DUMPSARENA

# Microsoft Azure IoT Developer

## Microsoft AZ-220

## Version Demo

**Total Demo Questions: 15**

**Total Premium Questions: 271**

**Buy Premium PDF**

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 2, New Update | 135 |
| Topic 3, Case Study 1 | 2 |
| Topic 4, Case Study 2 | 3 |
| Topic 5, Case Study 3 | 5 |
| Topic 6, Mixed Questions | 126 |
| Total | 271 |

## QUESTION NO: 1

You have an IoT device that has the following configurations:

• Hardware: Raspberry Pi

• Operating system: Raspberry Pi OS

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.** Install the IoT Edge runtime.

**B.** Create a module twin configuration.

**C.** Run the az iot hub module-identity update command.

**D.** Install the container runtime.

**ANSWER: A D**

## QUESTION NO: 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.

**E.** Create an Azure logic app that has a scheduled trigger.

**ANSWER: B C**

**Explanation:**

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

C: 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

## QUESTION NO: 3

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**

**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/

## QUESTION NO: 4

You have an Azure IoT solution.

You need to test that the solution remains functional if IoT Hub is affected by a regional outage.

What should you do?

**A.** From the IoT hub, set Allow public network access to Disabled.

**B.** From the IoT hub, start a manual failover.

**C.** From the Device Provisioning Service (DPS), unlink the IoT hub.

**D.** From the IoT hub, select Disable fallback route.

**ANSWER: B**

**Explanation:**

Manual failover is a feature of the IoT Hub service that allows customers to failover their hub's operations from a primary region to the corresponding Azure geo-paired region. Manual failover can be done in the event of a regional disaster or an extended service outage. You can also perform a planned failover to test your disaster recovery capabilities, although we recommend using a test IoT hub rather than one running in production. Reference:

https://docs.microsoft.com/en-us/azure/iot-hub/tutorial-manual-failover

## QUESTION NO: 5

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**

**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

## QUESTION NO: 6

You have an Azure IoT Central solution

You need to verify that telemetry messages from devices arrive to IoT Central.

What should you use?

**A.** the Azure IoT explorer

**B.** the az command in Azure CLI

**C.** Azure Service Bus Explorer

**D.** the Azure IoT Tools for VS Code extension pack

**ANSWER: B**

## QUESTION NO: 7 - (HOTSPOT)

You are creating an Azure Digital Twins Query.

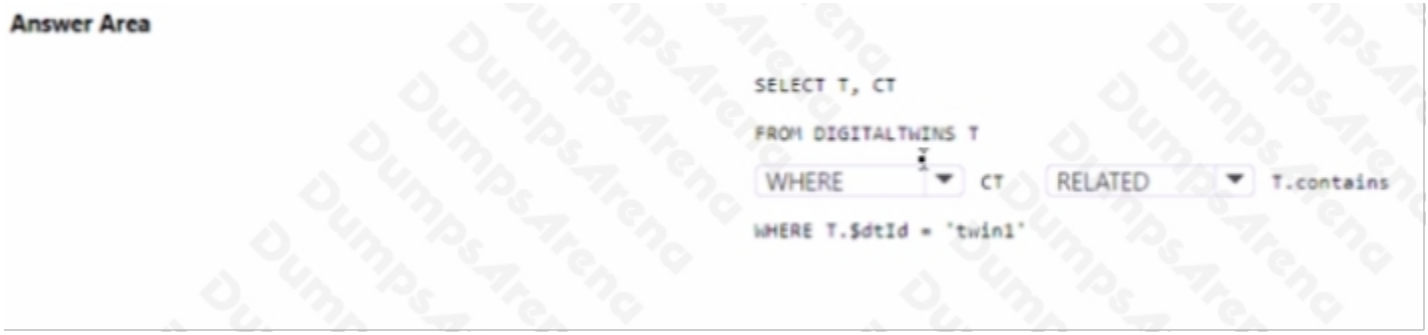
You need to return all the digital twins that have a contains relationship with a digital twin that has an ID of twin1.

How should you complete the query? To answer, select the appropriate options m the answer area

NOTE: Each correct selection is worth one point.


**ANSWER:**


**Explanation:**




## QUESTION NO: 8 - (HOTSPOT)

You have an Azure IoT solution that includes an Azure IoT hub and 50 IoT devices. The device twins have the following structure.

```
{
  "tags": {
    "deploymentLocation": "Building 4, Room 100"
  },
  "properties": {
    "desired": {
      "firmwareVersion": "2.0",
      },
    },
    "reported": {
      "firmwareVersion": "1.0",
      },
    }
  }
}
```

You need to configure message enrichments to add the following values to messages:

• The device deployment location

• The device firmware version

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

NOTE: Each correct selection is worth one point.


**ANSWER:**


**Explanation:**


## QUESTION NO: 9

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**

**Explanation:**

Note: Symptoms

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

Cause

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

https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-troubleshoot-error-409002-linkcreationconflict#symptoms
https://devblogs.microsoft.com/iotdev/understand-different-connection-strings-in-azure-iot-hub/

**QUESTION NO: 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 deploymentMan1.json

**B.** Create an IoT Edge deployment manifest that specifies the temperature module and the route to $upstream. From a Bash prompt, run the following command: az iot hub monitor-events --device-id Edge1 --hub-name Hub1

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

**D.** Create an IoT Edge deployment manifest that specifies the temperature module and the route to $upstream. From a Bash prompt, run the following command: az iot edge set-modules --device-id Edge1 --hub-name Hub1 --content 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

**QUESTION NO: 11**

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**

**QUESTION NO: 12 - (DRAG DROP)**

You have an Azure subscription that contains an Azure IoT hub and 100 IoT devices.

The devices connect to the IoT hub by using the Advanced Message Queuing Protocol (AMQP) protocol and authenticate to the IoT hub by using symmetric keys.

You need to configure the SASL PLAIN username for the AMQP connection.

How should you configure the username? To answer, drag the appropriate options to the correct targets. Each option 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:**


## QUESTION NO: 13

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

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

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

What should you do?

**A.** Configure the upstream protocol of the devices to use MQTT over TCP.

**B.** Configure the upstream protocol of the devices to use AMQP over WebSocket.

**C.** Connect the external networks to the IoT solution by using ExpressRoute.

**D.** Integrate cellular communication hardware onto the devices and avoid the use of the external networks.

**ANSWER: B**

**Explanation:**

AMQP over WebSockets uses port 443.

Reference:

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

## QUESTION NO: 14

You have an existing Azure IoT hub.

You use IoT Hub jobs to schedule long running tasks on connected devices.

Which three operations do the IoT Hub jobs support directly? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

**A.** Trigger Azure functions.

**B.** Invoke direct methods.

**C.** Update desired properties.

**D.** Send cloud-to-device messages.

**E.** Disable IoT device registry entries.

**F.** Update tags.

**ANSWER: B C F**

**Explanation:**

Consider using jobs when you need to schedule and track progress any of the following activities on a set of devices: ▪ Invoke direct methods

- Update desired properties
- Update tags

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

## QUESTION NO: 15 - (DRAG DROP)

DRAG DROP

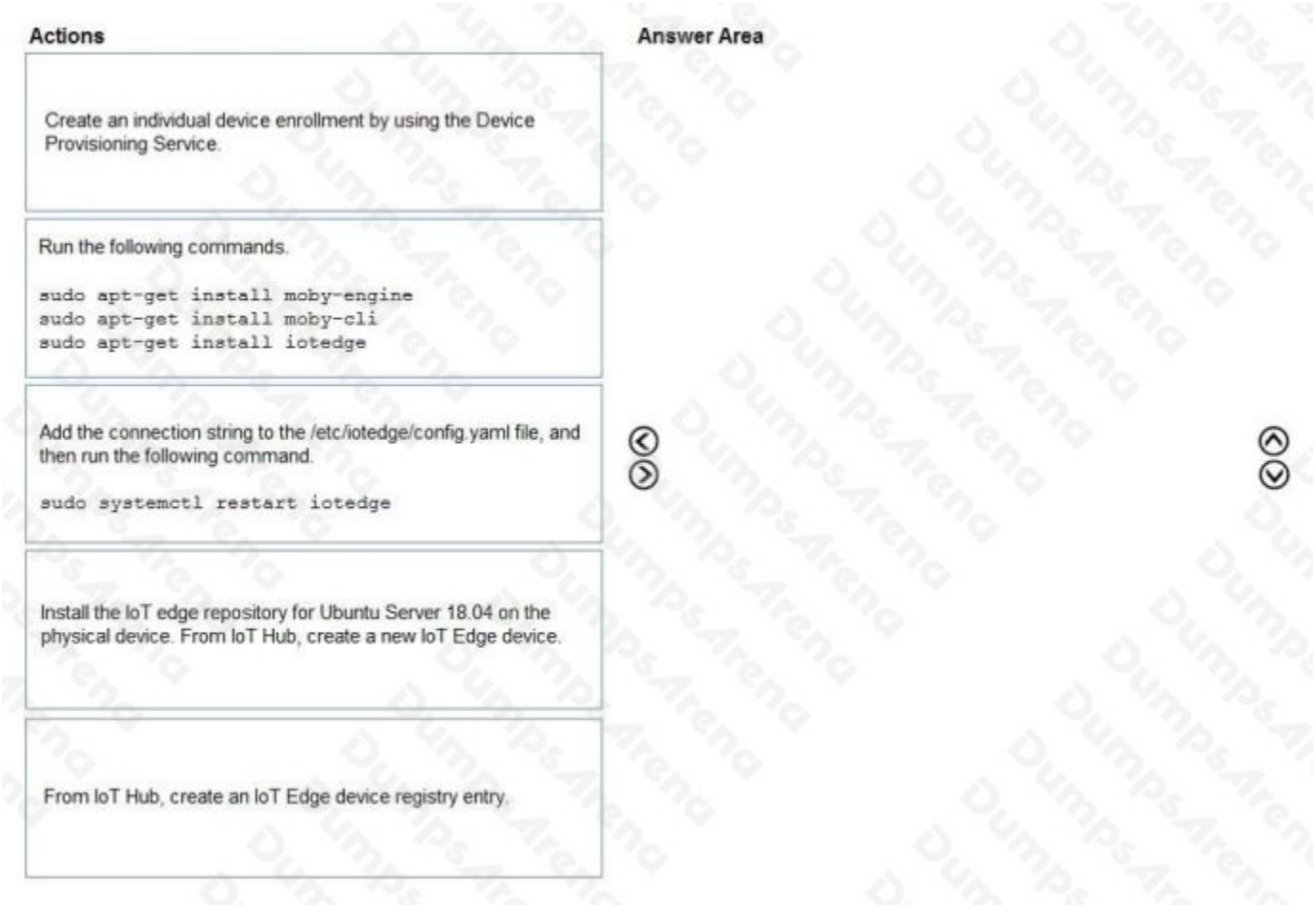
Your company is creating a new camera security system that will use Azure IoT Hub.

You plan to use an Azure IoT Edge device that will run Ubuntu Server 18.04.

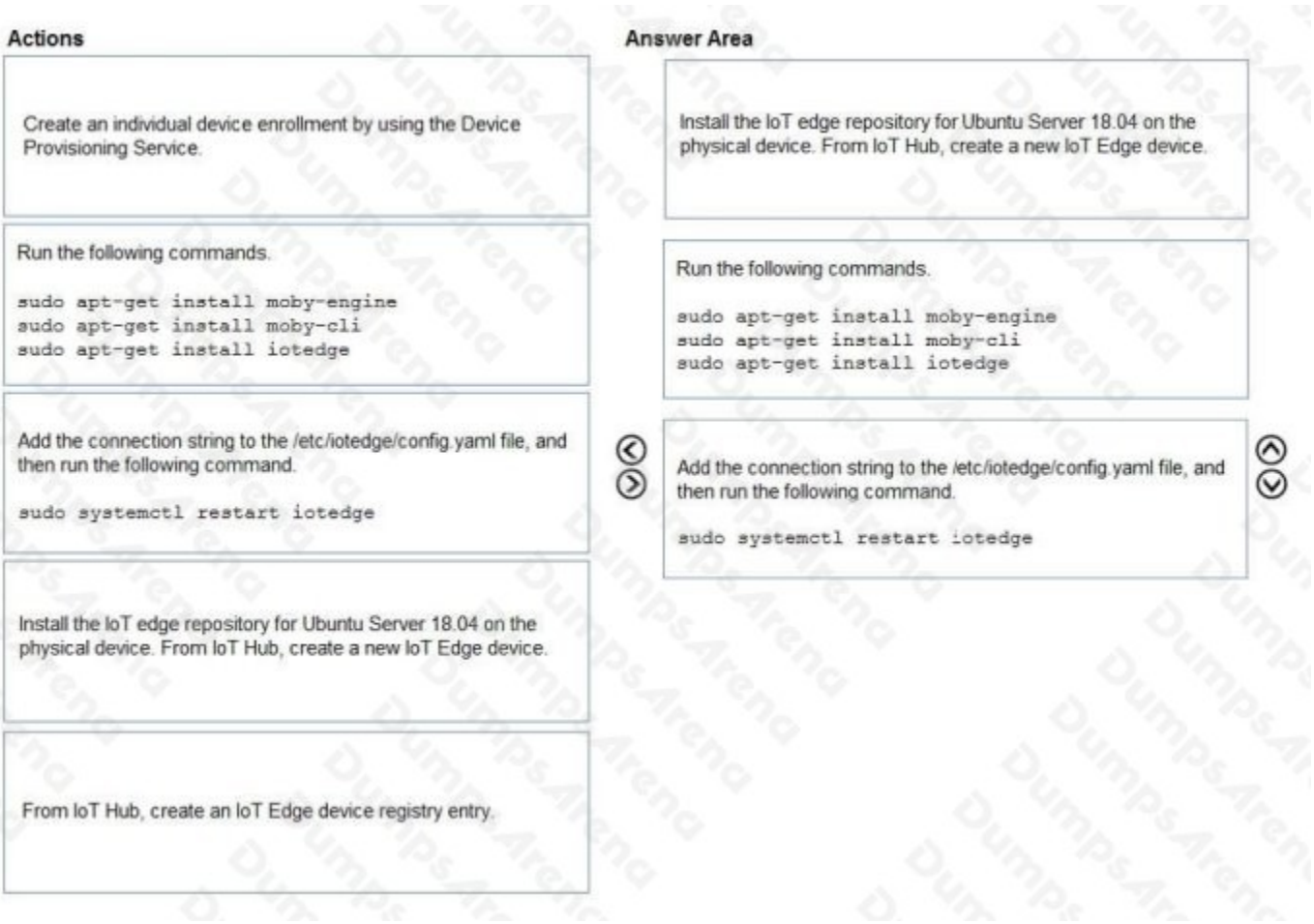
You need to configure the IoT Edge device.

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.

**Select and Place:**




**ANSWER:**




**Explanation:**

Step1: Install the IoT edge repository for Ubuntu Server 18.04 on the physical device. From IoT hub, create a new IoT Edge device.

Prepare your device to access the Microsoft installation packages.

Install the repository configuration that matches your device operating system.

Ubuntu Server 18.04: curl https://packages.microsoft.com/config/ubuntu/18.04/multiarch/prod.list > ./microsoft-prod.list

In your IoT Hub in the Azure portal, IoT Edge devices are created and managed separately from IOT devices that are not edge enabled.

1. Sign in to the Azure portal and navigate to your IoT hub.

2. In the left pane, select IoT Edge from the menu.

3. Select Add an IoT Edge device.

4. Provide a descriptive device ID. Use the default settings to auto-generate authentication keys and connect the new device to your hub.

5. Select Save.

Step 2: 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 3: Add the connection string to the /etc/iotedge/config.yaml file,..

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