



Microsoft

Exam Questions AZ-220

Microsoft Azure IoT Developer

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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 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

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 4

- (Exam Topic 3)

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.

- A. Mastered
- B. Not Mastered

Answer: A

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 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 archive 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/lot-hub/iot-hub-troubleshoot-connectivity>

NEW QUESTION 7

- (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 8

- (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 9

- (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 10

- (Exam Topic 3)

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: D

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

- (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 13

- (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 16

- (Exam Topic 3)

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

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 20

- (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 23

- (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: 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

Explanation:

You may find it necessary to deprovision devices that were previously auto-provisioned through the Device Provisioning Service.

In general, deprovisioning a device involves two steps:

*1. Disenroll the device from your provisioning service, to prevent future auto-provisioning. Depending on whether you want to revoke access temporarily or permanently, you may want to either disable or delete an enrollment entry.

*2. Deregister the device from your IoT Hub, to prevent future communications and data transfer. Again, you can temporarily disable or permanently delete the device's entry in the identity registry for the IoT Hub where it was provisioned.

Reference:

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

NEW QUESTION 25

- (Exam Topic 3)

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

You plan to use Azure functions to process all the telemetry messages from the devices before storing the messages.

You need to configure the functions binding for the IoT hub.

Which two configuration details should you use to configure the binding? Each Answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. the name of the resource group that contains the IoT hub

B. the IoT hub's connection string shared access key that has Service connect permissions

C. the connection string of the Azure Event Hub-compatible endpoint from the IoT Hub built-in endpoints

D. the Azure Event-Hub compatible name

Answer: CD

Explanation:

EventHubName: Functions 2.x and higher. The name of the event hub. When the event hub name is also present in the connection string, that value overrides this property at runtime.

Connection: The name of an app setting that contains the connection string to the event hub's namespace. Copy this connection string by clicking the Connection Information button for the namespace, not the event hub itself. This connection string must have send permissions to send the message to the event stream.

Reference:

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

NEW QUESTION 30

- (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 use an Azure policy to apply tags to a resource group. 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 32

- (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/iotedge-dev: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 33

- (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 36

- (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 38

.....

Relate Links

100% Pass Your AZ-220 Exam with ExamBible Prep Materials

<https://www.exambible.com/AZ-220-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>