T19:41:28.8839751Z",
        "fanSpeed": {
          "$lastUpdated": "2019-10-24T19:41:28.8839751Z"
        }
      },
      "$version": 8
    }
  },
  "capabilities": {
    "iotEdge": false
  }
}

```



exam-tests.com

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

| Statements | Yes | No |
|---|-----------------------|-----------------------|
| You can add a property that contains multiple nested values to the device twin. | <input type="radio"/> | <input type="radio"/> |
| The device twin will set fanSpeed for the physical IoT device to 73. | <input type="radio"/> | <input type="radio"/> |
| You can change the device identity of the physical IoT device by modifying the deviceId property. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements | Yes | No |
|---|----------------------------------|----------------------------------|
| You can add a property that contains multiple nested values to the device twin. | <input checked="" type="radio"/> | <input type="radio"/> |
| The device twin will set fanSpeed for the physical IoT device to 73. | <input checked="" type="radio"/> | <input type="radio"/> |
| You can change the device identity of the physical IoT device by modifying the deviceId property. | <input type="radio"/> | <input checked="" type="radio"/> |

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-device-twins>

NEW QUESTION: 87

You have an Azure IoT hub that uses a Device Provision Service instance.

You plan to deploy 100 IoT devices.

You need to confirm the identity of the devices by using the Device Provision Service.

Which three device attestation mechanisms can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. X.509 certificates
- B. Trusted Platform Module (TPM) 2.0
- C. Trusted Platform Module (TPM) 1.2
- D. Symmetric key
- E. Device Identity Composition Engine (DICE)

D18912E1457D5D1DDCBD40AB3BF70D5D

F. 509 certificates based on the standard X.509 certificate authentication flow.

Trusted Platform Module (TPM) based on a nonce challenge, using the TPM 2.0 standard for keys to present a signed Shared Access Signature (SAS) token. This does not require a physical TPM on the device, but the service expects to attest using the endorsement key per the TPM spec.

Symmetric Key based on shared access signature (SAS) Security tokens, which include a hashed signature and an embedded expiration.

Answer: A,B,D (LEAVE A REPLY)

The Device Provisioning Service supports the following forms of attestation:

Reference:

<https://docs.microsoft.com/en-us/azure/iot-dps/concepts-service#attestation-mechanism>

NEW QUESTION: 88

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 20 IoT devices deployed across two floors of a building. The devices on the first floor must be set to 60 degrees. The devices on the second floor must be set to 80 degrees.

The device twins are configured to use a tag that identifies the floor on which the twins are located.

You create the following automatic configuration for the devices on the first floor.

```
{
  "id": "first_floor_devices",
  "schemaVersion": null,
  "labels": {
    "Version": "1"
  },
  "content": {
    "deviceContent": {
      "properties.desired.ac": {
        "temperature": 60
      }
    }
  },
  "targetCondition": "tags.floor-'first'",
  "createdTimeUtc": "2020-12-08T04:06:56.651Z",
  "lastUpdatedTimeUtc": "2020-12-08T04:06:56.651Z",
  "priority": 1,
  ...
}
```



You create the following automatic configuration for the devices on the second floor.

```

{
  "id": "second_floor_devices",
  "schemaVersion": null,
  "labels": {
    "Version": "1"
  },
  "content": {
    "deviceContent": {
      "properties.desired.ac": {
        "temperature": 80
      }
    }
  },
  "targetCondition": "*",
  "createdTimeUtc": "2020-12-08T04:11:08.561Z",
  "lastUpdatedTimeUtc": "2020-12-09T18:50:55.070Z",
  "priority": 10,
  ...
}

```



The IoT devices on the first floor report that the temperature is set to 80 degrees.

You need to ensure that the first-floor devices are set to the correct temperature.

Solution: In the automatic configuration for the second-floor devices, you set Version to 2.

Does this meet the goal?

A. Yes

B. No

Answer: ([SHOW ANSWER](#))

Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/module-deployment-monitoring?view=iotedge-2020-11>

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-automatic-device-management-cli>

NEW QUESTION: 89

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: ([SHOW ANSWER](#))

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>

NEW QUESTION: 90

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: ([SHOW ANSWER](#))

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: 91

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 ([LEAVE A REPLY](#))

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>

Valid AZ-220 Dumps shared by BraindumpsPass.com for Helping Passing AZ-220 Exam! BraindumpsPass.com now offer the **newest AZ-220 exam dumps**, the BraindumpsPass.com AZ-220 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com AZ-220 dumps with Test Engine here:
<https://www.braindumpspass.com/Microsoft/AZ-220-practice-exam-dumps.html> (205 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 92

You need to recommend a solution to keep device properties synced to IoT Hub. The solution must minimize data loss caused by the connectivity issues.

What should you include in the recommendation?

- A. Azure Event Grid
- B. a cloud-to-device message
- C. IoT Hub device twins
- D. the IoT Hub direct method

Answer: C (LEAVE A REPLY)

Explanation

Scenario: You discover connectivity issues between the IoT gateway devices and iotHub1, which cause IoT devices to lose connectivity and messages.

To synchronize state information between a device and an IoT hub, you use device twins. A device twin is a JSON document, associated with a specific device, and stored by IoT Hub in the cloud where you can query them. A device twin contains desired properties, reported properties, and tags.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/tutorial-device-twins>

NEW QUESTION: 93

You have an Azure IoT hub that receives messages from an IoT device. The messages are serialized as Protobuf.

You need the IoT hub to route the messages.

What should you do first?

- A. From the Azure portal, add desired properties to the device twin.

- B. Configure the IoT device to add application properties to the messages.
- C. From the Azure portal, configure the IoT hub to add message enrichments.
- D. Configure the IoT device to add ASCII-encoded properties to the body of the messages.

Answer: A (LEAVE A REPLY)

Device twins store device-related information that:

Device and back ends can use to synchronize device conditions and configuration.

The solution back end can use to query and target long-running operations.

Desired properties. Used along with reported properties to synchronize device configuration or conditions. The solution back end can set desired properties, and the device app can read them.

The device app can also receive notifications of changes in the desired properties.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-device-twins>

NEW QUESTION: 94

You have an Azure IoT Central application that includes a Device Provisioning Service instance. You need to connect IoT devices 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.

The screenshot shows an exam question interface with two main sections: 'Actions' and 'Answer Area'. The 'Actions' section contains five items in a list: 'Flash unique credentials to the devices.', 'Obtain the credential.', 'Generate device credentials.', 'Associate the devices to a template and approve the connections.', and 'Connect the devices to IoT Central.' Each item has a small circular icon to its right. The 'Answer Area' is currently empty, with a large Microsoft logo watermark and a set of up/down arrow icons on the right side.

Answer:

The screenshot shows the same exam question interface as above, but with the 'Answer Area' populated. The actions are arranged in the following order from top to bottom: 'Generate device credentials.', 'Flash unique credentials to the devices.', 'Connect the devices to IoT Central.', 'Associate the devices to a template and approve the connections.', and 'Obtain the credential.' Each action in the answer area is enclosed in a dashed red box, and the up/down arrow icons on the right are active, indicating they have been moved from the 'Actions' list.

Explanation

Step: With DPS (Device Provisioning Service) you can generate device credentials and configure the devices offline without registering the devices through IoT Central UI.

Connect devices that use SAS tokens without registering

1. Copy the IoT Central application's group primary key
2. Use the dps-keygen tool to generate the device SAS keys. Use the group primary key from the previous step. The device IDs must be lower-case:
`dps-keygen -mk:<group primary key> -di:<device ID>`
3. The OEM flashes each device with a device ID, a generated device SAS key, and the application ID scope value.
4. When you switch on a device, it first connects to DPS to retrieve its IoT Central registration information.

The device initially has a device status Unassociated on the Devices page and isn't assigned to a device template. On the Devices page, Migrate the device to the appropriate device template. Device provisioning is now complete, the device status is now Provisioned, and the device can start sending data.

On the Administration > Device connection page, the Auto approve option controls whether you need to manually approve the device before it can start sending data.

Reference:

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

NEW QUESTION: 95

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 Stream Analytics job that receives input from an Azure IoT hub and sends the outputs to Azure Blob storage. The job has compatibility level 1.1 and six streaming units.

You have the following query for the job.

```
SELECT COUNT(*) AS Count, TollBoothID
INTO BlobOutput
FROM IoTHubInput
GROUP BY TumblingWindow(minute, 3), TollBoothID
```

You plan to increase the streaming unit count to 12.

You need to optimize the job to take advantage of the additional streaming units and increase the throughput.

Solution: You change the compatibility level of the job to 1.2.

Does this meet the goal?

A. Yes

B. No

Answer: ([SHOW ANSWER](#))

Explanation

Max number of Streaming Units with one step and with no partitions is 6.

Reference:

<https://docs.microsoft.com/en-us/azure/stream-analytics/stream-analytics-parallelization>

NEW QUESTION: 96

You have an Azure IoT hub.

You plan to attach three types of IoT devices as shown in the following table.

| Name | Specification | Note |
|----------------------------------|---|--|
| Transparent Field Gateway Device | High-power device with a fast processor and 4 GB of RAM | Will connect to multiple devices, each with its own credentials, by using the same TLS connection. |
| Low Resource Device | Low resource specifications, battery-operated, and 512 KB of RAM | Will connect directly to an IoT hub and will NOT connect to any other devices. Will use cloud-to-device messages. |
| Limited Sensor Device | Extremely low-power device with a limited microcontroller (MCU) and 256 KB of RAM | Will NOT support the Azure SDK. Messages must be as small as possible. |

You need to select the appropriate communication protocol for each device.

What should you select? To answer, drag the appropriate protocols to the correct devices. Each protocol 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.

Protocols

AMQP

HTTPS

MQTT

Answer Area

| Device | Protocol |
|-----------------------------------|----------|
| Transparent Field Gateway Device: | Protocol |
| Low Resource Device: | Protocol |
| Limited Sensor Device: | Protocol |

Answer:

Protocols

AMQP

HTTPS

MQTT

Answer Area

| Device | Protocol |
|-----------------------------------|----------|
| Transparent Field Gateway Device: | AMQP |
| Low Resource Device: | MQTT |
| Limited Sensor Device: | HTTPS |

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-protocols>

NEW QUESTION: 97

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



Answer Area

Device symmetric key

Microsoft

@

.

Deviceld

IoT hub name

root

sas

Shared access signature (SAS) token

exam-tests.com

Answer:

Options



Answer Area

Device symmetric key

Deviceld

@

IoT hub name

Deviceld

IoT hub name

root

sas

Shared access signature (SAS) token

exam-tests.com

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-dev-guide-sas>

NEW QUESTION: 98

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: ([SHOW ANSWER](#))

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: 99

You have an Azure IoT solution that includes a standard tier Azure IoT hub and an IoT device.

The device sends one 100-KB device-to-cloud message every hour.

You need to calculate the total daily message consumption of the device. What is the total daily message consumption of the device?

A. 24

B. 600

C. 2,400

D. 4,800

Answer: **B** ([LEAVE A REPLY](#))

100 KB * 24 is around 2,400 bytes.

The 100 KB message is divided into 4 KB blocks, and it is billed for 25 messages. 25 times 24 is

600 Note: The maximum message size for messages sent from a device to the cloud is 256 KB.

These messages are metered in 4 KB blocks for the paid tiers so for instance if the device sends a 16 KB message via the paid tiers it will be billed as 4 messages.

Reference:

<https://azure.microsoft.com/en-us/pricing/details/iot-hub/>

NEW QUESTION: 100

You have an Azure IoT Central application.

You need to connect an IoT device to the application.

Which two settings do you require in IoT Central to configure the device? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Group SAS Primary Key
- B. the IoT hub name
- C. Scope ID
- D. Application Name
- E. Device ID

Answer: A,C (LEAVE A REPLY)

Required connection information:

* Group primary key: In your IoT Central application, navigate to Administration > Device Connection > SAS- IoT-Devices. Make a note of the shared access signature Primary key value.

* ID scope: In your IoT Central application, navigate to Administration > Device Connection. Make a note of the ID scope value.

Reference:

<https://docs.microsoft.com/bs-cyrl-ba/azure/iot-central/core/tutorial-connect-device-python>

NEW QUESTION: 101

You are planning a proof of concept (POC) that will use an Azure IoT hub.

You have two self-signed client authentication certificates named Cert1 and Cert2. Cert1 has a basic constraint that contains Subject Type=CA. Cert2 has a basic constraint that contains Subject Type=End Entity.

You need to identify which certificates to use.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Certificate you can use to authenticate a leaf device to IoT Hub during testing:

| | |
|----------------------|---|
| | ▼ |
| Cert1 only | |
| Cert2 only | |
| Both Cert1 and Cert2 | |
| Neither certificate | |

Certificate that you can upload to IoT Hub as a verified certificate:

| | |
|----------------------|---|
| | ▼ |
| Cert1 only | |
| Cert2 only | |
| Both Cert1 and Cert2 | |
| Neither certificate | |



Answer:

Certificate you can use to authenticate a leaf device to IoT Hub during testing:

| | |
|----------------------|---|
| | ▼ |
| Cert1 only | |
| Cert2 only | |
| Both Cert1 and Cert2 | |
| Neither certificate | |

Certificate that you can upload to IoT Hub as a verified certificate:

| | |
|----------------------|---|
| | ▼ |
| Cert1 only | |
| Cert2 only | |
| Both Cert1 and Cert2 | |
| Neither certificate | |

Explanation

Certificate you can use to authenticate a leaf device to IoT Hub during testing:

| | |
|----------------------|---|
| | ▼ |
| Cert1 only | |
| Cert2 only | |
| Both Cert1 and Cert2 | |
| Neither certificate | |

Certificate that you can upload to IoT Hub as a verified certificate:

| | |
|----------------------|---|
| | ▼ |
| Cert1 only | |
| Cert2 only | |
| Both Cert1 and Cert2 | |
| Neither certificate | |

Box 1: Cert2 only

Cert2: 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.

Box 2: Cert1 only

Cert1: A root certificate is a self-signed X.509 certificate representing a certificate authority (CA). It is the terminus, or trust anchor, of the certificate chain. Root certificates can be self-issued by an organization or purchased from a root certificate authority.

Reference:

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

NEW QUESTION: 102

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 ([LEAVE A REPLY](#))

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>

NEW QUESTION: 103

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

You need to be notified about failed local logins to a subnet of 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 |
|--|-------------|
| Create a custom alert rule. | |
| Enable Azure Security Center for IoT. | |
| Configure the Diagnostics settings of the IoT hub. | |
| Create a shared access policy. | |
| Select a device security group. | |
| Create a message route. | |



Answer:

| Actions | Answer Area |
|--|---------------------------------------|
| Create a custom alert rule. | Enable Azure Security Center for IoT. |
| Enable Azure Security Center for IoT. | Select a device security group. |
| Configure the Diagnostics settings of the IoT hub. | Create a custom alert rule. |
| Create a shared access policy. | |
| Select a device security group. | |
| Create a message route. | |



Explanation:

Step 1: Enable Azure Security Center for IoT

Security alerts, such as failed local IoT hub logins, are stored in AzureSecurityOfThings.SecurityAlert table in the Log Analytics workspace configured for the Azure Security Center for IoT solution.

Step 2: Select a device security group

Update a device security group..

Step 3: Create a custom alert rule

..by creating a custom alert rule

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/asc-for-iot/how-to-security-data-access>

<https://docs.microsoft.com/en-us/rest/api/securitycenter/devicesecuritygroups/createorupdate>

NEW QUESTION: 104

You have three Azure IoT hubs named Hub1, Hub2, and Hub3, a Device Provisioning Service instance, and an IoT device named Device1.

Each IoT hub is deployed to a separate Azure region. Device enrollment uses the Lowest latency allocation policy.

The Device Provisioning Service uses the Lowest latency allocation policy. Device1 is auto-provisioned to Hub1 by using the Device Provisioning Service. Device1 regularly moves between regions.

You need to ensure that Device1 always connects to the IoT hub that has the lowest latency.

What should you do?

- A. Configure device attestation that uses X.509 certificates.
- B. Implement device certificate rolling.
- C. Disenroll and reenroll Device1.
- D. Configure the re-provisioning policy.

Answer: D (LEAVE A REPLY)

Automated re-provisioning support.

Microsoft added first-class support for device re-provisioning which allows devices to be reassigned to a different IoT solution sometime after the initial solution assignment. Re-provisioning support is available in two options:

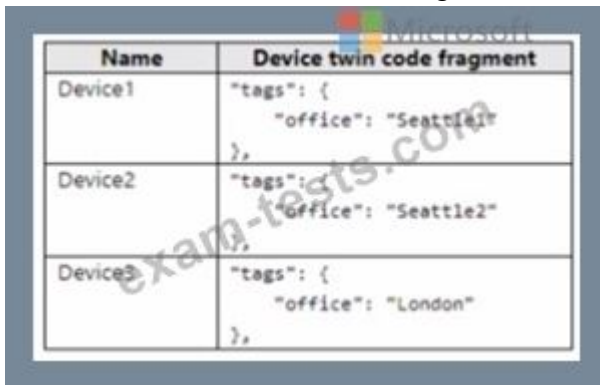
Factory reset, in which the device twin data for the new IoT hub is populated from the enrollment list instead of the old IoT hub. This is common for factory reset scenarios as well as leased device scenarios. Migration, in which device twin data is moved from the old IoT hub to the new IoT hub. This is common for scenarios in which a device is moving between geographies.

Reference:

<https://azure.microsoft.com/en-us/blog/new-year-newly-available-iot-hub-device-provisioning-service-features/>

NEW QUESTION: 105

You have an Azure IoT hub and three Azure IoT Edge devices. The device twin code for each device is shown in the following table.



| Name | Device twin code fragment |
|---------|--|
| Device1 | <pre>"tags": { "office": "Seattle1" },</pre> |
| Device2 | <pre>"tags": { "office": "Seattle2" },</pre> |
| Device3 | <pre>"tags": { "office": "London" },</pre> |

A standard automatic deployment is already applied.

You have three layered deployments. The deployment code for each deployment is shown in the following table.

| Name | Deployment code |
|-------------|--|
| Deployment1 | <pre> { "id": "deploy1", "priority": 90, "targetCondition": " tags.office='Seattle1' OR tags.office='Seattle2' ", ... "\$edgeAgent": { "properties.desired.modules.MyModule1": { ... } } "\$edgeHub": { "properties.desired.routes.MyModule1": "FROM /messages/modules/MyModule1/outputs/seattle1 INTO \$upstream", "properties.desired.routes.MyModule1A": "FROM /messages/modules/MyModule1/* INTO \$upstream" ... } } </pre> |
| Deployment2 | <pre> { "id": "deploy2", "priority": 80, "targetCondition": " tags.office='Seattle1' OR tags.office='Seattle2' OR tags.office='London' ", ... "\$edgeAgent": { "properties.desired.modules.MyModule1": { ... } } "\$edgeHub": { "properties.desired.routes.MyModule1": "FROM /messages/modules/MyModule1/outputs/seattle2 INTO \$upstream", "properties.desired.routes.MyModule1A": "FROM /messages/modules/MyModule1/* INTO \$upstream" "properties.desired.routes.MyModule1B": "FROM /messages/modules/MyModule1/* INTO \$upstream" ... } } </pre> |
| Deployment3 | <pre> { "id": "deploy3", "priority": 70, "targetCondition": " tags.office='London' ", - "\$edgeAgent": { "properties.desired.modules.MyModule1": { - }, "properties.desired.modules.MyModule2": { ... } } ... "\$edgeHub": { "properties.desired.routes.MyModule1": "FROM /messages/modules/MyModule1/* INTO \$upstream", "properties.desired.routes.MyModule2": "FROM /messages/modules/MyModule2/* INTO \$upstream" ... } } </pre> |



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



| Statements | Yes | No |
|--|-----------------------|-----------------------|
| Device1 routes messages to /messages/modules/MyModule1/outputs/seattle2. | <input type="radio"/> | <input type="radio"/> |
| Device2 has the MyModule1B route deployed. | <input type="radio"/> | <input type="radio"/> |
| Device3 has the MyModule2 route deployed. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area



| Statements | Yes | No |
|--|----------------------------------|----------------------------------|
| Device1 routes messages to /messages/modules/MyModule1/outputs/seattle2. | <input type="radio"/> | <input checked="" type="radio"/> |
| Device2 has the MyModule1B route deployed. | <input type="radio"/> | <input checked="" type="radio"/> |
| Device3 has the MyModule2 route deployed. | <input checked="" type="radio"/> | <input type="radio"/> |

NEW QUESTION: 106

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. | <div style="display: flex; justify-content: space-between; align-items: center;"> ⏪ ⏩ </div> <div style="display: flex; justify-content: space-between; align-items: center;"> ⏴ ⏵ </div> |
| 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> | |
| 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. | |

Answer:

Actions

Create an individual device enrollment by using the Device Provisioning Service.

Run the following commands.

```
sudo apt-get install moby-engine
sudo apt-get install moby-cli
sudo apt-get install iotedge
```

Add the connection string to the `/etc/iotedge/config.yaml` file, and then run the following command.

```
sudo systemctl restart iotedge
```

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.

Answer Area

Run the following commands.

```
sudo apt-get install moby-engine
sudo apt-get install moby-cli
sudo apt-get install iotedge
```

From IoT Hub, create an IoT Edge device registry entry.

Add the connection string to the `/etc/iotedge/config.yaml` file, and then run the following command.

```
sudo systemctl restart iotedge
```

Explanation

Actions

Create an individual device enrollment by using the Device Provisioning Service.

Run the following commands.

```
sudo apt-get install moby-engine
sudo apt-get install moby-cli
sudo apt-get install iotedge
```

Add the connection string to the `/etc/iotedge/config.yaml` file, and then run the following command.

```
sudo systemctl restart iotedge
```

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.

Answer Area

Run the following commands.

```
sudo apt-get install moby-engine
sudo apt-get install moby-cli
sudo apt-get install iotedge
```

From IoT Hub, create an IoT Edge device registry entry.

Add the connection string to the `/etc/iotedge/config.yaml` file, and then run the following command.

```
sudo systemctl restart iotedge
```

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>

Valid AZ-220 Dumps shared by BraindumpsPass.com for Helping Passing AZ-220 Exam! BraindumpsPass.com now offer the **newest AZ-220 exam dumps**, the BraindumpsPass.com AZ-220 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com AZ-220 dumps with Test Engine here: <https://www.braindumps.com/Microsoft/AZ-220-practice-exam-dumps.html> (205 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 107

You have an Azure IoT hub that receives messages from an IoT device. The messages are serialized as Protobuf.

You need the IoT hub to route the messages.

What should you do first?

- A. From the Azure portal, add desired properties to the device twin.
- B. Configure the IoT device to add application properties to the messages.
- C. From the Azure portal, configure the IoT hub to add message enrichments.
- D. Configure the IoT device to add ASCII-encoded properties to the body of the messages.

Answer: A (LEAVE A REPLY)

Explanation

Device twins store device-related information that:

Device and back ends can use to synchronize device conditions and configuration.

The solution back end can use to query and target long-running operations.

Desired properties. Used along with reported properties to synchronize device configuration or conditions. The solution back end can set desired properties, and the device app can read them.

The device app can also receive notifications of changes in the desired properties.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-device-twins>

NEW QUESTION: 108

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

Answer: B (LEAVE A REPLY)

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>

NEW QUESTION: 109

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. Upload to Azure Storage.
- D. Build an IoT Edge solution.
- E. Generate a shared access signature (SAS) token for Device 1.

Answer: (SHOW ANSWER)

D: Once you create IoT Edge modules with your business logic, you want to deploy them to your devices to operate at the edge.

B: 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.

You deploy modules to your device by applying the deployment manifest that you configured with the module information.

In the Visual Studio Code explorer view, expand the Azure IoT Hub section, and then expand the Devices node.

To confirm that the device you've chosen is an IoT Edge device, select it to expand the list of modules and verify the presence of \$edgeHub and \$edgeAgent. Every IoT Edge device includes these two modules.

Select Create Deployment for Single Device.

Navigate to the deployment manifest JSON file that you want to use, and click Select Edge Deployment Manifest.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/how-to-deploy-modules-vscode>

NEW QUESTION: 110

You need to meet the monitoring requirements for device metrics. What should you configure?

- A. Azure Stream Analytics
- B. Azure Time Series Insights

C. the Diagnostic settings

D. Microsoft Power BI

Answer: C ([LEAVE A REPLY](#))

Valid AZ-220 Dumps shared by BraindumpsPass.com for Helping Passing AZ-220 Exam! BraindumpsPass.com now offer the **newest AZ-220 exam dumps**, the BraindumpsPass.com AZ-220 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com AZ-220 dumps with Test Engine here:

<https://www.braindumpspass.com/Microsoft/AZ-220-practice-exam-dumps.html> (205 Q&As

Dumps, **40%OFF** Special Discount: **Exam-Tests**)