Exam Questions AZ-220

Microsoft Azure IoT Developer

https://www.2passeasy.com/dumps/AZ-220/

NEW QUESTION 1
- (Exam Topic 1)
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

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 2
- (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 3
- (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.

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 4
- (Exam Topic 3)
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: ADF

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 5
- (Exam Topic 3)
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: ACE

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 6
- (Exam Topic 3)
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

Explanation:
MQTT over WebSockets uses port 443. Reference:
https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-protocols

NEW QUESTION 7
- (Exam Topic 3)
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: CE

Explanation:
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 8
- (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 9
- (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 10
- (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 12
- (Exam Topic 3)
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.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Step 1: Register a device in IoT Hub
Before you can use your IoT devices with Azure IoT Edge, you must register them with your IoT hub. Once a device is registered, you can retrieve a connection string to set up your device for IoT Edge workloads.
Step 2: Configure the device connection string on a device client.
When you're ready to set up your device, you need the connection string that links your physical device with its identity in the IoT hub.
Step 3: Trigger a new send event from a device client. Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/how-to-register-device

NEW QUESTION 15
- (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 17
- (Exam Topic 3)
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.

A. Mastered
B. Not Mastered

Answer: A

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 18
- (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 22
- (Exam Topic 3)
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: AC

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 27
- (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 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

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 28
- (Exam Topic 3)
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

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 29
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual AZ-220 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the AZ-220 Product From:

https://www.2passeasy.com/dumps/AZ-220/

Money Back Guarantee

AZ-220 Practice Exam Features:

* AZ-220 Questions and Answers Updated Frequently

* AZ-220 Practice Questions Verified by Expert Senior Certified Staff

* AZ-220 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* AZ-220 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year