Microsoft.AZ-220.v2022-02-14.q144

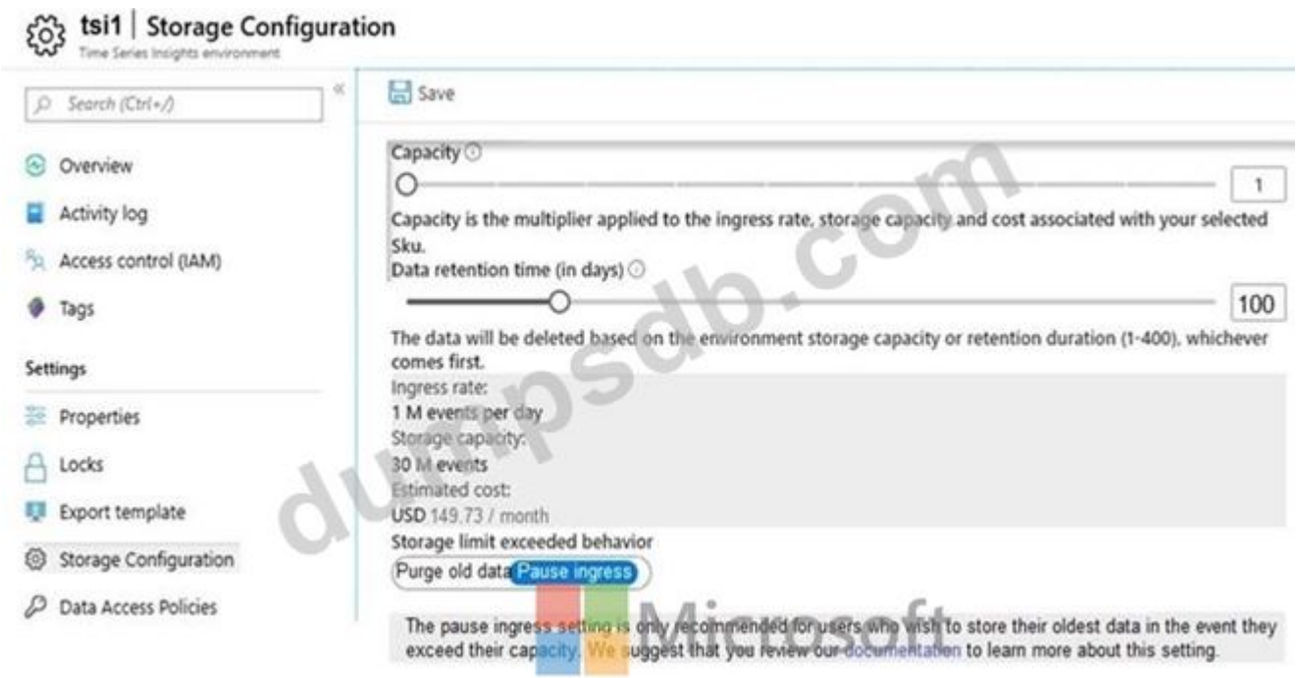
Exam Code:	AZ-220
Exam Name:	Microsoft Azure IoT Developer
Certification Provider:	Microsoft
Free Question Number:	144
Version:	v2022-02-14
# of views:	2137
# of Questions views:	1440
https://www.dumpsdb.com/dumps/Microsoft/AZ-220/Microsoft.AZ-220.v2022-02-14.q144	

NEW QUESTION: 1
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: 2

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: 3
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: 4
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: (SHOW ANSWER)
The IoT Hub publishes the Microsoft.Devices.DeviceDisconnected event type, which is published when a device is disconnected from an IoT hub.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-event-grid#event-types

NEW QUESTION: 5
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
Implement Edge Question Set 1

NEW QUESTION: 6
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: (SHOW ANSWER)

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

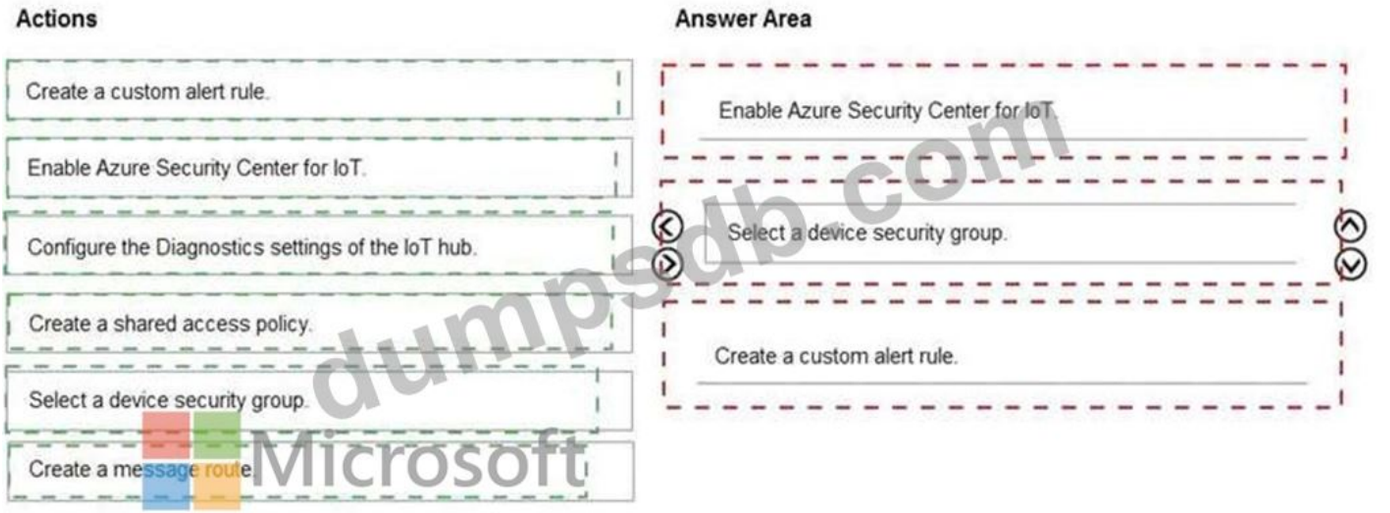
NEW QUESTION: 7

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

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

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

Answer:



Explanation

Step 1: Enable Azure Security Center for IoT

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

Step 2: Select a device security group

Update a device security group..

Step 3: Create a custom alert rule

by creating a custom alert rule

Reference:

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

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

NEW QUESTION: 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 IoT solution that includes an Azure IoT hub, a Device Provisioning Service instance, and
1,000 connected IoT devices.
All the IoT devices are provisioned automatically by using one enrollment group.
You need to temporarily disable the IoT devices from the connecting to the IoT hub.
Solution: From the Device Provisioning Service, you disable the enrollment group, and you disable device entries in the identity registry of the IoT hub to which the IoT devices are provisioned.
Does the solution meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
You may find it necessary to deprovision devices that were previously auto-provisioned through the Device Provisioning Service.
In general, deprovisioning a device involves two steps:
1. Disenroll the device from your provisioning service, to prevent future auto-provisioning. Depending on whether you want to revoke access temporarily or permanently, you may want to either disable or delete an enrollment entry.
2. Deregister the device from your IoT Hub, to prevent future communications and data transfer. Again, you can temporarily disable or permanently delete the device's entry in the identity registry for the IoT Hub where it was provisioned.
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/iot-dps/how-to-unprovision-devices

NEW QUESTION: 9
You have 10 IoT devices that connect to an Azure IoT hub named Hub1.
From Azure Cloud Shell, you run az iot hub monitor-events --hub-name Hub1 and receive the following error message: "az iot hub: 'monitor-events' is not in the 'az iot hub' command group. See 'az iot hub
--help'."
You need to ensure that you can run the command successfully. What should you run first?
A. az iot hub monitor-feedback --hub-name Hub1
B. az iot hub generate-sas-token --hub-name Hub1
C. az iot hub configuration list --hub-name Hub1
D. az extension add -name azure-cli-iot-ext
Answer: (SHOW ANSWER)
Explanation
Execute az extension add --name azure-cli-iot-ext once and try again.

In order to read the telemetry from your hub by CLI, you have to enable IoT Extension with the following commands:
Add: az extension add --name azure-cli-iot-ext
Reference:
https://github.com/MicrosoftDocs/azure-docs/issues/20843

NEW QUESTION: 10
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 Bush 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 Bush 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)
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: 11

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are developing a custom Azure IoT Edge module.
The module needs to identify the device ID of the local device.
Solution: You configure the module to read the device ID of the device twin.
Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
Device twins are JSON documents that store device state information including metadata, configurations, and conditions. Azure IoT Hub maintains a device twin for each device that you connect to IoT Hub.
Device identity properties. The root of the device twin JSON document contains the read-only properties from the corresponding device identity stored in the identity registry.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-device-twins

NEW QUESTION: 12
You have an Azure IoT hub that uses a Device Provisioning Service instance.
You create a new individual device enrollment that uses symmetric key attestation.
Which detail from the enrollment is required to auto provision the device by using the Device Provisioning Service?
A. the registration ID of the enrollment
B. the primary key of the enrollment
C. the device identity of the IoT hub
D. the hostname of the IoT hub
Answer: (SHOW ANSWER)
An enrollment is the record of devices or groups of devices that may register through auto-provisioning. The enrollment record contains information about the device or group of devices, including:
* the attestation mechanism used by the device
* the optional initial desired configuration
* desired IoT hub
the desired device ID
Note: Azure IoT auto-provisioning can be broken into three phases:
1. Service configuration - a one-time configuration of the Azure IoT Hub and IoT Hub Device Provisioning Service instances, establishing them and creating linkage between them.

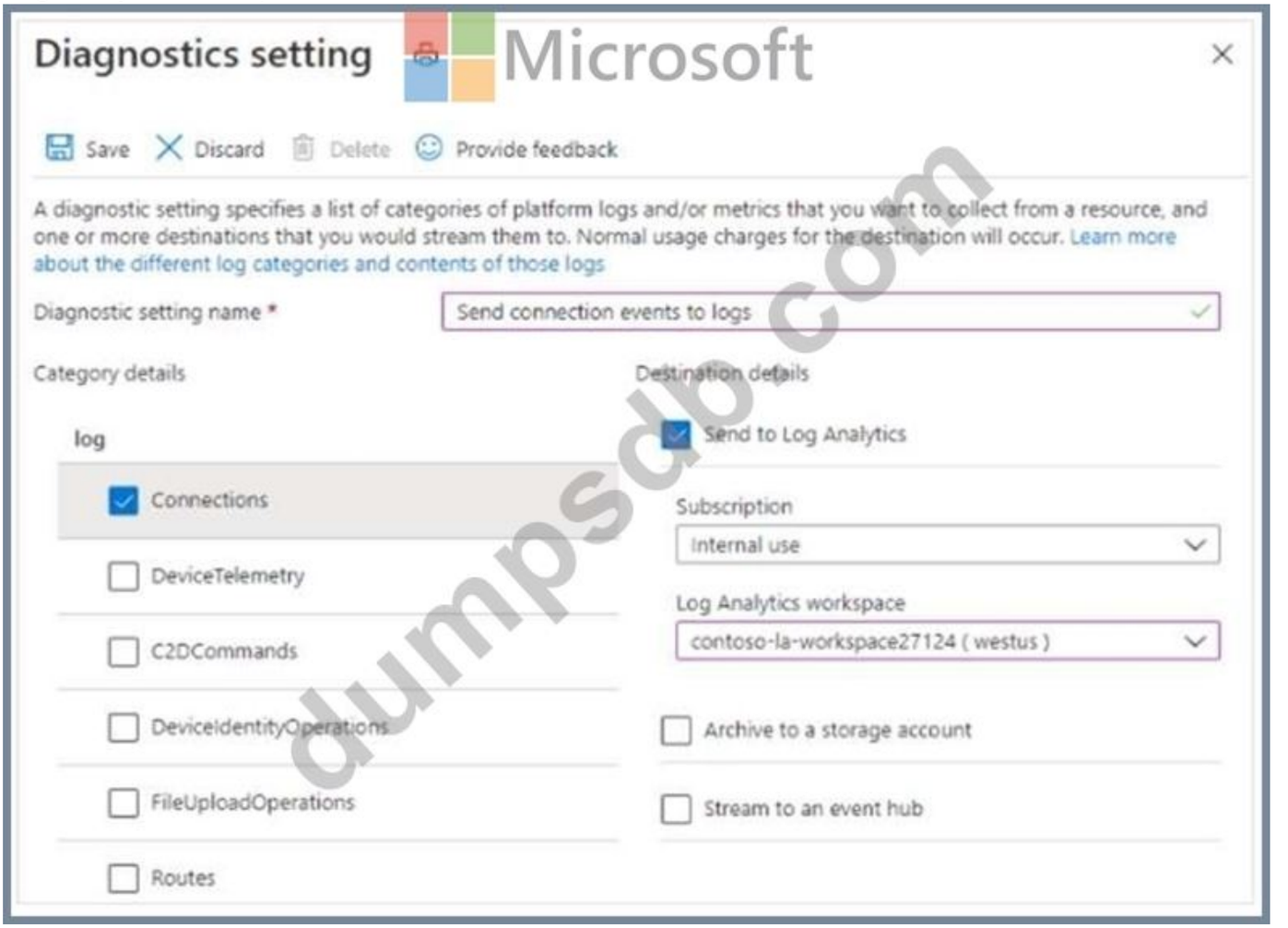
2. Device enrollment - the process of making the Device Provisioning Service instance aware of the devices that will attempt to register in the future. Enrollment is accomplished by configuring device identity information in the provisioning service, as either an "individual enrollment" for a single device, or a "group enrollment" for multiple devices.
3. Device registration and configuration
Reference:
https://docs.microsoft.com/en-us/azure/iot-dps/concepts-service#enrollment

NEW QUESTION: 13
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: You delete the enrollment group from the Device Provisioning Service. Does the solution meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Explanation
Instead, from the Device Provisioning Service, you disable the enrollment group, and you disable device entries in the identity registry of the IoT hub to which the IoT devices are provisioned.
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/iot-dps/how-to-unprovision-devices

NEW QUESTION: 14
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:



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: 15

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: B (LEAVE A REPLY)
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: 16
You have an Azure IoT solution that contains an Azure IoT hub and 100 IoT devices. The devices run Windows Server 2016.
You need to deploy the Azure Defender for IoT C#-based security agent to the devices.
What should you do first?
A. On the devices, initialize Trusted Platform Module (TPM).
B. From the IoT hub. create a system-assigned managed identity.
C. From the IoT hub. create a security module for the devices.
D. On the devices, set the PowerShell execution policy to Restricted.
Answer: C (LEAVE A REPLY)
Explanation
The IoT Edge security manager provides a safe framework for security service extensions through host-level modules. The IoT Edge security manager include
* Ensure safe operation of client agents for services including Device Update for IoT Hub and Azure Defender for IoT.
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/iot-edge-security-manager

NEW QUESTION: 17
You use Azure Security Center in an Azure IoT solution.
You need to exclude some security events. The solution must minimize development effort. What should you do?
A. Create an Azure function to filter security messages.

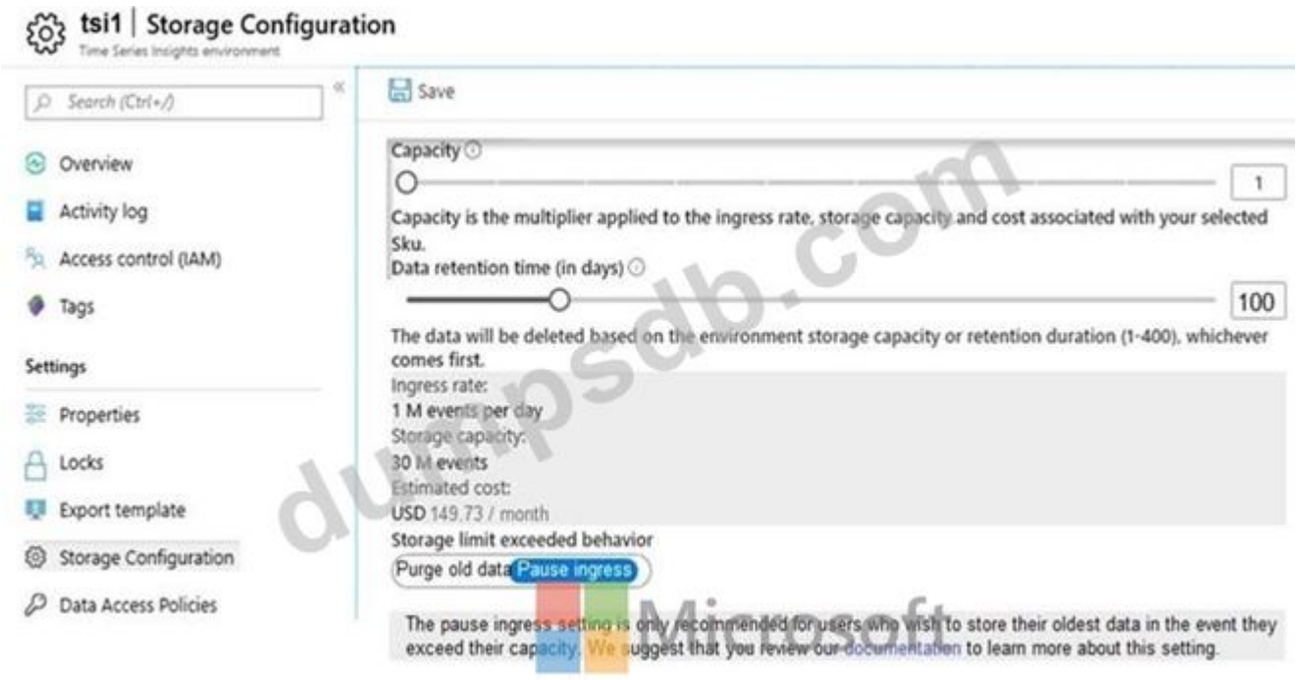
B. Add a configuration to the code of the physical IoT device.
C. Add configuration details to the device twin object.
D. Create an azureiotsecurity module twin and add configuration details to the module twin object.
Answer: (SHOW ANSWER)
Properties related to every Azure Security Center for IoT security agent are located in the agent configuration object, within the desired properties section, of the azureiotsecurity module.
To modify the configuration, create and modify this object inside the azureiotsecurity module twin identity. Note: Azure Security Center for IoT's security agent twin configuration object is a JSON format object. The configuration object is a set of controllable properties that you can define to control the behavior of the agent.
These configurations help you customize the agent for each scenario required. For example, automatically excluding some events, or keeping power consumption to a minimal level are possible by configuring these properties.
Reference:
https://docs.microsoft.com/en-us/azure/asc-for-iot/how-to-agent-configuration

NEW QUESTION: 18
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: D (LEAVE A REPLY)
Explanation
IoT Hub is one of the first Azure services to support distributed tracing. As more Azure services support distributed tracing, you'll be able 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

NEW QUESTION: 19
You have an existing Azure IoT hub.
You need to connect physical IoT devices to the IoT hub.
You are connecting the devices through a firewall that allows only port 443 and port 80.
Which three communication protocols can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. MQTT over WebSocket
B. AMQP
C. AMQP over WebSocket
D. MQTT
E. HTTPS
Answer: A,C,E (LEAVE A REPLY)
Explanation
MQTT over WebSockets, AMQP over WebSocket, and HTTPS use port 443.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-protocols

NEW QUESTION: 20
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: 21
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: 22
You have an Azure IoT solution that includes a standard tier Azure IoT hub and an IoT device. The device sends one 100-KB device-to-cloud message every hour.
You need to calculate the total daily message consumption of the device. What is the total daily message consumption of the device?
A. 24
B. 600
C. 2,400
D. 4,800
Answer: B (LEAVE A REPLY)
100 KB * 24 is around 2,400 bytes.
The 100 KB message is divided into 4 KB blocks, and it is billed for 25 messages. 25 times 24 is 600 Note: The maximum message size for messages sent from a device to the cloud is 256 KB. These messages are metered in 4 KB blocks for the paid tiers so for instance if the device sends a 16 KB message via the paid tiers it will be billed as 4 messages.
Reference:
https://azure.microsoft.com/en-us/pricing/details/iot-hub/

NEW QUESTION: 23
You need to configure Stream Analytics to meet the POV requirements.
What are two ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. From IoT Hub, create a custom event hub endpoint, and then configure the endpoint as an input to Stream Analytics.
B. Create a Stream Analytics module, and then deploy the module to all IoT Edge devices in the fleet.
C. Create an input in Stream Analytics that uses the built-in events endpoint of IoT Hub as the source.
D. Route telemetry to an Azure Blob storage custom endpoint, and then configure the Blob storage as a reference input for Stream Analytics.
Answer: A,C (LEAVE A REPLY)
Explanation/Reference:
Process and manage data
Question Set 3

NEW QUESTION: 24
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)
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: 25
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)
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: 26

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

NEW QUESTION: 27
You are planning a proof of concept (POC) that will use an Azure IoT hub.
You have two self-signed client authentication certificates named Cert1 and Cert2. Cert1 has a basic constraint that contains Subject Type=C You need to identify which certificates to use.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

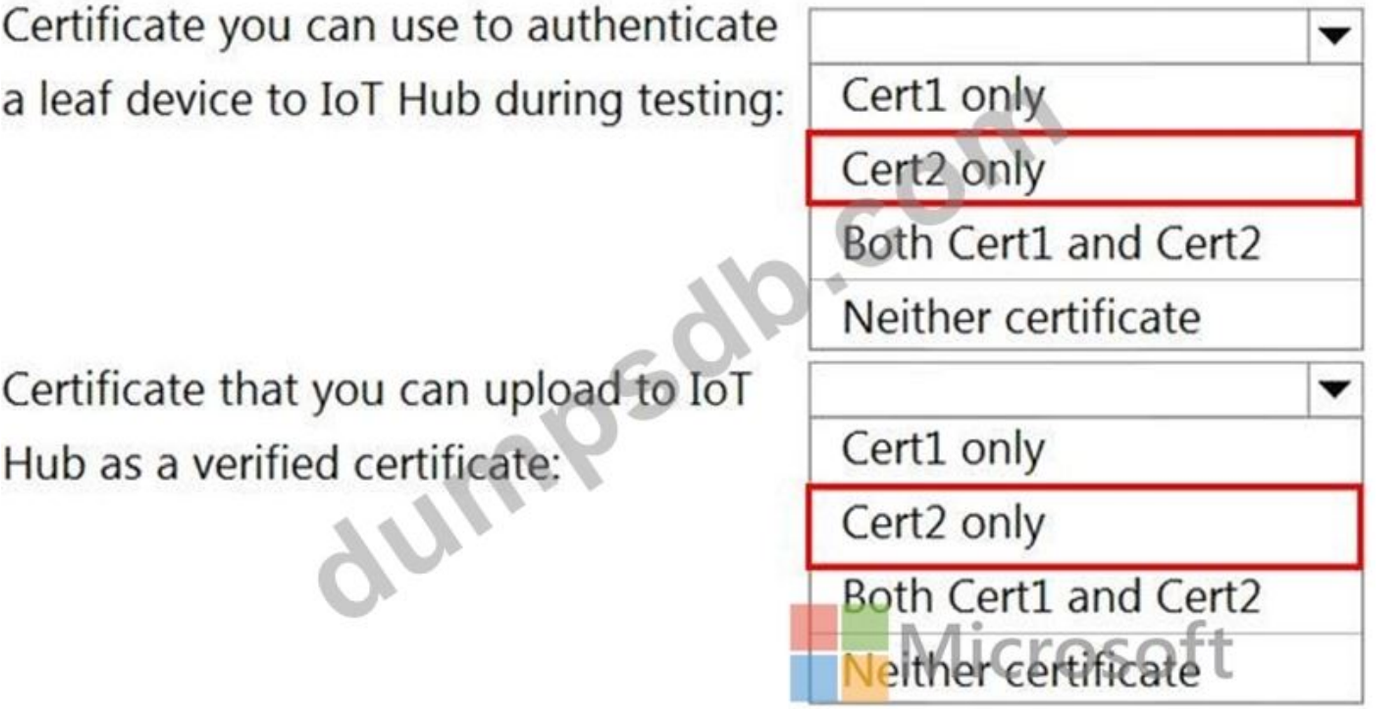
Certificate you can use to authenticate a leaf device to IoT Hub during testing:

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

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

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

Answer:

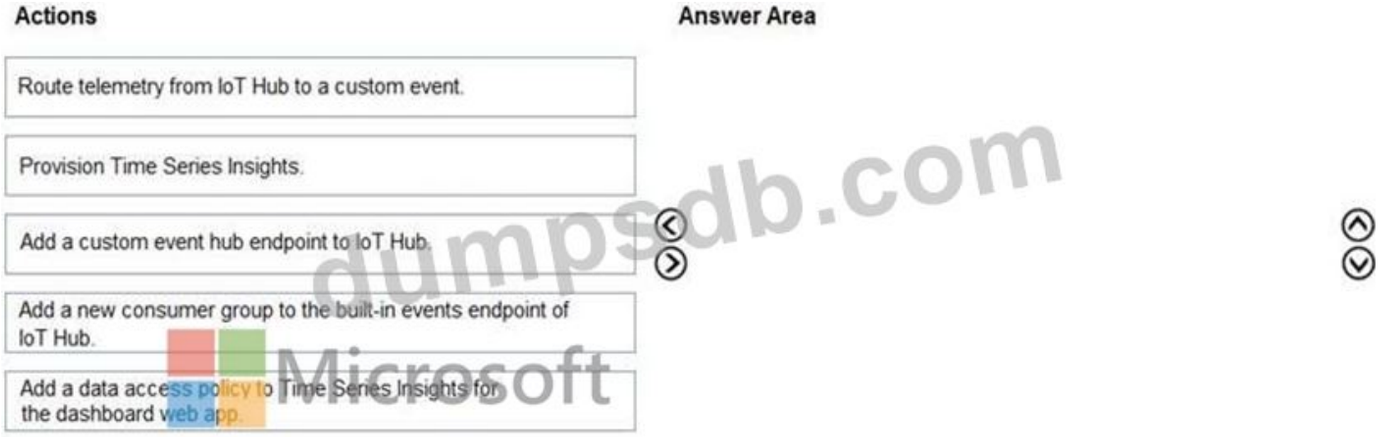


Explanation:
Box 1: Cert2 only
Cert2: The leaf certificate, or end-entity certificate, identifies the certificate holder. It has the root certificate in its certificate chain as well as zero or more intermediate certificates. The leaf certificate is not used to sign any other certificates. It uniquely 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

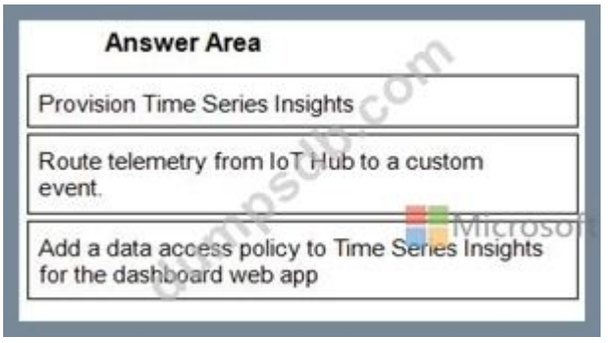
NEW QUESTION: 28
You have 1,000 devices that connect to an Azure IoT hub.
You are performing a scheduled check of deployed IoT devices. You plan to run the following command from the Azure CLI prompt.
aziot hub query --hub-name hub1 --query-command "SELECT * FROM devices WHERE connectionState = 'Disconnected'" What does the command return?
A. the Device Disconnected events
B. the device twins
C. the Connections logs
D. the device credentials
Answer: A (LEAVE A REPLY)

The IoT Hub publishes the Microsoft.Devices.DeviceDisconnected event type, which is published when a device is disconnected from an IoT hub.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-event-grid#event-types

NEW QUESTION: 29
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.



Answer:

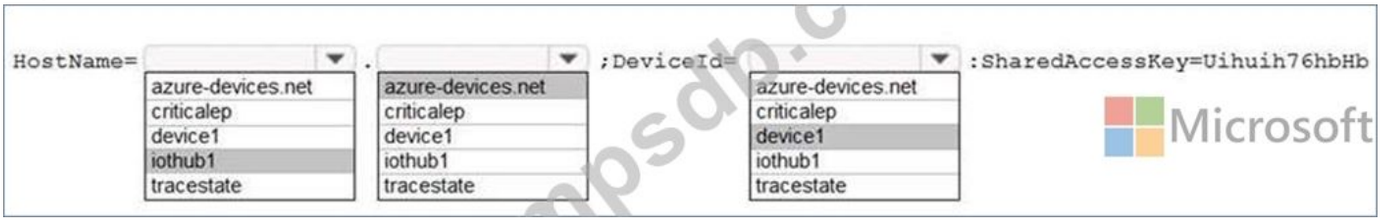


1 - Provision Time Series Insights
2 - Route telemetry from IoT Hub to a custom event.
3 - Add a data access policy to Time Series Insights for the dashboard web app Reference:
https://docs.microsoft.com/en-us/azure/time-series-insights/time-series-insights-update-create-environment

NEW QUESTION: 30
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.

Answer:

Explanation



Box 1: iothub1

The Azure IoT hub is named iothub1.

Box 2: azure-devices.net

The format of the device connection string looks like:

HostName={YourIoTHubName}.azure-devices.net;DeviceId=MyNodeDevice;SharedAccessKey={YourSharedA Box 1: device1 Device1 has a primary key of Uihuih76hbHb.

Reference:

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

NEW QUESTION: 31

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: B (LEAVE A REPLY)

Explanation

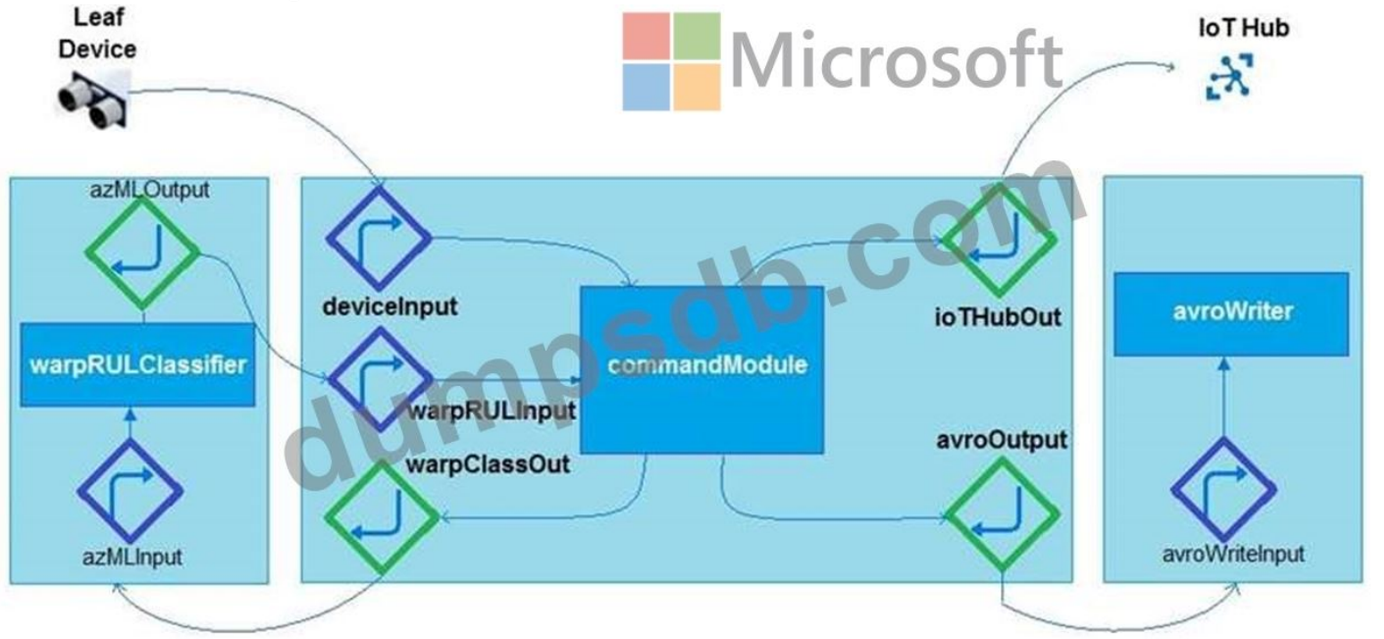
Note: IoT Hub is scaled and priced based on an allowed number of messages per day across all devices connected to that IoT Hub. If you exceed the allowed message threshold for your chosen tier and number of units, IoT Hub will begin rejecting new messages. To date, there is no built-in mechanism for 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: 32

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



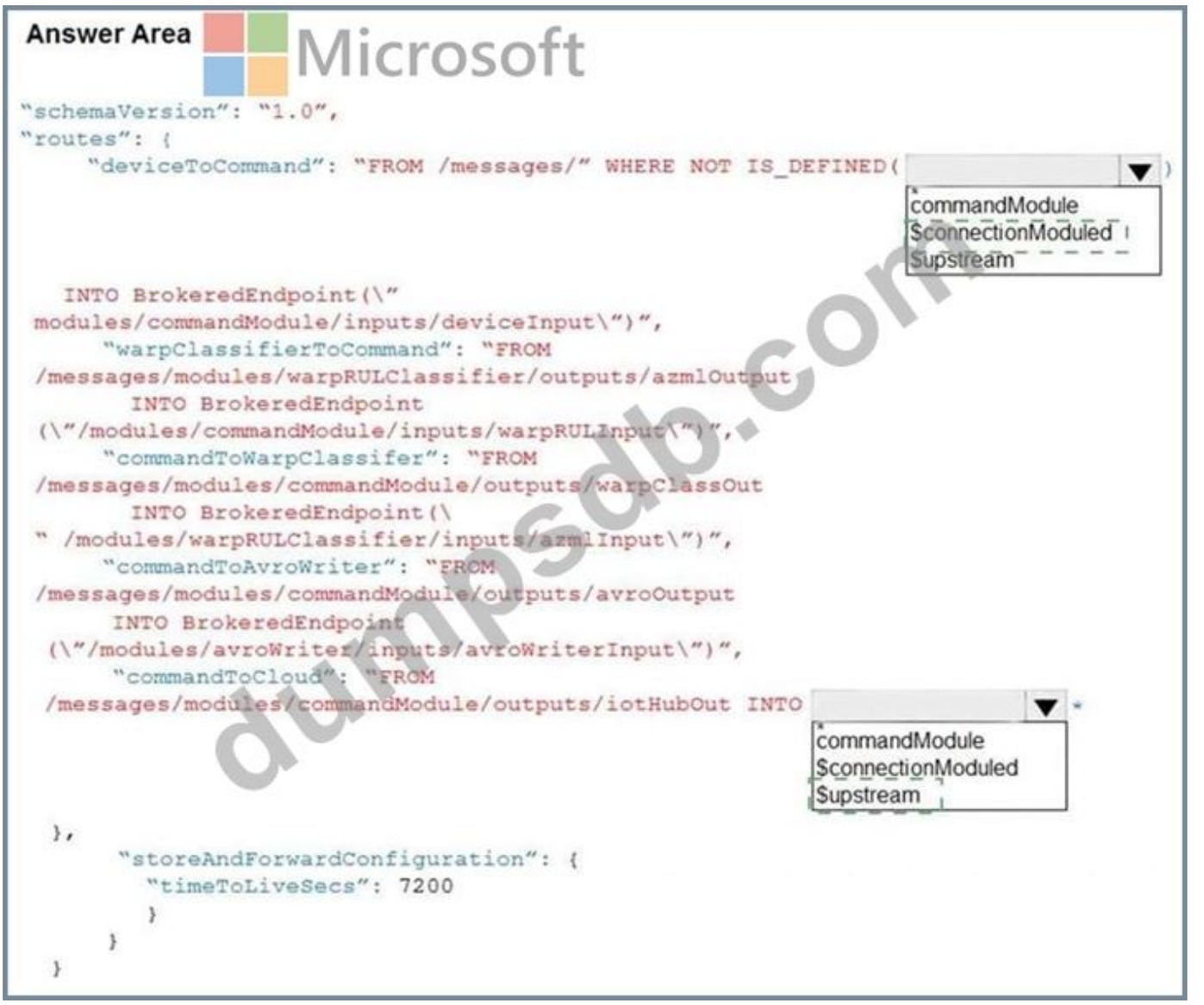
How should you complete the IoT Edge module routes? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

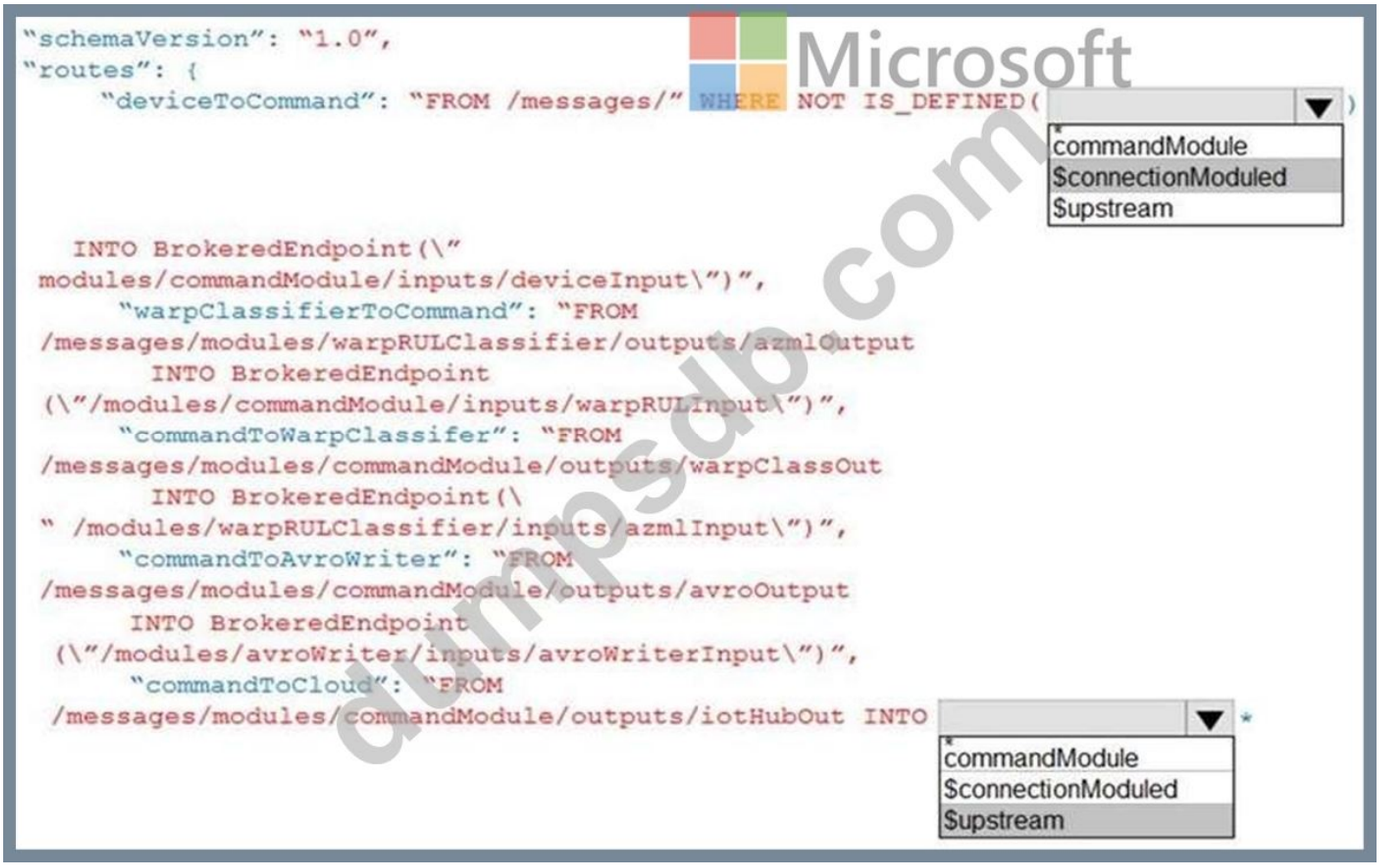
```
schemaVersion": "1.0",
routes": {
    "deviceToCommand": "FROM /messages/" WHERE NOT IS_DEFINED( [ * ▼ ]
                                                    commandModule
                                                    $connectionModuled
                                                    $upstream

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

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

Answer:



Explanation

Text, letter Description automatically generated



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: 33

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.

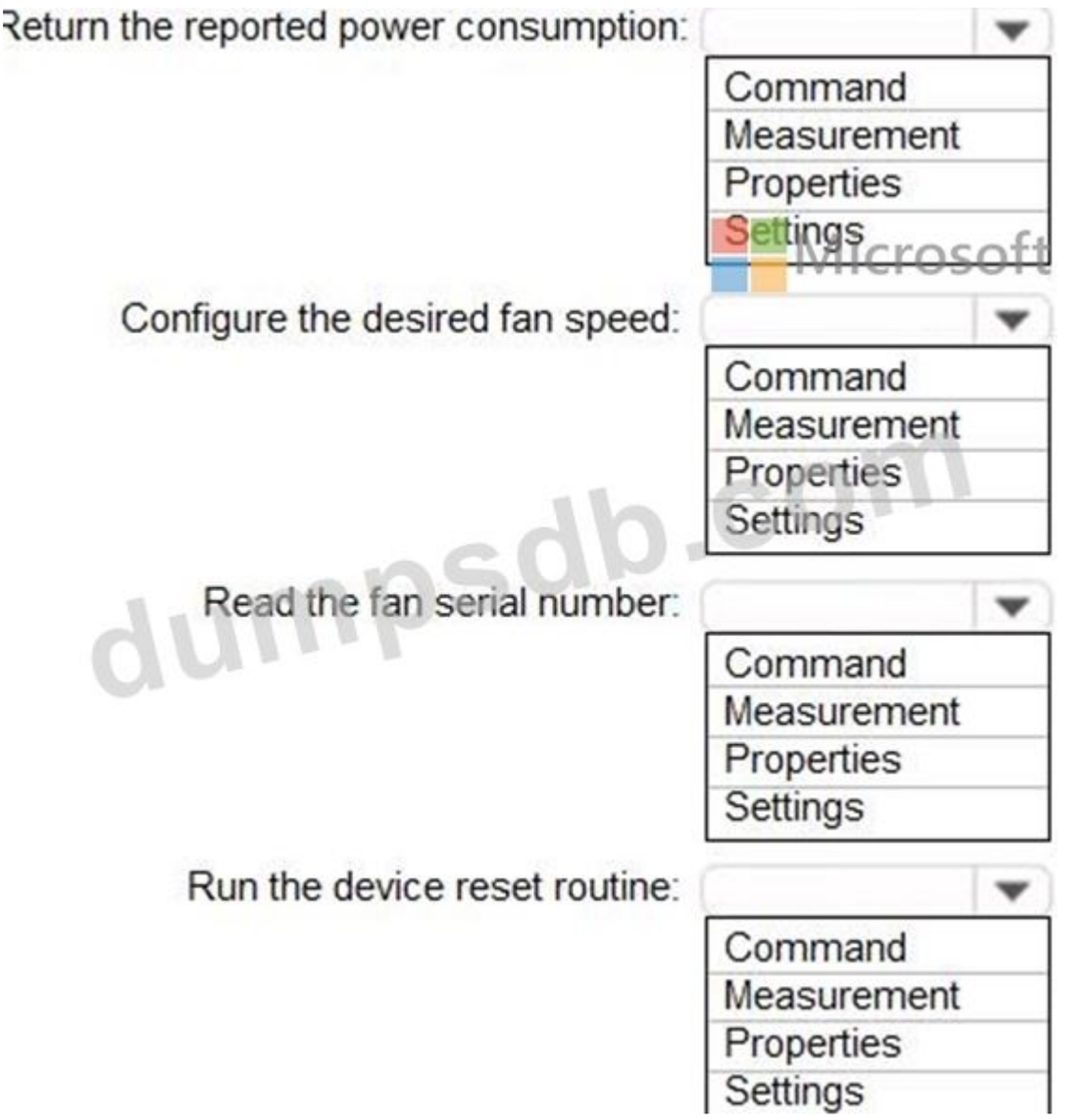
Configure the desired fan speed.

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.



Answer:

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: 34
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

NEW QUESTION: 35
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.
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 GET request to ContosoHub.azure-devices.net/devices/ContosoDevice1/ files/notifications.

Answer: (SHOW ANSWER)

Explanation

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}"

}

Reference:

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

NEW QUESTION: 36

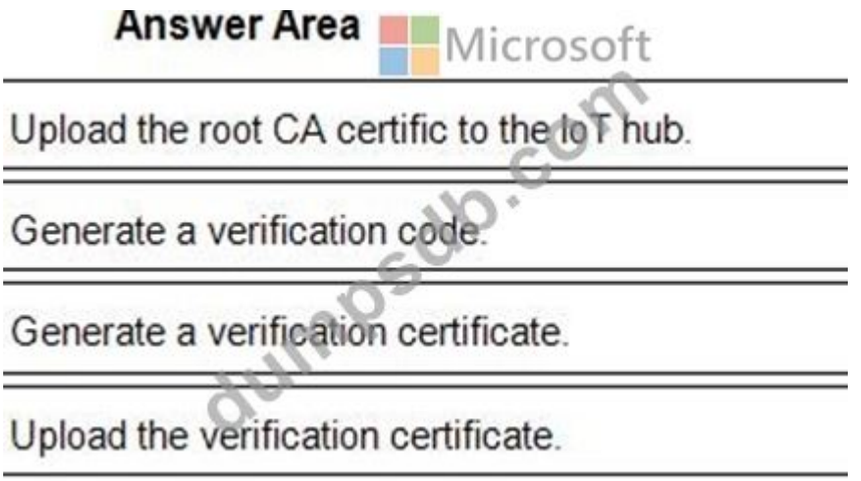
You have an Azure IoT solution that includes an Azure IoT hub.

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.

Answer:



1 - Upload the root CA certific 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: 37
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)
Explanation
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: 38
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: 39
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.

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: 40
You have an Azure IoT Central application that monitors 100 IoT devices.
You need to generate alerts when the temperature of a device exceeds 100 degrees. The solution must meet the following requirements:
* Minimize costs
* Minimize deployment time
What should you do?
A. Perform a data export to Azure Service Bus.
B. Create an email property in the device templates.

C. Perform a data export to Azure Blob storage and create an Azure function.
D. Create a rule that uses an email action.
Answer: (SHOW ANSWER)
Explanation
You can create rules in IoT Central that trigger actions, such as sending an email, in response to telemetrybased conditions, such as device temperature exceeding a threshold.
Reference:
https://docs.microsoft.com/en-us/azure/iot-central/core/howto-configure-rules-advanced

NEW QUESTION: 41
You have an Azure IoT solution that includes multiple Azure IoT hubs in different geographic locations and a single Device Provision Service instance.
You need to configure device enrollment to assign devices to the appropriate IoT hub based on the following requirements:
* The registration ID of the device
* The geographic location of the device
The load between the IoT hubs in the same geographic location must be balanced.
What should you use to assign the devices to the IoT hubs?
A. Static configuration (via enrollment list only)
B. Lowest latency
C. Evenly weighted distribution
D. Custom (Use Azure Function)
Answer: (SHOW ANSWER)
Explanation
Set the Device Provisioning Service allocation policy
The allocation policy is a Device Provisioning Service setting that determines how devices are assigned to an IoT hub. There are three supported allocation policies:
* Lowest latency: Devices are provisioned to an IoT hub based on the hub with the lowest latency to the
* device.
* Evenly weighted distribution (default): Linked IoT hubs are equally likely to have devices provisioned to them. This is the default setting. If you are provisioning devices to only one IoT hub, you can keep this setting.
* Static configuration via the enrollment list: Specification of the desired IoT hub in the enrollment list takes priority over the Device Provisioning Service-level allocation policy.
Reference:
https://docs.microsoft.com/en-us/azure/iot-dps/tutorial-provision-multiple-hubs

NEW QUESTION: 42
How should you complete the GROUP BYclause 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)
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.
Incorrect Answers:
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
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 questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
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 device fleet and issue alerts for 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 supports 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.

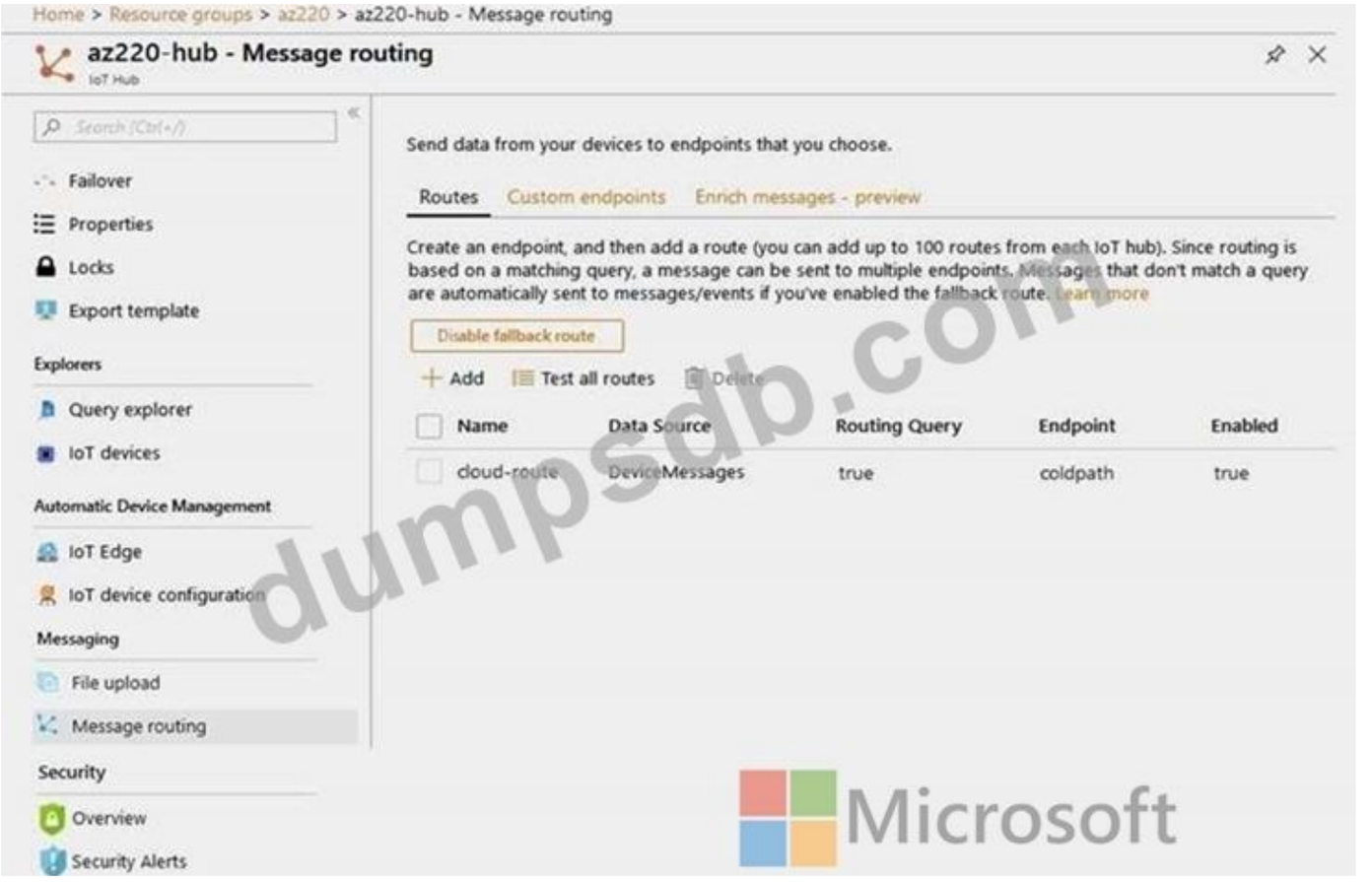
Requirements. Throttle and Quotas

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: 43

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

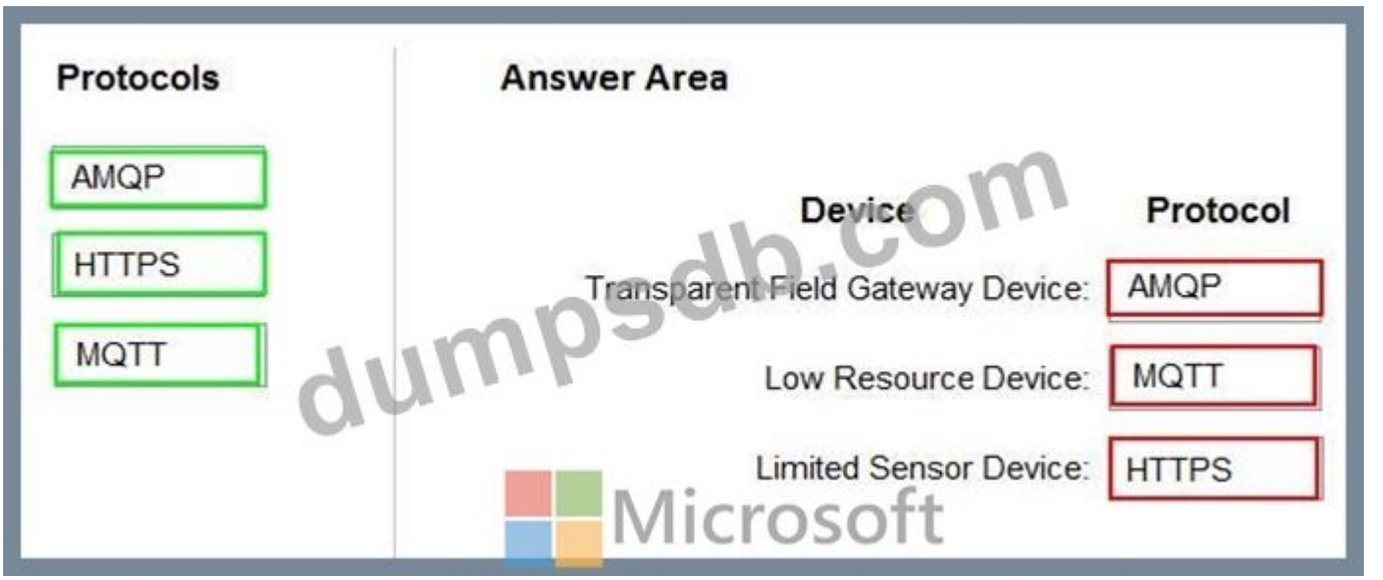
HTTPS

MQTT

Answer Area

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

Answer:



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

NEW QUESTION: 44
You need to visualize Azure IoT Hub telemetry data by using Microsoft Power BI.
Which service should you connect to the IoT hub?
A. Azure Event Grid
B. SendGrid
C. Azure Stream Analytics
D. Azure Notification Hubs
Answer: C (LEAVE A REPLY)
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: 45
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
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.

NEW QUESTION: 46

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: 47

You have an Azure IoT hub.

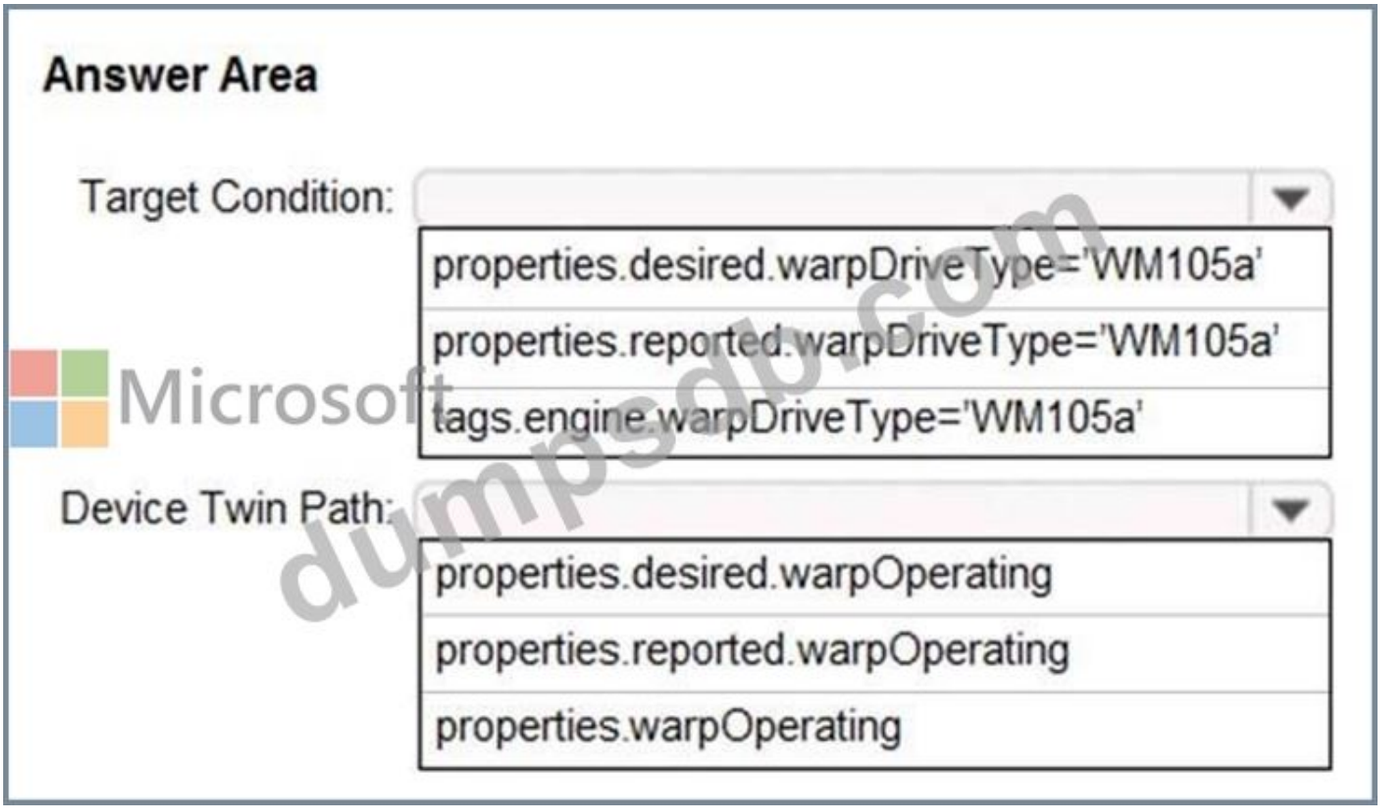
You plan to deploy 1,000 IoT devices by using automatic device management.

The device twin is shown below.

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:

Answer Area

Explanation:
Box 1: tags.engine.warpDriveType='VM105a'
Use tags to target twins. Before you create a configuration, you must specify which devices or modules you want to affect. Azure IoT Hub identifies devices and using tags in the device twin, and identifies modules using tags in the module twin.
Box 2: properties.desired.warpOperating
The twin path, which is the path to the JSON section within the twin desired properties that will be set.
For example, you could set the twin path to properties.desired.chiller-water and then provide the following JSON content:
{
"temperature": 66,
"pressure": 28
}
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-automatic-device-management

NEW QUESTION: 48
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

NEW QUESTION: 49
You have an existing Azure IoT hub.
You need to connect physical IoT devices to the IoT hub.
You are connecting the devices through a firewall that allows only port 443 and port 80.
Which three communication protocols can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. MQTT over WebSocket
B. AMQP
C. AMQP over WebSocket
D. MQTT
E. HTTPS
Answer: A,C,E (LEAVE A REPLY)
MQTT over WebSockets, AMQP over WebSocket, and HTTPS use port 443.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-protocols

NEW QUESTION: 50
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You are developing a custom Azure IoT Edge module.
The module needs to identify the device ID of the local device.
Solution: You configure the module to read the IOTEDGE_DEVICEID environment variable.
Does this meet the goal?
A. Yes
B. No

Answer: B (LEAVE A REPLY)

Explanation

The Azure ID of the current device is available on the IOTEDGE_DEVICEID environment variable.

Instead read the device ID of the device twin.

Note: Device twins are JSON documents that store device state information including metadata, configurations, and conditions. Azure IoT Hub maintains a device twin for each device that you connect to IoT Hub.

Device identity properties. The root of the device twin JSON document contains the read-only properties from the corresponding device identity stored in the identity registry.

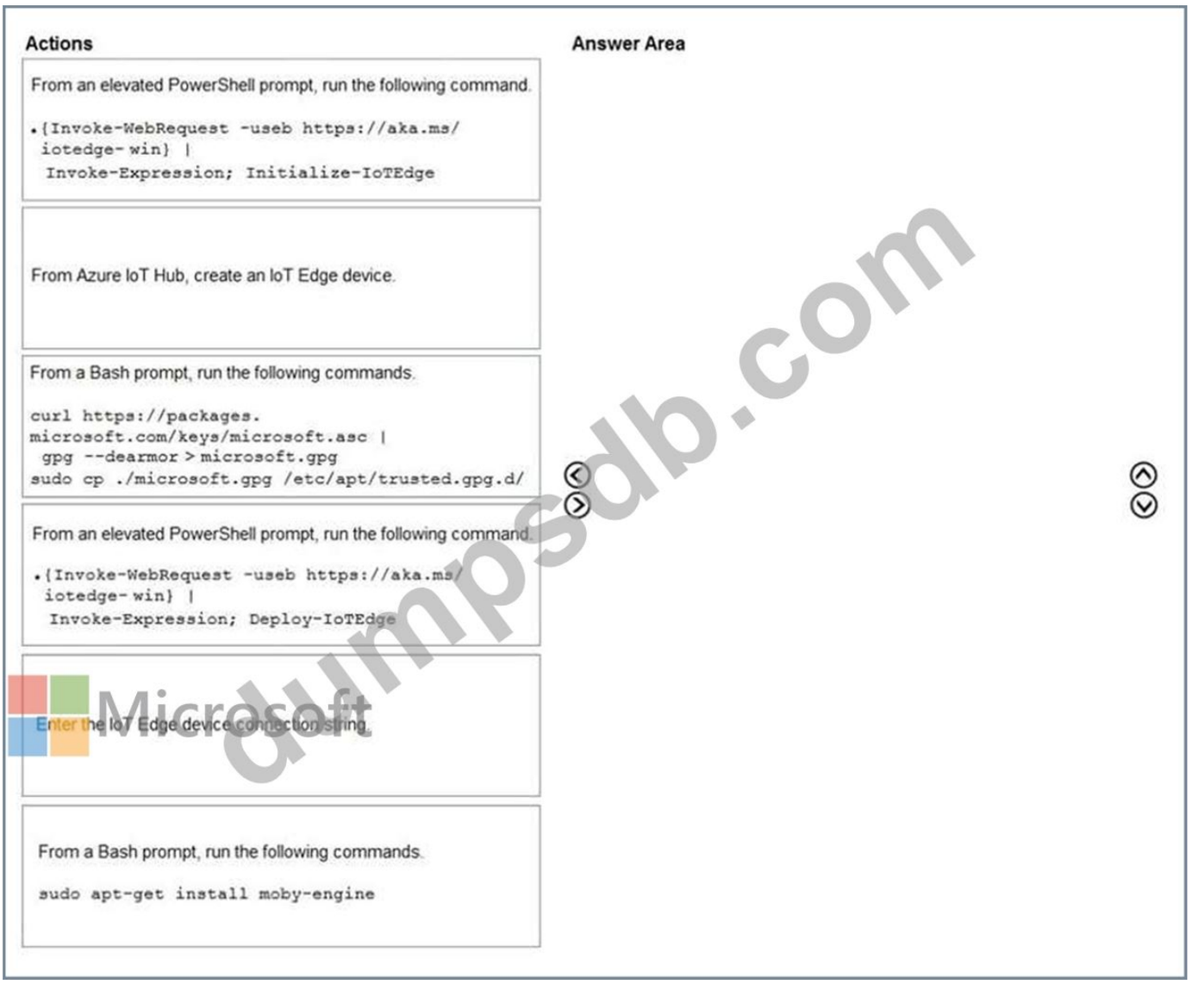
Reference:

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

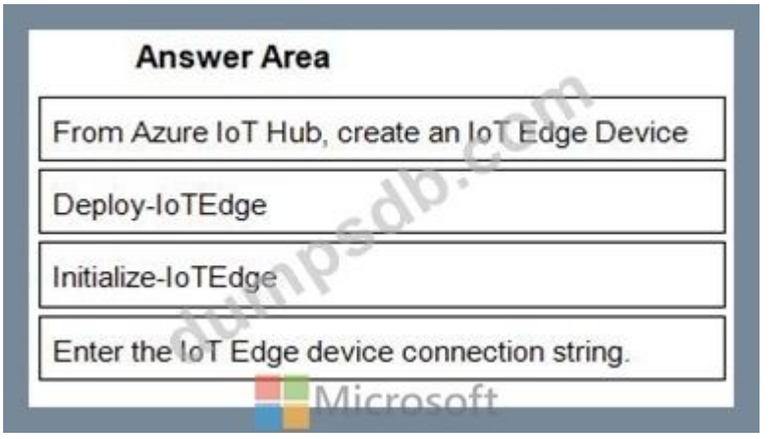
NEW QUESTION: 51

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

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



Answer:



1 - From Azure IoT Hub, create an IoT Edge Device

2 - Deploy-IoTEdge

3 - Initialize-IoTEdge

4 - Enter the IoT Edge device connection string.

Reference:

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

NEW QUESTION: 52

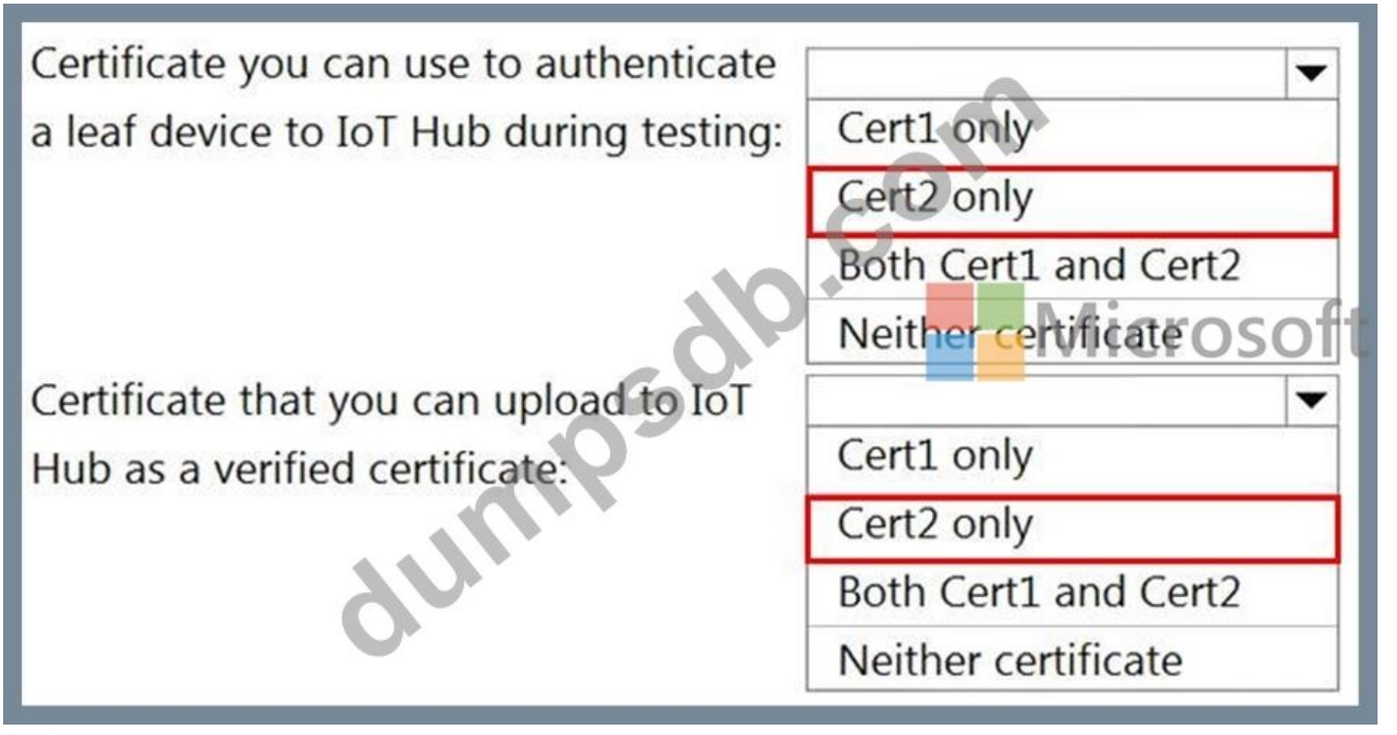
You are planning a proof of concept (POC) that will use an Azure IoT hub.

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.

Answer:



Reference:

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

NEW QUESTION: 53

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

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

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

You have the following query for the job.

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

You plan to increase the streaming unit count to 12.

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

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

Does this meet the goal?

A. Yes

B. No

Answer: B (LEAVE A REPLY)

Explanation

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

Reference:

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

NEW QUESTION: 54

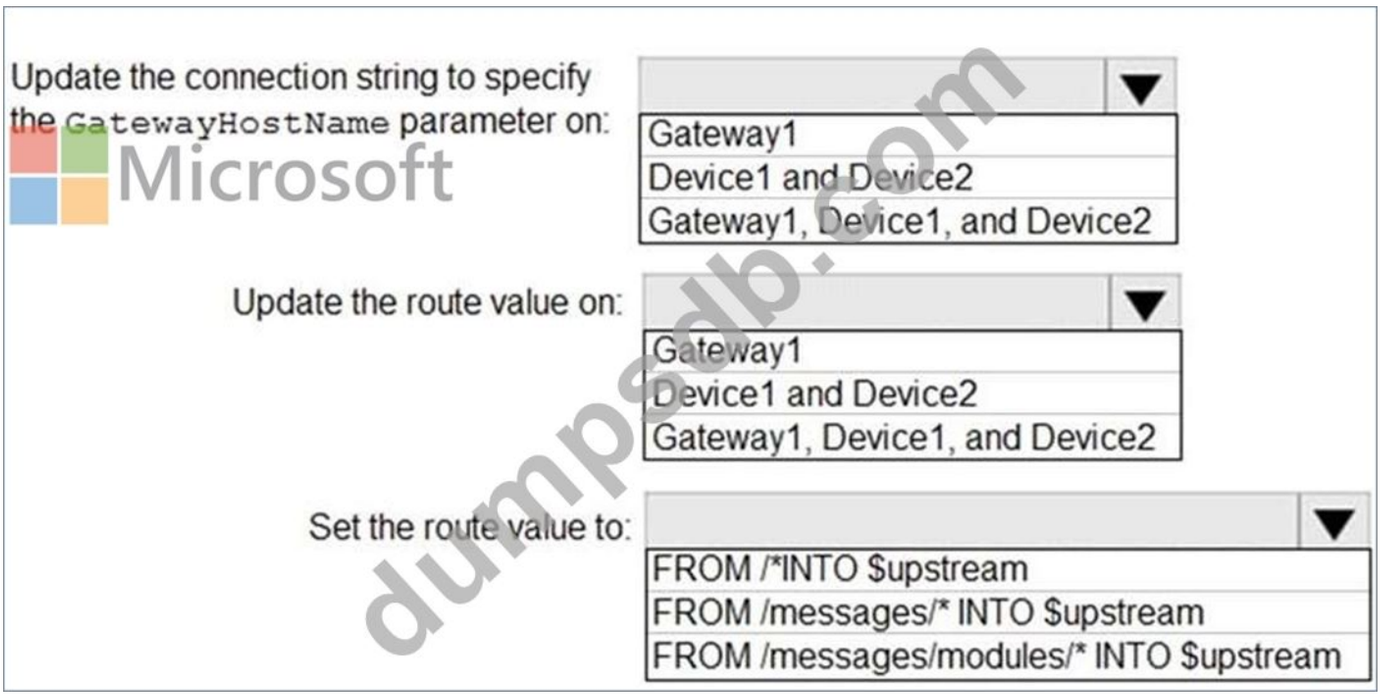
You have an Azure subscription that contains an Azure IoT hub and two IoT devices named Device1 and Device2.

You plan to deploy an Azure IoT Edge gateway device named Gateway1.

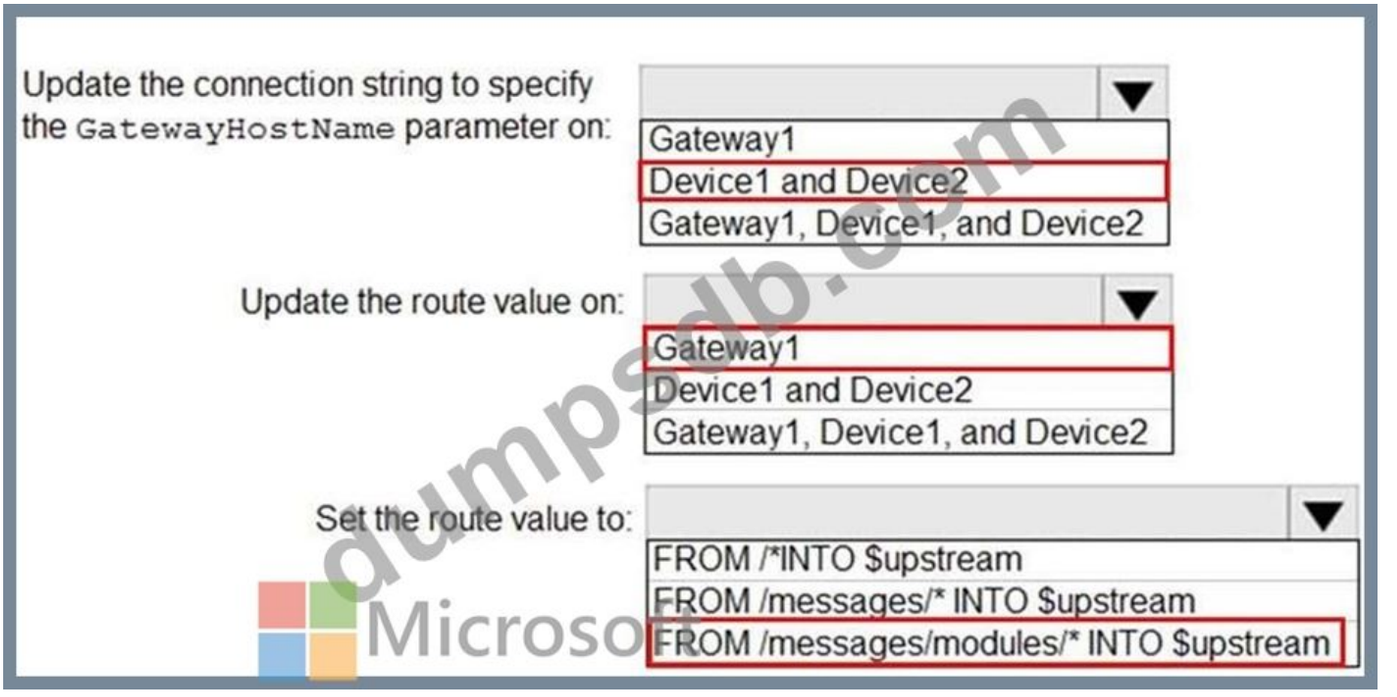
You need to ensure that all device-to-cloud messages and twin change notifications from Device1 and Device2 to the IoT hub are routed by using Gateway1.

What tasks should you perform to configure the devices? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



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

NEW QUESTION: 55

You have an Azure IoT solution that includes an Azure IoT hub, 100 Azure IoT Edge devices, and 500 leaf devices.

You need to perform a key rotation across the devices.

Which three types of entities should you update? Each Answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. the $edgeHub module identity

B. the $edgeAgent module identity

C. the leaf module identities
D. the IoT Edge device identities
E. the iothubowner policy credentials
F. the leaf device identities
Answer: (SHOW ANSWER)
Explanation
To get authorization to connect to IoT Hub, devices and services must send security tokens signed with either a shared access or symmetric key. These keys are stored with a device identity in the identity registry.
An IoT Hub identity registry can be accessed like a dictionary, by using the deviceId or moduleId as the key.
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/iot-dps/how-to-control-access
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-identity-registry

NEW QUESTION: 56
You have an Azure subscription that contains an Azure IoT hub and two Azure IoT Edge devices named Device1 and Device2.
You need to ensure that the IoT hub only accepts connections from Device1 and Device2.
What should you configure?
A. a private endpoint connection
B. Azure API Management
C. Azure Active Directory (Azure AD) Identity Protection
D. a gateway device
Answer: A (LEAVE A REPLY)
Explanation
Ingress connectivity to IoT Hub using Azure Private Link.
A private endpoint is a private IP address allocated inside a customer-owned VNet via which an Azure resource is reachable. Through Azure Private Link, you can set up a private endpoint for your IoT hub to allow services inside your VNet to reach IoT Hub without requiring traffic to be sent to IoT Hub's public endpoint.
Similarly, your on-premises devices can use Virtual Private Network (VPN) or ExpressRoute peering to gain connectivity to your VNet and your IoT Hub (via its private endpoint). As a result, you can restrict or completely block off connectivity to your IoT hub's public endpoints by using IoT Hub IP filter or the public network access toggle. This approach keeps connectivity to your Hub using the private endpoint for devices.
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/virtual-network-support

NEW QUESTION: 57
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 correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. The ipV4tag 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 Monitor, troubleshoot, and optimize IoT solutions 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": {
    "iotEdge": false
  }
}
```

Existing Environment. Azure Stream Analytics
Each room will have between three to five sensors that will generate readings that are sent to a single IoT gateway device. The IoT gateway device will forward all the readings to iothub1 at intervals of between 10 and
60 seconds.
You plan to use a gateway pattern so that each IoT gateway device will have its own IoT Hub device identity.
You draft the following query, which is missing the GROUP BYclause.
SELECT
AVG(temperature),
System.TimeStamp() AS AsaTime
FROM
Iothub
You plan to use a 30-second period to calculate the average temperature reading of the sensors.
You plan to minimize latency between the condition reported by the sensors and the corresponding alert issued by the Stream Analytics job.
Existing Environment. Device Messages
The IoT gateway devices will send messages that contain the following JSON data whenever the temperature exceeds a specified threshold.

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


The levelproperty will be used to route the messages to an Azure Service Bus queue endpoint named criticalep.
Existing Environment. Issues
You discover connectivity issues between the IoT gateway devices and iothub1, which cause IoT devices to lose connectivity and messages.
Requirements. Planning Changes
Contoso plans to make the following changes:
* Use Stream Analytics to process and view data.
* Use Azure Time Series Insights to visualize data.
* Implement a system to sync device statuses and required settings.
* Add extra information to messages by using message enrichment.
* Create a notification system to send an alert if a condition exceeds a specified threshold.
* Implement a system to identify what causes the intermittent connection issues and lost messages.

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

NEW QUESTION: 58
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: B (LEAVE A REPLY)
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: 59
You have an Azure subscription that contains a resource group named RG1.
You need to deploy the Device Provisioning Service. The solution must ensure that the Device Provisioning Service can accept new device enrollments.
You create a Device Provisioning Service instance.
Which two actions should you perform next? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. From the Linked IoT hubs blade of the Device Provisioning Service, link an Azure IoT hub.
B. From the Azure portal, create a new Azure IoT hub.
C. From the Manage allocation policy blade of the Device Provisioning Service, configure an allocation policy.
D. From the Certificates blade of the Device Provisioning Service, upload an X.509 certificate to the Device Provisioning Service.
Answer: A,C (LEAVE A REPLY)

A: The Device Provisioning Service can only provision devices to IoT hubs that have been linked to it.
C: Allocation policy. The service-level setting that determines how Device Provisioning Service assigns devices to an IoT hub. There are three supported allocation policies:
* Lowest latency: devices are provisioned to an IoT hub with the lowest latency to the device.
* Evenly weighted distribution
* Static configuration via the enrollment list
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/iot-dps/concepts-service

NEW QUESTION: 60
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)
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

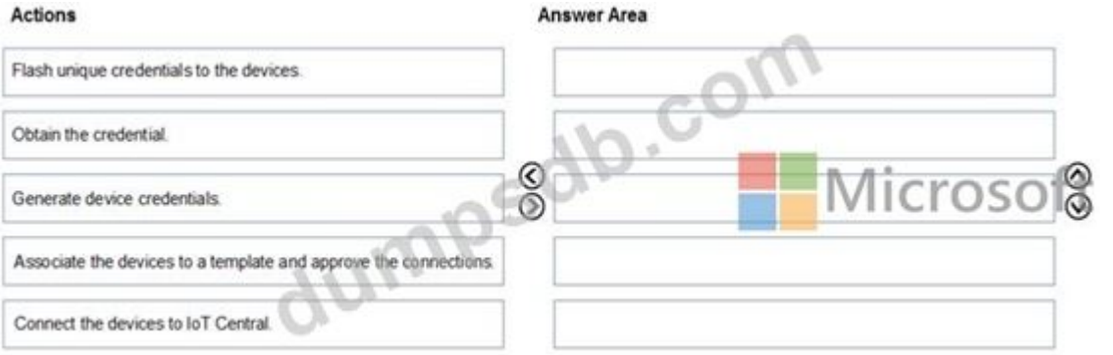
NEW QUESTION: 61
You have an Azure IoT solution that includes a standard tier Azure IoT hub and an IoT device.
The device sends one 100-KB device-to-cloud message every hour.
You need to calculate the total daily message consumption of the device. What is the total daily message consumption of the device?
A. 24
B. 600
C. 2,400
D. 4,800
Answer: B (LEAVE A REPLY)
Explanation
100 KB * 24 is around 2,400 bytes.
The 100 KB message is divided into 4 KB blocks, and it is billed for 25 messages. 25 times 24 is 600 Note: The maximum message size for messages sent from a device to the cloud is 256 KB.

These messages are metered in 4 KB blocks for the paid tiers so for instance if the device sends a 16 KB message via the paid tiers it will be billed as 4 messages.
Reference:
https://azure.microsoft.com/en-us/pricing/details/iot-hub/

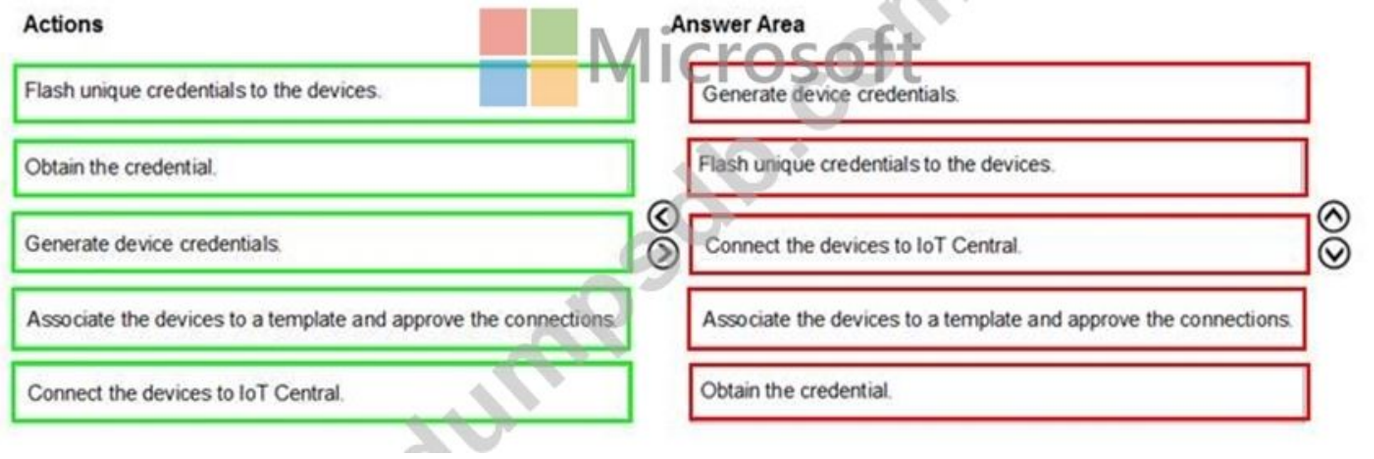
NEW QUESTION: 62
You have an Azure IoT solution that includes an Azure IoT Hub named Hub1 and an Azure IoT Edge device named Edge1. Edge1 connects to Hub1.
You need to deploy a temperature module to Edge1.
What should you do?
A. From the Azure portal, navigate to Hub1 and select IoT Edge. Select Edge1, 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 Bush 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 Bush 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: 63
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.



Answer:



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: 64
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: 65
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/iotedgedev:2.0
D. mycr.azurecr.io/temperature-module:latest
E. mcr.microsoft.com/azureiotedge-hub:1.0
Answer: B,D,E (LEAVE A REPLY)
Each IoT Edge device runs at least two modules: $edgeAgent and $edgeHub, which are part of the IoT Edge runtime. IoT Edge device can run multiple additional modules for any number of processes. Use a deployment manifest to tell your device which modules to install and how to configure them to work together.
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/module-composition
Process and manage data
Testlet 1
Case Study
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.
Overview
A company named Contoso, Ltd. is creating a building monitoring system that will monitor the temperature, humidity, and light level at various points in a building's internal structure.

Contoso will test the system at a single building located in the United Kingdom. The building has 25 floors.
Each floor has 15 rooms.
Existing Environment. Current State of Development
Contoso produces a set of Bluetooth sensors that read the temperature and humidity. The sensors connect to IoT gateway devices that relay the data.
All the IoT gateway devices connect to an Azure IoT hub named iothub1.
Existing Environment. Device Twin
You plan to implement device twins by using the following JSON sample.

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

Existing Environment. Azure Stream Analytics
Each room will have between three to five sensors that will generate readings that are sent to a single IoT gateway device. The IoT gateway device will forward all the readings to iothub1 at intervals of between 10 and
60 seconds.
You plan to use a gateway pattern so that each IoT gateway device will have its own IoT Hub device identity.
You draft the following query, which is missing the GROUP BYclause.
SELECT
AVG(temperature),
System.TimeStamp() AS AsaTime
FROM
Iothub
You plan to use a 30-second period to calculate the average temperature reading of the sensors.
You plan to minimize latency between the condition reported by the sensors and the corresponding alert issued by the Stream Analytics job.
Existing Environment. Device Messages
The IoT gateway devices will send messages that contain the following JSON data whenever the temperature exceeds a specified threshold.

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


The levelproperty will be used to route the messages to an Azure Service Bus queue endpoint named criticalep.
Existing Environment. Issues
You discover connectivity issues between the IoT gateway devices and iothub1, which cause IoT devices to lose connectivity and messages.
Requirements. Planned Changes
Contoso plans to make the following changes:
* Use Stream Analytics to process and view data.
* Use Azure Time Series Insights to visualize data.
* Implement a system to sync device statuses and required settings.
* Add extra information to messages by using message enrichment.
* Create a notification system to send an alert if a condition exceeds a specified threshold.
* Implement a system to identify what causes the intermittent connection issues and lost messages.

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

NEW QUESTION: 66
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 Bush 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 Bush 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": {
    "iotEdge": false
  }
}
```

Existing Environment. Azure Stream Analytics
Each room will have between three to five sensors that will generate readings that are sent to a single IoT gateway device. The IoT gateway device will forward all the readings to iothub1 at intervals of between 10 and
60 seconds.
You plan to use a gateway pattern so that each IoT gateway device will have its own IoT Hub device identity.
You draft the following query, which is missing the GROUP BYclause.
SELECT
AVG(temperature),
System.TimeStamp() AS AsaTime
FROM
Iothub
You plan to use a 30-second period to calculate the average temperature reading of the sensors.
You plan to minimize latency between the condition reported by the sensors and the corresponding alert issued by the Stream Analytics job.
Existing Environment. Device Messages
The IoT gateway devices will send messages that contain the following JSON data whenever the temperature exceeds a specified threshold.

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


The levelproperty will be used to route the messages to an Azure Service Bus queue endpoint named criticalep.
Existing Environment. Issues
You discover connectivity issues between the IoT gateway devices and iothub1, which cause IoT devices to lose connectivity and messages.
Requirements. Planning Changes
Contoso plans to make the following changes:
* Use Stream Analytics to process and view data.
* Use Azure Time Series Insights to visualize data.
* Implement a system to sync device statuses and required settings.
* Add extra information to messages by using message enrichment.
* Create a notification system to send an alert if a condition exceeds a specified threshold.
* Implement a system to identify what causes the intermittent connection issues and lost messages.

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

NEW QUESTION: 67
You use Azure Security Center in an Azure IoT solution.
You need to exclude some security events. The solution must minimize development effort. What should you do?
A. Create an Azure function to filter security messages.
B. Add a configuration to the code of the physical IoT device.
C. Add configuration details to the device twin object.
D. Create an azureiotsecurity module twin and add configuration details to the module twin object.
Answer: D (LEAVE A REPLY)
Explanation
Properties related to every Azure Security Center for IoT security agent are located in the agent configuration object, within the desired properties section, of the azureiotsecurity module.
To modify the configuration, create and modify this object inside the azureiotsecurity module twin identity.
Note: Azure Security Center for IoT's security agent twin configuration object is a JSON format object. The configuration object is a set of controllable properties that you can define to control the behavior of the agent.
These configurations help you customize the agent for each scenario required. For example, automatically excluding some events, or keeping power consumption to a minimal level are possible by configuring these properties.
Reference:
https://docs.microsoft.com/en-us/azure/asc-for-iot/how-to-agent-configuration

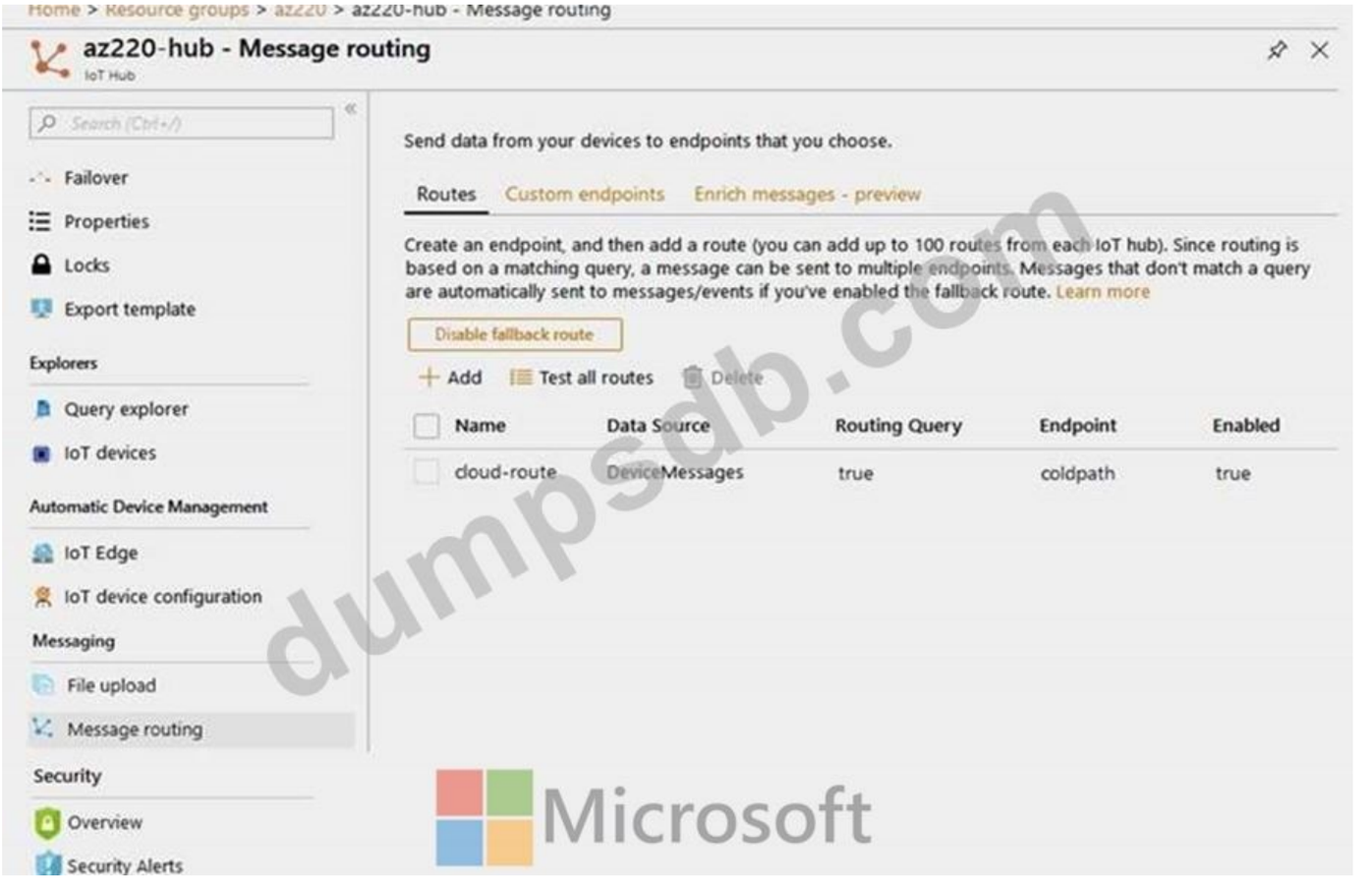
NEW QUESTION: 68
You need to configure Stream Analytics to meet the POV requirements.
What are two ways to achieve the goal? Each Answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. From IoT Hub, create a custom event hub endpoint, and then configure the endpoint as an input to Stream Analytics.
B. Create a Stream Analytics module, and then deploy the module to all IoT Edge devices in the fleet.

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

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

Answer: A,C (LEAVE A REPLY)

Explanation



NEW QUESTION: 69

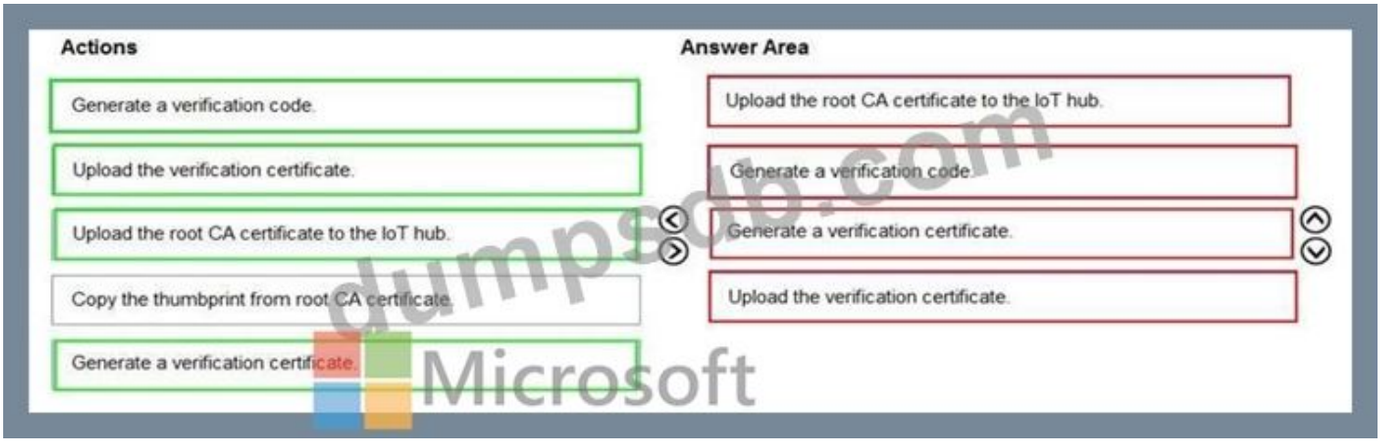
You have an Azure IoT solution that includes an Azure IoT hub.

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.

Answer:



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

NEW QUESTION: 70
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

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.	○	●

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: 71

You are troubleshooting an Azure IoT hub.

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

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

A. Routes

B. DeviceTelemetry

C. Connections

D. C2DCommands

Answer: B (LEAVE A REPLY)

Explanation

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

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

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

Reference:

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

NEW QUESTION: 72

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

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

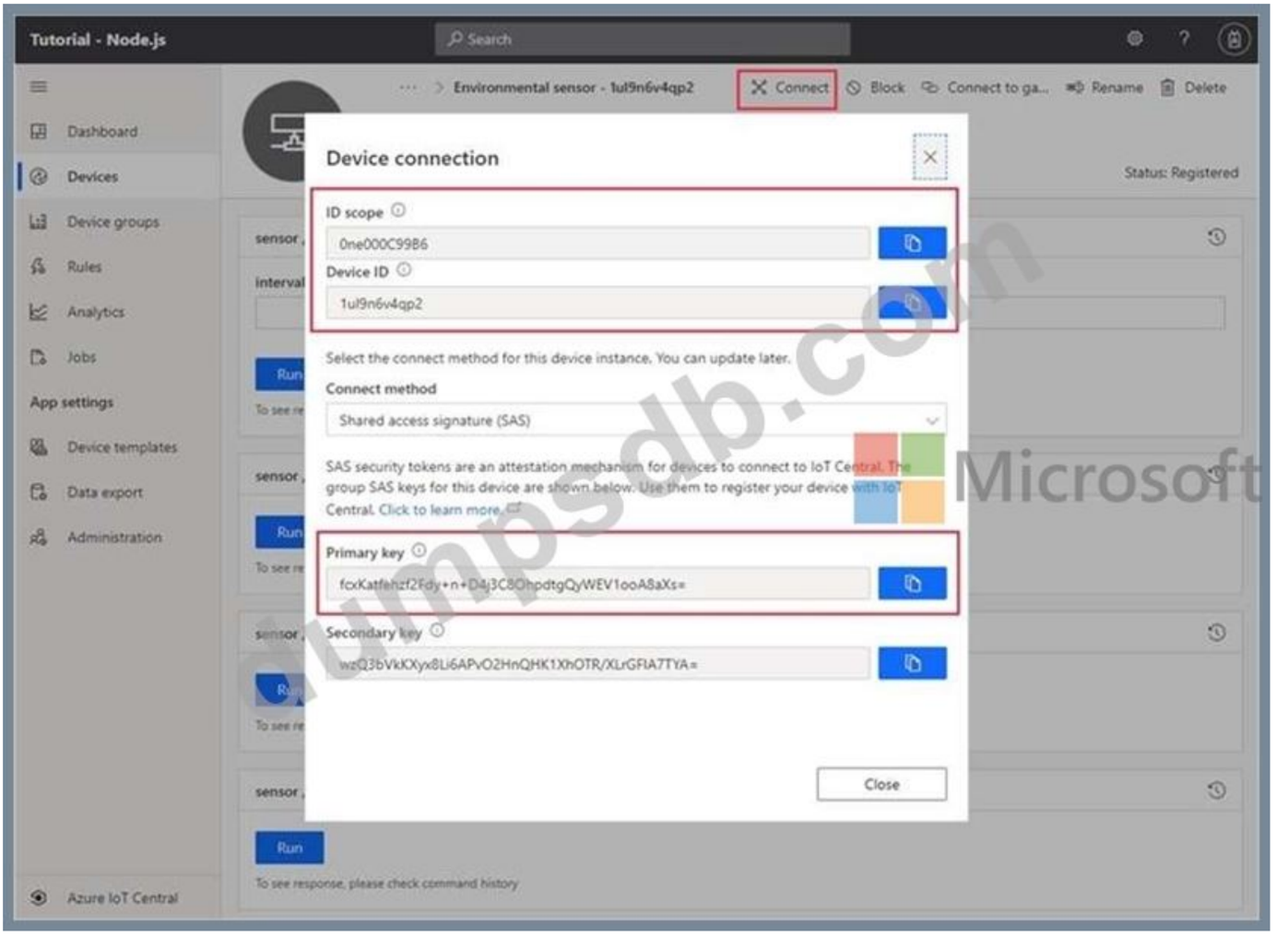
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Answer:

1 - Enable Azure Security Center for IoT

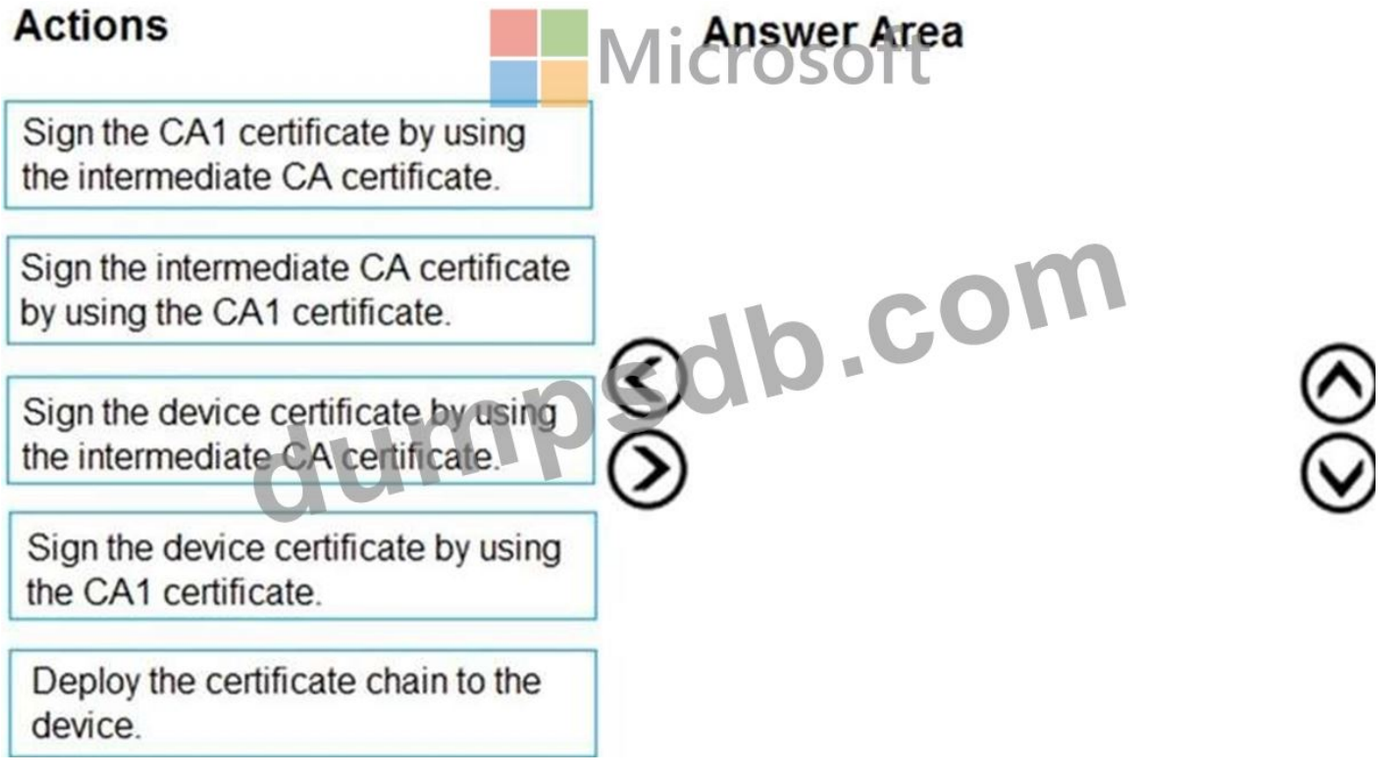
2 - Select a device security group
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/asc-for-iot/how-to-security-data-access
https://docs.microsoft.com/en-us/rest/api/securitycenter/devicesecuritygroups/createorupdate

NEW QUESTION: 73
You have an Azure IoT Central application.
You need to connect an IoT device to the application.
Which two settings do you require in IoT Central to configure the device? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. Group SAS Primary Key
B. the IoT hub name
C. Scope ID
D. Application Name
E. Device ID
Answer: C,E (LEAVE A REPLY)
In your Azure IoT Central application, add a real device to the device template
1. On the Devices page, select the Environmental sensor device template.
2. Select + New.
3. Make sure that Simulated is Off. Then select Create.
Click on the device name, and then select Connect. Make a note of the device connection information on the Device Connection page - ID scope, Device ID, and Primary key. You need these values when you create your device code:



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

NEW QUESTION: 74
You have an Azure IoT hub named Hub1 and a root certification authority (CA) named CA1. Hub1 is configured to use X.509 certificate device authentication.
You and a custom manufacturing partner complete a proof of possession flow.
You plan to deploy IoT devices manufactured by the custom manufacturing partner. Each device will have a certificate generated by an intermediate C You need to ensure that the custom devices can connect successfully to Hub1.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

1 - Sign the intermediate CA certificate by using the CA1 certificate.
2 - Sign the device certificate by using the intermediate CA
3 - Deploy the certificate chain to the device.
Reference:
https://docs.microsoft.com/en-us/azure/iot-dps/concepts-x509-attestation

NEW QUESTION: 75
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)
In general, deprovisioning a device involves two steps:
* 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.
* 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/en-us/azure/iot-dps/how-to-unprovision-devices

NEW QUESTION: 76
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have 20 IoT devices deployed across two floors of a building. The devices on the first floor must be set to 60 degrees. The devices on the second floor must be set to 80 degrees.
The device twins are configured to use a tag that identifies the floor on which the twins are located.
You create the following automatic configuration for the devices on the first floor.

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

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

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

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

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

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

Does this meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/module-deployment-monitoring?view=iotedge-2020-11
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-automatic-device-management-cli

NEW QUESTION: 77
You have an Azure subscription that contains a resource group named RG1.
You need to deploy the Device Provisioning Service. The solution must ensure that the Device Provisioning Service can accept new device enrollments.
You create a Device Provisioning Service instance.
Which two actions should you perform next? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. From the Linked IoT hubs blade of the Device Provisioning Service, link an Azure IoT hub.
B. From the Azure portal, create a new Azure IoT hub.
C. From the Manage allocation policy blade of the Device Provisioning Service, configure an allocation policy.
D. From the Certificates blade of the Device Provisioning Service, upload an X.509 certificate to the Device Provisioning Service.
Answer: D (LEAVE A REPLY)
Explanation
A: The Device Provisioning Service can only provision devices to IoT hubs that have been linked to it.
C: Allocation policy. The service-level setting that determines how Device Provisioning Service assigns devices to an IoT hub. There are three supported allocation policies:
Lowest latency: devices are provisioned to an IoT hub with the lowest latency to the device.
Evenly weighted distribution Static configuration via the enrollment list Reference:
https://docs.microsoft.com/bs-latn-ba/azure/iot-dps/concepts-service

NEW QUESTION: 78

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/iotedgedev:2.0
D. mycr.azurecr.io/temperature-module:latest
E. mcr.microsoft.com/azureiotedge-hub:1.0
Answer: B,D,E (LEAVE A REPLY)
Each IoT Edge device runs at least two modules: $edgeAgent and $edgeHub, which are part of the IoT Edge runtime. IoT Edge device can run multiple additional modules for any number of processes. Use a deployment manifest to tell your device which modules to install and how to configure them to work together.
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/module-composition

NEW QUESTION: 79
You need to configure Stream Analytics to meet the POV requirements.
What are two ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. Route telemetry to an Azure Blob storage custom endpoint, and then configure the Blob storage as a reference input for Stream Analytics.
B. Create an input in Stream Analytics that uses the built-in events endpoint of IoT Hub as the source.
C. Create a Stream Analytics module, and then deploy the module to all IoT Edge devices in the fleet.
D. From IoT Hub, create a custom event hub endpoint, and then configure the endpoint as an input to Stream Analytics.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 80
You have an Azure IoT solution that includes a standard tier Azure IoT hub and an IoT device.
The device sends one 100-KB device-to-cloud message every hour.
You need to calculate the total daily message consumption of the device.
What is the total daily message consumption of the device?
A. 24
B. 600
C. 2,400

D. 4,800

Answer: B (LEAVE A REPLY)

100 KB * 24 is around 2,400 bytes.

The 100 KB message is divided into 4 KB blocks, and it is billed for 25 messages. 25 times 24 is 600 Note: The maximum message size for messages sent from a device to the cloud is 256 KB. These messages are metered in 4 KB blocks for the paid tiers so for instance if the device sends a 16 KB message via the paid tiers it will be billed as 4 messages.

Reference:

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

NEW QUESTION: 81

During the POV phase, telemetry from IoT Hub stops flowing to the hot path. The cold path continues to work.

What should you do to restore the hot path?

A. Modify cold-route to send only some telemetry data to the cold path.

B. Create an explicit route for the hot path.

C. Run the Test all routes action.

D. Disable the fallback route.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 82

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 schedule an IoT Hub job to update the twin tags and you query for job progress.

Does this meet the goal?

A. yes

B. No

Answer: B (LEAVE A REPLY)

Explanation

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

Note: IoT Hub provides three options for device apps to expose functionality to a back-end app:

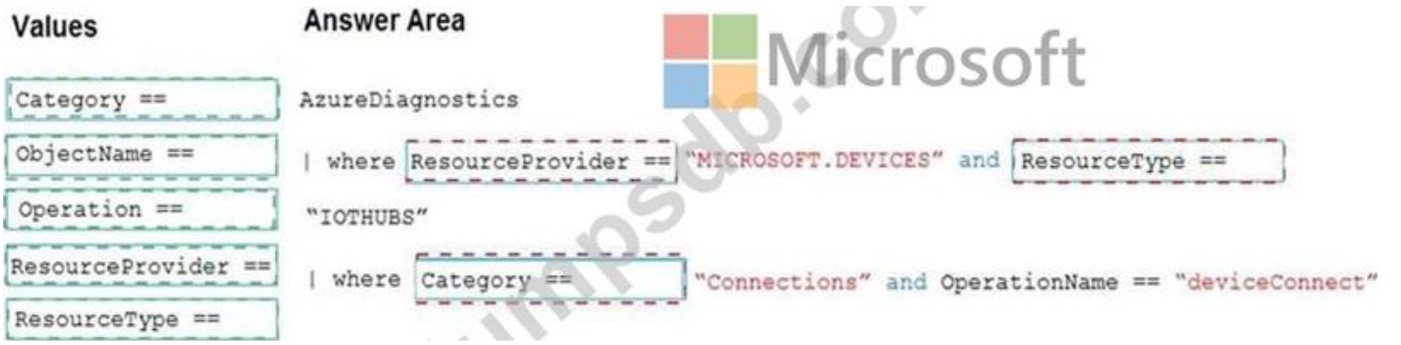
* Twin's desired properties for long-running commands intended to put the device into a certain desired state. For example, set the telemetry send interval to 30 minutes.

* 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: 83
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: 84
You are troubleshooting device connections to and disconnections from an Azure IoT hub.
You configure diagnostic logging for the IoT hub to send to Log Analytics.
You need to generate a report that displays the device connection and disconnection events.
How should you complete the query? To answer, drag the appropriate values to the correct targets. 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.

Answer:



Explanation

Graphical user interface, text Description automatically generated

Box 1: ResourceProvider ==

Query to monitor your IoT hub connectivity Errors: Identify device connection errors.

AzureDiagnostics

| where ResourceProvider == "MICROSOFT.DEVICES" and ResourceType == "IOTHUBS"

| where Category == "Connections" and Level == "Error"

Box 2: ResourceType ==

Box 3: Category ==

Reference:

https://docs.microsoft.com/en-us/azure/iot-hub/monitor-iot-hub

NEW QUESTION: 85

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

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

You are developing a custom Azure IoT Edge module.

The module needs to identify the device ID of the local device.

Solution: You configure the module to read the IOTEDGE_DEVICEID environment variable.

Does this meet the goal?

A. Yes

B. No

Answer: B (LEAVE A REPLY)

The Azure ID of the current device is available on the IOTEDGE_DEVICEID environment variable.

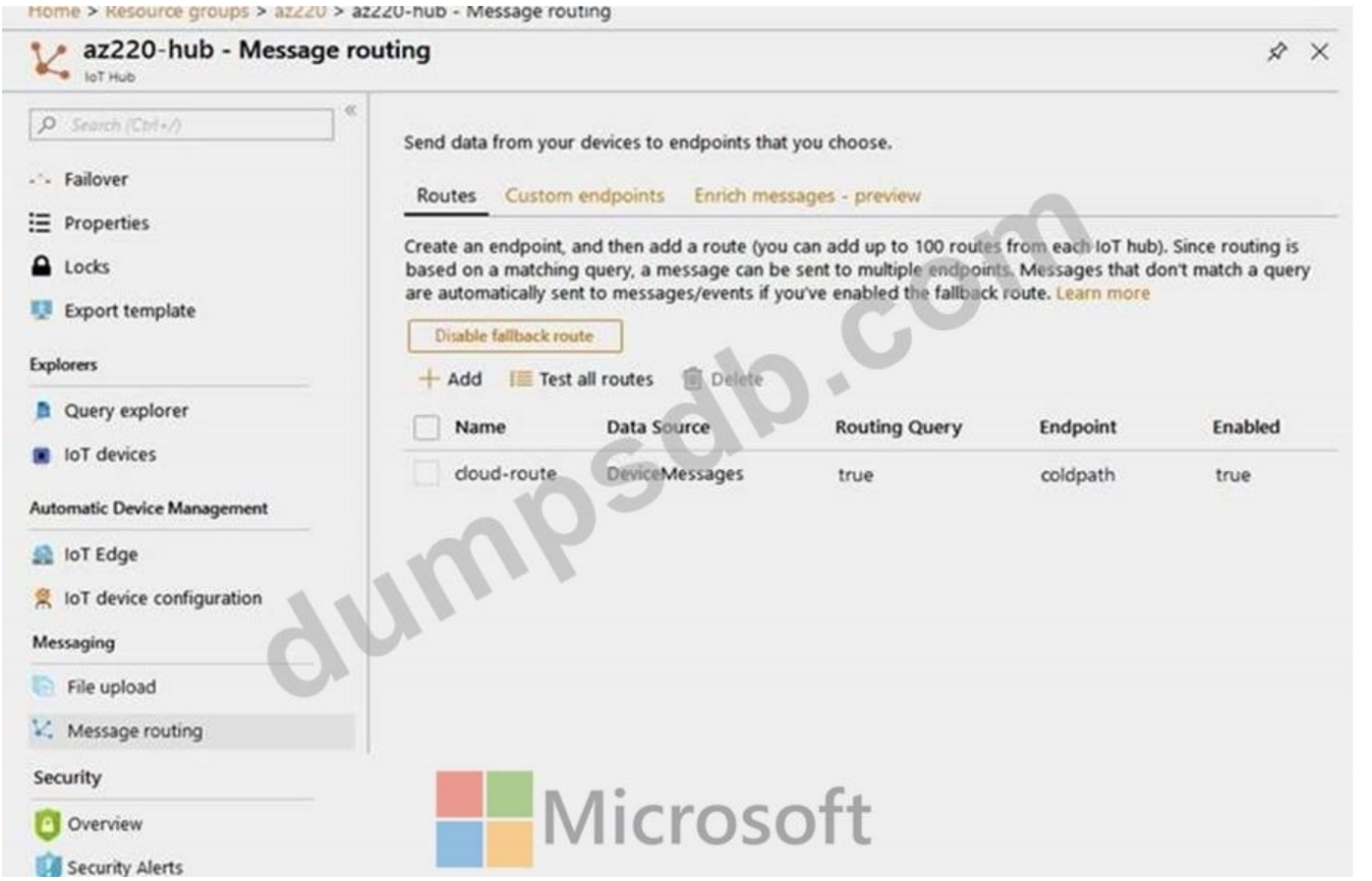
Instead read the device ID of the device twin.
Note: Device twins are JSON documents that store device state information including metadata, configurations, and conditions. Azure IoT Hub maintains a device twin for each device that you connect to IoT Hub.
Device identity properties. The root of the device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

NEW QUESTION: 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/iotedgedev:2.0
D. mycr.azurecr.io/temperature-module:latest
E. mcr.microsoft.com/azureiotedge-hub:1.0
Answer: B,D,E (LEAVE A REPLY)
Explanation
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 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)
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: 88
You need to configure Stream Analytics to meet the POV requirements.
What are two ways to achieve the goal? Each Answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. From IoT Hub, create a custom event hub endpoint, and then configure the endpoint as an input to Stream Analytics.
B. Create a Stream Analytics module, and then deploy the module to all IoT Edge devices in the fleet.
C. Create an input in Stream Analytics that uses the built-in events endpoint of IoT Hub as the source.
D. Route telemetry to an Azure Blob storage custom endpoint, and then configure the Blob storage as a reference input for Stream Analytics.
Answer: A,C (LEAVE A REPLY)



NEW QUESTION: 89

You have an Azure IoT hub.

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

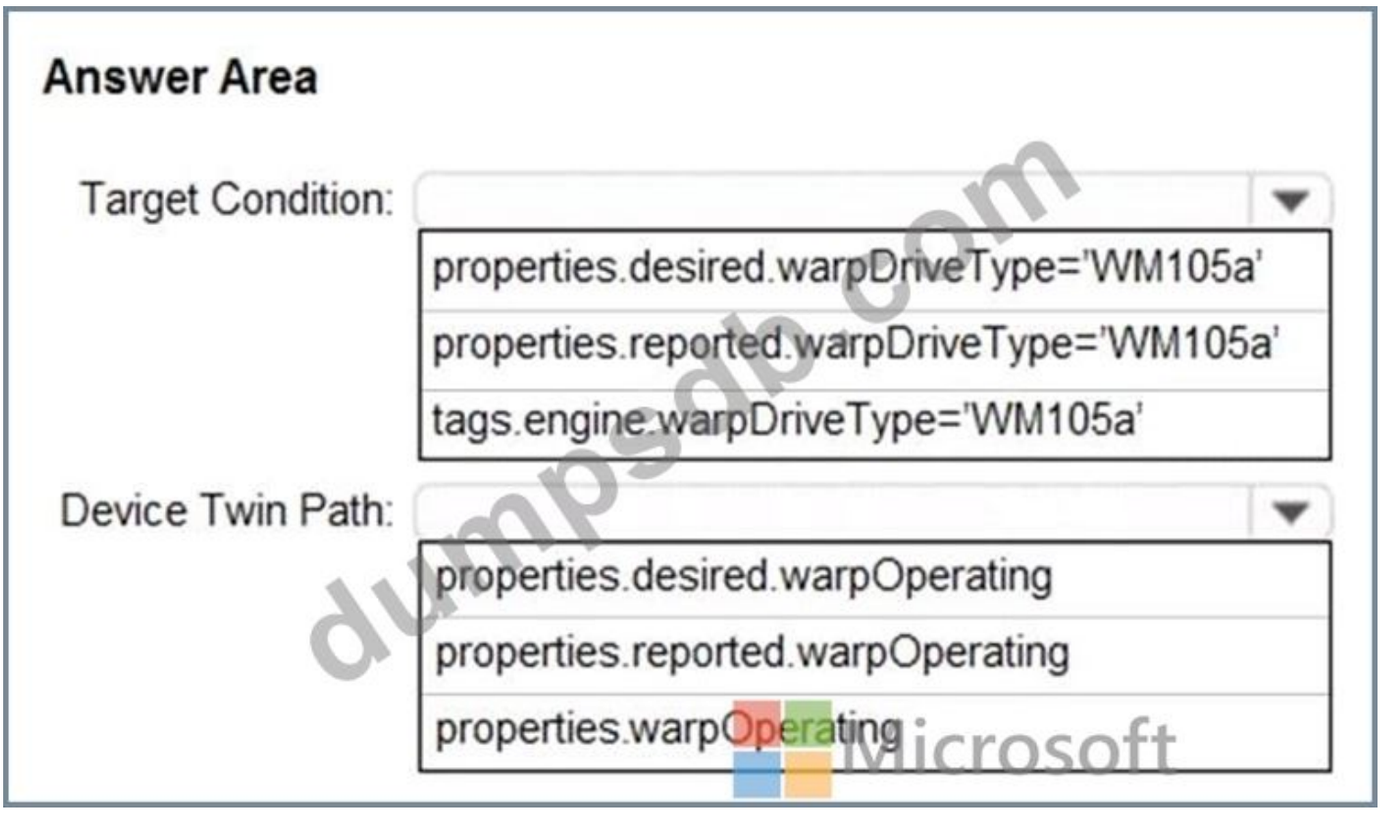
The device twin is shown below.

```
{
  "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
    }
  }
}
```

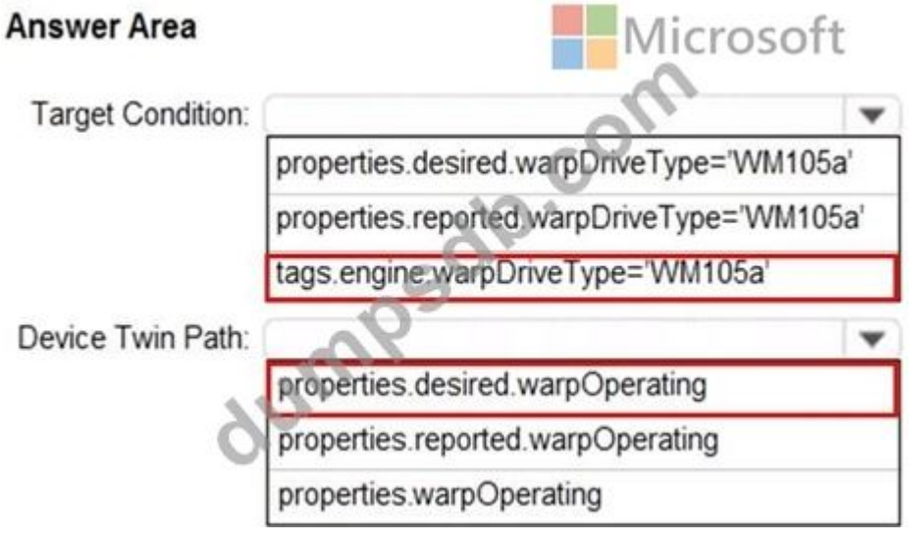

You need to configure automatic device management for the deployment.

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:



Explanation:

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

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

Box 2: properties.desired.warpOperating

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

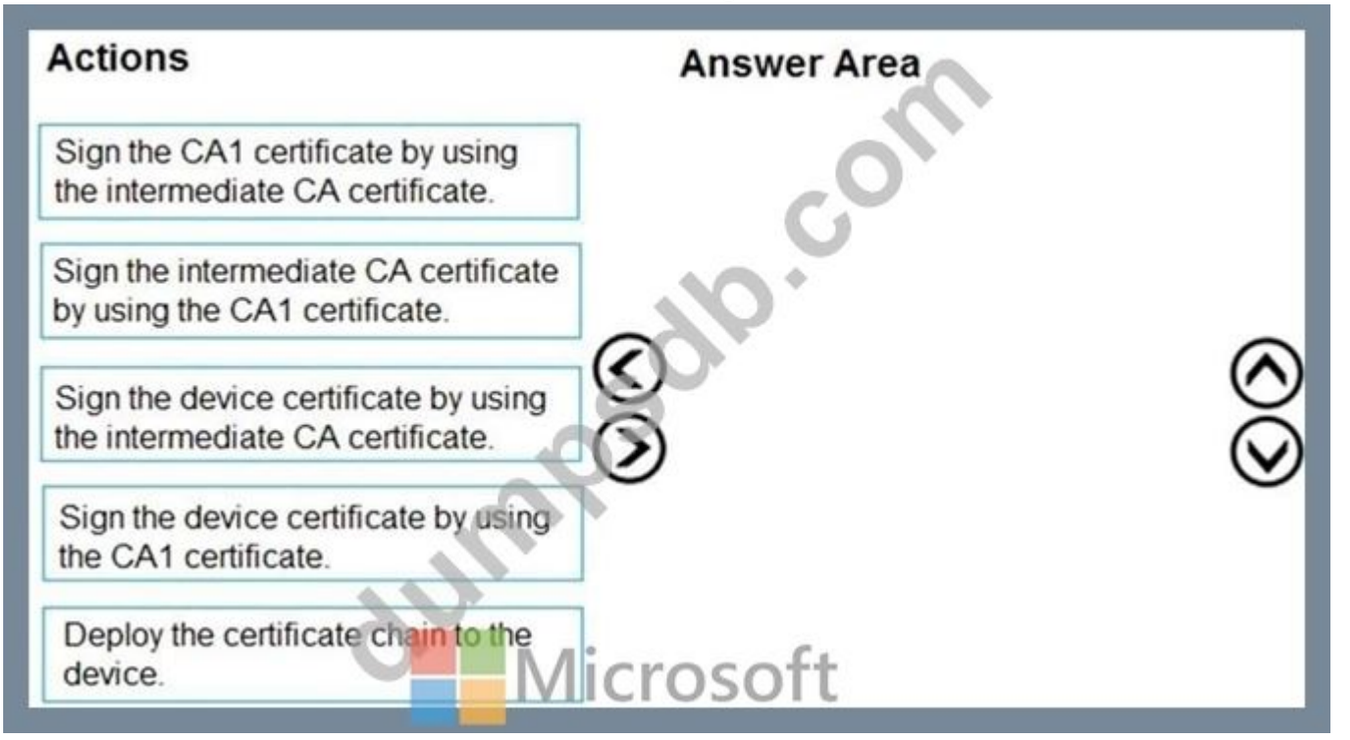
For example, you could set the twin path to properties.desired.chiller-water and then provide the following JSON content:

{

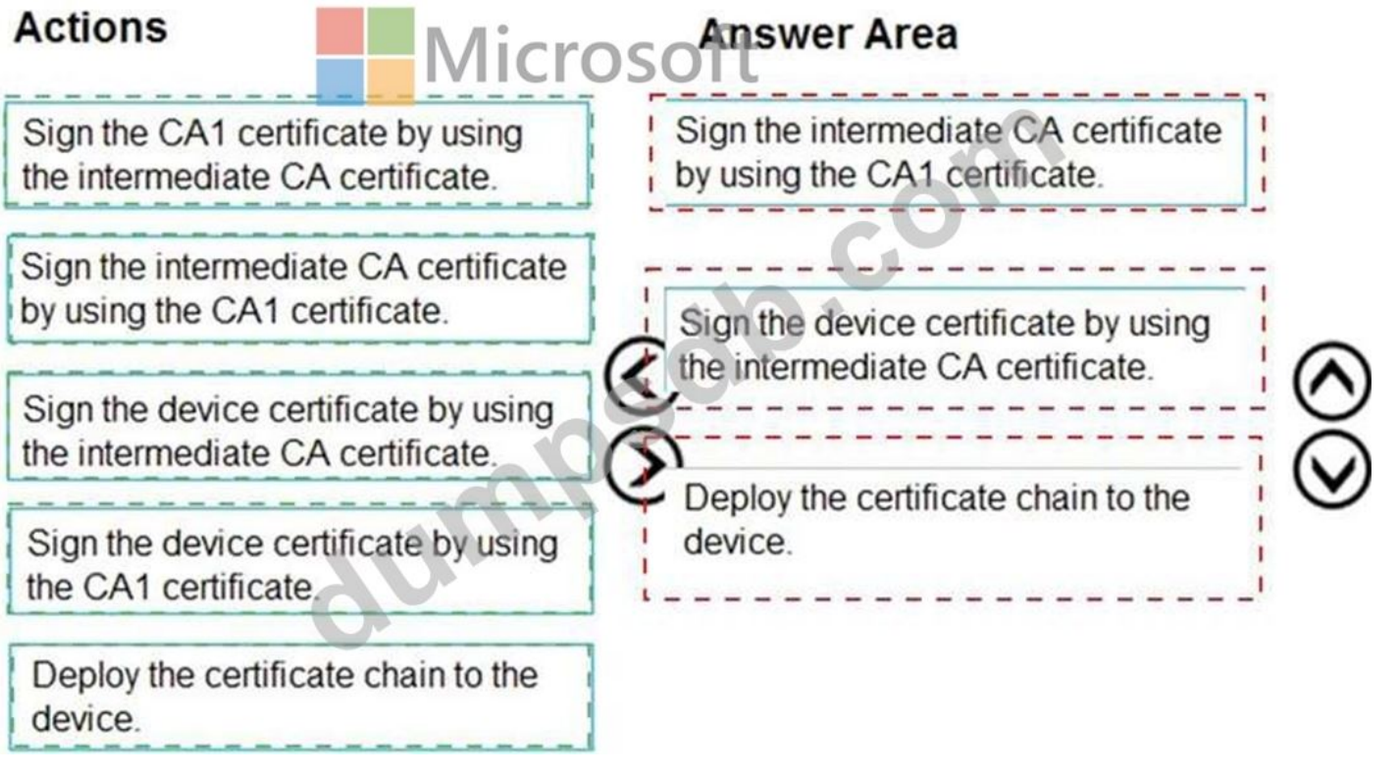
"temperature": 66,

"pressure": 28
}
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-automatic-device-management

NEW QUESTION: 90
You have an Azure IoT hub named Hub1 and a root certification authority (CA) named CA1. Hub1 is configured to use X.509 certificate device authentication.
You and a custom manufacturing partner complete a proof of possession flow.
You plan to deploy IoT devices manufactured by the custom manufacturing partner. Each device will have a certificate generated by an intermediate CA. The devices will authenticate by using device certificates signed by the partner.
You need to ensure that the custom devices can connect successfully to Hub1.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

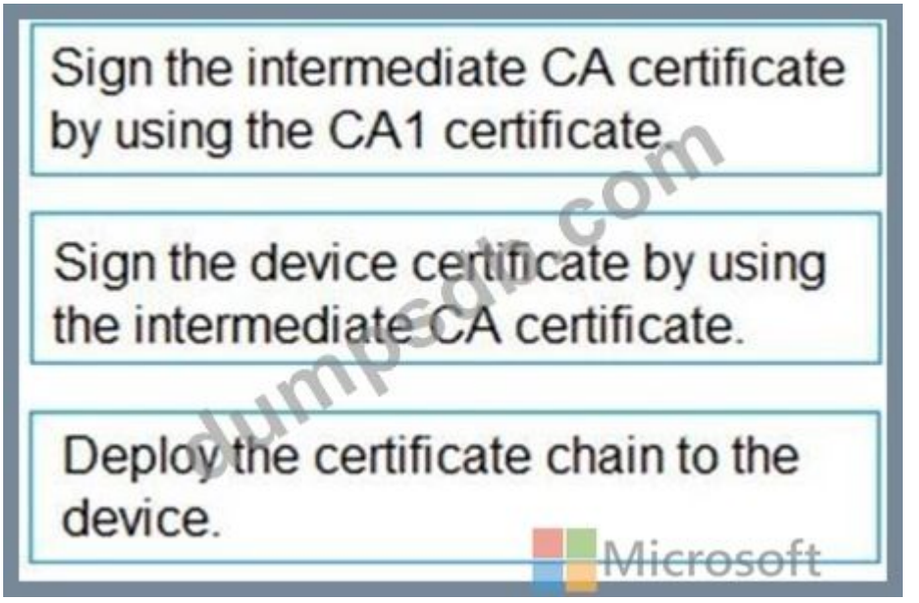


Answer:



Explanation

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



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

X.509 certificates are typically arranged in a certificate chain of trust in which each certificate in the chain is signed by the private key of the next higher certificate, and so on, terminating in a self-signed root certificate.

This arrangement establishes a delegated chain of trust from the root certificate generated by a trusted root certificate authority (CA) down through each intermediate CA to the end-entity "leaf" certificate installed on a device.

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

An intermediate certificate is an X.509 certificate, which has been signed by the root certificate (or by another intermediate certificate with the root certificate in its chain). The last intermediate certificate in a chain is used to sign the leaf certificate. An intermediate certificate can also be referred to as an intermediate CA certificate.
Box 3: Deploy the certificate chain to the device.
The leaf certificate, or end-entity certificate, identifies the certificate holder. It has the root certificate in its certificate chain as well as zero or more intermediate certificates. The leaf certificate is not used to sign any other certificates. It uniquely identifies the device to the provisioning service and is sometimes referred to as the device certificate. During authentication, the device uses the private key associated with this certificate to respond to a proof of possession challenge from the service.
Reference:
https://docs.microsoft.com/en-us/azure/iot-dps/concepts-x509-attestation

NEW QUESTION: 91
You have an Azure IoT Central solution that includes multiple IoT devices. The devices report temperature, humidity, and pressure.
You need to export the sensor data captured during a 48-hour period as a CSV file.
What should you use in IoT Central?
A. Devices
B. Jobs
C. Device groups
D. Analytics
Answer: (SHOW ANSWER)
Azure IoT Central provides rich analytics capabilities to analyze historical trends and correlate telemetry from your devices. To get started, select Analytics on the left pane.
The analytics user interface has three main components:
Data configuration panel: On the configuration panel, select the device group for which you want to analyze the data. Next, select the telemetry that you want to analyze and select the aggregation method for each telemetry. The Group By control helps to group the data by using device properties as dimensions.
Time control: Use the time control to select the duration for which you want to analyze the data.
Chart control: The chart control visualizes the data as a line chart.
Reference:
https://docs.microsoft.com/en-us/azure/iot-central/core/howto-create-analytics

NEW QUESTION: 92
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: 93
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.
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 GET request 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: 94
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: 95
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.

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: 96

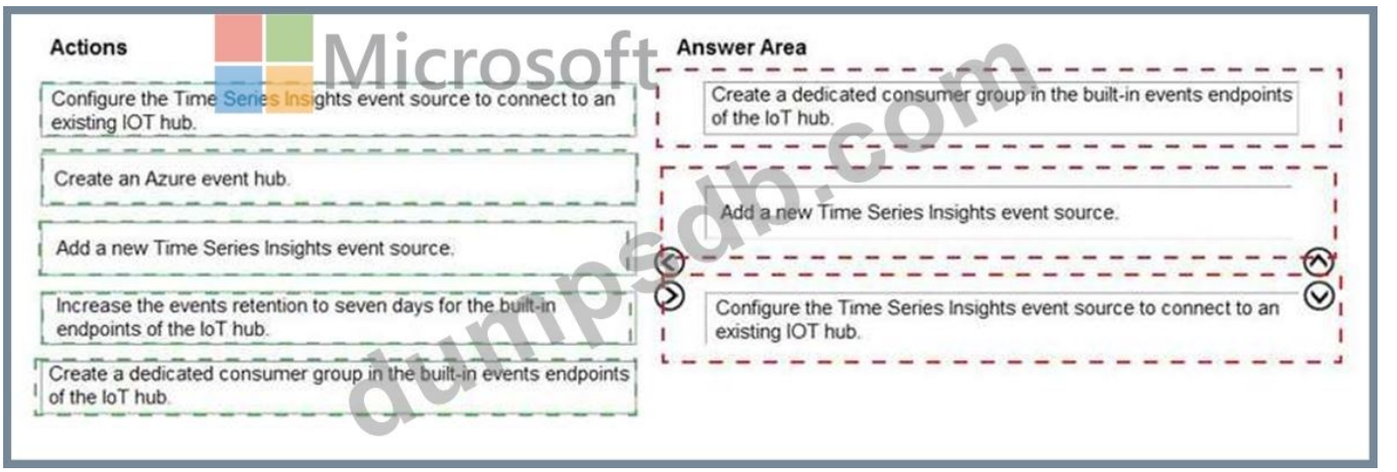
You have an Azure IoT solution that includes a basic tier Azure IoT hub named Hub1 and a Raspberry Pi device named Device1. Device1 connects to Hub1.

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

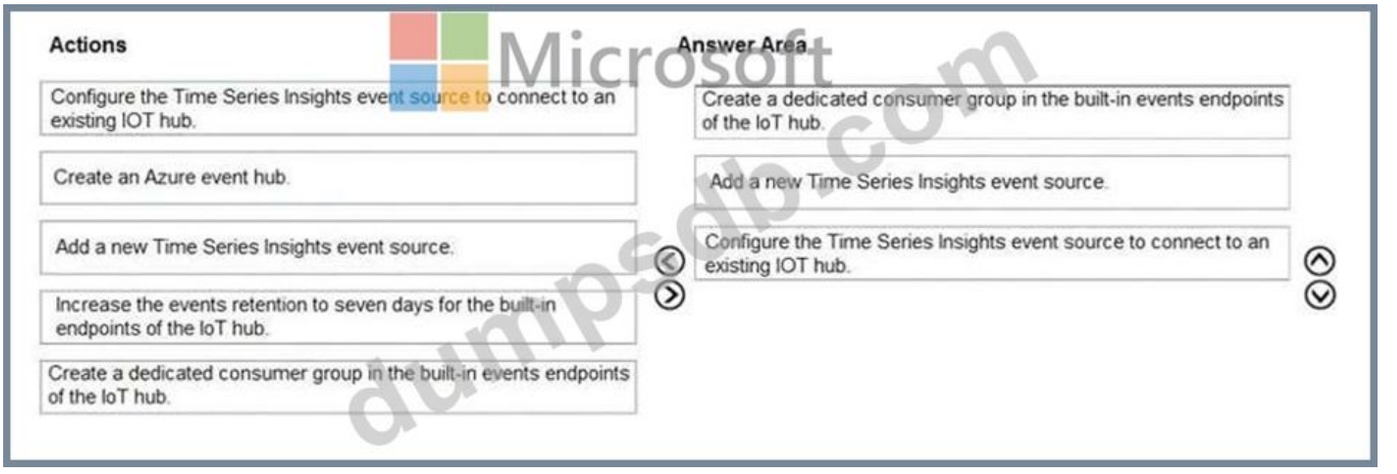
When you start the new Raspberry Pi device, you receive the following error message in the diagnostic logs of Hub1: "409002 LinkCreationConflict." You need to ensure that Device1 and the new Raspberry Pi device can run simultaneously without error.
Which two actions should you perform? Each correct answer 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)
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#symptoms
https://devblogs.microsoft.com/iotdev/understand-different-connection-strings-in-azure-iot-hub/

NEW QUESTION: 97
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.

Answer:



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

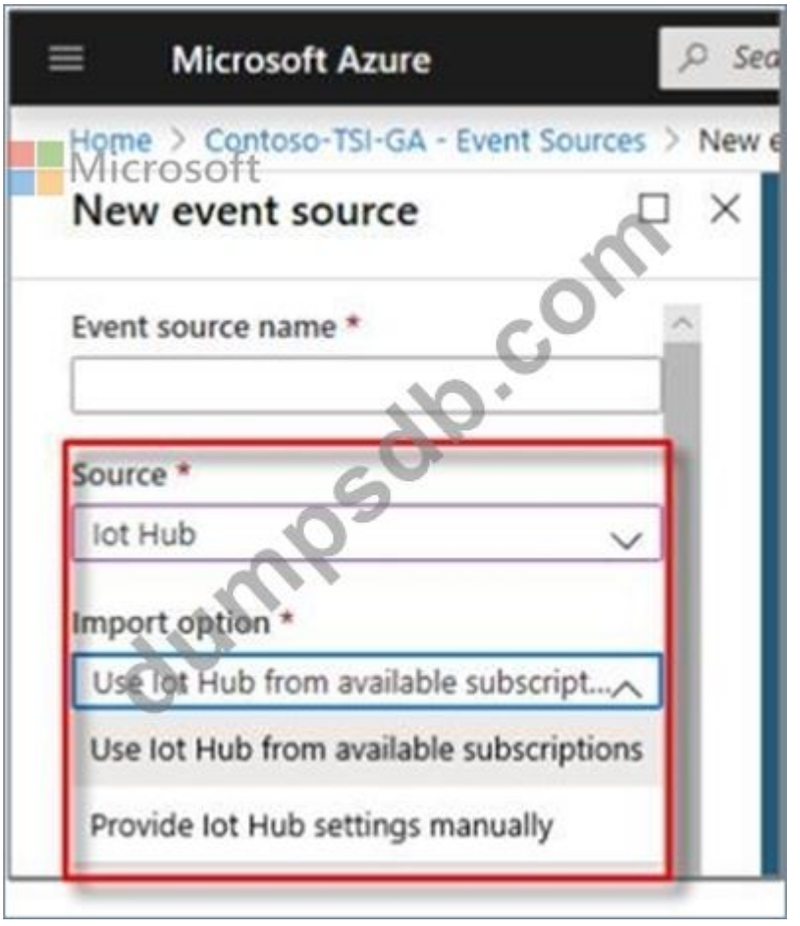
* Sign in to the Azure portal.
* In the left menu, select All resources. Select your Time Series Insights environment.
* Under Settings, select Event Sources, and then select Add.
* In the New event source pane, for Event source name, enter a name that's unique to this Time Series Insights environment. 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.

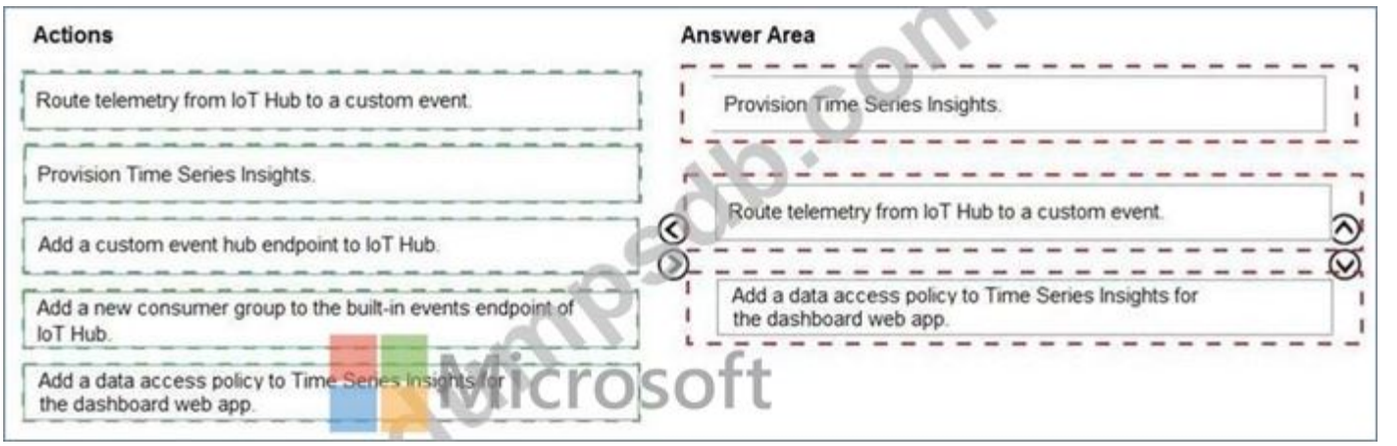
This option is the easiest approach.



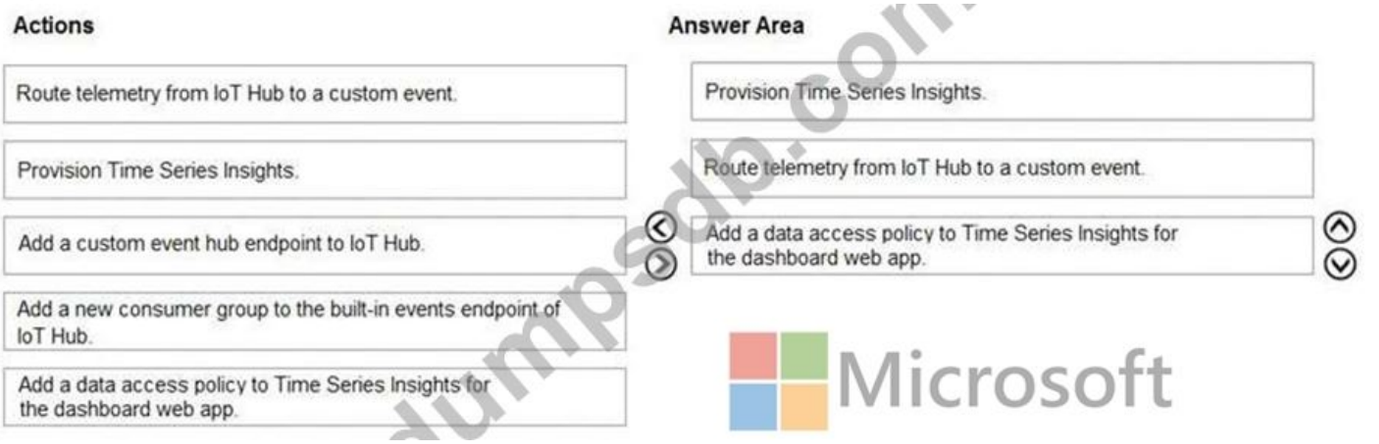
Reference:
https://docs.microsoft.com/en-us/azure/time-series-insights/time-series-insights-how-to-add-an-event-source-ioth

NEW QUESTION: 98
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.

Answer:



Explanation



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: 99

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.	○	○

Reference:

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

NEW QUESTION: 100

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.

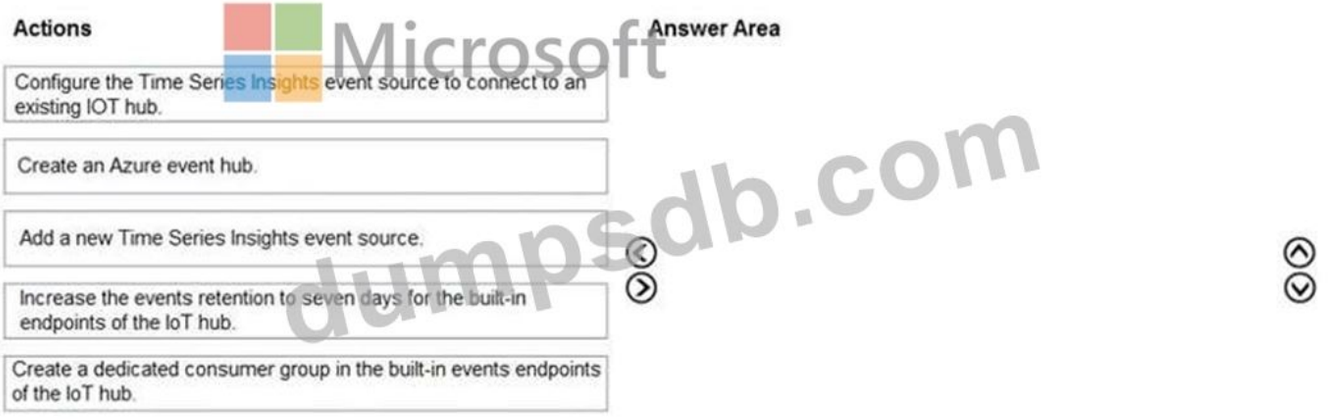
NOTE: Each correct selection is worth one point.

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: 101
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.



Answer:

Answer Area

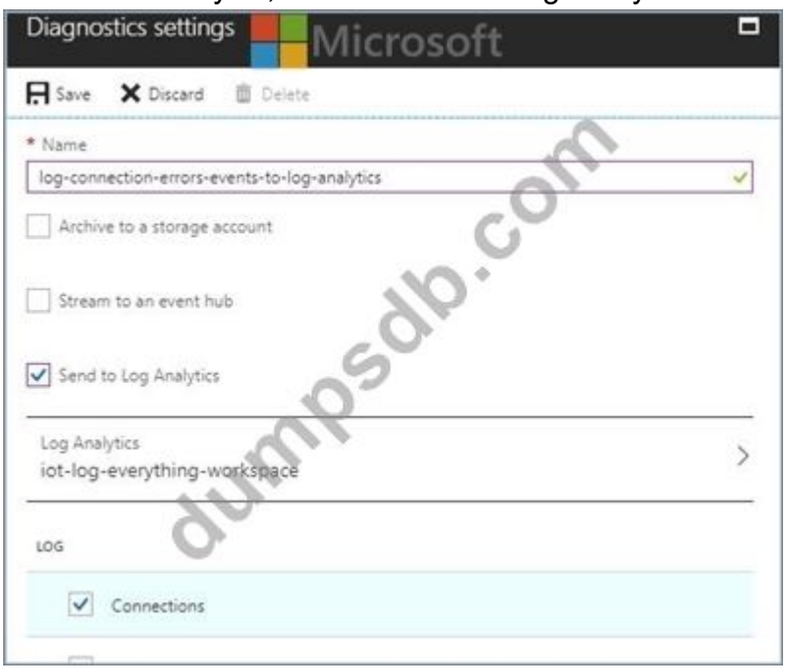
Create a dedicated consumer group.
Add a new Time Series Insights event source.
Configure the Time Series event source to connect to an existing IOT hub

1 - Create a dedicated consumer group..
2 - Add a new Time Series Insights event source.
3 - Configure the Time Series event source to connect to an existing IOT hub Reference: https://docs.microsoft.com/en-us/azure/time-series-insights/time-series-insights-how-to-add-an-event-source-iothub

NEW QUESTION: 102
You have 20 devices that connect to an Azure IoT hub.
You open Azure Monitor as shown in the exhibit. (Click the Exhibit tab.)

You discover that telemetry is not being received from five IoT devices.
You need to identify the names of the devices that are not generating telemetry and visualize the dat a. What should you do first?
A. Add the Number of throttling errors metric and archive the logs to an Azure storage account.
B. Configure diagnostics for Routes and stream the logs to Azure Event Hubs.
C. Add the Telemetry messages sent metric and archieve the logs to an Azure Storage account.
D. Configure diagnostics for Connections and send the logs to Azure Log Analytics.
Answer: (SHOW ANSWER)
To log device connection events and errors, turn on diagnostics for IoT Hub. We recommend turning on these logs as early as possible, because if diagnostic logs aren't enabled, when device disconnects occur, you won't have any information to troubleshoot the problem with.
Sign in to the Azure portal.
Browse to your IoT hub.
Select Diagnostics settings.
Select Turn on diagnostics.

Enable Connections logs to be collected.
For easier analysis, turn on Send to Log Analytics



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

NEW QUESTION: 103
You deploy an Azure Digital Twins instance.
You are developing client code that will modify digital twin data.
You run the client code and receive the following response for an Azure Digital Twins API.
403 (Forbidden)
You need to configure access control for the Azure Digital Twins instance to ensure that the client code can modify the data.
Which role should you assign?
A. Contributor
B. Azure Digital Twins Data Owner
C. Owner
D. Managed Application Operator Role
Answer: B (LEAVE A REPLY)
Explanation
Most often, this error indicates that your Azure role-based access control (Azure RBAC) permissions for the service aren't set up correctly. Many actions for an Azure Digital Twins instance require you to have the Azure Digital Twins Data Owner role on the instance you are trying to manage.
Reference:
https://docs.microsoft.com/en-us/azure/digital-twins/troubleshoot-error-403

NEW QUESTION: 104

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.

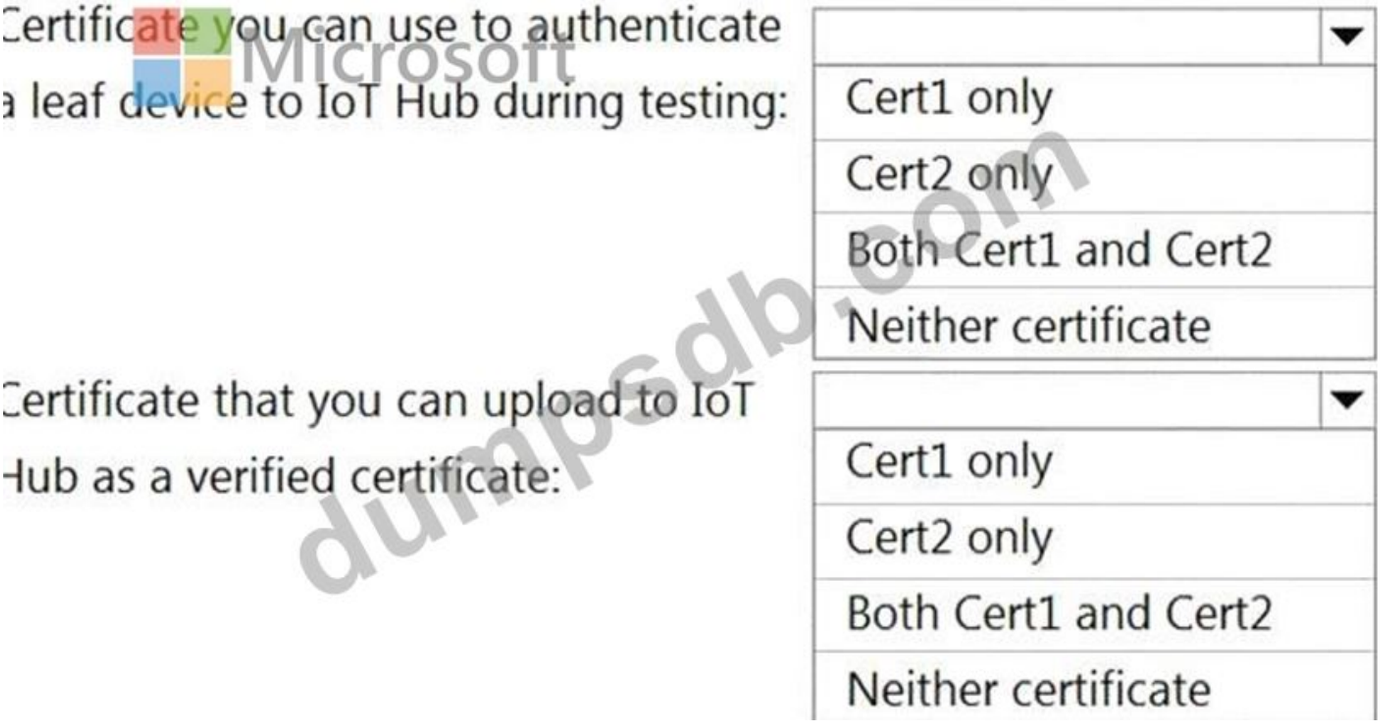
Tier	Direct method	Device-to-cloud message	Price per month
B1	40/sec/unit	400,000/day/unit	$10/unit
S1	40/sec/unit	400,000/day/unit	$25/unit
S2	120/sec/unit	6,000,000/day/unit	$250/unit

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

NEW QUESTION: 105
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.

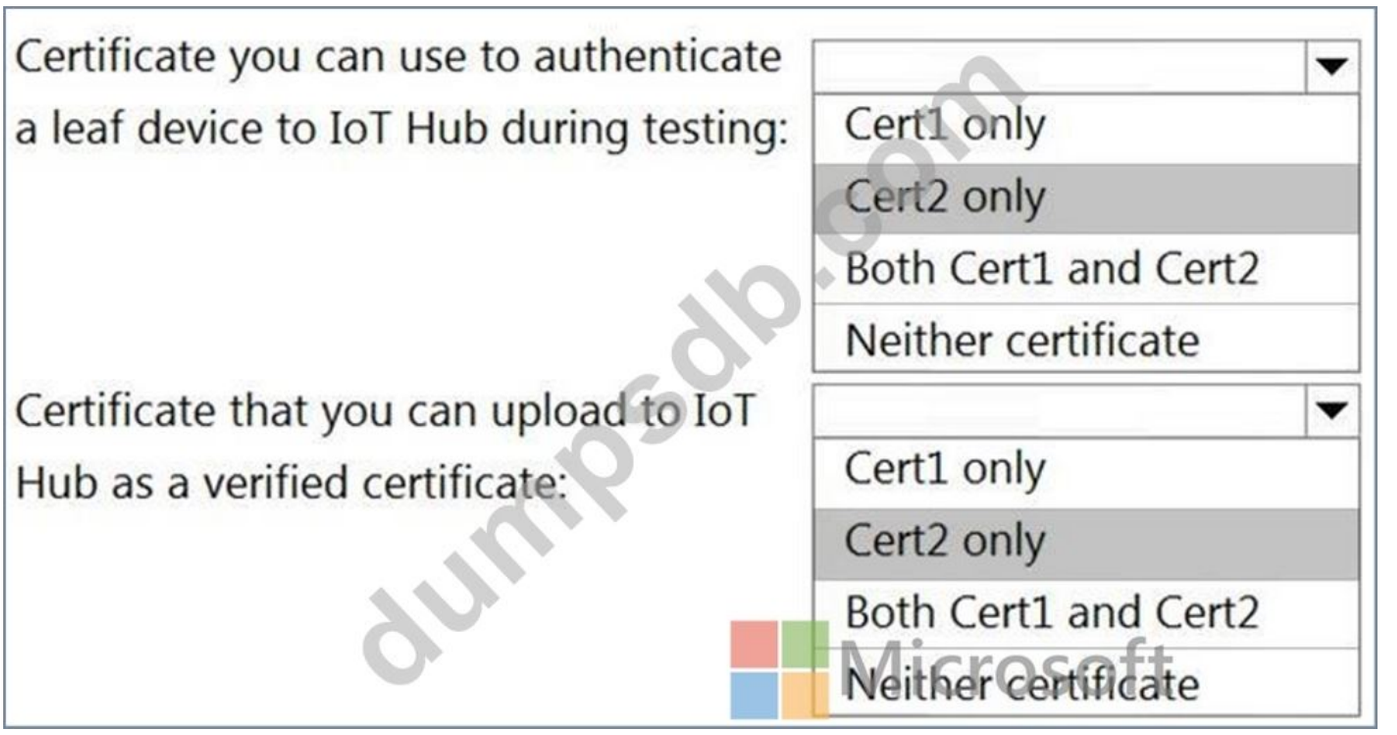
What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:

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: 106

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

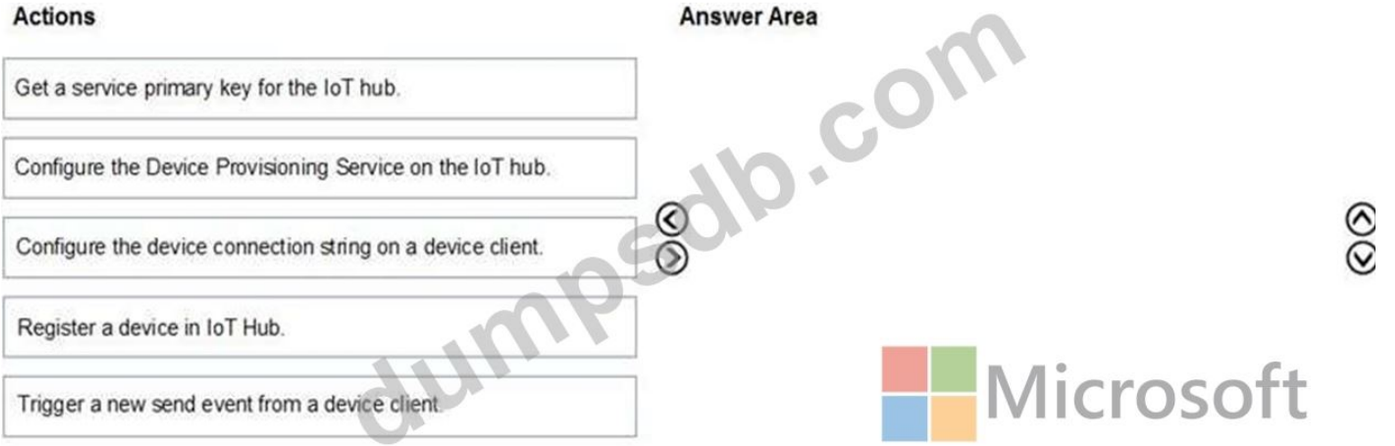
Answer: B (LEAVE A REPLY)

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

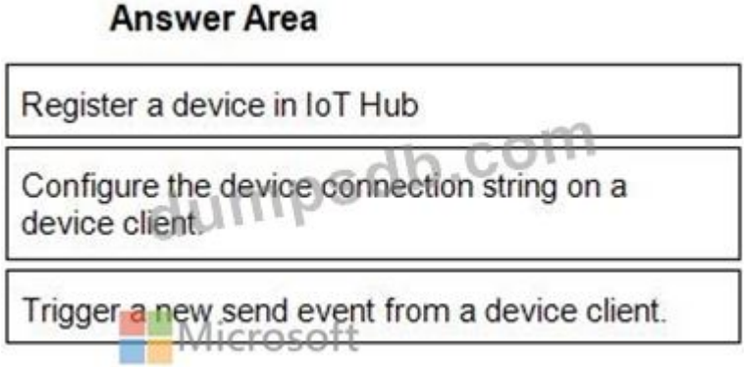
Each Time Series Insights event source must have its own dedicated consumer group that isn't shared with any other consumer. If multiple readers consume events from the same consumer group, all readers are likely to exhibit failures.

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

NEW QUESTION: 107
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.



Answer:



1 - Register a device in IoT Hub
2 - Configure the device connection string on a device client.
3 - Trigger a new send event from a device client.
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/how-to-register-device

NEW QUESTION: 108

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.

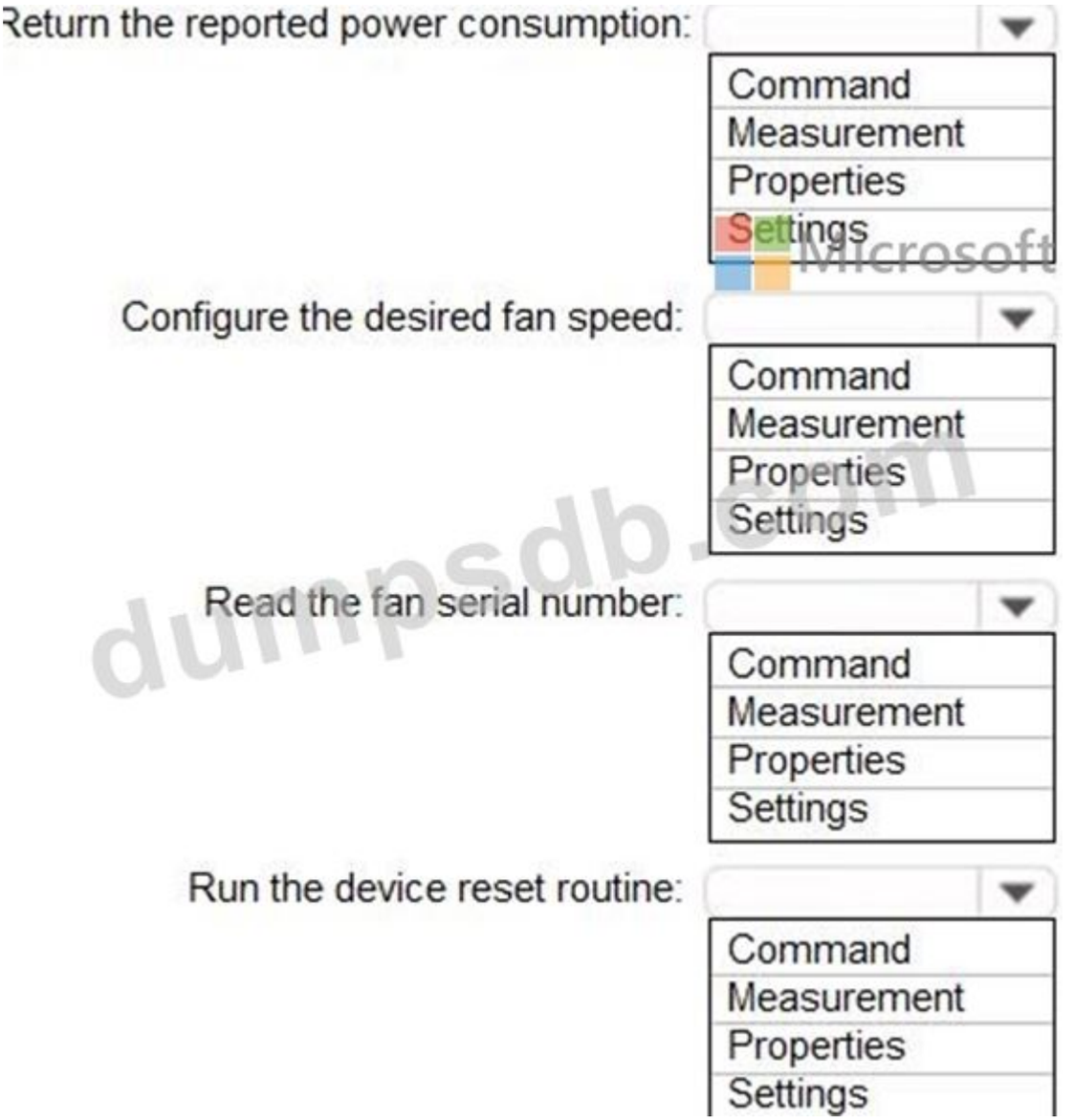
Configure the desired fan speed.

Run the device reset routine.

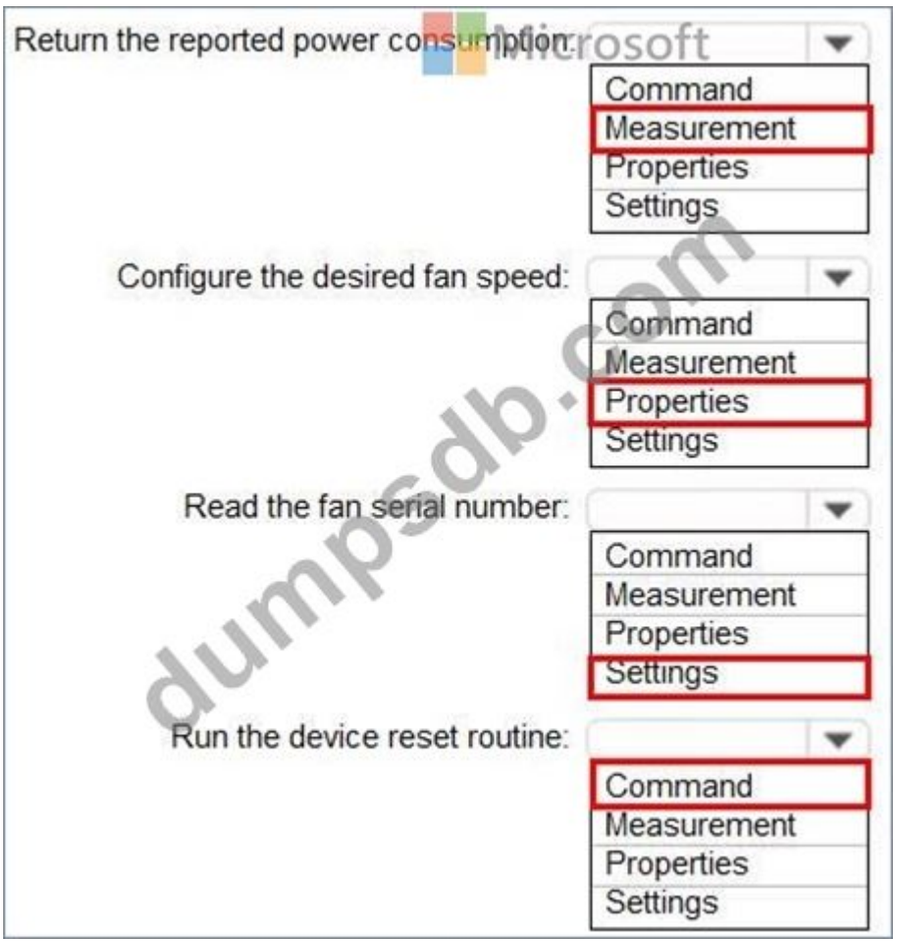
Read the fan serial number.

Which option should you use for each activity? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.



Answer:



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

NEW QUESTION: 109
During the POV phase, telemetry from IoT Hub stops flowing to the hot path. The cold path continues to work.
What should you do to restore the hot path?
A. Disable the fallback route.
B. Run the Test all routes action.
C. Create an explicit route for the hot path.
D. Modify cold-route to send only some telemetry data to the cold path.
Answer: C (LEAVE A REPLY)
Explanation
Explanation/Reference:
Process and manage data
Question Set 3

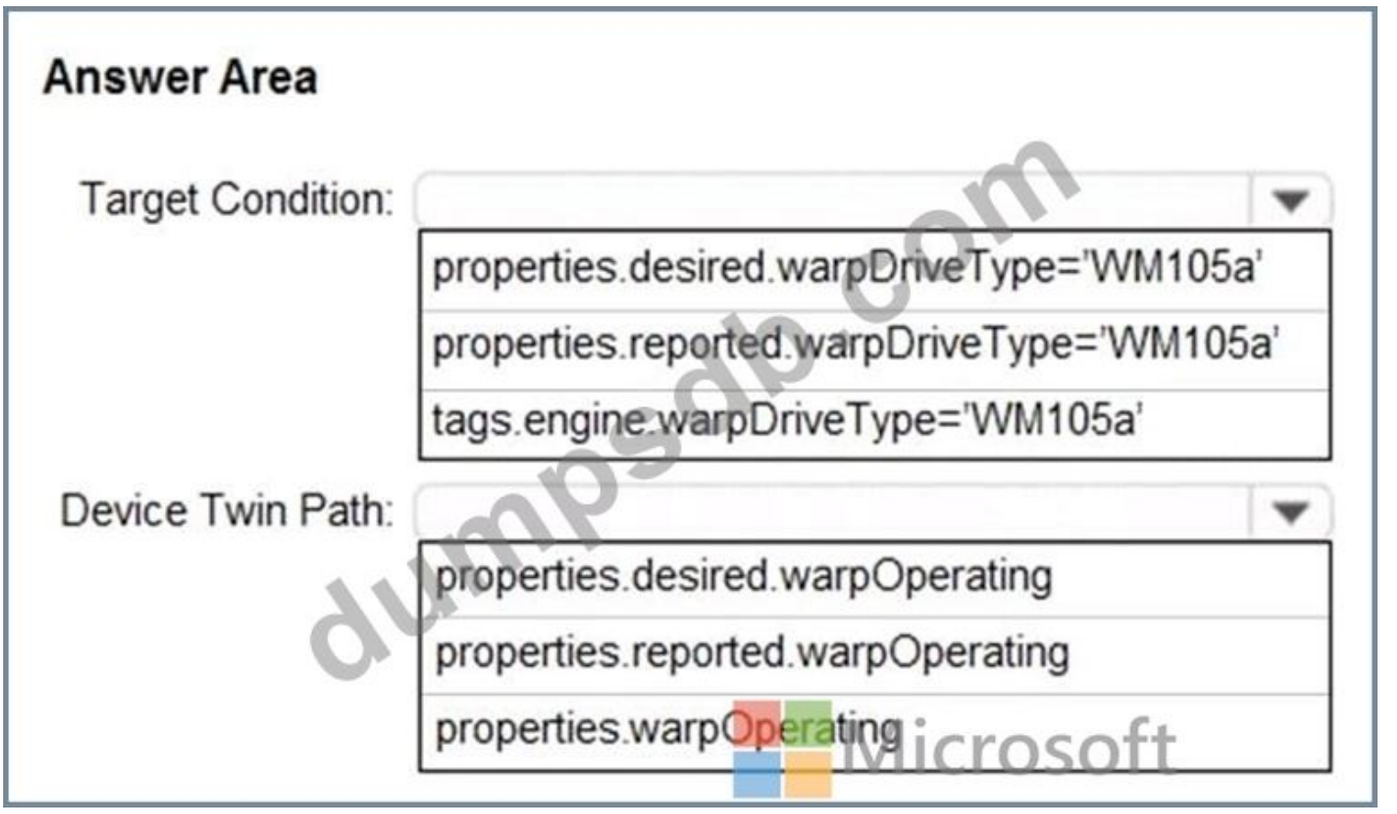
NEW QUESTION: 110
You have an Azure IoT hub.
You plan to deploy 1,000 IoT devices by using automatic device management.
The device twin is shown below.

```
{
  "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
    }
  }
}
```

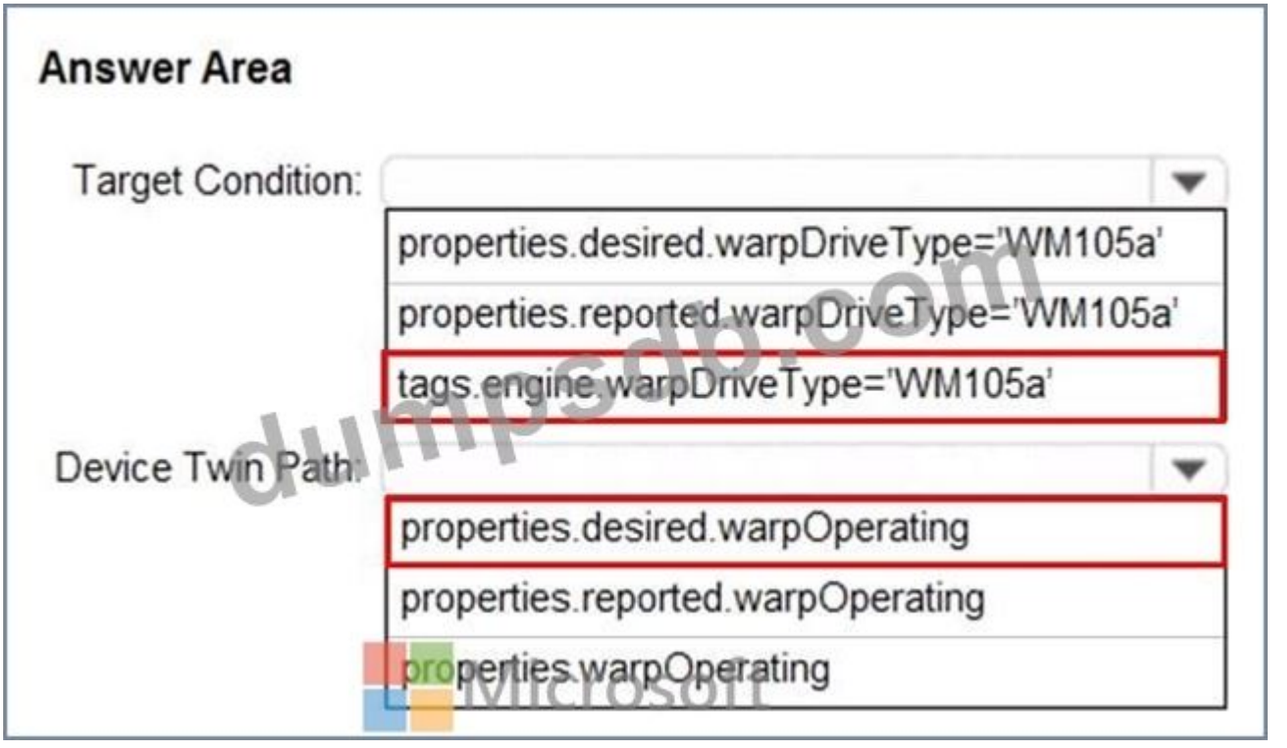

You need to configure automatic device management for the deployment.

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.



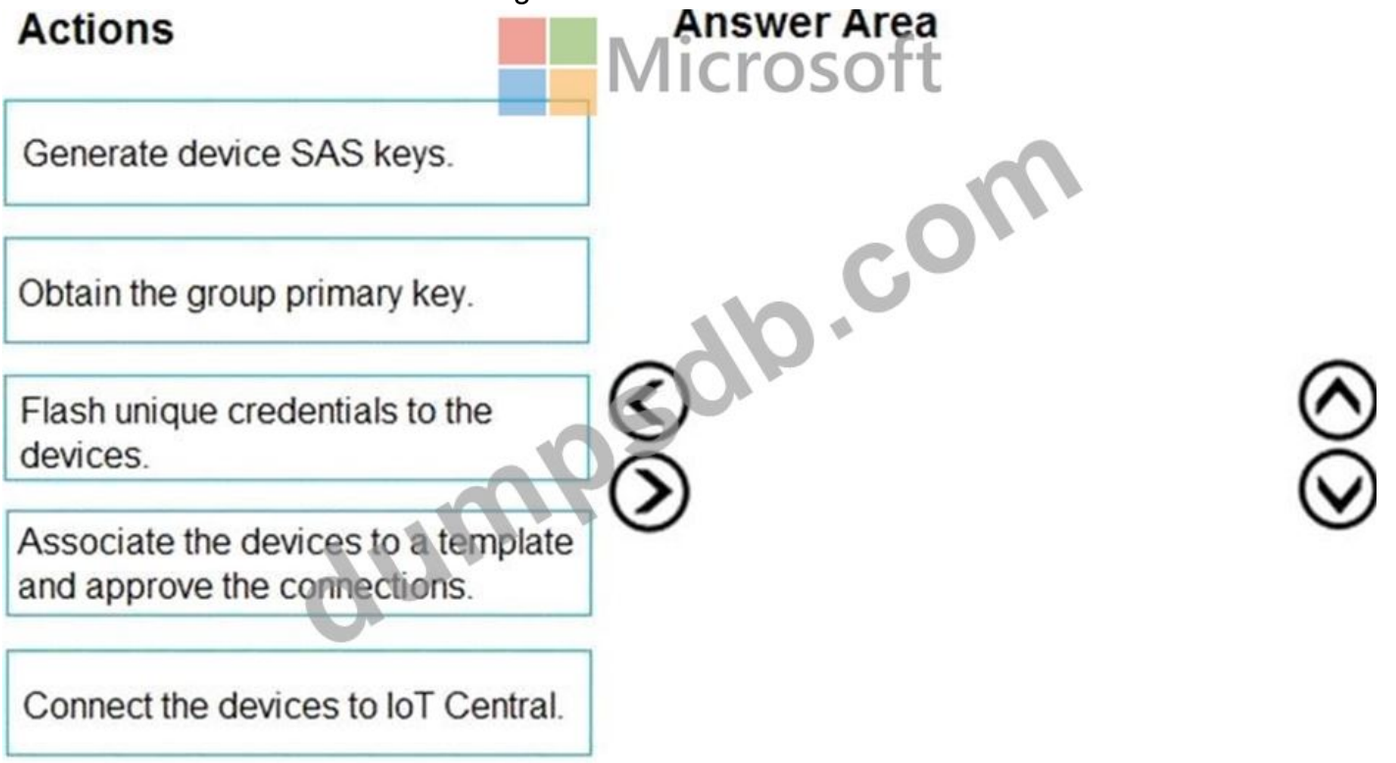
Answer:



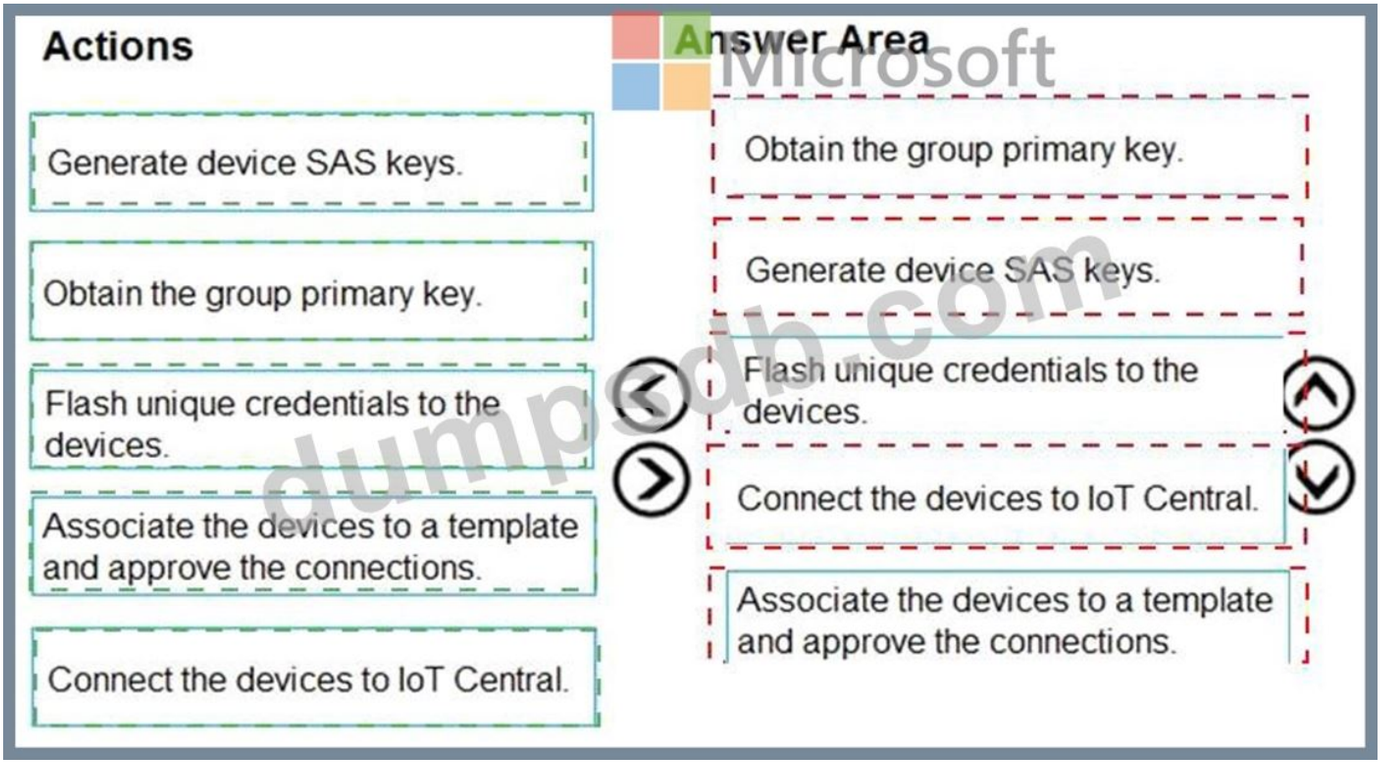
Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-automatic-device-management

NEW QUESTION: 111
You have an Azure IoT Central application.
You need to connect IoT devices that use SAS tokens to the application without first registering the devices.

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

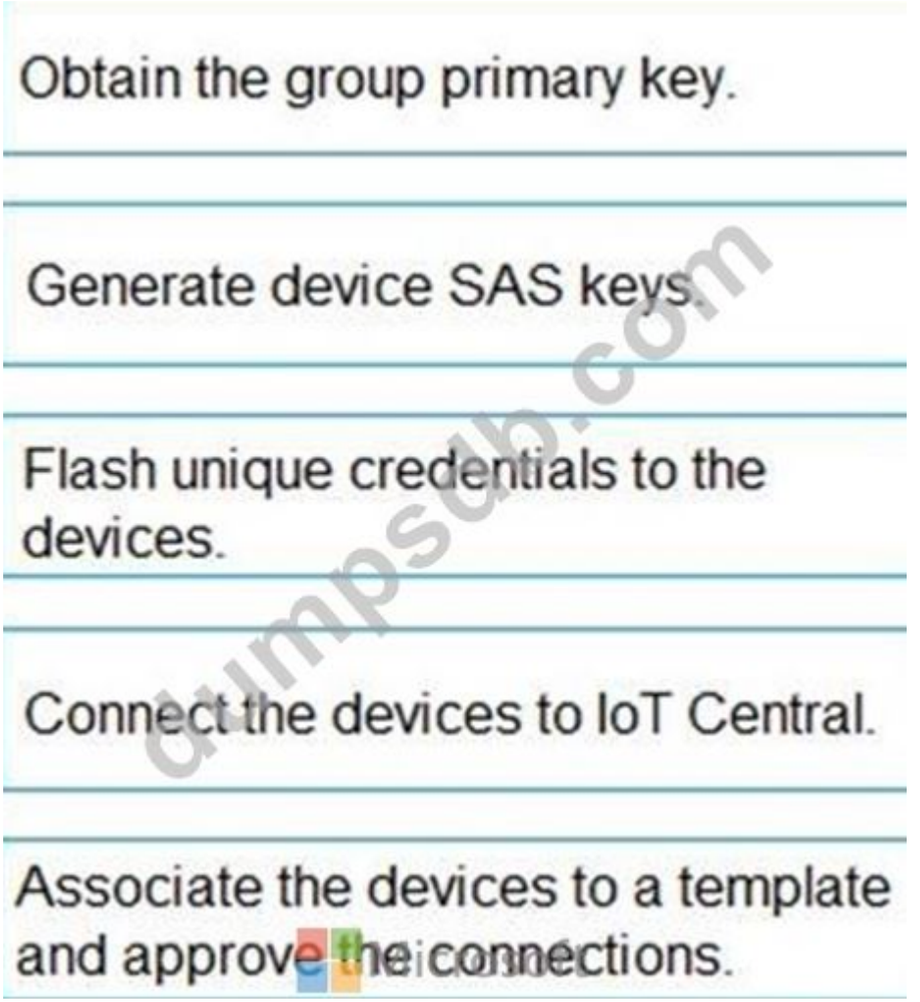


Answer:



Explanation

Graphical user interface, text, application Description automatically generated

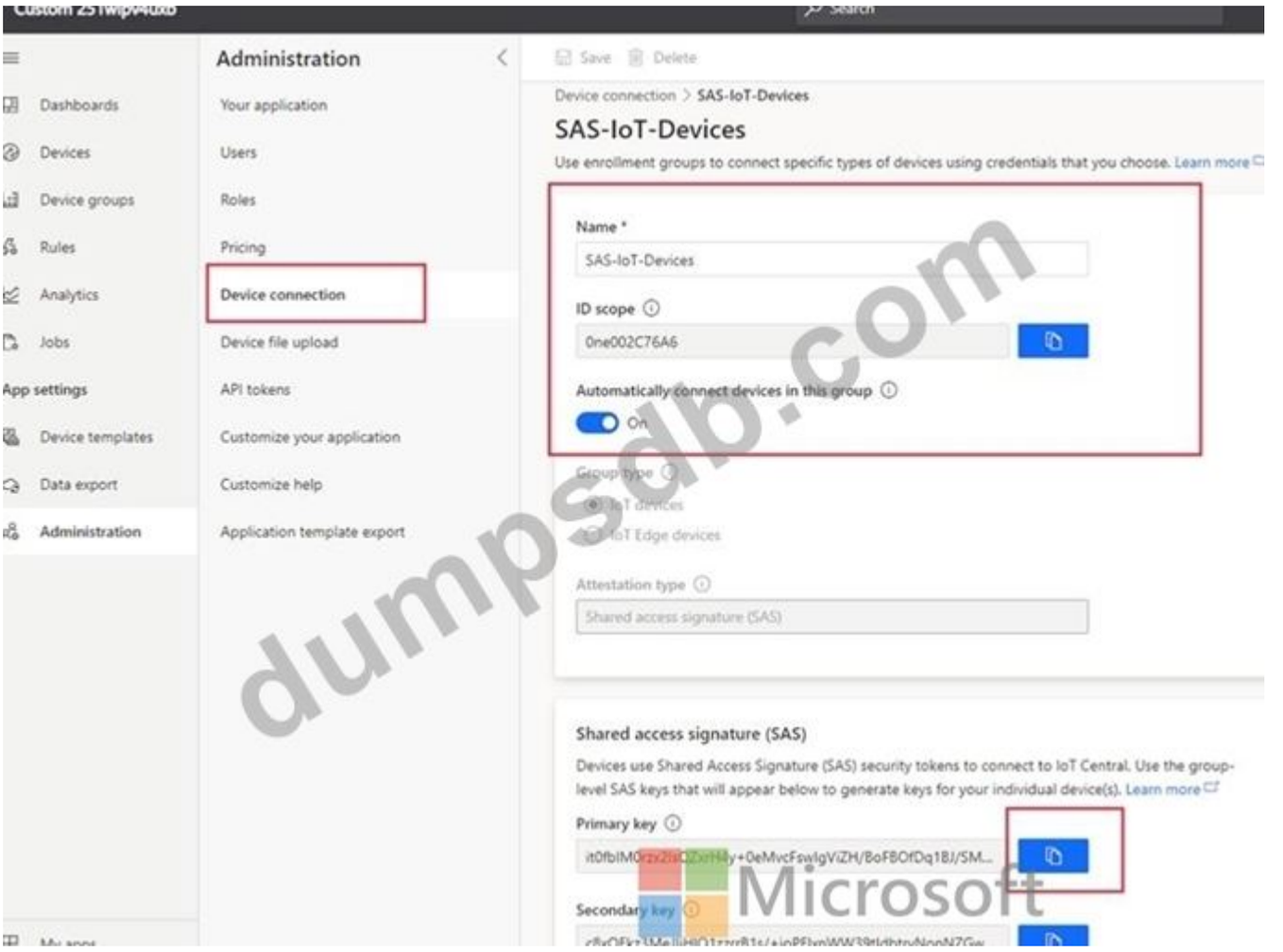


Automatically register devices that use SAS tokens:

Step 1: Obtain the group primary key

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

Graphical user interface, application, Teams Description automatically generated



Step 2: Generate device SAS Keys.

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

Step 3: Flash unique credentials to the devices.

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

Step 4: Connect the devices to IoT Central

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

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

Step 5: Associate the devices to a template and approve the connections.

The IoT Central application uses the model ID sent by the device to associate the registered device with a device template.

Reference:

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

NEW QUESTION: 112

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/

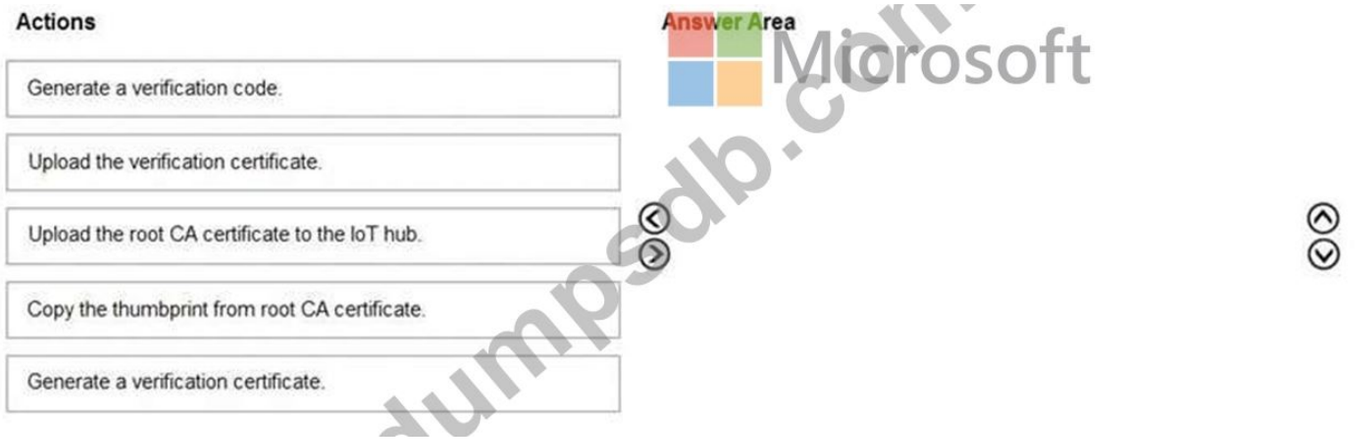
NEW QUESTION: 113
How should you complete the GROUP BY clause to meet the Streaming Analytics requirements?
A. GROUP BY HoppingWindow(Second, 60, 30)
B. GROUP BY TumblingWindow(Second, 30)
C. GROUP BY SlidingWindow(Second, 30)
D. GROUP BY SessionWindow(Second, 30, 60)
Answer: B (LEAVE A REPLY)
Scenario: 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

NEW QUESTION: 114
You have an Azure IoT hub and 15,000 IoT devices that monitor temperature. The IoT hub has four partitions.
Each IoT device sends a 1-KB message every five seconds.

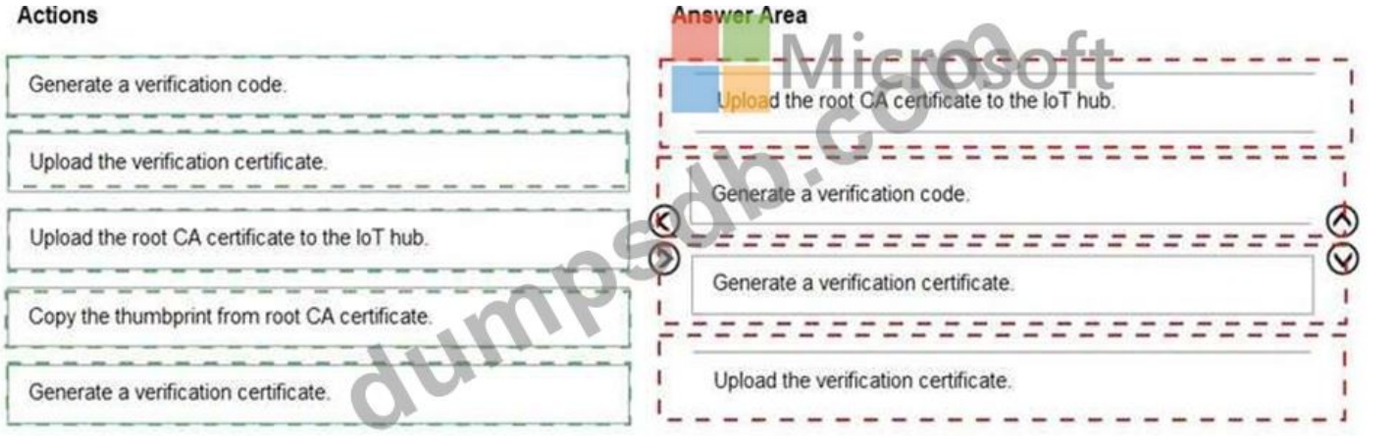
You plan to use Azure Stream Analytics to process the telemetry stream and generate an alert when temperatures exceed a defined threshold.
You need to recommend the minimum number of streaming units to configure for Stream Analytics.
What should you recommend?
A. 1
B. 3
C. 6
D. 12
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/stream-analytics/stream-analytics-parallelization#calculate-the-maximum

NEW QUESTION: 115
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)
Explanation
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

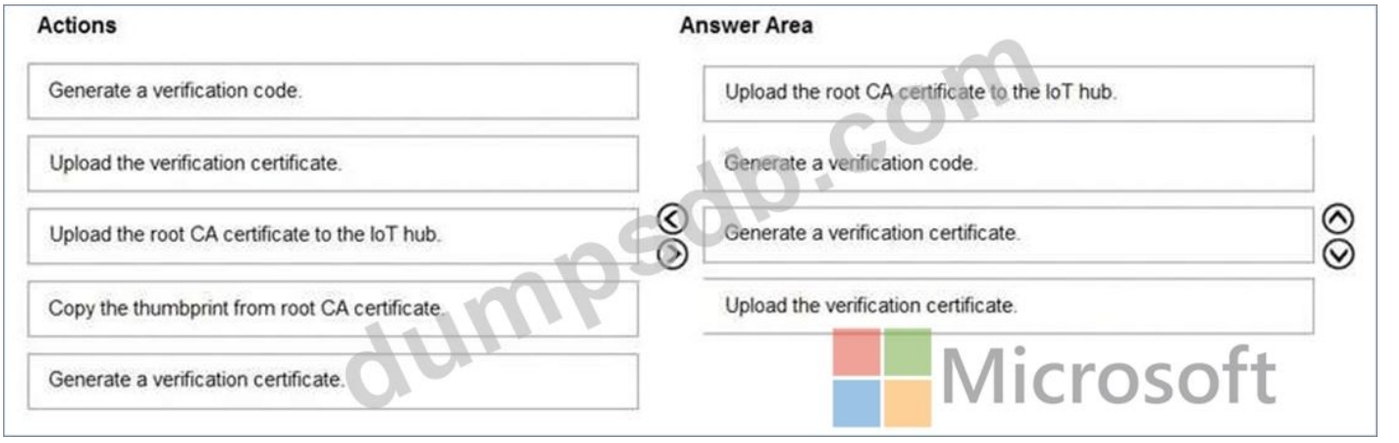
NEW QUESTION: 116
You have an Azure IoT solution that includes an Azure IoT hub.
You receive a root certification authority (CA) certificate from the security department at your company.
You need to configure the IoT hub to use the root CA certificate.
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation

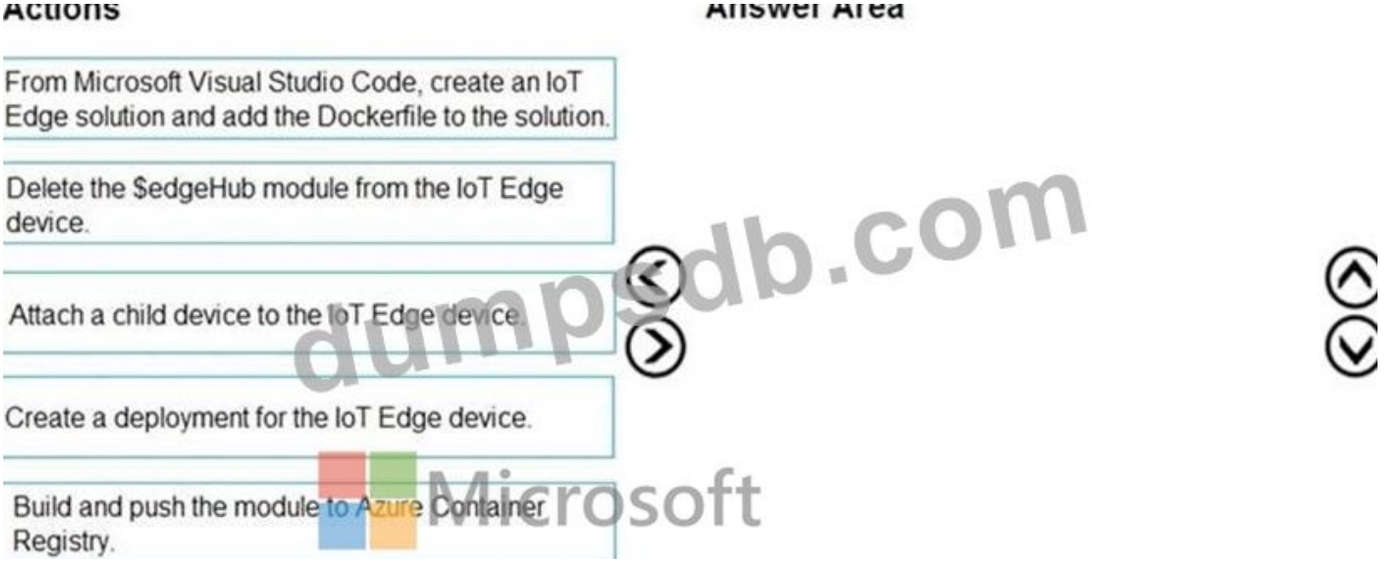


Reference:
https://docs.microsoft.com/bs-latn-ba/azure/iot-hub/iot-hub-security-x509-get-started

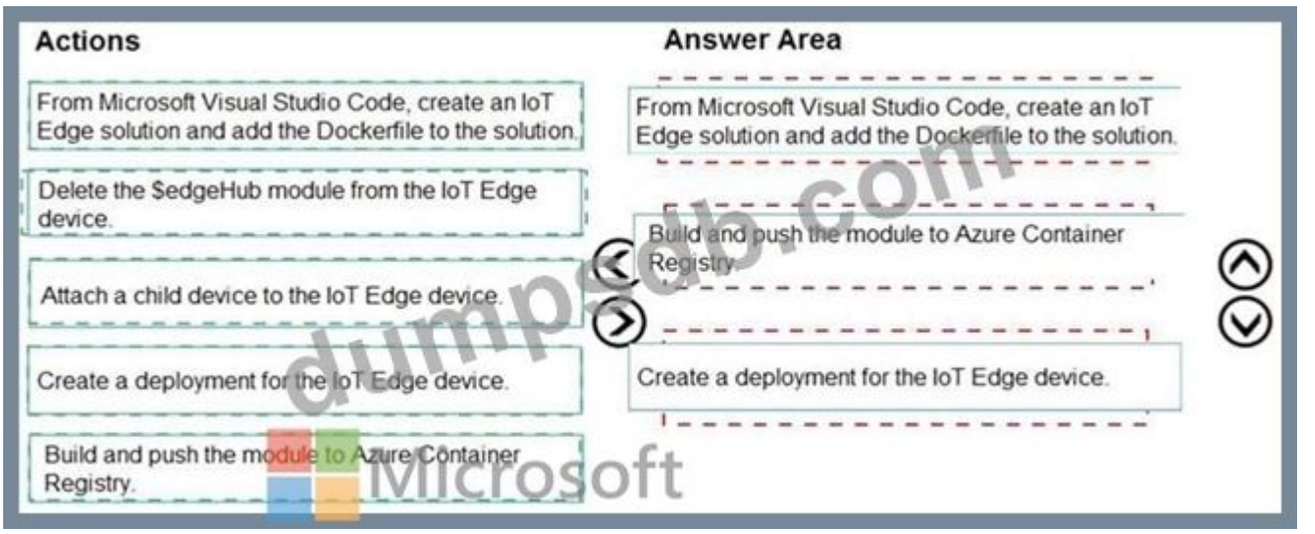
NEW QUESTION: 117
You have an Azure IoT hub that uses a Device Provision Service instance.
You plan to deploy 100 IoT devices.
You need to confirm the identity of the devices by using the Device Provision Service.
Which three device attestation mechanisms can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.
A. X.509 certificates

B. Trusted Platform Module (TPM) 2.0
C. Trusted Platform Module (TPM) 1.2
D. Symmetric key
E. Device Identity Composition Engine (DICE)
Answer: A,B,D (LEAVE A REPLY)
The Device Provisioning Service supports the following forms of attestation:
* X.509 certificates based on the standard X.509 certificate authentication flow.
* Trusted Platform Module (TPM) based on a nonce challenge, using the TPM 2.0 standard for keys to present a signed Shared Access Signature (SAS) token. This does not require a physical TPM on the device, but the service expects to attest using the endorsement key per the TPM spec.
* Symmetric Key based on shared access signature (SAS) Security tokens, which include a hashed signature and an embedded expiration.
Reference:
https://docs.microsoft.com/en-us/azure/iot-dps/concepts-service#attestation-mechanism

NEW QUESTION: 118
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.

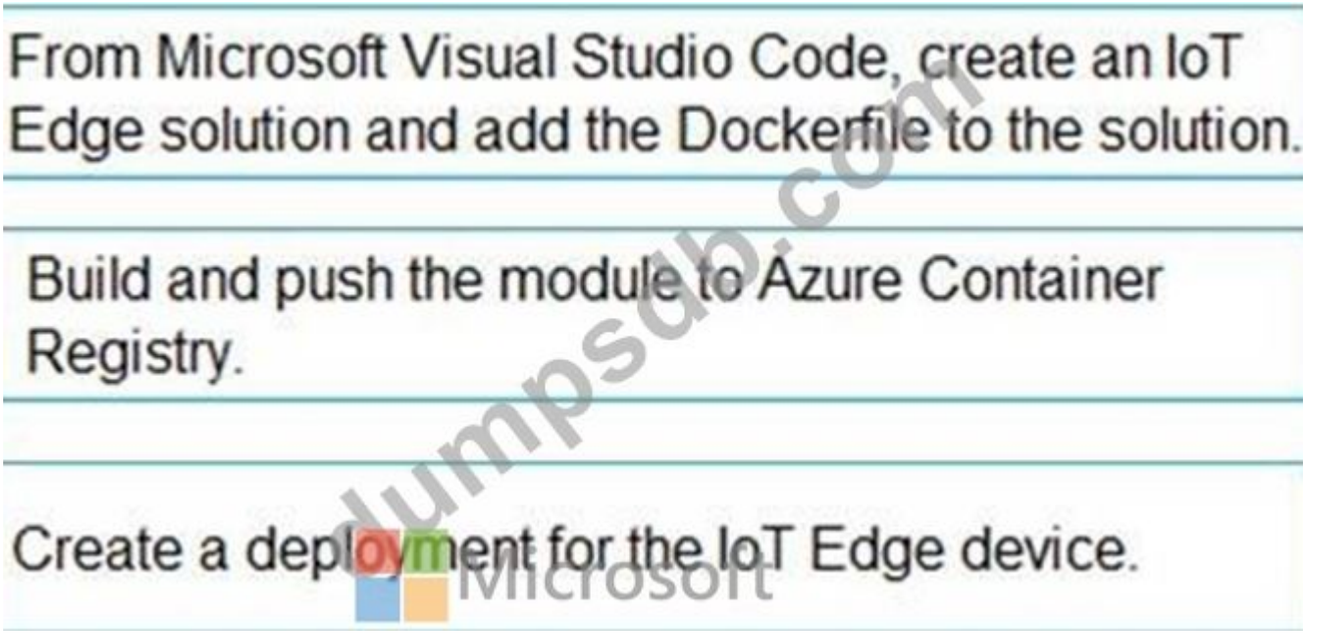


Answer:



Explanation

Graphical user interface, text Description automatically generated with medium confidence



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: 119

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

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

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

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

A. Add the Number of throttling errors metric and archive the logs to an Azure storage account.

B. Configure diagnostics for Routes and stream the logs to Azure Event Hubs.

C. Add the Telemetry messages sent metric and archieve the logs to an Azure Storage account.

D. Configure diagnostics for Connections and send the logs to Azure Log Analytics.

Answer: D (LEAVE A REPLY)

To log device connection events and errors, turn on diagnostics for IoT Hub. We recommend turning on these logs as early as possible, because if diagnostic logs aren't enabled, when device disconnects occur, you won't have any information to troubleshoot the problem with.

Sign in to the Azure portal.

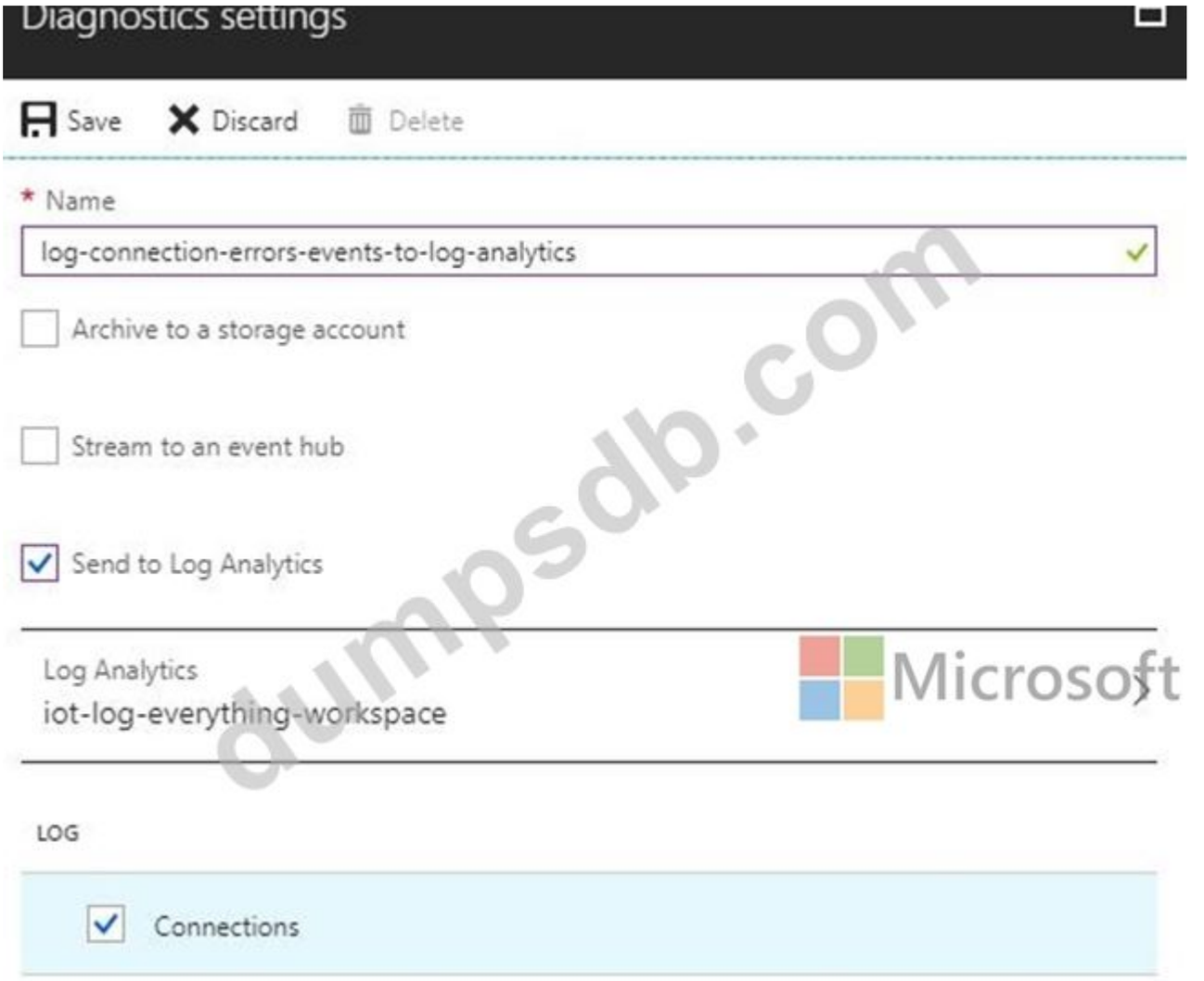
Browse to your IoT hub.

Select Diagnostics settings.

Select Turn on diagnostics.

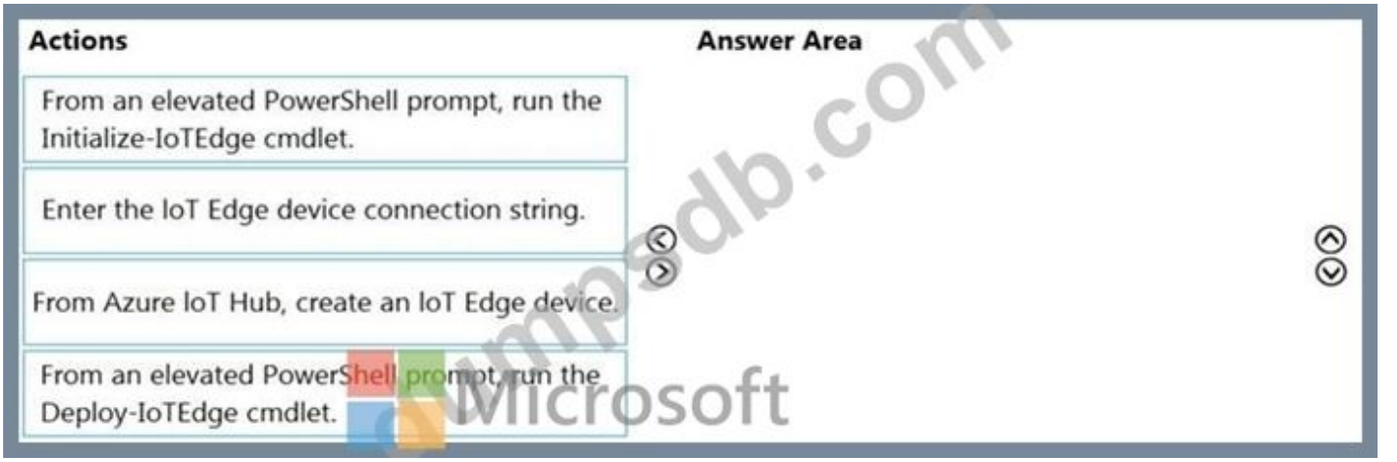
Enable Connections logs to be collected.

For easier analysis, turn on Send to Log Analytics

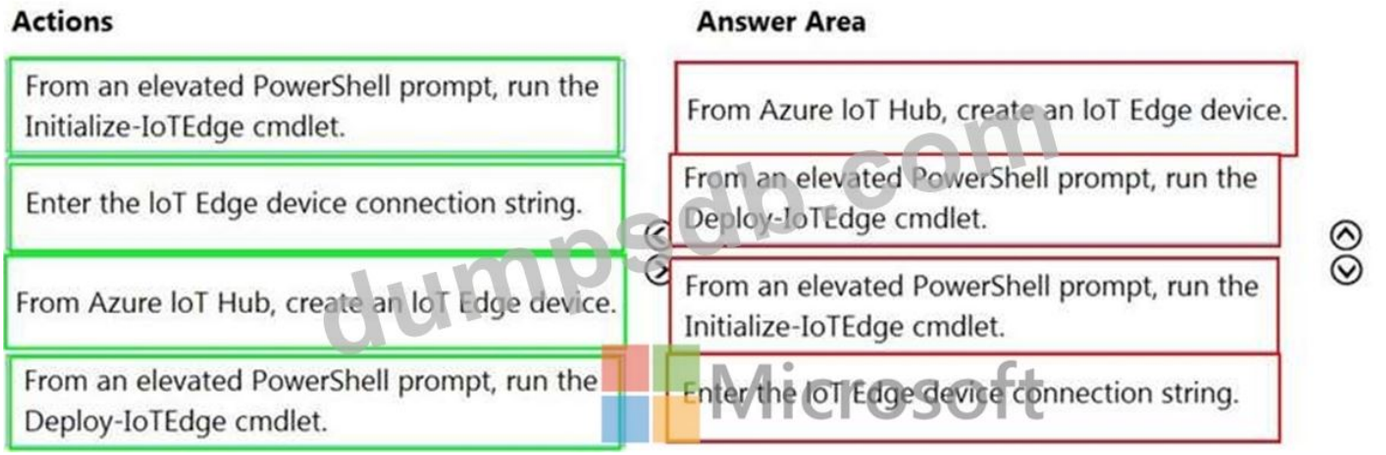


Reference:
https://docs.microsoft.com/bs-cyrl-ba/azure/Iot-hub/iot-hub-troubleshoot-connectivity

NEW QUESTION: 120
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.



Answer:



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: 121

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

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

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

You have the following query for the job.

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

You plan to increase the streaming unit count to 12.

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

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

Does this meet the goal?

A. Yes

B. No

Answer: B (LEAVE A REPLY)

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

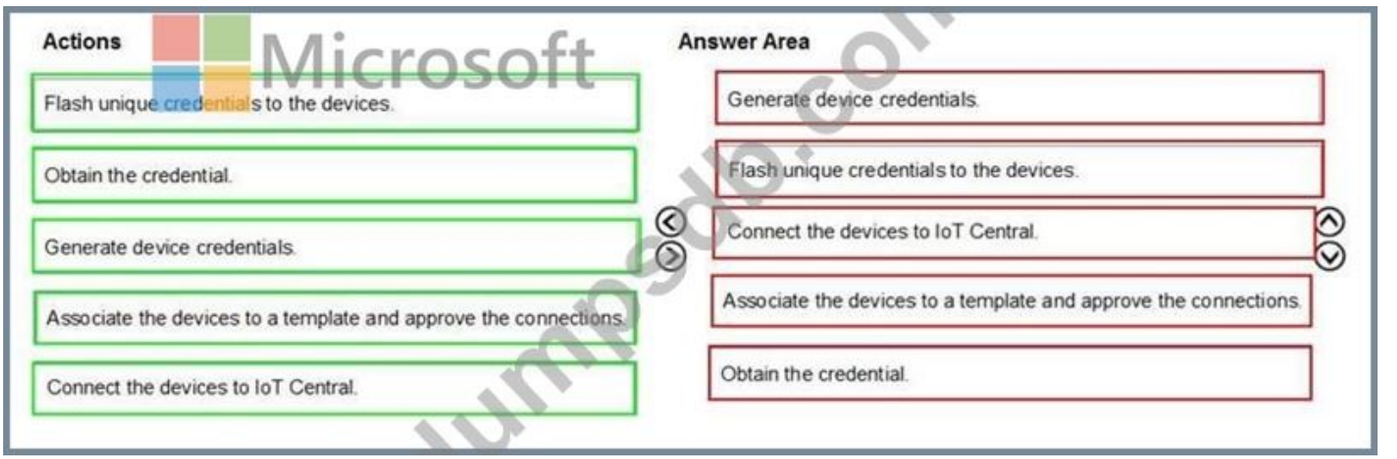
NEW QUESTION: 122

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.

Answer:



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: 123

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:

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

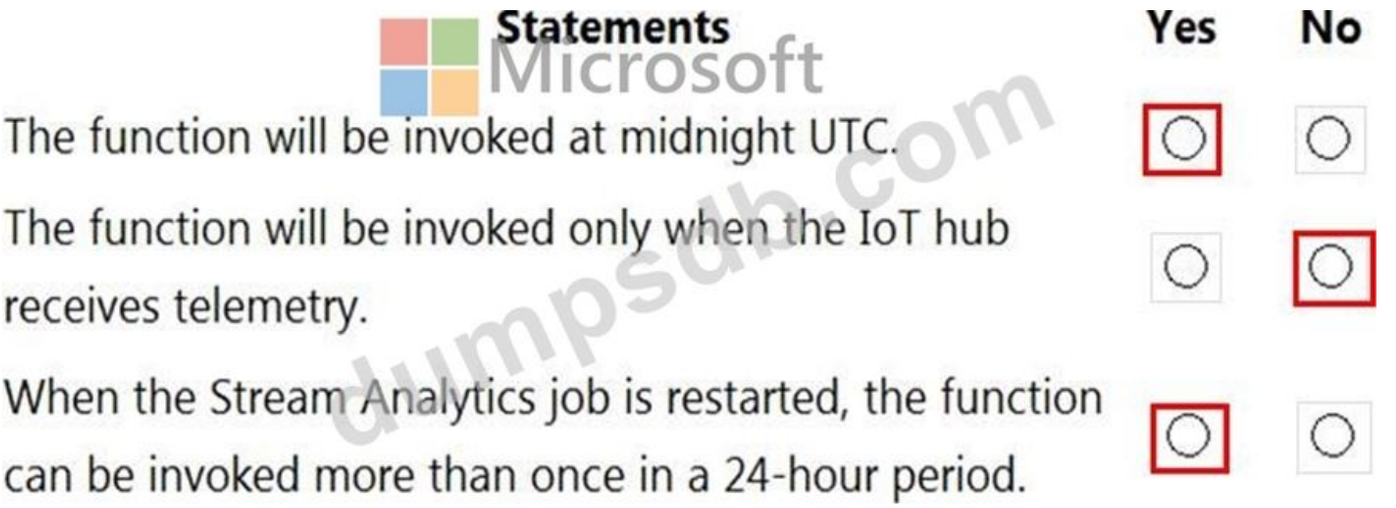
NEW QUESTION: 124
You create an Azure Stream Analytics job that has the following query.

```
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:



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

NEW QUESTION: 125
You use Azure Security Center in an Azure IoT solution.
You need to exclude some security events. The solution must minimize development effort.
What should you do?
A. Create an Azure function to filter security messages.
B. Add a configuration to the code of the physical IoT device.
C. Add configuration details to the device twin object.
D. Create an azureiotsecurity module twin and add configuration details to the module twin object.
Answer: D (LEAVE A REPLY)
Properties related to every Azure Security Center for IoT security agent are located in the agent configuration object, within the desired properties section, of the azureiotsecurity module.
To modify the configuration, create and modify this object inside the azureiotsecurity module twin identity.
Note: Azure Security Center for IoT's security agent twin configuration object is a JSON format object. The configuration object is a set of controllable properties that you can define to control the behavior of the agent.
These configurations help you customize the agent for each scenario required. For example, automatically excluding some events, or keeping power consumption to a minimal level are possible by configuring these properties.
Reference:
https://docs.microsoft.com/en-us/azure/asc-for-iot/how-to-agent-configuration

NEW QUESTION: 126
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: A (LEAVE A REPLY)

The device telemetry is usually passed as JSON from the device through the IoT Hub - this is handled nicely by Azure Streaming Analytics queries.

The IoT Hub message routing should be configured as follows: Data source: Device Telemetry Messages Routing query: true (as the routing query is an expression that evaluates to true or false for each received message, the simplest way to send all messages to the endpoint is to just supply true as the query).

Reference:

https://darenmay.com/blog/azure-iot-streaming-analytics-data-lake-analytics-and-json/

NEW QUESTION: 127

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: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/module-deployment-monitoring?view=iotedge-2020-11
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-automatic-device-management-cli

NEW QUESTION: 128
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: A (LEAVE A REPLY)
Explanation
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: 129
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/

NEW QUESTION: 130
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Standard tier Azure IoT hub and a fleet of IoT devices.
The devices connect to the IoT hub by using either Message Queuing Telemetry Transport (MQTT) or Advanced Message Queuing Protocol (AMQP).
You need to send data to the IoT devices and each device must respond. Each device will require three minutes to process the data and respond.
Solution: You use cloud-to-device messages and watch the cloud-to-device feedback endpoint for successful acknowledgement.
Does this meet the goal?
A. Yes
B. No
Answer: B (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 Implement Edge
Question Set 1

NEW QUESTION: 131
You have an Azure IoT solution that includes an Azure IoT hub, 100 Azure IoT Edge devices, and 500 leaf devices.
You need to perform a key rotation across the devices.
Which three types of entities should you update? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. the $edgeHub module identity
B. the $edgeAgent module identity
C. the leaf module identities
D. the IoT Edge device identities
E. the iothubowner policy credentials
F. the leaf device identities
Answer: A,D,F (LEAVE A REPLY)
To get authorization to connect to IoT Hub, devices and services must send security tokens signed with either a shared access or symmetric key. These keys are stored with a device identity in the identity registry.
An IoT Hub identity registry can be accessed like a dictionary, by using the deviceId or moduleId as the key.
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/iot-dps/how-to-control-access
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-identity-registry

NEW QUESTION: 132
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

NEW QUESTION: 133
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Azure IoT solution that includes an Azure IoT hub, a Device Provisioning Service instance, and 1,000 connected IoT devices.
All the IoT devices are provisioned automatically by using one enrollment group.
You need to temporarily disable the IoT devices from connecting to the IoT hub.
Solution: You disconnect the Device Provisioning Service from the IoT hub.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)

Instead, from the Device Provisioning Service, you disable the enrollment group, and you disable device entries in the identity registry of the IoT hub to which the IoT devices are provisioned.
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/iot-dps/how-to-unprovision-devices

NEW QUESTION: 134
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: B (LEAVE A REPLY)
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: 135
You have 10 IoT devices that connect to an Azure IoT hub named Hub1.
From Azure Cloud Shell, you run aziot hub monitor-events --hub-name Hub1 and receive the following error message: "aziot hub: 'monitor-events' is not in the 'aziot hub' command group. See 'aziot hub
--help'."
You need to ensure that you can run the command successfully. What should you run first?
A. aziot hub monitor-feedback --hub-name Hub1
B. aziot hub generate-sas-token --hub-name Hub1
C. aziot hub configuration list --hub-name Hub1

D. az extension add -name azure-cli-iot-ext

Answer: (SHOW ANSWER)

Execute az extension add --name azure-cli-iot-ext once and try again.

In order to read the telemetry from your hub by CLI, you have to enable IoT Extension with the following commands:

Add: az extension add --name azure-cli-iot-ext

Reference:

https://github.com/MicrosoftDocs/azure-docs/issues/20843

NEW QUESTION: 136

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: (SHOW ANSWER)

Explanation

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

NEW QUESTION: 137
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 primary key of the enrollment
B. the device identity of the IoT hub
C. the hostname of the IoT hub
D. the registration ID of the enrollment
Answer: B (LEAVE A REPLY)

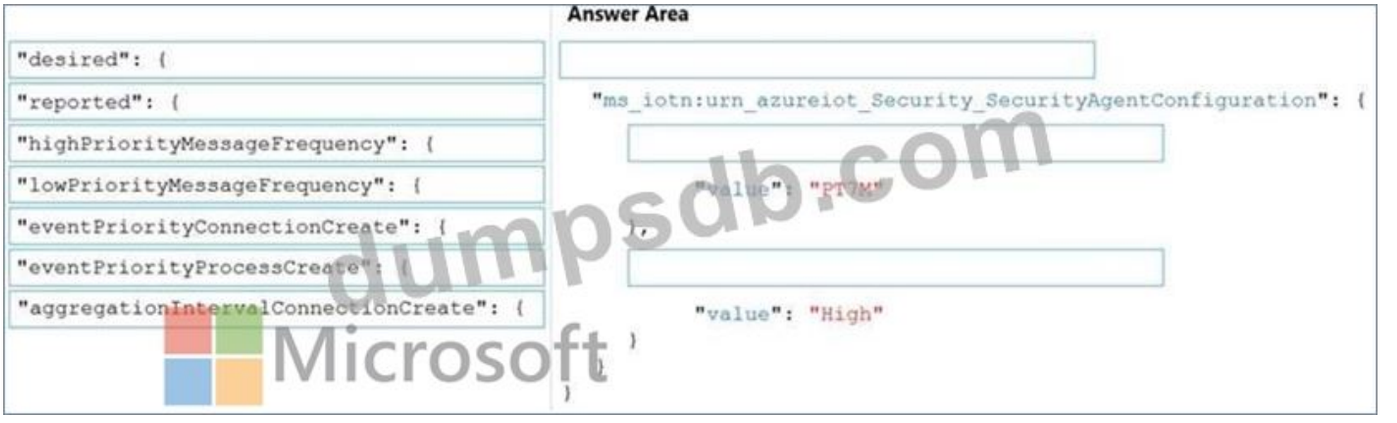
NEW QUESTION: 138
What should you do to identify the cause of the connectivity issues?

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 Provision and manage devices Question Set 2

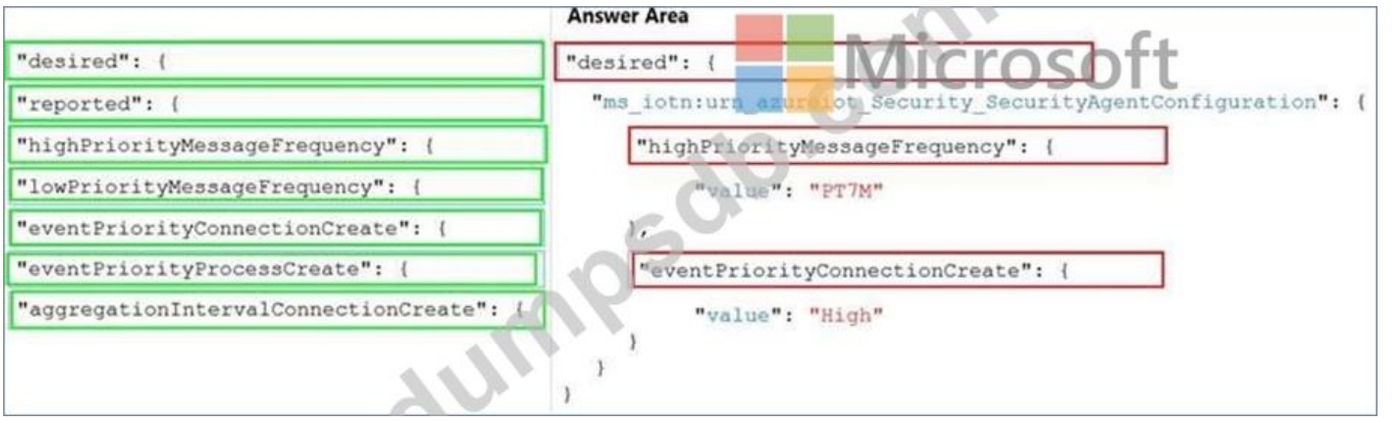
NEW QUESTION: 139
You have three Azure IoT hubs named Hub1, Hub2, and Hub3, a Device Provisioning Service instance, and an IoT device named Device1.
Each IoT hub is deployed to a separate Azure region. Device enrollment uses the Lowest latency allocation policy.
The Device Provisioning Service uses the 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: (SHOW ANSWER)

Explanation
Automated re-provisioning support.
Microsoft added first-class support for device re-provisioning which allows devices to be reassigned to a different IoT solution sometime after the initial solution assignment. Re-provisioning support is available in two options:
Factory reset, in which the device twin data for the new IoT hub is populated from the enrollment list instead of the old IoT hub. This is common for factory reset scenarios as well as leased device scenarios. Migration, in which device twin data is moved from the old IoT hub to the new IoT hub. This is common for scenarios in which a device is moving between geographies.
Reference:
https://azure.microsoft.com/en-us/blog/new-year-newly-available-iot-hub-device-provisioning-service-features/

NEW QUESTION: 140
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.



Answer:



NEW QUESTION: 141

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": {
    "iotEdge": false
  }
}
```


Existing Environment. Azure Stream Analytics

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

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

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

SELECT

AVG(temperature),

System.TimeStamp() AS AsaTime

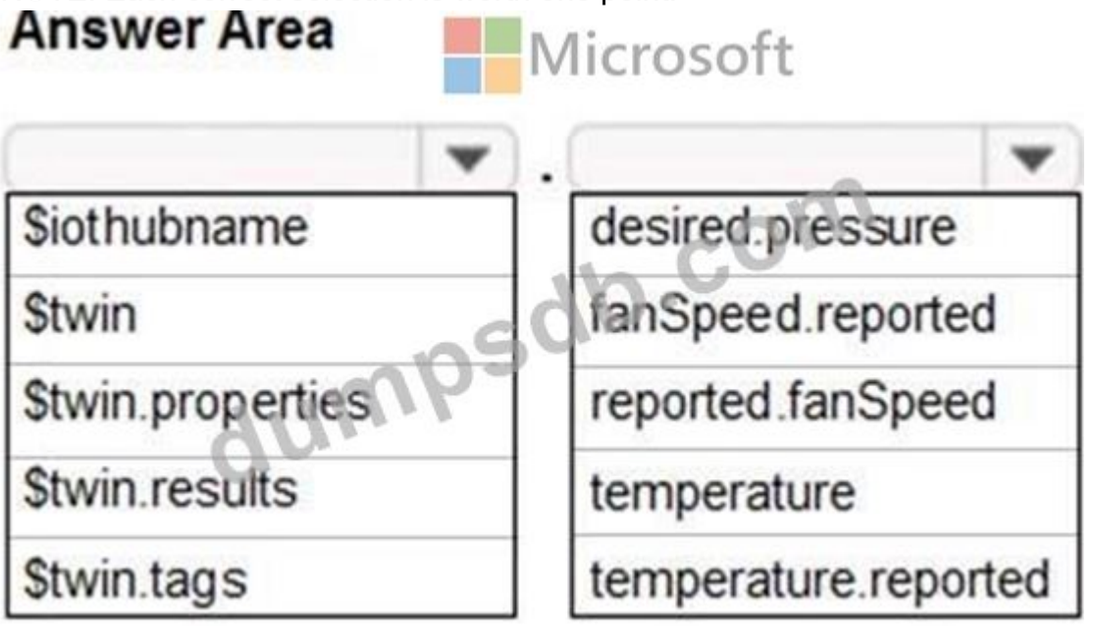
FROM

Iothub
You plan to use a 30-second period to calculate the average temperature reading of the sensors.
You plan to minimize latency between the condition reported by the sensors and the corresponding alert issued by the Stream Analytics job.
Existing Environment. Device Messages
The IoT gateway devices will send messages that contain the following JSON data whenever the temperature exceeds a specified threshold.

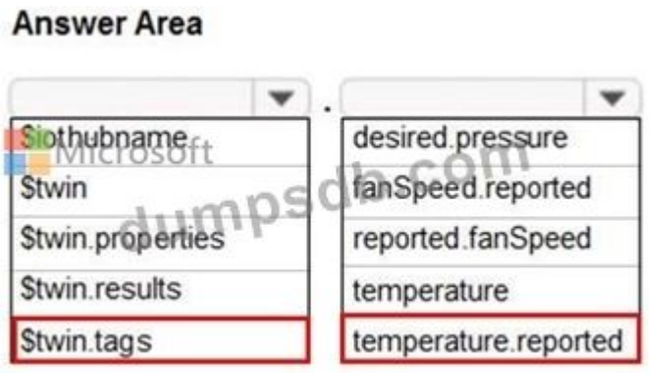
The level property will be used to route the messages to an Azure Service Bus queue endpoint named criticalep.
Existing Environment. Issues
You discover connectivity issues between the IoT gateway devices and iothub1, which cause IoT devices to lose connectivity and messages.
Requirements. Planning Changes
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: 142
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:



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

NEW QUESTION: 143
You have an Azure IoT solution.
You need to create a digital twin model.
Which language should you use?
A. XHTML
B. DTDL
C. YAML
D. XML
Answer: (SHOW ANSWER)
Explanation
Azure Digital Twins models are represented in the JSON-LD-based Digital Twin Definition Language (DTDL).

Reference:
https://docs.microsoft.com/en-us/azure/digital-twins/concepts-models
Topic 2, 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 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.
Existing Environment. Current State of Development
Contoso produces a set of Bluetooth sensors that read the temperature and humidity. The sensors connect to IoT gateway devices that relay the data.
All the IoT gateway devices connect to an Azure IoT hub named iothub1.
Existing Environment. Device Twin
You plan to implement device twins by using the following JSON sample.

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


Existing Environment. Azure Stream Analytics

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

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

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

SELECT

AVG(temperature),

System.TimeStamp() AS AsaTime

FROM

Iothub

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

You plan to minimize latency between the condition reported by the sensors and the corresponding alert issued by the Stream Analytics job.

Existing Environment. Device Messages

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

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: 144

You plan to deploy an Azure IoT hub.

The IoT hub must support the following:

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

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

A. one unit of the S1 tier

B. one unit of the B2 tier

C. one unit of the B1 tier

D. one unit of the S3 tier

Answer: D (LEAVE A REPLY)

Explanation

2500* 6 KB * 12 = 180,000 KB/minute = 180 MB/Minute.

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

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

Reference:

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