

Microsoft.AZ-220.v2022-10-07.q122

Exam Code:	AZ-220
Exam Name:	Microsoft Azure IoT Developer
Certification Provider:	Microsoft
Free Question Number:	122
Version:	v2022-10-07
# of views:	2058
# of Questions views:	1220
https://www.freepdfdumps.com/Microsoft.AZ-220.v2022-10-07.q122.html	

NEW QUESTION: 1

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: C (LEAVE A REPLY)

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: 2

You have an Azure IoT Central application.

You add an IoT device named Oven1 to the application. Oven1 uses an IoT Central template for industrial ovens. You need to send an email to the managers group at your company as soon as the oven temperature falls below 400 degrees. Which two actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. Create a SendGrid account in the same resource group as the IoT Central application.
- B. Add a condition that has Time Aggregation set to Off.
- C. Add a condition that has Aggregation set to Minimum.
- D. Add the Manager role to the IoT Central application.
- E. From IoT Central, create a telemetry rule for the template.

Answer: B,E (LEAVE A REPLY)

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

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

B: Configure the rule conditions.

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

1. Select Temperature in the Telemetry dropdown.
2. Next, choose Is less than as the Operator and enter 400 as the Value.

Tutorial application Search

Rules > Temperature monitor

Temperature monitor

☒ Enabled

Target devices

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

Device template *

Sensor Controller

+ Filter

Conditions

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

Time aggregation

☒ Off

Telemetry *	Operator *	Value *
Temperature	Is greater than	70

+ Condition

Actions

Microsoft

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

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

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

Reference:

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

NEW QUESTION: 3

You have an Azure IoT Edge automatic deployment named D1 that deploys a temperature module to five IoT Edge devices.

D1 has a deployment priority of 10 and the following module configuration.

```
"TemperatureModule": {
  "properties.desired": {
    "SendData": true,
    "SendInterval": 5
  }
}
```

You need to create a new layered deployment that will add a new twin property named ReportingMode. The new deployment must not overwrite the existing module configurations set by D1.

How should you configure the deployment? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Deployment Priority:

▼

1

10

20

Deployment Configuration:

"TemperatureModule": {

▼

"poperties.desired":{

"poperties.desired.reportingSettings":{

"properties.reported": {

"properties.tags": {

"ReportingMode": "batch"

Microsoft

Answer:

Deployment Priority:

	▼
1	
10	
20	

Deployment Configuration:

TemperatureModule: {

	▼
"properties.desired": {	
"properties.desired.reportingSettings": {	
"properties.reported": {	
"properties.tags": { }	
"ReportingMode": "batch"	
}	
}	

Explanation

Text Description automatically generated with low confidence

Deployment Priority:

▼

1

10

20

Deployment Configuration:

TemperatureModule: {

▼

"properties.desired":{

"properties.desired.reportingSettings":{

"properties.reported": {

"properties.tags": {

"ReportingMode": "batch"

}

}

}

Box 1: 1

A priority defines whether a deployment should be applied to a targeted device relative to other deployments.

A deployment priority is a positive integer, with larger numbers denoting higher priority. If an IoT Edge device is targeted by more than one deployment, the deployment with the highest priority applies.

Deployments with lower priorities are not applied, nor are they merged. If a device is targeted with two or more deployments with equal priority, the most recently created deployment (determined by the creation timestamp) applies.

Box 2: "properties.tags": {

You create a deployment manifest and then define which devices it applies to based on tags in the device twin.

Reference:

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

NEW QUESTION: 4

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

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

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

Does this meet the goal?

A. Yes

B. No

Answer: A (LEAVE A REPLY)

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: 5

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.

Actions	Answer Area
Flash unique credentials to the devices.	
Obtain the credential.	
Generate device credentials.	
 Associate the devices to a template and approve the connections.	
 Connect the devices to IoT Central.	

Answer:

Actions	Answer Area
Flash unique credentials to the devices.	Generate device credentials.
Obtain the credential.	Flash unique credentials to the devices.
Generate device credentials.	Connect the devices to IoT Central.
Associate the devices to a template and approve the connections.	Associate the devices to a template and approve the connections.
Connect the devices to IoT Central.	Obtain the credential.

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: 6

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: B,C (LEAVE A REPLY)

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: 7

You have 100 devices that connect to an Azure IoT hub named Hub1. The devices connect by using a symmetric key.

You deploy an IoT hub named Hub2.

You need to migrate 10 devices from Hub1 to Hub2. The solution must ensure that the devices retain the existing symmetric key.

What should you do?

A. Add a desired property to the device twin of Hub2. Update the endpoint of the 10 devices to use Hub2.

B. Add a desired property to the device twin of Hub1. Recreate the device identity on Hub2.

C. Recreate the device identity on Hub2. Update the endpoint of the 10 devices to use Hub2.

D. Disable the 10 devices on Hub1. Update the endpoint of the 10 devices to use Hub2.

Answer: B (LEAVE A REPLY)

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> Provision and manage devices Question Set 1

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 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)

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 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 Area

▼ Stiohubname Stwin Stwin.properties Stwin.results Stwin.tags	▼ desired.pressure fanSpeed.reported reported.fanSpeed temperature temperature.reported
--	--

Answer:

Answer Area

▼ Stiohubname Stwin Stwin.properties Stwin.results Stwin.tags	▼ desired.pressure fanSpeed.reported reported.fanSpeed temperature temperature.reported
--	--

Reference:

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

NEW QUESTION: 10

You plan to deploy Azure Time Series Insights.

What should you create on iothub1 before you deploy Time Series Insights?

- A. a new message route
- B. a new consumer group
- C. a new shared access policy
- D. an IP filter rule

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

Create a dedicated consumer group in the IoT hub for the Time Series Insights environment to consume from.

Each Time Series Insights event source must have its own dedicated consumer group that isn't shared with any other consumer. If multiple readers consume events from the same consumer group, all readers are likely to exhibit failures.

Reference:

<https://docs.microsoft.com/en-us/azure/time-series-insights/time-series-insights-how-to-add-an-event-source- iothub>

NEW QUESTION: 11

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

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

Explanation

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>

NEW QUESTION: 12

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: ([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: 13

HOTSPOT

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.

Hot Area:

Answer Area

Siothubname \$twin \$twin.properties \$twin.results \$twin.tags	.	desired.pressure fanSpeed.reported reported.fanSpeed temperature temperature.reported
--	---	--

Answer:

Answer Area

Siothubname \$twin \$twin.properties \$twin.results \$twin.tags	.	desired.pressure fanSpeed.reported reported.fanSpeed temperature temperature.reported
--	---	--

Explanation/Reference:

<https://docs.microsoft.com/bs-cyrl-ba/azure/iot-hub/iot-hub-message-enrichments-overview> Process and manage data Testlet 2 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.

Requirements. Planned Changes

ADatum is developing an Azure IoT solution to monitor environmental conditions. The IoT solution consists of hardware devices and cloud services. All the devices will communicate directly to Azure IoT Hub.

The hardware devices will be deployed to the branch offices and will collect data about various environmental conditions such as temperature, humidity, air quality, and noise level. The devices will be wired by using Power over Ethernet (PoE) connections.

ADatum is developing the solution in the following three phases: proof of value (POV), pilot, and production.

Requirements. POV Requirements

The POV phase will demonstrate that a technical solution is viable. During this phase, 100 devices will be deployed to the main office and Azure Stream Analytics will be connected to an IoT hub to generate real-time alerts. Stream Analytics will perform the following processing:

- * Calculate the median rate of the telemetry across the entire devices that exceed the median rate by a factor of 4.
- * Compare the current telemetry to the specified thresholds and issue alerts when telemetry values are out of range.
- * Ensure that all message content during this phase is human readable to simplify debugging.

Requirements. Pilot Requirements

During the pilot phase, devices will be deployed to 10 offices. Each office will have up to 1,000 devices.

During this phase, you will add Azure Time Series Insights in parallel to Stream Analytics to support real-time graphs and queries in a dashboard web app.

The pilot deployment must minimize operating costs.

Requirements. Production Requirements

The production phase will include all the offices.

The production deployment will have one IoT hub in each Azure region. Devices must connect to the IoT hub in their region.

The production phase must meet the following requirements:

- * Ensure that the IoT solution can support performance and scale targets.
- * Ensure that the IoT solution support up to 1,000 devices per office.
- * Minimize operating costs of the IoT solution.

Requirements. Technical Requirements

Datum identifies the following requirements for the planned IoT solution:

- * The solution must generate real-time alerts when a fire condition is detected in an office. All the devices in that office must trigger an audible alarm siren within 10 seconds of the alert.
- * A dashboard UI must display alerts and the system status in real time and must allow device operators to make adjustments to the system.
- * Each device will send hourly updates to IoT Hub. Condition alerts will be sent immediately.
- * Multiple types of devices will collect telemetry that has different schemas.
- * IoT Hub must perform message routing based on the message body.
- * Direct methods must be used for cloud-to-device communication.
- * Reports must be provided monthly, quarterly, and annually.
- * Stored data queries must be as efficient as possible.
- * The device message size will be under 4 KB.
- * Development effort must be minimized.

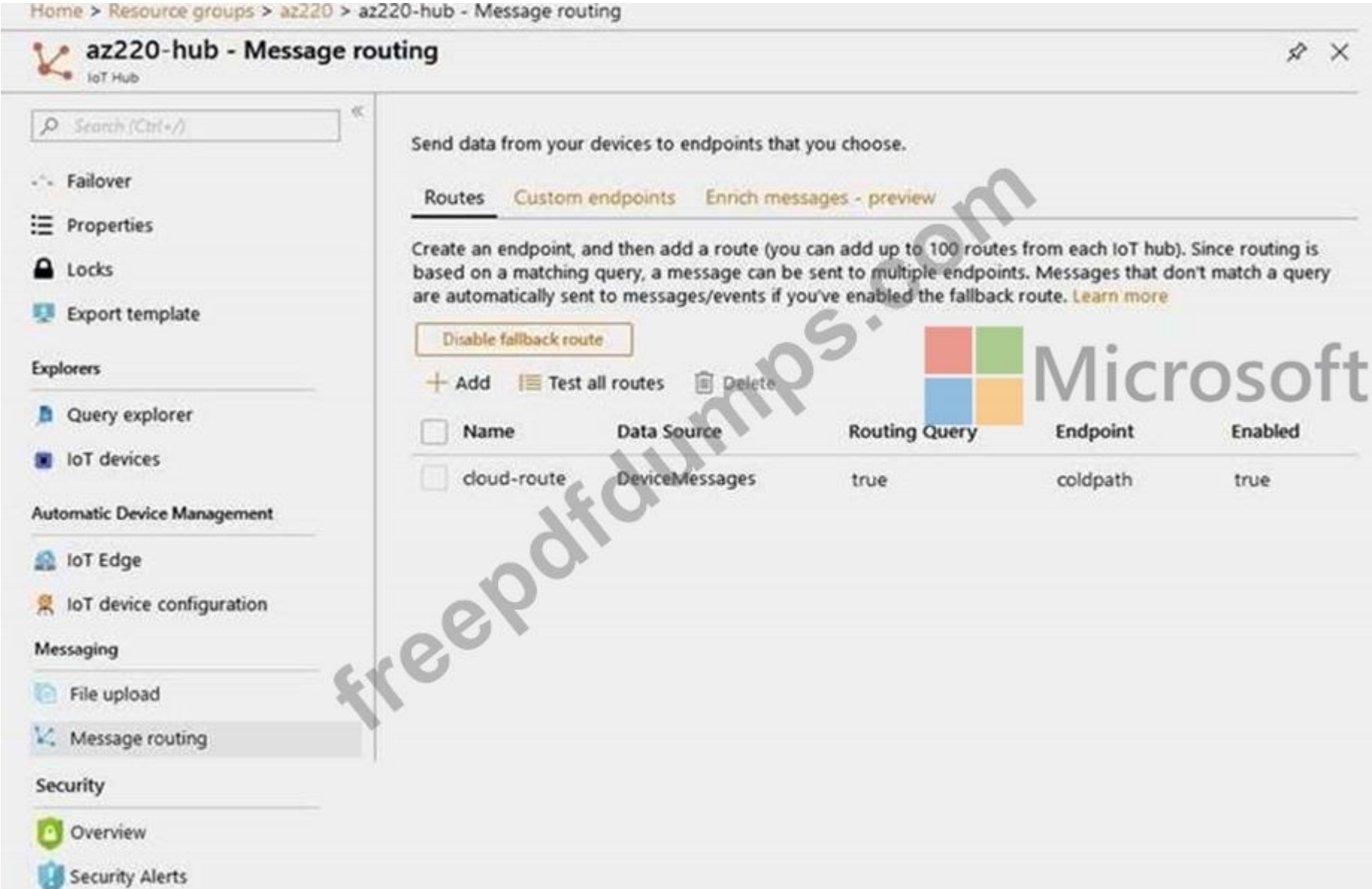
Requirements. Throttle and Quotas

The relevant throttles and quotas for various IoT Hub tiers are shown in the following table.

Tier	Direct method	Device-to-cloud message	Price per month
B1	40/sec/unit	400,000/day/unit	\$10/unit
S1	40/sec/unit	400,000/day/unit	\$25/unit
S2	120/sec/unit	6,000,000/day/unit	\$250/unit

Requirements. IoT Hub Routing

You plan to implement IoT Hub routing during the POV phase as shown in the following exhibit.



NEW QUESTION: 14

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

Explanation:

Box 1: AMQP
Use AMQP on field and cloud gateways to take advantage of connection multiplexing across devices.

Box 2: MQTT
MQTT is used on all devices that do not require to connect multiple devices (each with its own per-device credentials) over the same TLS connection.

Box 3: HTTPS
Use HTTPS for devices that cannot support other protocols.

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

NEW QUESTION: 15

Your company develops a custom module and exports the module as a Linux Dockerfile.
You need to deploy the module to an Azure IoT Edge device that runs Ubuntu Server 18.04.

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

- From Microsoft Visual Studio Code, create an IoT Edge solution and add the Dockerfile to the solution.
- Delete the \$edgeHub module from the IoT Edge device.
- Attach a child device to the IoT Edge device.
- Create a deployment for the IoT Edge device.
- Build and push the module to Azure Container Registry.

Answer Area



Answer:

Actions

- From Microsoft Visual Studio Code, create an IoT Edge solution and add the Dockerfile to the solution.
- Delete the \$edgeHub module from the IoT Edge device.
- Attach a child device to the IoT Edge device.
- Create a deployment for the IoT Edge device.
- Build and push the module to Azure Container Registry.

Answer Area

- From Microsoft Visual Studio Code, create an IoT Edge solution and add the Dockerfile to the solution.
- Build and push the module to Azure Container Registry.
- Create a deployment for the IoT Edge device.



Explanation

Graphical user interface, text Description automatically generated with medium confidence

From Microsoft Visual Studio Code, create an IoT Edge solution and add the Dockerfile to the solution.

Build and push the module to Azure Container Registry.

Create a deployment for the IoT Edge device.

Step 1: From Microsoft Visual Studio Code,...

The Azure IoT Tools extension provides project templates for all supported IoT Edge module languages in Visual Studio Code. These templates have all the files and code that you need to deploy a working module to test IoT Edge, or give you a starting point to customize the template with your own business logic.

Step 2: Build and push the module to Azure Container Registry

Build and push your solution. Review the module code and the deployment. Then build the SampleModule container image and push it to your container registry.

Step 3: Create a deployment for the IoT Edge device.

Verify that the built container images are stored in your container registry, then deploy the modules to the device.

Reference:

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

NEW QUESTION: 16

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 Bash 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.

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

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.

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: 18

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: (SHOW ANSWER)

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: 19

You have an Azure IoT Edge module named SampleModule that runs on a device named Device1.

You make changes to the code of SampleModule by using Microsoft Visual Studio Code.

You need to push the code to the container registry and then deploy the module to Device1.

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

NOTE: Each correct selection is worth one point.

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

Answer: B,C (LEAVE A REPLY)

Explanation

C: Configure a deployment manifest. A deployment manifest is a JSON document that describes which modules to deploy, how data flows between the modules, and desired properties of the module twins.

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

Reference:

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

NEW QUESTION: 20

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: 21

You have an Azure IoT solution that includes several Azure IoT hubs.

A new alerting feature was recently added to the IoT devices. The feature uses a new device twin reported property named alertCondition. You need to send alerts to an Azure Service Bus queue named MessageAlerts. The alerts must include alertCondition and the name of the IoT hub.

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

NOTE: Each correct selection is worth one point.

A. Configure File upload for each IoT hub. Configure the device to send a file to an Azure Storage container that contains the device name and status message.

B. Add the following message enrichments:

Name = iotHubName

Value = \$twin.tag.location

Endpoint = MessageAlert

C. Create an IoT Hub routing rule that has a data source of Device Twin Change Events and select the endpoint for MessageAlerts.

D. Add the following message enrichments:

Name = iotHubName

Value = \$iothubname

Endpoint = MessageAlert

E. Create an IoT Hub routing rule that has a data source of Device Telemetry Messages and select the endpoint for MessageAlerts.

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

B: Message enrichments is the ability of the IoT Hub to stamp messages with additional information before the messages are sent to the designated endpoint. One reason to use message enrichments is to include data that can be used to simplify downstream processing. For example, enriching device telemetry messages with a device twin tag can reduce load on customers to make device twin API calls for this information.

D: Applying enrichments

The messages can come from any data source supported by IoT Hub message routing, including the following examples:

* -->device twin change notifications -- changes in the device twin

* device telemetry, such as temperature or pressure

* device life-cycle events, such as when the device is created or deleted Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-message-enrichments-overview>

NEW QUESTION: 22

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.

Actions

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.

Answer Area

Answer:

Actions

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.

Answer Area

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.

Explanation

Actions

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.

Answer Area

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.

- Step 1: Provision Time Series Insights
- Select Provision new IoT Hub to create a new IoT hub.
- Step 2: Route telemetry from IoT Hub to a custom event.

Step 3: Add a data access policy to Time Series Insights for the dashboard web app Scenario: Requirements. Pilot Requirements During the pilot phase, devices will be deployed to 10 offices. Each office will have up to 1,000 devices.

During this phase, you will add Azure Time Series Insights in parallel to Stream Analytics to support real-time graphs and queries in a dashboard web app.

The pilot deployment must minimize operating costs.

Reference:

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

NEW QUESTION: 23

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 update the twin desired property and check the corresponding reported property.

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: 24

You are developing an Azure IoT solution for a shipping company. The company's ships will have sensors used for predictive maintenance. Some sensor devices will be MQTT-capable, and others will use Modbus.

Each ship has an internet connection that is available only when the ship is docked.

You create an Azure IoT hub.

You need to implement an IoT solution that uses Azure IoT Edge.

What should you do?

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

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

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

NEW QUESTION: 25

You have 10,000 IoT devices that connect to an Azure IoT hub. The devices do not support over-the-air (OTA) updates. You need to decommission 1,000 devices. The solution must prevent connections and autoenrollment for the decommissioned devices. 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 connectionState device twin property on all the devices.
- B.** Blacklist the X.509 root certification authority (CA) certificate for the enrollment group.
- C.** Delete the enrollment entry for the devices.
- D.** Remove the identity certificate from the hardware security module (HSM) of the devices.
- E.** Delete the device identity from the device registry of the IoT hub.

Answer: ([SHOW ANSWER](#)**)**

B: X.509 certificates are typically arranged in a certificate chain of trust. If a certificate at any stage in a chain becomes compromised, trust is broken. The certificate must be blacklisted to prevent Device Provisioning Service from provisioning devices downstream in any chain that contains that certificate.

C: Individual enrollments apply to a single device and can use either X.509 certificates or SAS tokens (in a real or virtual TPM) as the attestation mechanism. (Devices that use SAS tokens as their attestation mechanism can be provisioned only through an individual enrollment.) To blacklist a device that has an individual enrollment, you can either disable or delete its enrollment entry.

To blacklist a device that has an individual enrollment, you can either disable or delete its enrollment entry.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-dps/how-to-revoke-device-access-portal>

NEW QUESTION: 26

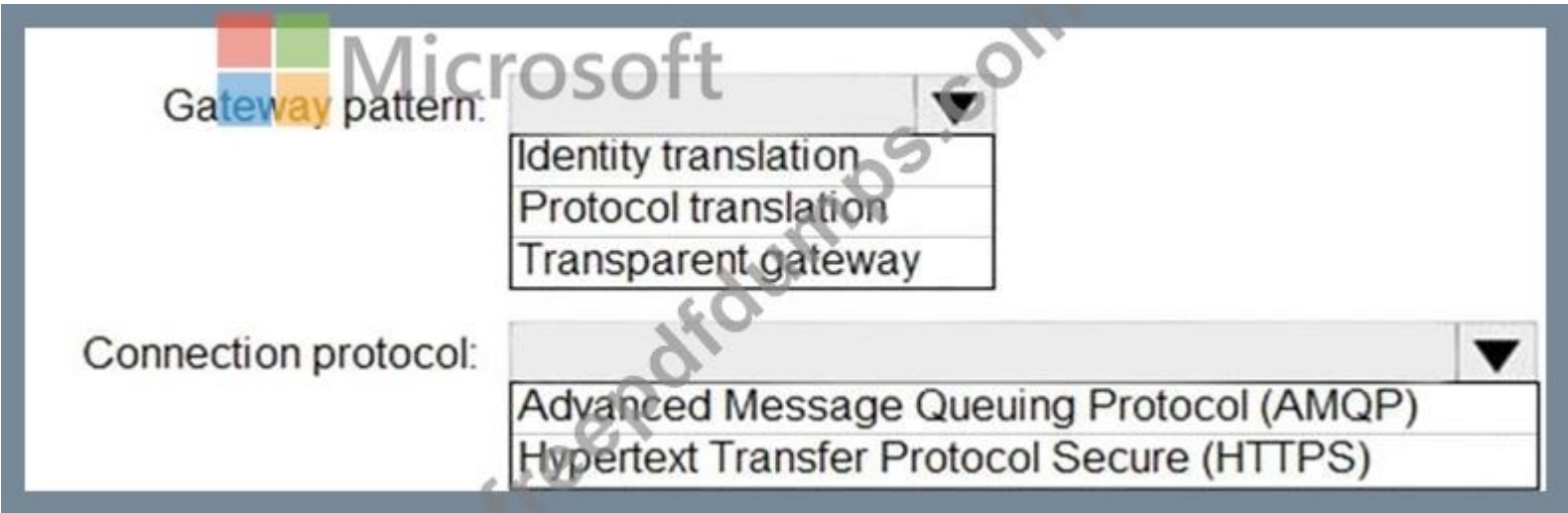
You have an Azure subscription that contains an Azure IoT hub, an Azure IoT Edge gateway, and 1,000 leaf devices. The leaf devices use a custom communication protocol that is NOT supported by the IoT hub.

You need to configure the gateway to meet the following requirements:

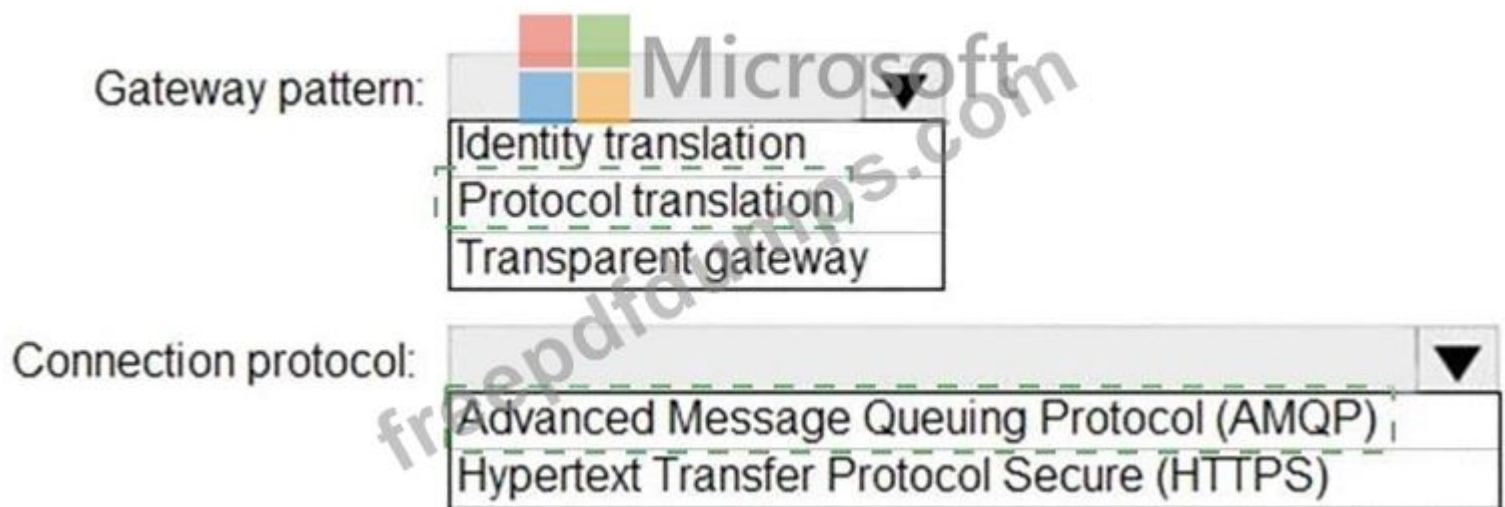
- * Minimize the number of connections between the gateway and the IoT hub.
- * Support addressing cloud-to-device messages to individual leaf devices.

How should you configure the gateway? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

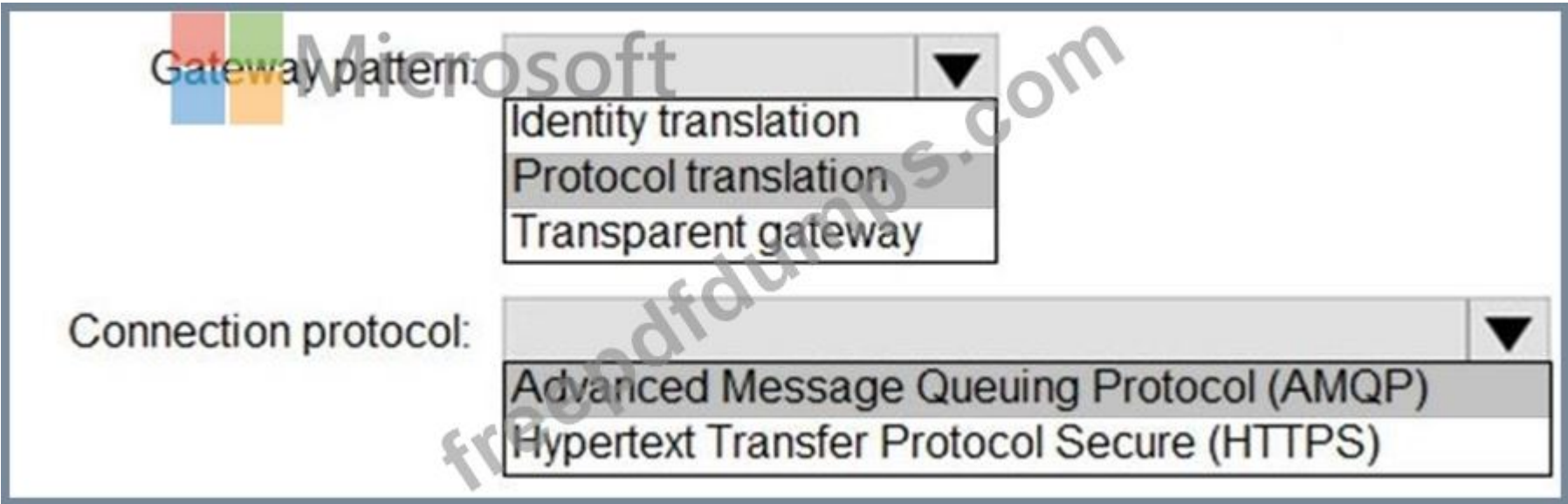


Answer:



Explanation

Graphical user interface, text, application, table Description automatically generated



Box 1: Protocol translation

In the protocol translation gateway pattern, only the IoT Edge gateway has an identity with IoT Hub. The translation module receives messages from downstream devices, translates them into a supported protocol, and then the IoT Edge device sends the messages on behalf of the downstream devices.

Box 2: Advanced MessageQueuing Protocol (AMQP)

Connection multiplexing - All devices connecting to IoT Hub through an IoT Edge gateway can use the same underlying connection. This multiplexing capability requires that the IoT Edge gateway uses AMQP as its upstream protocol.

Reference:

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

NEW QUESTION: 27

You plan to deploy a standard tier Azure IoT hub.

You need to perform an over-the-air (OTA) update on devices that will connect to the IoT hub by using scheduled jobs.

What should you use?

- A.** a device-to-cloud message
- B.** the device twin reported properties
- C.** a cloud-to-device message
- D.** a direct method

Answer: D (LEAVE A REPLY)

Releases via the REST API.

All of the operations that can be performed from the Console can also be automated using the REST API. You might do this to automate your build and release process, for example.

You can build firmware using the Particle CLI or directly using the compile source code API.

Note: Over-the-air (OTA) firmware updates are a vital component of any IoT system. Over-the-air firmware updates refers to the practice of remotely updating the code on an embedded device.

Reference:

<https://docs.particle.io/tutorials/device-cloud/ota-updates/>

NEW QUESTION: 28

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)

Explanation

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

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: 29

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.	☐	☐
The device twin will set fanSpeed for the physical IoT device to 73.	☐	☐
You can change the device identity of the physical IoT device by modifying the deviceId property.	☐	☐

Answer:

Statements	Yes	No
You can add a property that contains multiple nested values to the device twin.	☒	☐
The device twin will set fanSpeed for the physical IoT device to 73.	☒	☐
You can change the device identity of the physical IoT device by modifying the deviceId property.	☐	☒

Reference:

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

NEW QUESTION: 30

You have an Azure IoT solution that includes an Azure IoT hub and 100 Azure IoT Edge devices.

You plan to deploy the IoT Edge devices to external networks. The firewalls of the external networks only allow traffic on port 80 and port 443.

You need to ensure that the devices can connect to the IoT hub. The solution must minimize costs.

What should you do?

- A. Configure the devices for extended offline operations.
- B. Configure the upstream protocol of the devices to use MQTT over WebSocket.
- C. Connect the external networks to the IoT solution by using ExpressRoute.
- D. Configure the devices to use an HTTPS proxy.

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

MQTT over WebSockets uses port 443.

Reference:

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

```

{
  "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
}
}

```



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
lothub
```

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: 31

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.	☐	☐
The function will be invoked only when the IoT hub receives telemetry.	☐	☐
When the Stream Analytics job is restarted, the function can be invoked more than once in a 24-hour period.	☐	☐

Answer:

Statements	Yes	No
The function will be invoked at midnight UTC.	☒	☐
The function will be invoked only when the IoT hub receives telemetry.	☐	☒
When the Stream Analytics job is restarted, the function can be invoked more than once in a 24-hour period.	☒	☐

Explanation

Statements	Yes	No
The function will be invoked at midnight UTC.	☒	☐
The function will be invoked only when the IoT hub receives telemetry.	☐	☒
When the Stream Analytics job is restarted, the function can be invoked more than once in a 24-hour period.	☒	☐

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

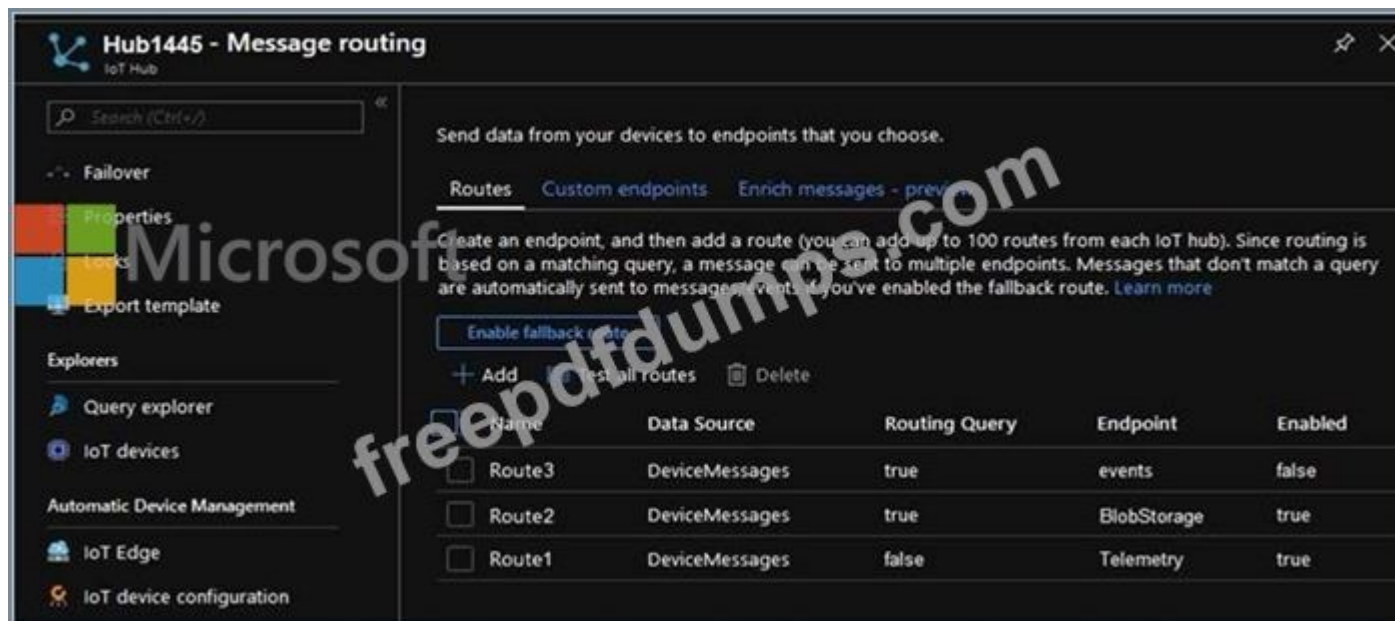
Reference:

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

Valid AZ-220 Dumps shared by Actual4test.com for Helping Passing AZ-220 Exam! Actual4test.com now offer the **newest AZ-220 exam dumps**, the Actual4test.com AZ-220 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-220 dumps with Test Engine here: https://www.actual4test.com/AZ-220_examcollection.html (205 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 32

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: (SHOW ANSWER)

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: 33

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:	<table><tr><td></td><td>▼</td></tr><tr><td colspan="2">Cert1 only</td></tr><tr><td colspan="2">Cert2 only</td></tr><tr><td colspan="2">Both Cert1 and Cert2</td></tr><tr><td colspan="2">Neither certificate</td></tr></table>		▼	Cert1 only		Cert2 only		Both Cert1 and Cert2		Neither certificate	
	▼										
Cert1 only											
Cert2 only											
Both Cert1 and Cert2											
Neither certificate											
Certificate that you can upload to IoT Hub as a verified certificate:	<table><tr><td></td><td>▼</td></tr><tr><td colspan="2">Cert1 only</td></tr><tr><td colspan="2">Cert2 only</td></tr><tr><td colspan="2">Both Cert1 and Cert2</td></tr><tr><td colspan="2">Neither certificate</td></tr></table>		▼	Cert1 only		Cert2 only		Both Cert1 and Cert2		Neither 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: 34

You have an Azure IoT solution that includes a basic tier Azure IoT hub named Hub1 and a Raspberry Pi device named Device1. Device1 connects to Hub1.

You back up Device1 and restore the backup to a new Raspberry Pi device.

When you start the new Raspberry Pi device, you receive the following error message in the diagnostic logs of Hub1: "409002 LinkCreationConflict." You need to ensure that Device1 and the new Raspberry Pi device can run simultaneously without error.

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

NOTE: Each correct selection is worth one point.

- A. On the new Raspberry Pi device, modify the connection string.
- B. From Hub1, modify the device shared access policy.
- C. Upgrade Hub1 to the standard tier.
- D. From Hub1, create a new consumer group.
- E. From Hub1, create a new IoT device.

Answer: A,E (LEAVE A REPLY)

Explanation

Note: Symptoms

You see the error 409002 LinkCreationConflict in logs along with device disconnection or cloud-to-device message failure.

Cause

Generally, this error happens when IoT Hub detects a client has more than one connection. In fact, when a new connection request arrives for a device with an existing connection, IoT Hub closes the existing connection with this error.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-troubleshoot-error-409002-linkcreationconflict#symptom>

<https://devblogs.microsoft.com/iotdev/understand-different-connection-strings-in-azure-iot-hub/>

NEW QUESTION: 35

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:

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: 36

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.

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

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: 37

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.

Actions

Flash unique credentials to the devices.

Obtain the credential.

Generate device credentials.

Associate the devices to a template and approve the connections.

Connect the devices to IoT Central.

Answer Area

⬅️

➡️

⬅️

➡️

Microsoft

Answer:

Actions

Flash unique credentials to the devices.

Obtain the credential.

Generate device credentials.

Associate the devices to a template and approve the connections.

Connect the devices to IoT Central.

Answer Area

➡️

⬅️

⬅️

➡️

Generate device credentials.

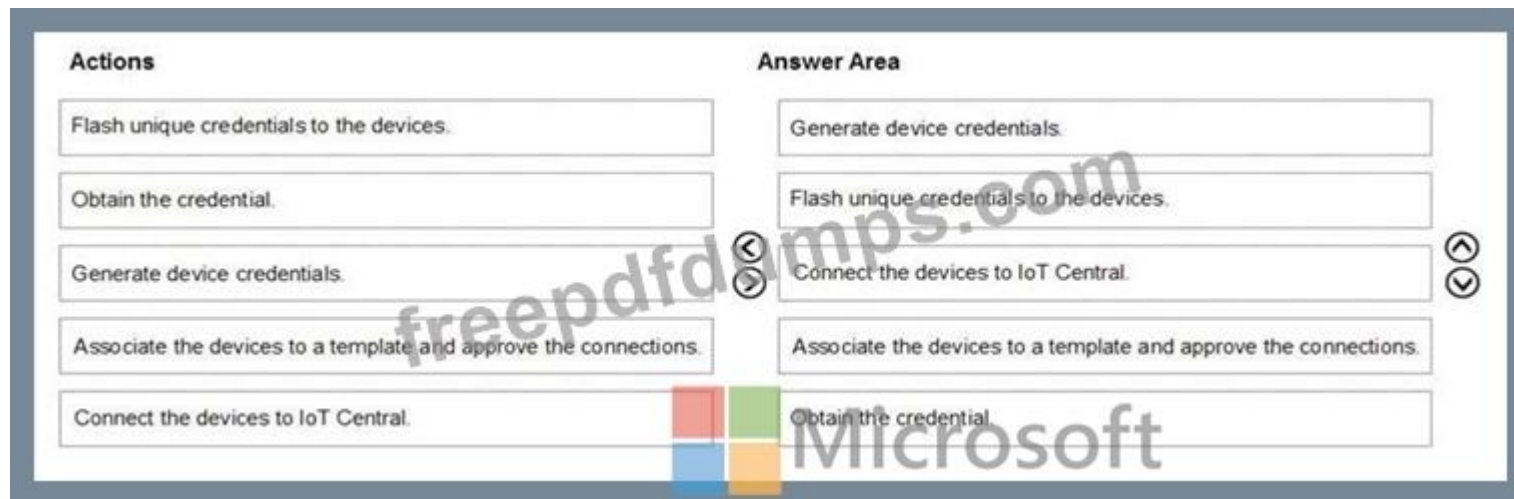
Flash unique credentials to the devices.

Connect the devices to IoT Central.

Associate the devices to a template and approve the connections.

Obtain the credential.

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.

e:

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

NEW QUESTION: 38

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.

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:

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

Explanation:

Box 1: tags.engine.warpDriveType='WM105a'

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>

NEW QUESTION: 39

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: D (LEAVE A REPLY)

Explanation

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: 40

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: 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: 41

You have an Azure subscription that contains an Azure IoT hub and two Azure IoT Edge devices named Device1 and Device2.

You need to ensure that the IoT hub only accepts connections from Device1 and Device2.

What should you configure?

A. a private endpoint connection

B. Azure API Management

C. Azure Active Directory (Azure AD) Identity Protection

D. a gateway device

Answer: (SHOW ANSWER)

Ingress connectivity to IoT Hub using Azure Private Link.

A private endpoint is a private IP address allocated inside a customer-owned VNet via which an Azure resource is reachable. Through Azure Private Link, you can set up a private endpoint for your IoT hub to allow services inside your VNet to reach IoT Hub without requiring traffic to be sent to IoT Hub's public endpoint. Similarly, your on-premises devices can use Virtual Private Network (VPN) or ExpressRoute peering to gain connectivity to your VNet and your IoT Hub (via its private endpoint). As a result, you can restrict or completely block off connectivity to

your IoT hub's public endpoints by using IoT Hub IP filter or the public network access toggle. This approach keeps connectivity to your Hub using the private endpoint for devices.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/virtual-network-support>

NEW QUESTION: 42

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: 43

You have an instance of Azure Time Series Insights and an Azure IoT hub that receives streaming telemetry from IoT devices.

You need to configure Time Series Insights to receive telemetry from 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
Configure the Time Series Insights event source to connect to an existing IOT hub.	
Create an Azure event hub.	
Add a new Time Series Insights event source.	
Increase the events retention to seven days for the built-in endpoints of the IoT hub.	
Create a dedicated consumer group in the built-in events endpoints of the IoT hub.	

Microsoft

Answer:

Actions

- Configure the Time Series Insights event source to connect to an existing IOT hub.
- Create an Azure event hub.
- Add a new Time Series Insights event source.
- Increase the events retention to seven days for the built-in endpoints of the IoT hub.
- Create a dedicated consumer group in the built-in events endpoints of the IoT hub.

Answer Area

- Increase the events retention to seven days for the built-in endpoints of the IoT hub.
- Add a new Time Series Insights event source.
- Configure the Time Series Insights event source to connect to an existing IOT hub.

Microsoft

Explanation:

Step 1: Create a dedicated consumer group..

Add a consumer group to your IoT hub.

Applications use consumer groups to pull data from Azure IoT Hub. To reliably read data from your IoT hub, provide a dedicated consumer group that's used only by this Time Series Insights environment.

Step 2: Add a new Time Series Insights event source.

Add a new event source

Sign in to the Azure portal.

In the left menu, select All resources. Select your Time Series Insights environment.

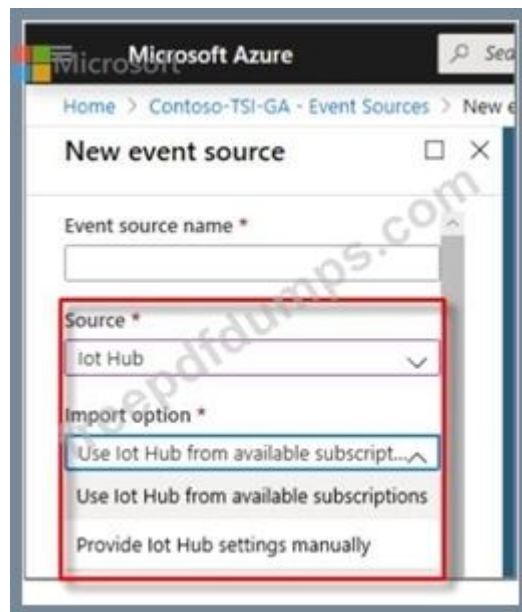
Under Settings, select Event Sources, and then select Add.

In the New event source pane, for Event source name, enter a name that's unique to this Time Series Insights environment. For example, enter event-stream.

Step 3: Configure the Time Series event source to connect to an existing IOT hub Step 4: For Source, select IoT Hub.

Step 5: Select a value for Import option:

If you already have an IoT hub in one of your subscriptions, select Use IoT Hub from available subscriptions. This option is the easiest approach.



Reference:

<https://docs.microsoft.com/en-us/azure/time-series-insights/time-series-insights-how-to-add-an-event-source-iotHub>

NEW QUESTION: 44

From the Device Provisioning Service, you create an enrollment as shown in the exhibit.

 **enrollment1**
Enrollment Group Details

 Save  Refresh  Regenerate keys

Settings Registration Records

 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.

Attestation Type
Symmetric Key

Primary Key
*****  

Secondary Key
*****  

IoT Edge device 

☐ True ☒ False

Select how you want to assign devices to hubs
Evenly weighted distribution 

Select the IoT hubs this group can be assigned to: 

iothub-contoso.azure-devices.net 

[Link a new IoT hub](#)

Select how you want device data to be handled on re-provisioning *   Microsoft

Re-provision and migrate data 

Enable entry 

☒ Enable ☐ Disable

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 HMAC-SHA256 hash of the device's registration ID
- D. the endorsement key of the device's Trusted Platform Module (TPM)

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

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: 45

You have an Azure IoT solution that includes an Azure IoT hub and 100 Azure IoT Edge devices.

You plan to deploy the IoT Edge devices to external networks. The firewalls of the external networks only allow traffic on port 80 and port 443.

You need to ensure that the devices can connect to the IoT hub. The solution must minimize costs.

What should you do?

- A.** Configure the upstream protocol of the devices to use MQTT over TCP.
- B.** Configure the upstream protocol of the devices to use AMQP over WebSocket.
- C.** Connect the external networks to the IoT solution by using ExpressRoute.
- D.** Integrate cellular communication hardware onto the devices and avoid the use of the external networks.

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

Explanation

AMQP over WebSockets uses port 443.

Reference:

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

NEW QUESTION: 46

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 Actual4test.com for Helping Passing AZ-220 Exam! Actual4test.com now offer the **newest AZ-220 exam dumps**, the Actual4test.com AZ-220 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-220 dumps with Test Engine here: https://www.actual4test.com/AZ-220_examcollection.html (205 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 47

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:



Explanation:

Box 1: AMQP

Use AMQP on field and cloud gateways to take advantage of connection multiplexing across devices.

Box 2: MQTT

MQTT is used on all devices that do not require to connect multiple devices (each with its own per-device credentials) over the same TLS connection.

Box 3: HTTPS

Use HTTPS for devices that cannot support other protocols.

Reference:

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

NEW QUESTION: 48

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: ([SHOW ANSWER](#))

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: 49

You are developing an Azure IoT solution for a shipping company. The company's ships will have sensors used for predictive maintenance. Some sensor devices will be MQTT-capable, and others will use Modbus.

Each ship has an internet connection that is available only when the ship is docked.

You create an Azure IoT hub.

You need to implement an IoT solution that uses Azure IoT Edge.

What should you do?

A. Configure an IoT Edge gateway. Deploy an IoT Edge Modbus module. From the Azure portal, create IoT devices and add connection strings to the devices.

B. Add the MQTT devices to the IoT hub and configure an IoT Edge gateway. From the IoT Edge gateway device, assign the MQTT devices as child devices of the gateway. Use the File upload feature of IoT Hub when internet connectivity is available.

C. Add the MQTT devices to the IoT hub. configure an IoT Edge gateway, and set Enable connection to IoT Hub to Disable. From the IoT Edge gateway device, assign the MQTT devices as child devices of the gateway. Deploy the IoT Edge Modbus module.

D. Add the MQTT devices to the IoT hub and configure an IoT Edge gateway. From the IoT Edge gateway device, assign the MQTT devices as child devices of the gateway. Deploy an IoT Edge Modbus module.

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

Explanation

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

NEW QUESTION: 50

You plan to deploy a standard tier Azure IoT hub.

You need to perform an over-the-air (OTA) update on devices that will connect to the IoT hub by using scheduled jobs.

What should you use?

A. a device-to-cloud message

B. the device twin reported properties

C. a cloud-to-device message

D. a direct method

Answer: (SHOW ANSWER)

Explanation

Releases via the REST API.

All of the operations that can be performed from the Console can also be automated using the REST API. You might do this to automate your build and release process, for example.

You can build firmware using the Particle CLI or directly using the compile source code API.

Note: Over-the-air (OTA) firmware updates are a vital component of any IoT system. Over-the-air firmware updates refers to the practice of remotely updating the code on an embedded device.

Reference:

<https://docs.particle.io/tutorials/device-cloud/ota-updates/>

NEW QUESTION: 51

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

You have 1,000 legacy IoT devices that only support MAC address or serial number identities. The device do NOT have a security feature that can be used to securely identify the device or a hardware security module (HSM).

You plan to deploy the devices to a secure environment.

You need to configure the Device Provisioning Service instance to ensure that all the devices are identified securely before they receive updates.

Which attestation mechanism should you choose?

A. Trusted Platform Module (TPM) 1.2 attestation

B. symmetric key attestation

C. X.509 certificates

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

Explanation

A common problem with many legacy devices is that they often have an identity that is composed of a single piece of information. This identity information is usually a MAC address or a serial number. Legacy devices may not have a certificate, TPM, or any other security feature that can be used to securely identify the device.

The Device Provisioning Service for IoT hub includes symmetric key attestation. Symmetric key attestation can be used to identify a device based off information like the MAC address or a serial number.

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/iot-dps/how-to-legacy-device-symm-key>

NEW QUESTION: 52

You are writing code to provision IoT devices by using the Device Provisioning Service.

Which two details from the Overview blade of the Device Provisioning Service are required to provision a new IoT client device? To answer, select the appropriate detail in the answer area.

NOTE: Each correct selection is worth one point.

All services > Device Provisioning Services > contosodps

contosodps
Device Provisioning Service

Search (Ctrl+/) « → Move □ Delete ↻ Refresh

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Quick Start
- Shared access policies

Resource group (change) contosoorg	Service endpoint contosodps.azure-devices-provisioning.net
Status Active	Global device endpoint global.azure-devices-provisioning.net
Location East US	ID Scope 0ne00098F73
Subscription (change) Free Trial	Pricing and scale tier S1
Subscription ID fea9f87-1546-43c4-a4d0-3d04db60a598	
Tags (change) Click here to add tags	

Answer:

All services > Device Provisioning Services > contosodps

contosodps
Device Provisioning Service

Search (Ctrl+/) « → Move □ Delete ↻ Refresh

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Quick Start
- Shared access policies

Resource group (change) contosoorg	Service endpoint contosodps.azure-devices-provisioning.net
Status Active	Global device endpoint global.azure-devices-provisioning.net
Location East US	ID Scope 0ne00098F73
Subscription (change) Free Trial	Pricing and scale tier S1
Subscription ID fea9f87-1546-43c4-a4d0-3d04db60a598	
Tags (change) Click here to add tags	

Explanation



Box 1: ID Scope

In the Azure portal, select the Overview blade for your Device Provisioning service and copy the ID Scope value. The ID Scope is generated by the service and guarantees uniqueness. It is immutable and used to uniquely identify the registration IDs.

Box 2: Global device endpoint

The `global_prov_uri` variable, which allows the IoT Hub client registration API `IoTHubClient_LL_CreateFromDeviceAuth` to connect with the designated Device Provisioning Service instance.

Example code:

```
static const char* global_prov_uri = "global.azure-devices-provisioning.net"; static const char* id_scope = "[ID Scope]"; Reference:  
https://docs.microsoft.com/en-us/azure/iot-dps/tutorial-set-up-device
```

NEW QUESTION: 53

You enable Azure Security Center for IoT.

You need to onboard a device to Azure Security Center.

What should you do?

- A. Add the azureiotsecurity module identity to the Azure IoT Hub device identity.
- B. Open incoming TCP port 8883 on the device.
- C. Modify the connection string of the device.
- D. Install an X.509 certificate on the hardware security module (HSM) of the device.

Answer: (SHOW ANSWER)

Use the following workflow to deploy and test your Azure Security Center for IoT security agents:

1. Enable Azure Security Center for IoT service to your IoT Hub
2. If your IoT Hub has no registered devices, Register a new device.
3. Create an azureiotsecurity security module for your devices.

Azure Security Center for IoT makes use of the module twin mechanism and maintains a security module twin named `azureiotsecurity` for each of your devices.

Note: To manually create a new `azureiotsecurity` module twin for a device use the following instructions:

1. In your IoT Hub, locate and select the device you wish to create a security module twin for.
2. Click on your device, and then on Add module identity.
3. In the Module Identity Name field, enter azureiotsecurity.
4. Click Save.

Reference:

<https://docs.microsoft.com/en-us/azure/asc-for-iot/quickstart-create-security-twin>

NEW QUESTION: 54

You enable Azure Security Center for IoT.

You need to onboard a device to Azure Security Center. What should you do?

- A.** Add the azureiotsecurity module identity to the Azure IoT Hub device identity.
- B.** Open incoming TCP port 8883 on the device.
- C.** Modify the connection string of the device.
- D.** Install an X.509 certificate on the hardware security module (HSM) of the device.

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

Use the following workflow to deploy and test your Azure Security Center for IoT security agents:

1. Enable Azure Security Center for IoT service to your IoT Hub
2. If your IoT Hub has no registered devices, Register a new device.
3. Create an azureiotsecurity security module for your devices.

Azure Security Center for IoT makes use of the module twin mechanism and maintains a security module twin named azureiotsecurity for each of your devices.

Note: To manually create a new azureiotsecurity module twin for a device use the following instructions:

1. In your IoT Hub, locate and select the device you wish to create a security module twin for.
2. Click on your device, and then on Add module identity.
3. In the Module Identity Name field, enter azureiotsecurity.
4. Click Save.

Reference:

<https://docs.microsoft.com/en-us/azure/asc-for-iot/quickstart-create-security-twin>

NEW QUESTION: 55

You have an IoT device that gathers data in a CSV file named Sensors.csv.

You deploy an Azure IoT hub that is accessible at ContosoHub.azure-devices.net.

You need to ensure that Sensors.csv is uploaded to the IoT hub.

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

NOTE: Each correct selection is worth one point.

- A.** Upload Sensors.csv by using the IoT Hub REST API.
- B.** From the Azure subscription, select the IoT hub, select Message routing, and then configure a route to storage.
- C.** From the Azure subscription, select the IoT hub, select File upload, and then configure a storage container.
- D.** Configure the device to use a GETrequest to ContosoHub.azure-devices.net/devices/ContosoDevice1/files/ notifications.

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

C: To use the file upload functionality in IoT Hub, you must first associate an Azure Storage account with your hub. Select File upload to display a list of file upload properties for the IoT hub that is being modified.

For Storage container: Use the Azure portal to select a blob container in an Azure Storage account in your current Azure subscription to associate with your IoT Hub. If necessary, you can create an Azure Storage account on the Storage accounts blade and blob container on the Containers A: IoT Hub has an endpoint specifically for devices to request a SAS URI for storage to upload a file. To start the file upload process, the device sends a POST request to {iot hub}.azure-devices.net/devices/{deviceId}/files with the following JSON body:

```
{  
  "blobName": "{name of the file for which a SAS URI will be generated}"  
}
```

Incorrect Answers:

D: Deprecated: initialize a file upload with a GET. Use the POST method instead.

Reference:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/iot-hub/iot-hub-configure-file-upload.md>

NEW QUESTION: 56

You have an Azure IoT solution that includes an Azure IoT Hub named Hub1 and an Azure IoT Edge device named Edge1. Edge1 connects to Hub1.

You need to deploy a temperature module to Edge1.

What should you do?

A. From the Azure portal, navigate to Hub1 and select IoT Edge. Select Edge1, and then select Manage Child Devices. From a Bash prompt, run the following command:

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

B. Create an IoT Edge deployment manifest that specifies the temperature module and the route to \$upstream. From a Bash prompt, run the following command:

```
az iot hub monitor-events-device-id Edge1 -hub-name Hub1
```

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

D. Create an IoT Edge deployment manifest that specifies the temperature module and the route to \$upstream. From a Bash prompt, run the following command:

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

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:

```
az iot edge set-modules --device-id [device id] --hub-name [hub name] --content [file path] Reference:
```

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

```

{
  "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
}
}

```



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
lothub
```

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: 57

How should you complete the GROUP BY clause to meet the Streaming Analytics requirements?

- A.** GROUP BY HoppingWindow(Second, 60, 30)
- B.** GROUP BY TumblingWindow(Second, 30)
- C.** GROUP BY SlidingWindow(Second, 30)
- D.** GROUP BY SessionWindow(Second, 30, 60)

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

Scenario: You plan to use a 30-second period to calculate the average temperature reading of the sensors.

Tumbling window functions are used to segment a data stream into distinct time segments and perform a function against them, such as the example below. The key differentiators of a Tumbling window are that they repeat, do not overlap, and an event cannot belong to more than one tumbling window.

InAnswers:

A: Hopping window functions hop forward in time by a fixed period. It may be easy to think of them as Tumbling windows that can overlap, so events can belong to more than one Hopping window result set.

Reference:

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

Topic 1, Contoso

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.

```

{
  "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
  }
}

```



freepaidumps.com

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
lothub
```

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. 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: 58

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

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

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

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

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

Does this meet the goal?

A. Yes

B. No

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

Explanation

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

Instead use a translation gateway.

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

Reference:

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

NEW QUESTION: 59

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)

Explanation

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

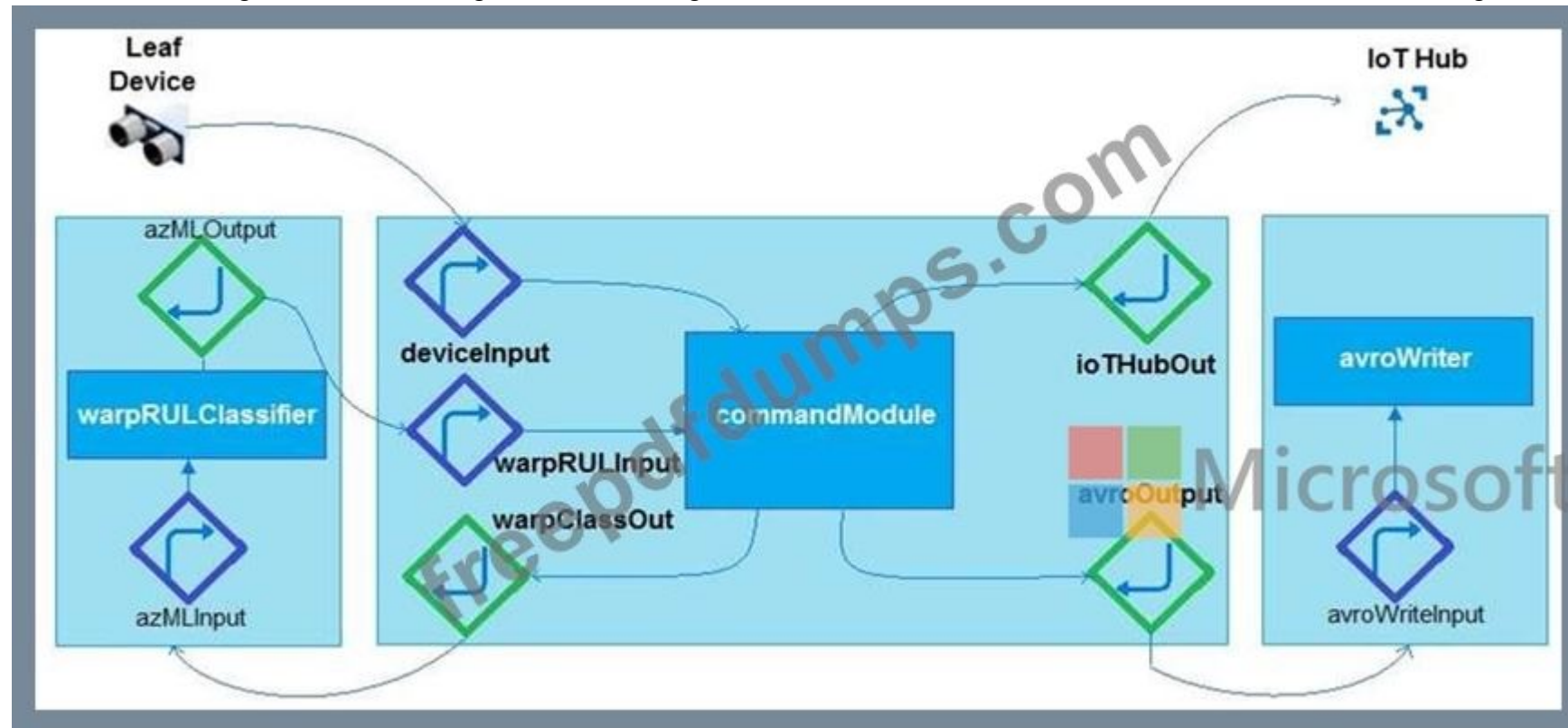
* Update tags

Reference:

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

NEW QUESTION: 60

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
\$connectionModuleed
Supstream



commandModule
\$connectionModuleed
Supstream

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
  }
}
```

commandModule
\$connectionModule
Supstream

commandModule
\$connectionModule
Supstream



Reference:

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

NEW QUESTION: 61

You need to enable telemetry message tracing through the entire IoT solution.

What should you do?

- A. Monitor device lifecycle events.
- B. Upload IoT device logs by using the File upload feature.
- C. Enable the DeviceTelemetry diagnostic log and stream the log data to an Azure event hub.
- D. Implement distributed tracing.

Answer: (SHOW ANSWER)

IoT Hub is one of the first Azure services to support distributed tracing. As more Azure services support distributed tracing, you'll be able to trace IoT messages throughout the Azure services involved in your solution.

Note:

Enabling distributed tracing for IoT Hub gives you the ability to:

- * Precisely monitor the flow of each message through IoT Hub using trace context. This trace context includes correlation IDs that allow you to correlate events from one component with events from another component. It can be applied for a subset or all IoT device messages using device twin.
- * Automatically log the trace context to Azure Monitor diagnostic logs.
- * Measure and understand message flow and latency from devices to IoT Hub and routing endpoints.

Start considering how you want to implement distributed tracing for the non-Azure services in your IoT solution.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-distributed-tracing> Monitor, troubleshoot, and optimize IoT solutions Question Set 2

Valid AZ-220 Dumps shared by Actual4test.com for Helping Passing AZ-220 Exam! Actual4test.com now offer the **newest AZ-220 exam dumps**, the Actual4test.com AZ-220 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-220 dumps with Test Engine here: https://www.actual4test.com/AZ-220_examcollection.html (205 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 62

You have an Azure IoT hub and 15,000 IoT devices that monitor temperature. The IoT hub has four partitions. Each IoT device sends a 1-KB message every five seconds.

You plan to use Azure Stream Analytics to process the telemetry stream and generate an alert when temperatures exceed a defined threshold.

You need to recommend the minimum number of streaming units to configure for Stream Analytics.

What should you recommend?

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

Answer: D (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 63

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.

"desired": {

"reported": {

"highPriorityMessageFrequency": {

"lowPriorityMessageFrequency": {

"eventPriorityConnectionCreate": {

"eventPriorityProcessCreate": {

"aggregationIntervalConnectionCreate": {

Answer Area

Microsoft

"ms_iotn:urn_azureiot_Security_SecurityAgentConfiguration": {

"value": "PT7M"

"value": "High"

}

}

}

Answer:

"desired": {

"reported": {

"highPriorityMessageFrequency": {

"lowPriorityMessageFrequency": {

"eventPriorityConnectionCreate": {

"eventPriorityProcessCreate": {

"aggregationIntervalConnectionCreate": {

Answer Area

Microsoft

"desired": {

"ms_iotn:urn_azureiot_Security_SecurityAgentConfiguration": {

"highPriorityMessageFrequency": {

"value": "PT7M"

"eventPriorityConnectionCreate": {

"value": "High"

}

}

}

Explanation


```

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

```

NEW QUESTION: 64

You have an Azure IoT Edge module named SampleModule that runs on a device named Device1.

You make changes to the code of SampleModule by using Microsoft Visual Studio Code.

You need to push the code to the container registry and then deploy the module to Device1.

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

NOTE: Each correct selection is worth one point.

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

Answer: B,C (LEAVE A REPLY)

C: Configure a deployment manifest. A deployment manifest is a JSON document that describes which modules to deploy, how data flows between the modules, and desired properties of the module twins.

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

Reference:

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

NEW QUESTION: 65

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)

Explanation

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: 66

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

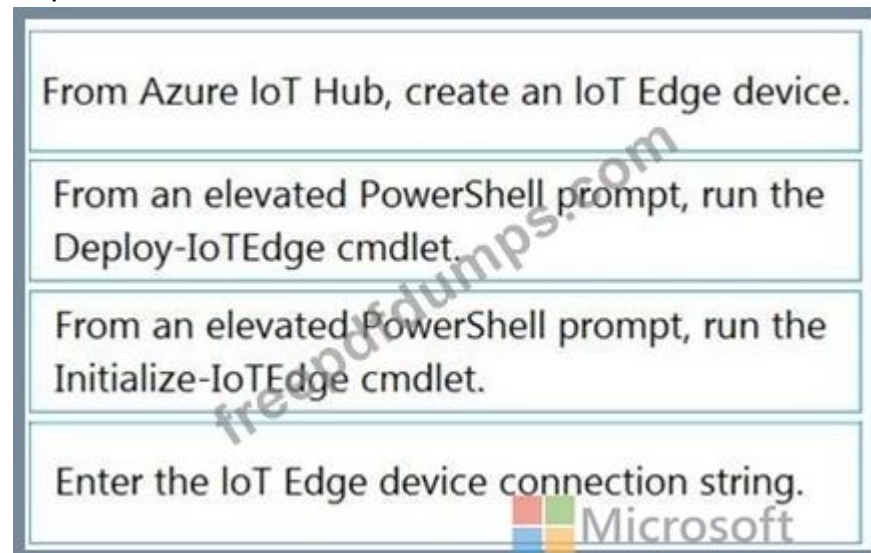
Answer:
Actions

- 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



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: 67

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](#))

Explanation

Create an endpoint for Azure Digital Twins.

These are the supported types of endpoints that you can create for your instance:

- * Event Grid
- * Event Hubs
- * Service Bus

Note: In Azure Digital Twins, you can route event notifications to downstream services or connected compute resources. This is done by first setting up endpoints that can receive the events. You can then create event routes that specify which events generated by Azure Digital Twins are delivered to which endpoints.

Reference:

<https://docs.microsoft.com/en-us/azure/digital-twins/how-to-manage-routes>

NEW QUESTION: 68

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: 69

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:

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

Answer:

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

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

Explanation:

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

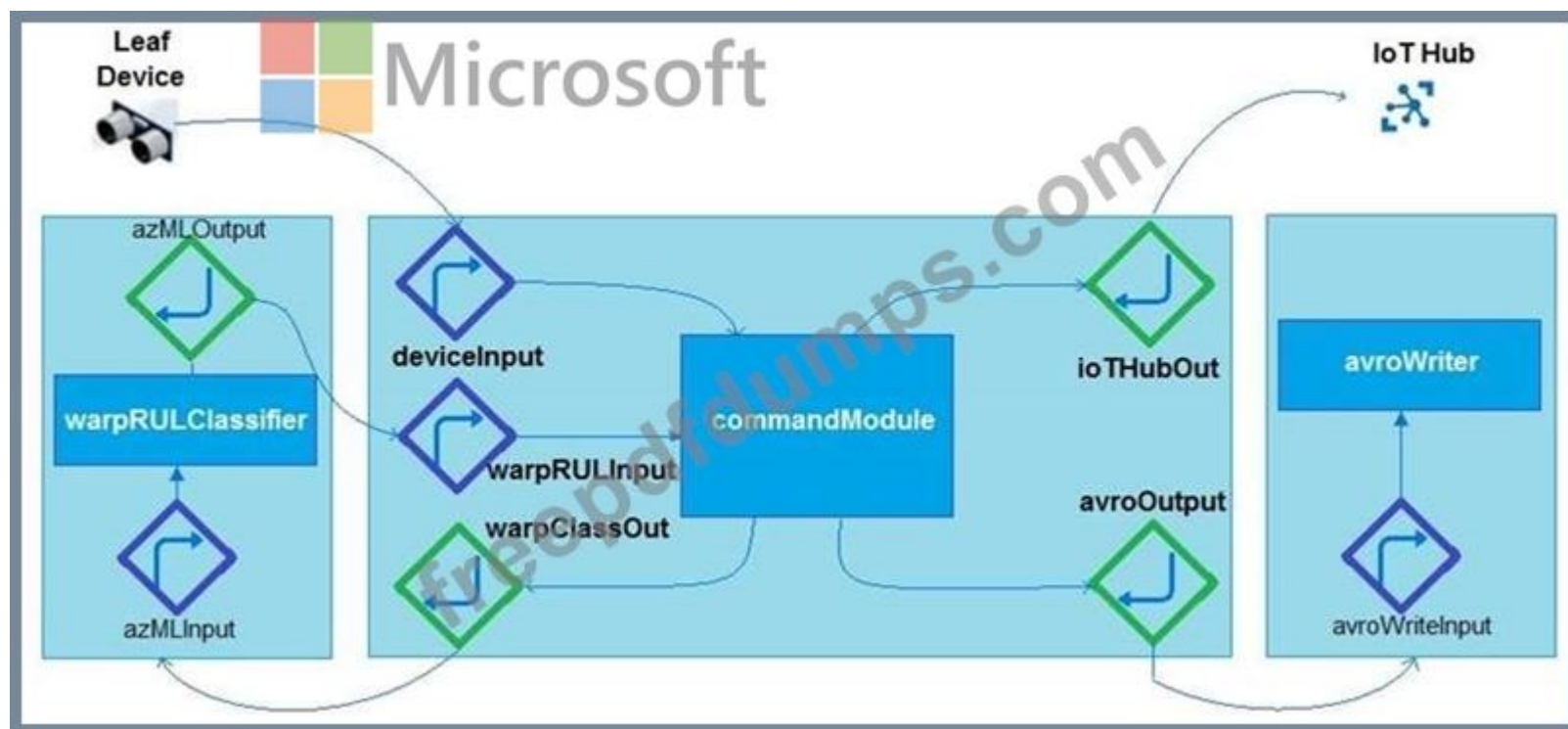
Cert1: A root certificate is a self-signed X.509 certificate representing a certificate authority (CA). It is the terminus, or trust anchor, of the certificate chain. Root certificates can be self-issued by an organization or purchased from a root certificate authority.

Reference:

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

NEW QUESTION: 70

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
Supstream

commandModule
\$connectionModule
Supstream

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
  }
}
```

▼

commandModule
\$connectionModuleed
Supstream

Microsoft

commandModule
\$connectionModuleed
Supstream

Explanation
Text, letter Description automatically generated

```
"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
```

commandModule

\$connectionModuled

Supstream

commandModule

\$connectionModuled

Supstream

Box 1: \$connectionModuled

Add a route that tells the edge hub to route any message received by the IoT Edge device that was not sent by an IoT Edge module.

Box 2: \$upstream

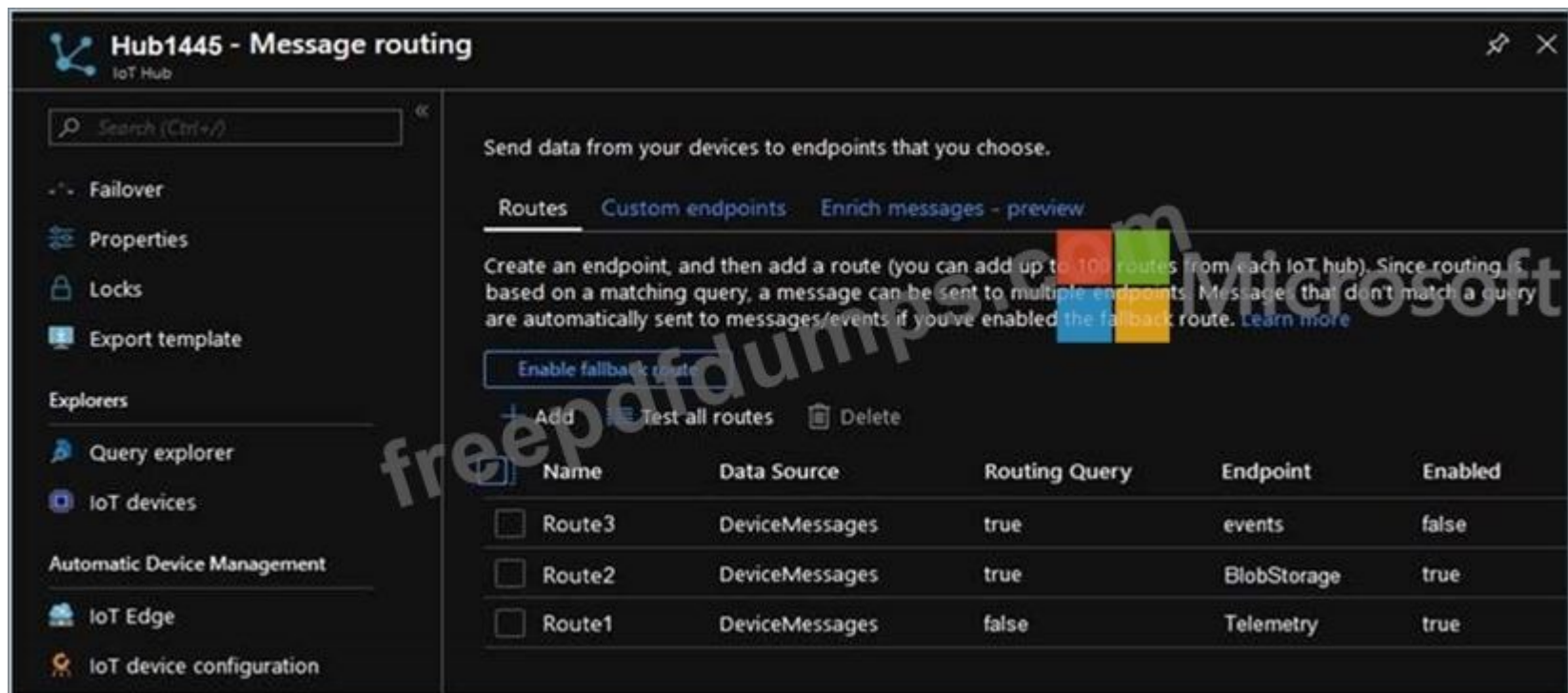
Send messages to \$upstream, which passes the messages to the connected IoT Hub.

Reference:

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

NEW QUESTION: 71

You have an Azure Stream Analytics job that connects to an Azure IoT hub named Hub1445 as a streamingdata 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: (SHOW ANSWER)

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: 72

You have an Azure IoT hub.

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

What should you do?

- A. From the Security settings of the IoT hub, select Secure your IoT solution.
- B. From the Diagnostics settings of the IoT hub, select Add diagnostic setting.
- C. From Defender, add a security policy.
- D. From Defender, configure security alerts.

Answer: (SHOW ANSWER)

Reference:

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

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 question, 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 use an Azure policy to apply tags to a resource group. Does the solution meet the goal?

A. Yes

B. No

Answer: ([SHOW ANSWER](#))

Explanation

Instead add the desired properties to the device twin.

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

NEW QUESTION: 74

You have an Azure IoT solution that includes an Azure IoT Hub named Hub1 and an Azure IoT Edge device named Edge1. Edge1 connects to Hub1.

You need to deploy a temperature module to Edge1. What should you do?

A. From the Azure portal, navigate to Hub1 and select IoT Edge. Select Edge1, and then select Manage Child Devices. From a Bash prompt, run the following command:

`az iot edge set-modules -device-id Edge1 -hub-name Hub1 -content C:`

`\deploymentMan1.json`

B. Create an IoT Edge deployment manifest that specifies the temperature module and the route to \$upstream. From a Bash prompt, run the following command:

`az iot hub monitor-events-device-id Edge1 -hub-name Hub1`

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

D. Create an IoT Edge deployment manifest that specifies the temperature module and the route to \$upstream. From a Bash prompt, run the following command:

`az iot edge set-modules -device-id Edge1 -hub-name Hub1 -content C:`

`\deploymentMan1.json`

Answer: ([SHOW ANSWER](#))

Explanation

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

Change directories into the folder where your deployment manifest is saved. If you used one of the VS Code IoT Edge templates, use the deployment.json file in the config folder of your solution directory and not the deployment.template.json file.

Use the following command to apply the configuration to an IoT Edge device:

`az iot edge set-modules --device-id [device id] --hub-name [hub name] --content [file path]` Reference:

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

NEW QUESTION: 75

You have an Azure IoT solution that includes an Azure IoT Hub named Hub1 and an Azure IoT Edge device named Edge1. Edge1 connects to Hub1.

You need to deploy a temperature module to Edge1. What should you do?

A. From the Azure portal, navigate to Hub1 and select IoT Edge. Select Edge1, and then select Manage Child Devices. From a Bash prompt, run the following command:

`az iot edge set-modules -device-id Edge1 -hub-name Hub1 -content C:`

`\deploymentMan1.json`

B. Create an IoT Edge deployment manifest that specifies the temperature module and the route to \$upstream. From a Bash prompt, run the following command:

`az iot hub monitor-events-device-id Edge1 -hub-name Hub1`

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

D. Create an IoT Edge deployment manifest that specifies the temperature module and the route to \$upstream.

From a Bash prompt, run the following command:

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

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:

`az iot edge set-modules --device-id [device id] --hub-name [hub name] --content [file path]`

Reference:

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

NEW QUESTION: 76

You deploy an Azure IoT hub.

You need to demonstrate that the IoT hub can receive messages from a 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

- Get a service primary key for the IoT hub.
- Configure the Device Provisioning Service on the IoT hub.
- Configure the device connection string on a device client.
- Register a device in IoT Hub.
- Trigger a new send event from a device client.

Answer Area

Answer:

Actions

- Get a service primary key for the IoT hub.
- Configure the Device Provisioning Service on the IoT hub.
- Configure the device connection string on a device client.
- Register a device in IoT Hub.
- Trigger a new send event from a device client.

Answer Area

- Register a device in IoT Hub.
- Configure the device connection string on a device client.
- Trigger a new send event from a device client.

Explanation:

Step 1: Register a device in IoT Hub

Before you can use your IoT devices with Azure IoT Edge, you must register them with your IoT hub. Once a device is registered, you can retrieve a connection string to set up your device for IoT Edge workloads.

Step 2: Configure the device connection string on a device client.

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.

Step 3: Trigger a new send event from a device client.

Reference:

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

Valid AZ-220 Dumps shared by Actual4test.com for Helping Passing AZ-220 Exam! Actual4test.com now offer the **newest AZ-220 exam dumps**, the Actual4test.com AZ-220 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-220 dumps with Test Engine here: https://www.actual4test.com/AZ-220_examcollection.html (205 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 77

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: ([SHOW ANSWER](#))

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: 78

You have an Azure IoT solution that includes an Azure IoT hub.

You receive a root certification authority (CA) certificate from the security department at your company.

You need to configure the IoT hub to use the root CA certificate.

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
Generate a verification code.	 
Upload the verification certificate.	
Upload the root CA certificate to the IoT hub.	
Copy the thumbprint from root CA certificate.	
Generate a verification certificate.	

Answer:

Answer Area
Upload the root CA certificate to the IoT hub.
Generate a verification code.
Generate a verification certificate.
Upload the verification certificate.

- 1 - Upload the root CA certificate to the IoT hub.
- 2 - Generate a verification code.
- 3 - Generate a verification certificate.
- 4 - Upload the verification certificate.

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/iot-hub/iot-hub-security-x509-get-started>

NEW QUESTION: 79

What should you do to identify the cause of the connectivity issues?

- A. Send cloud-to-device messages to the IoT devices.
- B. Use the heartbeat pattern to send messages from the IoT devices to iothub1.
- C. Monitor the connection status of the device twin by using an Azure function.
- D. Enable the collection of the Connections diagnostics logs and set up alerts for the connected devices count metric.

Answer: D (LEAVE A REPLY)

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

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.

Step 1:

1. Sign in to the Azure portal.
2. Browse to your IoT hub.

3. Select Diagnostics settings.
4. Select Turn on diagnostics.
5. Enable Connections logs to be collected.
6. For easier analysis, turn on Send to Log Analytics (see pricing).

Step 2:

Set up alerts for device disconnect at scale

To get alerts when devices disconnect, configure alerts on the Connected devices (preview) metric.

Reference:

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

NEW QUESTION: 80

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

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

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

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

Solution: You configure the sensors to connect directly to the IoT hub.

Does this meet the goal?

A. Yes

B. No

Answer: B (LEAVE A REPLY)

Instead use a translation gateway.

Note: In the protocol translation gateway pattern, only the IoT Edge gateway has an identity with IoT Hub. The translation module receives messages from downstream devices, translates them into a supported protocol, and then the IoT Edge device sends the messages on behalf of the downstream devices. All information looks like it is coming from one device, the gateway.

Reference:

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

NEW QUESTION: 81

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.

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: 82

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

You are performing a scheduled check of deployed IoT devices.

You plan to run the following command from the Azure CLI prompt.

az iot hub query --hub-name hub1 --query-command "SELECT * FROM devices WHERE connectionState = 'Disconnected'" What does the command return?

- A. the Device Disconnected events
- B. the device twins
- C. the Connections logs
- D. the device credentials

Answer: B (LEAVE A REPLY)

Device twin queries: IoT Hub exposes the device twins as a document collection called devices. For example, the following query retrieves the whole set of device twins:

```
SELECT * FROM devices
```

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-query-language#device-and-module-twin-queries>

NEW QUESTION: 83

How should you complete the GROUP BY clause to meet the Streaming Analytics requirements?

- A. GROUP BY HoppingWindow(Second, 60, 30)
- B. GROUP BY TumblingWindow(Second, 30)
- C. GROUP BY SlidingWindow(Second, 30)
- D. GROUP BY SessionWindow(Second, 30, 60)

Answer: (SHOW ANSWER)

Explanation

Scenario: You plan to use a 30-second period to calculate the average temperature reading of the sensors.

Tumbling window functions are used to segment a data stream into distinct time segments and perform a function against them, such as the example below. The key differentiators of a Tumbling window are that they repeat, do not overlap, and an event cannot belong to more than one tumbling window.

InAnswers:

A: Hopping window functions hop forward in time by a fixed period. It may be easy to think of them as Tumbling windows that can overlap, so events can belong to more than one Hopping window result set.

Reference:

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

NEW QUESTION: 84

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

You have 1,000 legacy IoT devices that only support MAC address or serial number identities. The devices do NOT have a security feature that can be used to securely identify the device or a hardware security module (HSM).

You plan to deploy the devices to a secure environment.

You need to configure the Device Provisioning Service instance to ensure that all the devices are identified securely before they receive updates.

Which attestation mechanism should you choose?

A. Trusted Platform Module (TPM) 1.2 attestation

B. symmetric key attestation

C. X.509 certificates

Answer: B (LEAVE A REPLY)

A common problem with many legacy devices is that they often have an identity that is composed of a single piece of information. This identity information is usually a MAC address or a serial number. Legacy devices may not have a certificate, TPM, or any other security feature that can be used to securely identify the device.

The Device Provisioning Service for IoT hub includes symmetric key attestation. Symmetric key attestation can be used to identify a device based off information like the MAC address or a serial number.

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/iot-dps/how-to-legacy-device-symm-key>

NEW QUESTION: 85

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:

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

	▼
Cert1 only	
Cert2 only	
Both Cert1 and Cert2	
Neither 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:

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

	▼
Cert1 only	
Cert2 only	
Both Cert1 and Cert2	
Neither 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: 86

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/dev:2.0

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

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

Answer: (SHOW ANSWER)

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>

NEW QUESTION: 87

You are developing an Azure IoT Central application.

You add a new custom device template to the application.

You need to add a fixed location value to the device template. The value must be updated by the physical IoT device, read-only to device operators, and not graphed by IoT Central.

What should you add to the device template?

A. a Location property

B. a Location telemetry

C. a Cloud property

Answer: A (LEAVE A REPLY)

Explanation

For example, a builder can create a device template for a connected fan that has the following characteristics:

- * Sends temperature telemetry

- * Sends location property

Reference:

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

NEW QUESTION: 88

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 and DeviceId dropdowns:

- azure-devices.net
- criticalep
- device1
- iothub1
- tracestate

Answer:

HostName= azure-devices.net criticalep device1 iothub1 tracestate ; DeviceId= azure-devices.net criticalep device1 iothub1 tracestate : SharedAccessKey=Uihuih76hbHb

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={YourIoT HubName}.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: 89

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.	☐	☐
The device twin will set fanSpeed for the physical IoT device to 73.	☐	☐
You can change the device identity of the physical IoT device by modifying the deviceId property.	☐	☐

Answer:

Statements	Yes	No
You can add a property that contains multiple nested values to the device twin.	☒	☐
The device twin will set fanSpeed for the physical IoT device to 73.	☒	☐
You can change the device identity of the physical IoT device by modifying the deviceId property.	☐	☒

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: 90

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.

Actions



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.

Answer Area

←

→

↑

↓

Answer:

Answer Area

Provision Time Series Insights

Route telemetry from IoT Hub to a custom event.

1 - Provision Time Series Insights

2 - Route telemetry from IoT Hub to a custom event.

Reference:

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

NEW QUESTION: 91

You have an Azure IoT solution that includes several Azure IoT hubs.

A new alerting feature was recently added to the IoT devices. The feature uses a new device twin reported property named alertCondition.

You need to send alerts to an Azure Service Bus queue named MessageAlerts. The alerts must include alertCondition and the name of the IoT hub.

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

NOTE: Each correct selection is worth one point.

A. Configure File upload for each IoT hub. Configure the device to send a file to an Azure Storage container that contains the device name and status message.

B. Add the following message enrichments:

Name = iotHubName

Value = \$twin.tag.location

Endpoint = MessageAlert

C. Create an IoT Hub routing rule that has a data source of Device Twin Change Events and select the endpoint for MessageAlerts.

D. Add the following message enrichments:

Name = iotHubName Value = \$iothubname

Endpoint = MessageAlert

E. Create an IoT Hub routing rule that has a data source of Device Telemetry Messages and select the endpoint for MessageAlerts.

Answer: B,D (LEAVE A REPLY)

Explanation

B: Message enrichments is the ability of the IoT Hub to stamp messages with additional information before the messages are sent to the designated endpoint. One reason to use message enrichments is to include data that can be used to simplify downstream processing. For example, enriching device telemetry messages with a device twin tag can reduce load on customers to make device twin API calls for this information.

D: Applying enrichments

The messages can come from any data source supported by IoT Hub message routing, including the following examples:

-->device twin change notifications -- changes in the device twin device telemetry, such as temperature or pressure device life-cycle events, such as when the device is created or deleted Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-message-enrichments-overview>

Valid AZ-220 Dumps shared by Actual4test.com for Helping Passing AZ-220 Exam! Actual4test.com now offer the **newest AZ-220 exam dumps**, the Actual4test.com AZ-220 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-220 dumps with Test Engine here: https://www.actual4test.com/AZ-220_examcollection.html (205 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 92

You have 100 devices that connect to an Azure IoT hub named Hub1. The devices connect by using a symmetric key.

You deploy an IoT hub named Hub2.

You need to migrate 10 devices from Hub1 to Hub2. The solution must ensure that the devices retain the existing symmetric key.

What should you do?

- A. Add a desired property to the device twin of Hub2. Update the endpoint of the 10 devices to use Hub2.
- B. Add a desired property to the device twin of Hub1. Recreate the device identity on Hub2.
- C. Recreate the device identity on Hub2. Update the endpoint of the 10 devices to use Hub2.
- D. Disable the 10 devices on Hub1. Update the endpoint of the 10 devices to use Hub2.

Answer: (SHOW ANSWER)

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: 93

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 IoT hub, you change the credentials for the shared access policy of the IoT devices. Does the solution meet the goal?

- A. Yes
- B. No

Answer: B (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 94

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.

```

{
  "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
}
}

```



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
lothub
```

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: 95

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

Transparent Field Gateway Device:

Low Resource Device:

Limited Sensor Device:

Protocol

Protocol

Protocol

Answer:

Protocols

AMQP

HTTPS

MQTT

Answer Area

Device

Transparent Field Gateway Device:

Low Resource Device:

Limited Sensor Device:

Protocol

AMQP

MQTT

HTTPS

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

NEW QUESTION: 96

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: (SHOW ANSWER)

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: 97

You have an Azure IoT hub that uses a Device Provisioning Service instance to automate the deployment of Azure IoT Edge devices.

The IoT Edge devices have a Trusted Platform Module (TPM) 2.0 chip.

From the Azure portal, you plan to add an individual enrollment to the Device Provisioning Service that will use the TPM of the IoT Edge devices as the attestation mechanism.

Which detail should you obtain before you can create the enrollment.

- A. the scope ID and the Device Provisioning Service endpoint
- B. the primary key of the Device Provisioning Service shared access policy and the global device endpoint
- C. the X.509 device certificate and the certificate chain
- D. the endorsement key and the registration ID

Answer: D (LEAVE A REPLY)

The TPM simulator's Registration ID and the Endorsement key, are used when you create an individual enrollment for your device.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/how-to-auto-provision-simulated-device-linux>

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 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)

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: 99

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:

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

Explanation:

Box 1: Measurement

Telemetry/measurement is a stream of values sent from the device, typically from a sensor. For example, a sensor might report the ambient temperature.

Box 2: Property

The template can provide a writeable fan speed property

Properties represent point-in-time values. For example, a device can use a property to report the target temperature it's trying to reach. You can set writeable properties from IoT Central.

Box 3: Settings

Box 4: Command

You can call device commands from IoT Central. Commands optionally pass parameters to the device and receive a response from the device. For example, you can call a command to reboot a device in 10 seconds.

Reference:

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

NEW QUESTION: 100

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:

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

Reference:

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

NEW QUESTION: 101

You have 1,000 devices that connect to a standard tier Azure IoT hub.

All the devices are commissioned and send telemetry events to the built-in IoT Hub endpoint. You configure message enrichment on the events endpoint and set the enrichment value to \$twin.tags.ipV4.

When you inspect messages on the events endpoint, you discover that all the messages are stamped with a string of "\$twin.tags.ipV4".

What are two possible causes of the issue? Each Answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. The ipV4 tag is a restricted twin property that is unavailable for message enrichment.
- B. A standard tier IoT hub does not support device twin properties in message enrichments.
- C. The device sending the message has no device twin.
- D. Message enrichment cannot be added to messages going to a built-in endpoint.
- E. The device twin path used for the value of the enrichment does not exist.
- F. The device twin property value used for message enrichment is set to "\$twin.tags.ipV4".

Answer: C,E (LEAVE A REPLY)

In some cases, if you are applying an enrichment with a value set to a tag or property in the device twin, the value will be stamped as a string value. For example, if an enrichment value is set to \$twin.tags.field, the messages will be stamped with the string "\$twin.tags.field" rather than the value of that field from the twin. This happens in the following cases:

(C) Your IoT Hub is in the standard tier, but the device sending the message has no device twin.

(E) Your IoT Hub is in the standard tier, but the device twin path used for the value of the enrichment does not exist. For example, if the enrichment value is set to \$twin.tags.location, and the device twin does not have a location property under tags, the message is stamped with the string "\$twin.tags.location".

Your IoT Hub is in the basic tier. Basic tier IoT hubs do not support device twins.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-message-enrichments-overview>

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

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: 103

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

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



Microsoft

freepdfdumps.com

⬅️
➡️

⬆️
⬆️

Answer:

Answer Area

Run the following commands

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

Add the connection string to..

- 1 - Run the following commands
- 2 - From IoT Hub, create an IoT Edge device registry entry.
- 3 - Add the connection string to..

Reference:

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

NEW QUESTION: 104

You have an Azure IoT hub.

You need to check whether the IoT hub was affected by an outage.

What should you select in the Azure portal? To answer, select the appropriate option in the answer area.

NOTE: Each correct selection is worth one point.

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

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

Explanation

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

NEW QUESTION: 105

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You 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: 106

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this 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: 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>

AZ-220

Number: AZ-220

Passing Score: 800

Time Limit: 120 min

File Version: 1

AZ-220

Implement the IoT solution infrastructure

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.


```

{
  "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 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. 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.

Implement the IoT solution infrastructure

Question Set 2

Valid AZ-220 Dumps shared by Actual4test.com for Helping Passing AZ-220 Exam! Actual4test.com now offer the **newest AZ-220 exam dumps**, the Actual4test.com AZ-220 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-220 dumps with Test Engine here: https://www.actual4test.com/AZ-220_examcollection.html (205 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 107

You are deploying an Azure IoT Edge solution that includes multiple IoT Edge devices.

You need to configure module-to-module routing.

To which section of the deployment manifest should you add the routes?

- A. storeAndForwardConfiguration
- B. \$edgeHub
- C. modules
- D. systemModules

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

Explanation

Routes are declared in the \$edgeHub desired properties.

Reference:

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

NEW QUESTION: 108

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: ([SHOW ANSWER](#)**)**

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>

Topic 1, ADatum

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 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 button to return to the question.

Requirements. Planned Changes

ADatum is developing an Azure IoT solution to monitor environmental conditions. The IoT solution consists of hardware devices and cloud services. All the devices will communicate directly to Azure IoT Hub.

The hardware devices will be deployed to the branch offices and will collect data about various environmental conditions such as temperature, humidity, air quality, and noise level. The devices will be wired by using Power over Ethernet (PoE) connections.

ADatum is developing the solution in the following three phases: proof of value (POV), pilot, and production.

Requirements. POV Requirements

The POV phase will demonstrate that a technical solution is viable. During this phase, 100 devices will be deployed to the main office and Azure Stream Analytics will be connected to an IoT hub to generate real-time alerts. Stream Analytics will perform the following processing:

- * Calculate the median rate of the telemetry across the entire devices that exceed the median rate by a factor of 4.
- * Compare the current telemetry to the specified thresholds and issue alerts when telemetry values are out of range.
- * Ensure that all message content during this phase is human readable to simplify debugging.

Requirements. Pilot Requirements

During the pilot phase, devices will be deployed to 10 offices. Each office will have up to 1,000 devices.

During this phase, you will add Azure Time Series Insights in parallel to Stream Analytics to support real-time graphs and queries in a dashboard web app.

The pilot deployment must minimize operating costs.

Requirements. Production Requirements

The production phase will include all the offices.

The production deployment will have one IoT hub in each Azure region. Devices must connect to the IoT hub in their region.

The production phase must meet the following requirements:

- * Ensure that the IoT solution can support performance and scale targets.
- * Ensure that the IoT solution support up to 1,000 devices per office.
- * Minimize operating costs of the IoT solution.

Requirements. Technical Requirements

Datum identifies the following requirements for the planned IoT solution:

- * The solution must generate real-time alerts when a fire condition is detected in an office. All the devices in that office must trigger an audible alarm siren within 10 seconds of the alert.
- * A dashboard UI must display alerts and the system status in real time and must allow device operators to make adjustments to the system.
- * Each device will send hourly updates to IoT Hub. Condition alerts will be sent immediately.
- * Multiple types of devices will collect telemetry that has different schemas.
- * IoT Hub must perform message routing based on the message body.
- * Direct methods must be used for cloud-to-device communication.
- * Reports must be provided monthly, quarterly, and annually.
- * Stored data queries must be as efficient as possible.
- * The device message size will be under 4 KB.
- * Development effort must be minimized.

Requirements. Throttle and Quotas

The relevant throttles and quotas for various IoT Hub tiers are shown in the following table.

Tier	Direct method	Device-to-cloud message	Price per month
B1	40/sec/unit	400,000/day/unit	\$10/unit
S1	40/sec/unit	400,000/day/unit	\$25/unit
S2	120/sec/unit	6,000,000/day/unit	\$250/unit

Requirements. IoT Hub Routing

You plan to implement IoT Hub routing during the POV phase as shown in the following exhibit.

NEW QUESTION: 109

You have an Azure IoT hub that uses a Device Provisioning Service instance to automate the deployment of Azure IoT Edge devices. The IoT Edge devices have a Trusted Platform Module (TPM) 2.0 chip. From the Azure portal, you plan to add an individual enrollment to the Device Provisioning Service that will use the TPM of the IoT Edge devices as the attestation mechanism.

Which detail should you obtain before you can create the enrollment.

- A. the scope ID and the Device Provisioning Service endpoint
- B. the primary key of the Device Provisioning Service shared access policy and the global device endpoint
- C. the X.509 device certificate and the certificate chain
- D. the endorsement key and the registration ID

Answer: D (LEAVE A REPLY)

Explanation

The TPM simulator's Registration ID and the Endorsement key, are used when you create an individual enrollment for your device.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-edge/how-to-auto-provision-simulated-device-linux>

NEW QUESTION: 110

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

You discover that some of the devices fail to send data to the IoT hub.

You need to ensure that you can use Azure Monitor to troubleshoot the device connectivity issues.

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 Diagnostics settings of the IoT hub, select Archive to a storage account.

B. Collect the DeviceTelemetry, Connections, and Routes logs.

C. Collect all metrics.

D. From the Diagnostics settings of the IoT hub, select Send to Log Analytic.

E. Collect the JobsOperations, DeviceStreams, and FileUploadOperations logs.

Answer: B,D (LEAVE A REPLY)

The IoT Hub resource logs connections category emits operations and errors having to do with device connections. The following screenshot shows a diagnostic setting to route these logs to a Log Analytics workspace:

Diagnostics settings Microsoft

Save Discard Delete Provide feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

D diagnostic setting name * Send connection events to logs ✓

Category details

log

- ☒ Connections
- ☐ DeviceTelemetry
- ☐ C2DCommands
- ☐ DeviceIdentityOperations
- ☐ FileUploadOperations
- ☐ Routes

Destination details

☒ Send to Log Analytics

Subscription: Internal use

Log Analytics workspace: contoso-la-workspace27124 (westus)

☐ Archive to a storage account

☐ Stream to an event hub

Note: Azure Monitor: Route connection events to logs:

IoT hub continuously emits resource logs for several categories of operations. To collect this log data, though, you need to create a diagnostic setting to route it to a destination where it can be analyzed or archived. One such destination is Azure Monitor Logs via a Log Analytics workspace, where you can analyze the data using Kusto queries.

Reference:

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

NEW QUESTION: 111

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

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

Topic 1, Contoso

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.

```
{
  "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
  }
}
```



freepaidumps.com

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
lothub
```

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. 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.

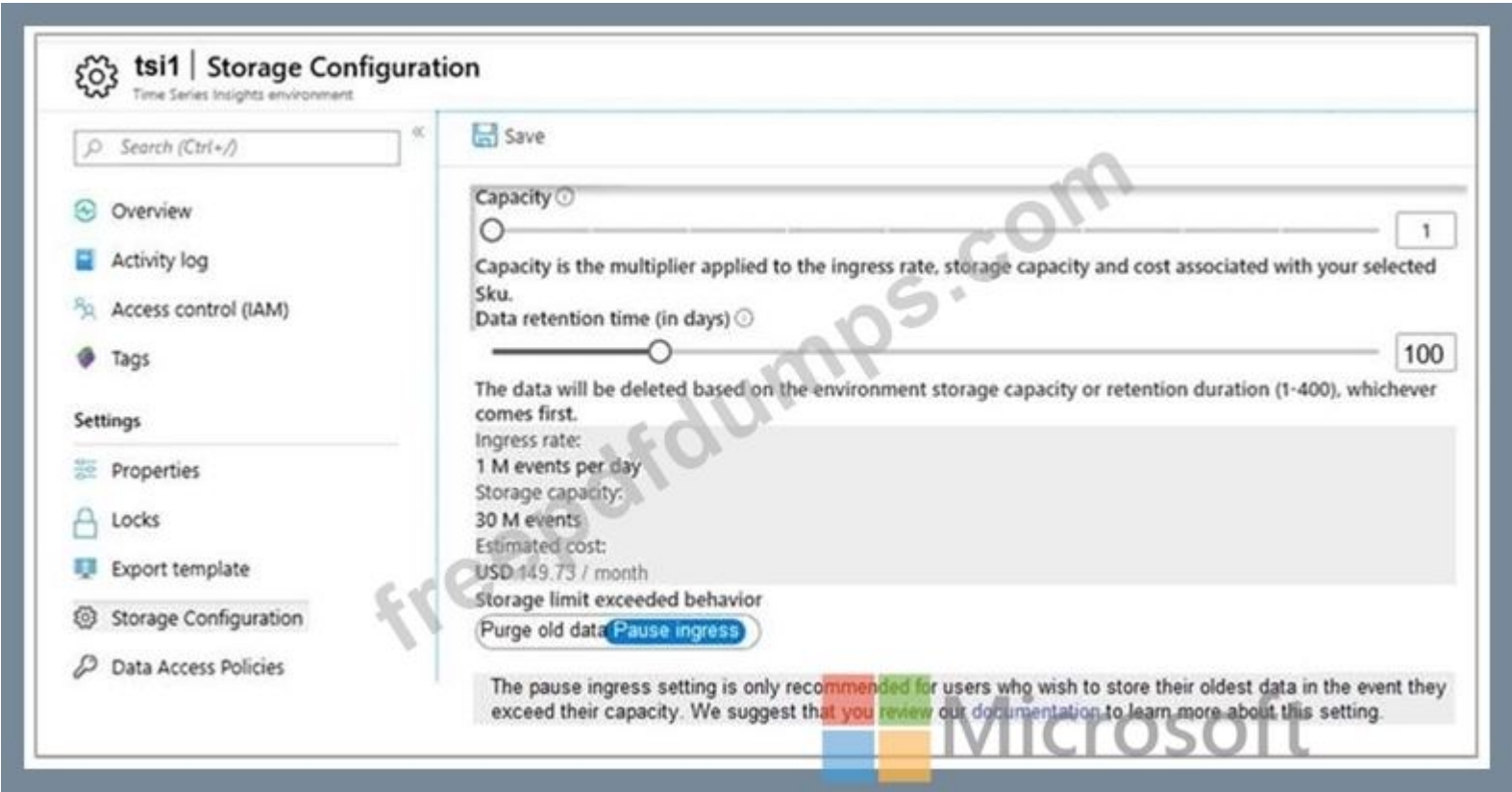
Requirements. Technical Requirements

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: 112

You have an Azure IoT hub named Hub1 and an Azure Time Series Insights environment named tsi1. Tsi1 connects to Hub1. The solution has been operational for 6 months. Tsi1 is configured as shown in the following exhibit.



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

Hub1 has seven days of retained telemetry.

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

NOTE: Each correct selection is worth one point.

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

Answer:

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

Reference:

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

NEW QUESTION: 113

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: D (LEAVE A REPLY)

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: 114

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: 115

You need to visualize Azure IoT Hub telemetry data by using Microsoft Power BI.

Which service should you connect to the IoT hub?

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

Answer: ([SHOW ANSWER](#))

Explanation

You can use Microsoft Power BI to visualize real-time sensor data that your Azure IoT hub receives. To do so, you configure an Azure Stream Analytics job to consume the data from IoT Hub and route it to a dataset in Power BI.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-live-data-visualization-in-power-bi>

NEW QUESTION: 116

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

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

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

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

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

Does this meet the goal?

- A. Yes
- B. No

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

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

Instead use a translation gateway.

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

Reference:

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

NEW QUESTION: 117

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

`aziot hub create --resource-group MyResourceGroup --name MyIotHub --sku B1 -- location westus --partition-count 4` What does MyIotHub support?

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

Answer: (SHOW ANSWER)

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: 118

You have an Azure IoT solution that includes an Azure IoT hub.

You plan to deploy 10,000 IoT devices.

You need to validate the performance of the IoT solution while 10,000 concurrently connected devices stream telemetry. The solution must minimize effort.

What should you deploy?

- A. an Azure IoT Device Simulation from Azure IoT Solution Accelerator
- B. an Azure function, an IoT Hub device SDK, and a timer trigger
- C. Azure IoT Central application and a template for the retail industry
- D. an Azure IoT Edge gateway configured as a protocol translation gateway

Answer: (SHOW ANSWER)

The IoT solution accelerators are complete, ready-to-deploy IoT solutions that implement common IoT scenarios. The scenarios include connected factory and device simulation.

Use the Device Simulation solution accelerator to run simulated devices that generate realistic telemetry. You can use this solution accelerator to test the behavior of the other solution accelerators or to test your own custom IoT solutions.

Reference:

<https://docs.microsoft.com/en-us/azure/iot-accelerators/about-iot-accelerators>

Topic 1, ADatum

Requirements

Planned Changes

ADatum is developing an Azure IoT solution to monitor environmental conditions. The IoT solution consists of hardware devices and cloud services. All the devices will communicate directly to Azure IoT Hub.

The hardware devices will be deployed to the branch offices and will collect data about various environmental conditions such as temperature, humidity, air quality, and noise level. The devices will be wired by using Power over Ethernet (PoE) connections.

ADatum is developing the solution in the following three phases: proof of value (POV), pilot, and production.

Requirements. POV Requirements

The POV phase will demonstrate that a technical solution is viable. During this phase, 100 devices will be deployed to the main office and Azure Stream Analytics will be connected to an IoT hub to generate real-time alerts. Stream Analytics will perform the following processing:

Calculate the median rate of the telemetry across the entire devices that exceed the median rate by a factor of 4.

Compare the current telemetry to the specified thresholds and issue alerts when telemetry values are out of range.

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

Requirements. Pilot Requirements

During the pilot phase, devices will be deployed to 10 offices. Each office will have up to 1,000 devices.

During this phase, you will add Azure Time Series Insights in parallel to Stream Analytics to support real-time graphs and queries in a dashboard web app.

The pilot deployment must minimize operating costs.

Requirements. Production Requirements

The production phase will include all the offices.

The production deployment will have one IoT hub in each Azure region. Devices must connect to the IoT hub in their region.

The production phase must meet the following requirements:

Ensure that the IoT solution can support performance and scale targets.

Ensure that the IoT solution support up to 1,000 devices per office.

Minimize operating costs of the IoT solution.

Requirements. Technical Requirements

Datum identifies the following requirements for the planned IoT solution:

The solution must generate real-time alerts when a fire condition is detected in an office. All the devices in that office must trigger an audible alarm siren within 10 seconds of the alert.

A dashboard UI must display alerts and the system status in real time and must allow device operators to make adjustments to the system.

Each device will send hourly updates to IoT Hub. Condition alerts will be sent immediately.

Multiple types of devices will collect telemetry that has different schemas.

IoT Hub must perform message routing based on the message body.

Direct methods must be used for cloud-to-device communication.

Reports must be provided monthly, quarterly, and annually.

Stored data queries must be as efficient as possible.

The device message size will be under 4 KB.

Development effort must be minimized.

Requirements. Throttle and Quotas

The relevant throttles and quotas for various IoT Hub tiers are shown in the following table.

Tier	Direct method	Device-to-cloud message	Price per month
B1	40/sec/unit	400,000/day/unit	\$10/unit
S1	40/sec/unit	400,000/day/unit	\$25/unit
S2	120/sec/unit	6,000,000/day/unit	\$250/unit

Requirements. IoT Hub Routing

You plan to implement IoT Hub routing during the POV phase as shown in the following exhibit.

NEW QUESTION: 119

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 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 tags to the device twin.

Does the solution meet the goal?

A. Yes

B. No

Answer: (SHOW ANSWER)

Instead add the desired properties to the device twin.

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

NEW QUESTION: 120

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: 121

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.

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>

Valid AZ-220 Dumps shared by Actual4test.com for Helping Passing AZ-220 Exam! Actual4test.com now offer the **newest AZ-220 exam dumps**, the Actual4test.com AZ-220 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-220 dumps with Test Engine here: https://www.actual4test.com/AZ-220_examcollection.html (205 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

NEW QUESTION: 122

You plan to deploy Azure Time Series Insights.

What should you create on iothub1 before you deploy Time Series Insights?

- A. a new message route
- B. a new consumer group
- C. a new shared access policy
- D. an IP filter rule

Answer: ([SHOW ANSWER](#))

Create a dedicated consumer group in the IoT hub for the Time Series Insights environment to consume from. Each Time Series Insights event source must have its own dedicated consumer group that isn't shared with any other consumer. If multiple readers consume events from the same consumer group, all readers are likely to exhibit failures.

Reference:

<https://docs.microsoft.com/en-us/azure/time-series-insights/time-series-insights-how-to-add-an-event-source- iothub>

Topic 2, A Datum

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.

Requirements. Planned Changes

ADatum is developing an Azure IoT solution to monitor environmental conditions. The IoT solution consists of hardware devices and cloud services. All the devices will communicate directly to Azure IoT Hub.

The hardware devices will be deployed to the branch offices and will collect data about various environmental conditions such as temperature, humidity, air quality, and noise level. The devices will be wired by using Power over Ethernet (PoE) connections.

ADatum is developing the solution in the following three phases: proof of value (POV), pilot, and production.

Requirements. POV Requirements

The POV phase will demonstrate that a technical solution is viable. During this phase, 100 devices will be deployed to the main office and Azure Stream Analytics will be connected to an IoT hub to generate real-time alerts. Stream Analytics will perform the following processing:

- * Calculate the median rate of the telemetry across the entire devices that exceed the median rate by a factor of 4.
- * Compare the current telemetry to the specified thresholds and issue alerts when telemetry values are out of range.
- * Ensure that all message content during this phase is human readable to simplify debugging.

Requirements. Pilot Requirements

During the pilot phase, devices will be deployed to 10 offices. Each office will have up to 1,000 devices.

During this phase, you will add Azure Time Series Insights in parallel to Stream Analytics to support real-time graphs and queries in a dashboard web app.

The pilot deployment must minimize operating costs.

Requirements. Production Requirements

The production phase will include all the offices.

The production deployment will have one IoT hub in each Azure region. Devices must connect to the IoT hub in their region.

The production phase must meet the following requirements:

Ensure that the IoT solution can support performance and scale targets.

Ensure that the IoT solution support up to 1,000 devices per office.

Minimize operating costs of the IoT solution.

Requirements. Technical Requirements

Datum identifies the following requirements for the planned IoT solution:

- * The solution must generate real-time alerts when a fire condition is detected in an office. All the devices in that office must trigger an audible alarm siren within 10 seconds of the alert.

- * A dashboard UI must display alerts and the system status in real time and must allow device operators to make adjustments to the system.
- * Each device will send hourly updates to IoT Hub. Condition alerts will be sent immediately.
- * Multiple types of devices will collect telemetry that has different schemas.
- * IoT Hub must perform message routing based on the message body.
- * Direct methods must be used for cloud-to-device communication.
- * Reports must be provided monthly, quarterly, and annually.
- * Stored data queries must be as efficient as possible.
- * The device message size will be under 4 KB.
- * Development effort must be minimized.

Requirements. Throttle and Quotas

The relevant throttles and quotas for various IoT Hub tiers are shown in the following table.

Tier	Direct method	Device-to-cloud message	Price per month
B1	40/sec/unit	400,000/day/unit	\$10/unit
S1	40/sec/unit	400,000/day/unit	\$25/unit
S2	120/sec/unit	6,000,000/day/unit	\$250/unit

Requirements. IoT Hub Routing

You plan to implement IoT Hub routing during the POV phase as shown in the following exhibit.

Valid AZ-220 Dumps shared by Actual4test.com for Helping Passing AZ-220 Exam! Actual4test.com now offer the **newest AZ-220 exam dumps**, the Actual4test.com AZ-220 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com AZ-220 dumps with Test Engine here: https://www.actual4test.com/AZ-220_examcollection.html (205 Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)