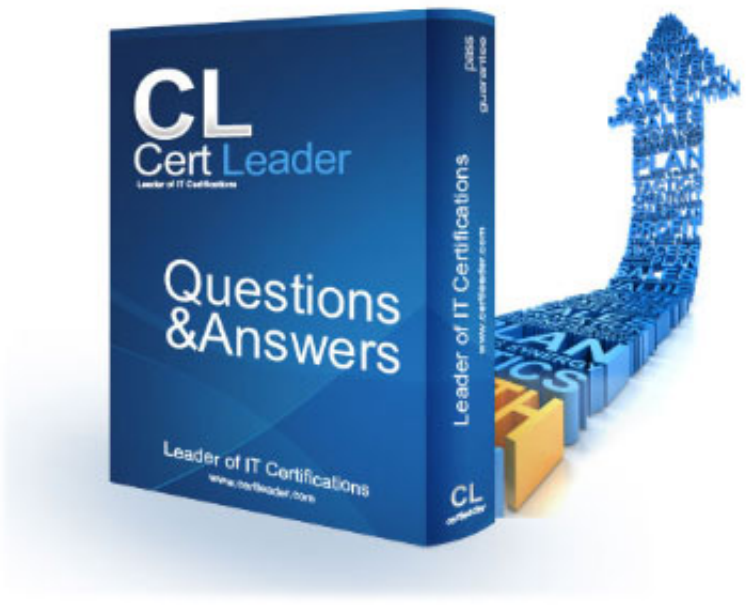
AZ-220 Dumps

Microsoft Azure IoT Developer

https://www.certleader.com/AZ-220-dumps.html



NEW QUESTION 1
- (Exam Topic 1)
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

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 2
- (Exam Topic 1)
You need to use message enrichment to add additional device information to messages sent from the IoT gateway devices when the reported temperature exceeds a critical threshold.
How should you configure the enrich message values? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

$iothubname	desired.pressure
$twin	fanSpeed.reported
$twin.properties	reported.fanSpeed
$twin.results	temperature
$twin.tags	temperature.reported

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 3
- (Exam Topic 1)
You create a new IoT device named device1 on iothub1. Device1 has a primary key of Uihuih76hbHb. How should you complete the device connection string? To answer, select the appropriate options in the
answer area.
NOTE: Each correct selection is worth one point.

HostName= [ ] . [ ] ;DeviceId= [ ] :SharedAccessKey=Uihuih76hbHb

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

A. Mastered
B. Not Mastered

Answer: A

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={YourShared Box 1: device1
Device1 has a primary key of Uihuih76hbHb. Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/quickstart-control-device-dotnet

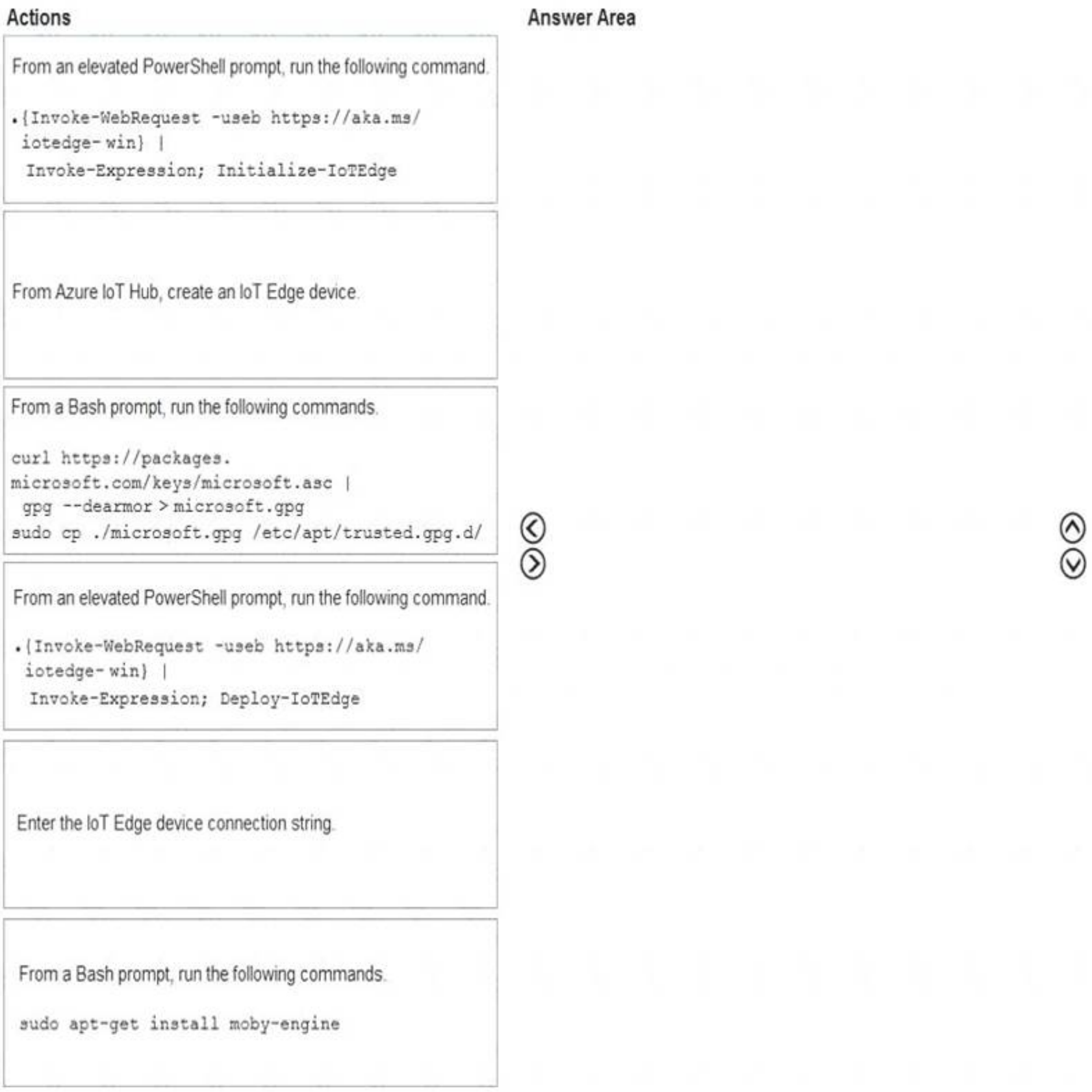
NEW QUESTION 4
- (Exam Topic 3)
You plan to deploy a standard tier Azure IoT hub.
You need to perform an over-the-air (OTA) update on devices that will connect to the IoT hub by using scheduled jobs.
What should you use?

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

Answer: D

Explanation:
Releases via the REST API.
All of the operations that can be performed from the Console can also be automated using the REST API. You might do this to automate your build and release process, for example.
You can build firmware using the Particle CLI or directly using the compile source code API.
Note: Over-the-air (OTA) firmware updates are a vital component of any IoT system. Over-the-air firmware updates refers to the practice of remotely updating the code on an embedded device.
Reference:
https://docs.particle.io/tutorials/device-cloud/ota-updates/

NEW QUESTION 5
- (Exam Topic 3)
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Step 1: From Azure IoT Hub, create an IoT Edge Device
Step 2: Deploy-IoTEdge
The Deploy-IoTEdge command checks that your Windows machine is on a supported version, turns on the containers feature, and then downloads the moby runtime and the IoT Edge runtime. The command defaults to using Windows containers.
{Invoke-WebRequest -useb https://aka.ms/iotedge-win} | Invoke-Expression; ` Deploy-IoTEdge
Step 3: Initialize-IoTEdge
The Initialize-IoTEdge command configures the IoT Edge runtime on your machine. The command defaults to manual provisioning with Windows containers.
{Invoke-WebRequest -useb https://aka.ms/iotedge Step 4: Enter the IoT Edge device connection string.
When prompted, provide the device connection string that you retrieved in step 1. The device connection string associates the physical device with a device ID in IoT Hub.
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/module-composition

NEW QUESTION 6
- (Exam Topic 3)
You have 20 devices that connect to an Azure IoT hub.
You open Azure Monitor as shown in the exhibit. (Click the Exhibit tab.)

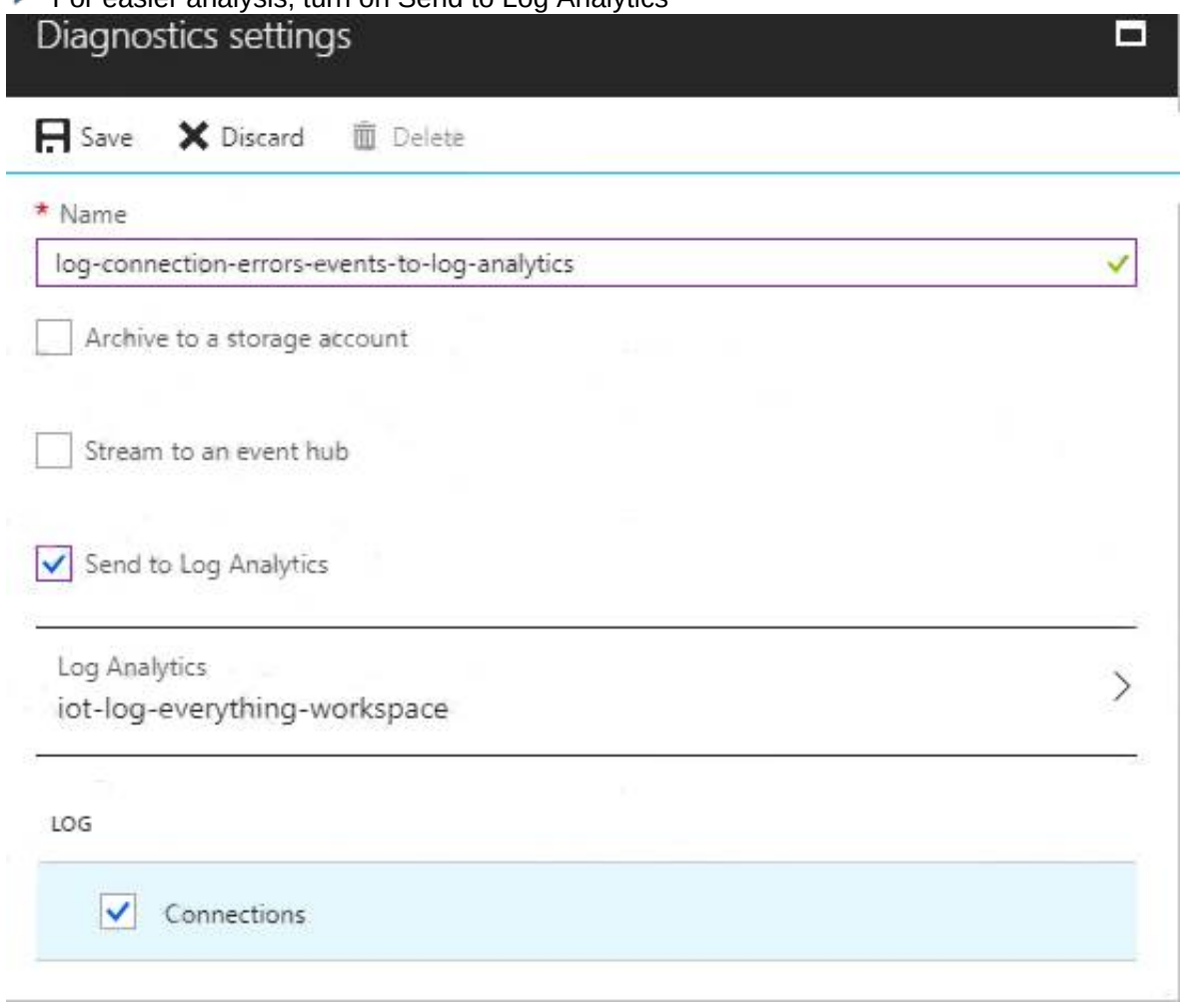
You discover that telemetry is not being received from five IoT devices.
You need to identify the names of the devices that are not generating telemetry and visualize the data. What should you do first?

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

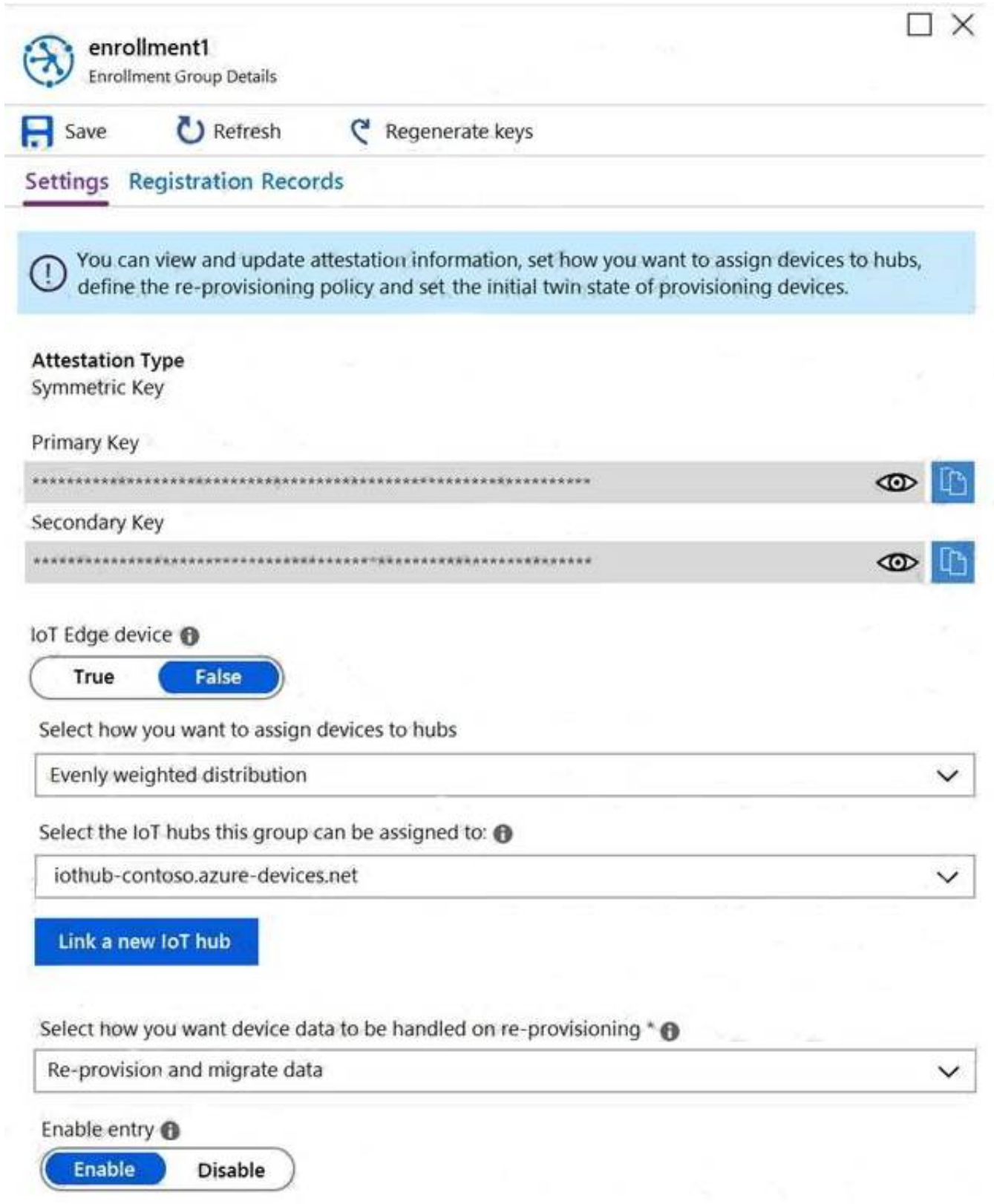
Explanation:
To log device connection events and errors, turn on diagnostics for IoT Hub. We recommend turning on these logs as early as possible, because if diagnostic logs aren't enabled, when device disconnects occur, you won't have any information to troubleshoot the problem with.

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



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

NEW QUESTION 7
- (Exam Topic 3)
From the Device Provisioning Service, you create an enrollment as shown in the exhibit. (Click the Exhibit tab.)



You need to deploy a new IoT device.
What should you use as the device identity during attestation?

A. a self-signed X.509 certificate
B. the random string of alphanumeric characters
C. the HMACSHA256 hash of the device's registration ID
D. the endorsement key of the device's Trusted Platform Module (TPM)

Answer: C

Explanation:
Each device uses its derived device key with your unique registration ID to perform symmetric key attestation with the enrollment during provisioning. To generate the device key, use the key you copied from your DPS
enrollment to compute an HMAC-SHA256 of the unique registration ID for the device and convert the result into Base64 format.
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/how-to-auto-provision-symmetric-keys

NEW QUESTION 8
- (Exam Topic 3)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this question, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have devices that connect to an Azure IoT hub. Each device has a fixed GPS location that includes latitude and longitude.
You discover that a device entry in the identity registry of the IoT hub is missing the GPS location.
You need to configure the GPS location for the device entry. The solution must prevent the changes from being propagated to the physical device.
Solution: You add tags to the device twin. Does the solution meet the goal?

A. Yes
B. No

Answer: B

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/

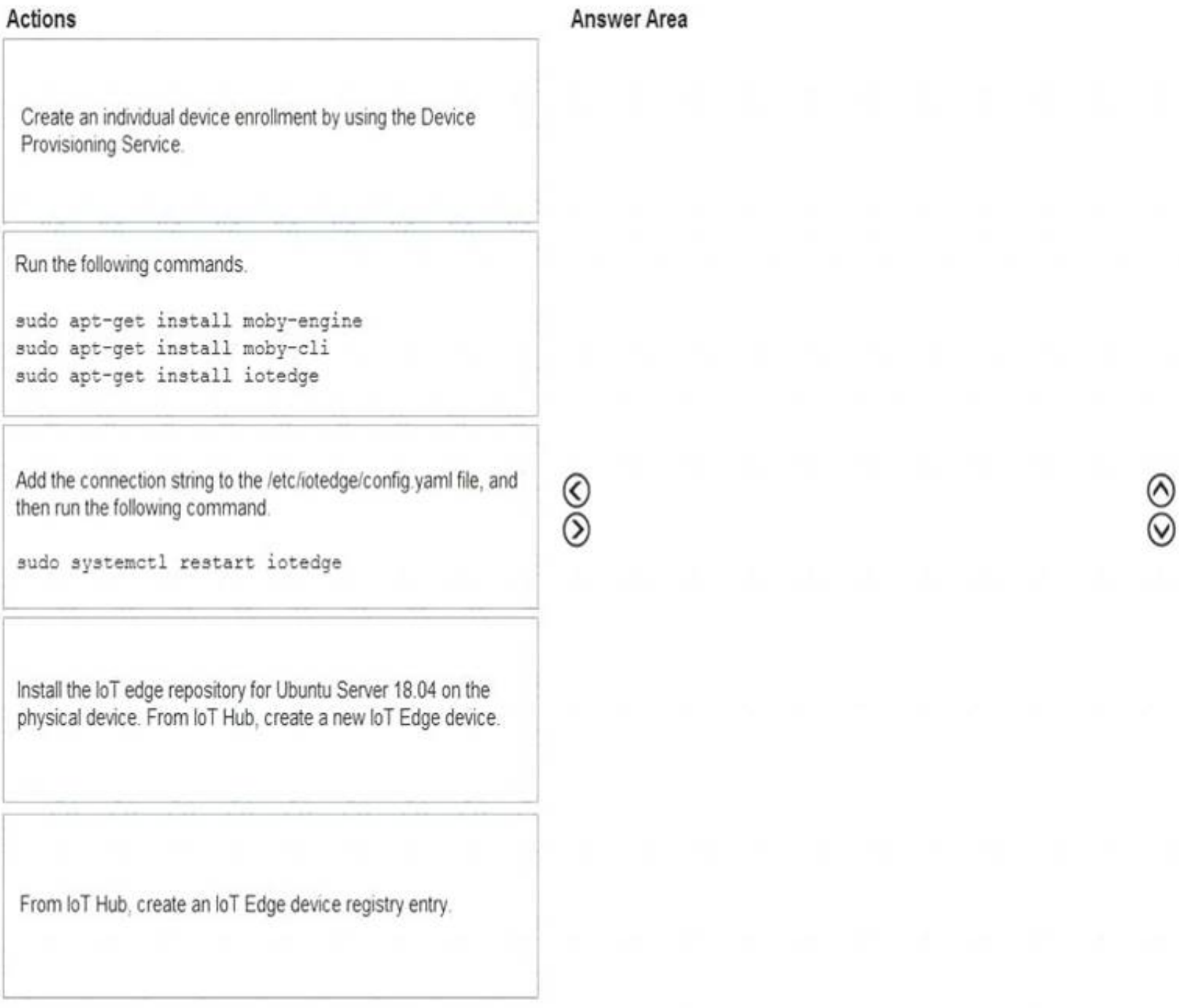
NEW QUESTION 9
- (Exam Topic 3)
You have an Azure IoT hub that is being taken from prototype to production.
You plan to connect IoT devices to the IoT hub. The devices have hardware security modules (HSMs). You need to use the most secure authentication method between the devices and the IoT hub. Company
policy prohibits the use of internally generated certificates. Which authentication method should you use?

A. an X.509 self-signed certificate
B. a certificate thumbprint
C. a symmetric key
D. An X.509 certificate signed by a root certification authority (CA).

Answer: D

Explanation:
Purchase X.509 certificates from a root certificate authority (CA). This method is recommended for production environments.
The hardware security module, or HSM, is used for secure, hardware-based storage of device secrets, and is the most secure form of secret storage. Both X.509 certificates and SAS tokens can be stored in the HSM
Reference:
https://docs.microsoft.com/en-us/azure/iot-dps/concepts-security

NEW QUESTION 10
- (Exam Topic 3)
Your company is creating a new camera security system that will use Azure IoT Hub. You plan to use an Azure IoT Edge device that will run Ubuntu Server 18.04.
You need to configure the IoT Edge device.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Step 1: Run the following commands Install the container runtime.
Azure IoT Edge relies on an OCI-compatible container runtime. For production scenarios, we recommended that you use the Moby-based engine provided below.
The Moby engine is the only container engine officially supported with Azure IoT Edge. Docker CE/EE container images are compatible with the Moby runtime.
Install the Moby engine.
sudo apt-get install moby-engine
Install the Moby command-line interface (CLI). The CLI is useful for development but optional for production deployments.
sudo apt-get install moby-cli
Install the security daemon. The package is installed at /etc/iotedge/. sudo apt-get install iotedge
Step 2: From Iot Hub,create an IoT Edge device registry entry.
Note: In your IoT Hub in the Azure portal, IoT Edge devices are created and managed separately from IOT devices that are not edge enabled.

- Sign in to the Azure portal and navigate to your IoT hub.
- In the left pane, select IoT Edge from the menu.
- Select Add an IoT Edge device.
- Provide a descriptive device ID. Use the default settings to auto-generate authentication keys and connect the new device to your hub.
- Select Save.

Retrieve the connection string in the Azure portal
*1. When you're ready to set up your device, you need the connection string that links your physical device with its identity in the IoT hub.
*2. From the IoT Edge page in the portal, click on the device ID from the list of IoT Edge devices.
*3. Copy the value of either Primary Connection String or Secondary Connection String.
Step 3: Add the connection string to..
To manually provision a device, you need to provide it with a device connection string that you can create by registering a new device in your IoT hub.
Open the configuration file.
sudo nano /etc/iotedge/config.yaml
Find the provisioning configurations of the file and uncomment the Manual provisioning configuration section. Update the value of device_connection_string with the connection string from your IoT Edge device.
Save and close the file.
After entering the provisioning information in the configuration file, restart the daemon: sudo systemctl restart iotedge
Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/how-to-install-iot-edge-linux

NEW QUESTION 10
- (Exam Topic 3)
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

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 15
- (Exam Topic 3)
You have an Azure IoT hub that uses a Device Provisioning Service instance.
You have 1,000 legacy IoT devices that only support MAC address or serial number identities. The device do NOT have a security feature that can be used to securely identify the device or a hardware security module (HSM).
You plan to deploy the devices to a secure environment.
You need to configure the Device Provisioning Service instance to ensure that all the devices are identified securely before they receive updates.
Which attestation mechanism should you choose?

A. Trusted Platform Module (TPM) 1.2 attestation
B. symmetric key attestation
C. X.509 certificates

Answer: B

Explanation:
A common problem with many legacy devices is that they often have an identity that is composed of a single piece of information. This identity information is usually a MAC address or a serial number. Legacy devices may not have a certificate, TPM, or any other security feature that can be used to securely identify the device. The Device Provisioning Service for IoT hub includes symmetric key attestation. Symmetric key attestation can be used to identify a device based off information like the MAC address or a serial number.
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/iot-dps/how-to-legacy-device-symm-key

NEW QUESTION 20
- (Exam Topic 3)
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: BDE

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 21
- (Exam Topic 3)
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

Explanation:
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 25
- (Exam Topic 3)
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: BC

Explanation:
B: X.509 certificates are typically arranged in a certificate chain of trust. If a certificate at any stage in a chain becomes compromised, trust is broken. The certificate must be blacklisted to prevent Device Provisioning Service from provisioning devices downstream in any chain that contains that certificate.
C: Individual enrollments apply to a single device and can use either X.509 certificates or SAS tokens (in a real or virtual TPM) as the attestation mechanism. (Devices that use SAS tokens as their attestation mechanism can be provisioned only through an individual enrollment.) To blacklist a device that has an individual enrollment, you can either disable or delete its enrollment entry.
To blacklist a device that has an individual enrollment, you can either disable or delete its enrollment entry. Reference:
https://docs.microsoft.com/en-us/azure/iot-dps/how-to-revoke-device-access-portal

NEW QUESTION 26
- (Exam Topic 3)
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 Edg
B. Select Edge1, and then select Manage Child Device
C. From a Bash prompt, run the following command:az iot edge set-modules -device-id Edge1 -hub-name Hub1 -content C:\deploymentMan1.json
D. Create an IoT Edge deployment manifest that specifies the temperature module and the route to$upstrea
E. From a Bush prompt, run the following command: az iot hub monitor-events-device-id Edge1 -hub-name Hub1
F. From the Azure portal, navigate to Hub1 and select IoT Edg
G. Select Edge1, select Device Twin, and then set the deployment manifest as a desired propert
H. From a Bash prompt, run the following commandaz iot hub monitor-events-device-id Edge1 -hub-name Hub1
I. Create an IoT Edge deployment manifest that specifies the temperature module and the route to$upstrea
J. 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

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 30
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your AZ-220 Exam with Our Prep Materials Via below:

https://www.certleader.com/AZ-220-dumps.html