AZ-220^{Q&As}

Microsoft Azure IoT Developer

Pass Microsoft AZ-220 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/az-220.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

Instant Download After Purchase

100% Money Back Guarantee

365 Days Free Update

800,000+ Satisfied Customers

QUESTION 1

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

Correct Answer: B

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

---

QUESTION 2

HOTSPOT

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.

Hot Area:

Answer Area

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

Correct Answer:

Answer Area

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

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

QUESTION 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

Correct Answer: B

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/

QUESTION 4

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
Hub1	Azure IoT Hub
DPS1	Azure IoT Hub Device Provisioning service (DPS)
CA1	Certification authority (CA)

You create a group enrollment in DPS1 and enroll 100 IoT devices. Each device is issued a leaf certificate from CA1. You need to deprovision a single IoT device from the group enrollment. The solution must not affect the other devices.

Solution: Solution: You create a disabled individual enrollment by using the X.509 certificate of CA1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

QUESTION 5

DRAG DROP

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.

Select and Place:

Actions

Answer Area

6 / 23

From an elevated PowerShell prompt, run the following command.

```
.{Invoke-WebRequest -useb https://aka.ms/
iotedge- win} |
  Invoke-Expression; Initialize-IoTEdge
```

From Azure IoT Hub, create an IoT Edge device.

From a Bash prompt, run the following commands.

```
curl https://packages.
microsoft.com/keys/microsoft.asc |
  gpg --dearmor > microsoft.gpg
sudo cp ./microsoft.gpg /etc/apt/trusted.gpg.d/
```

⊙
⊙

⊙
⊙

From an elevated PowerShell prompt, run the following command.

```
.{Invoke-WebRequest -useb https://aka.ms/
iotedge- win} |
  Invoke-Expression; Deploy-IoTEdge
```

Enter the IoT Edge device connection string.

From a Bash prompt, run the following commands.

```
sudo apt-get install moby-engine
```

Correct Answer:

Actions

Answer Area

From Azure IoT Hub, create an IoT Edge device.

From an elevated PowerShell prompt, run the following command.

```
.{Invoke-WebRequest -useb https://aka.ms/
iotedge-win} |
  Invoke-Expression; Deploy-IoTEdge
```

From a Bash prompt, run the following commands.

```
curl https://packages.
microsoft.com/keys/microsoft.asc |
  gpg --dearmor > microsoft.gpg
sudo cp ./microsoft.gpg /etc/apt/trusted.gpg.d/
```

From an elevated PowerShell prompt, run the following command.

```
.{Invoke-WebRequest -useb https://aka.ms/
iotedge-win} |
  Invoke-Expression; Initialize-IoTEdge
```

Enter the IoT Edge device connection string.

From a Bash prompt, run the following commands.

```
sudo apt-get install moby-engine
```

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

QUESTION 6

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

Correct Answer: B

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

QUESTION 7

HOTSPOT

You have an Azure IoT hub and three Azure IoT Edge devices. The device twin code for each device is shown in the following table.

Name	Device twin code fragment
Device1	"tags": { "office": "Seattle1" },
Device2	"tags": { "office": "Seattle2" },
Device3	"tags": { "office": "London" },

A standard automatic deployment is already applied.

You have three layered deployments. The deployment code for each deployment is shown in the following table.

Name	Deployment code
| Deployment1 | ```
{
    "id": "deploy1",
    "priority": 90,
     "targetCondition": " tags.office='Seattle1' OR tags.office='Seattle2' ",
...
"$edgeAgent": {
                "properties.desired.modules.MyModule1": {
...
"$edgeHub": {
                "properties.desired.routes.MyModule1": "FROM
/messages/modules/MyModule1/outputs/seattle1 INTO $upstream",
                "properties.desired.routes.MyModule1A": "FROM /messages/modules/MyModule1/* INTO
$upstream"
...
}
``` |
| Deployment2 | ```
{
    "id": "deploy2",
    "priority": 80,
     "targetCondition": " tags.office='Seattle1' OR tags.office='Seattle2' OR tags.office='London'
",
...
"$edgeAgent": {
                "properties.desired.modules.MyModule1": {
...
"$edgeHub": {
                "properties.desired.routes.MyModule1": "FROM
/messages/modules/MyModule1/ouputs/seattle2 INTO $upstream",
                "properties.desired.routes.MyModule1A": "FROM /messages/modules/MyModule1/* INTO
$upstream"
                "properties.desired.routes.MyModule1B": "FROM /messages/modules/MyModule1/* INTO
$upstream"
...
``` |
| Deployment3 | ```
{
    "id": "deploy3",
    "priority": 70,
     "targetCondition": " tags.office='London' ",
-
"$edgeAgent": {
                "properties.desired.modules.MyModule1": {
-
                },
                "properties.desired.modules.MyModule2": {
...
                }
...
"$edgeHub": {
                "properties.desired.routes.MyModule1": "FROM /messages/modules/MyModule1/* INTO
$upstream",
                "properties.desired.routes.MyModule2": "FROM /messages/modules/MyModule2/* INTO
$upstream"
...
}
``` |

For each of the following statements, select Yes if the statement is true. Otherwise select No. NOTE: Each correct

selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
Device1 routes messages to /messages/modules/MyModule1/outputs/seattle2.	○	○
Device2 has the MyModule1B route deployed.	○	○
Device3 has the MyModule2 route deployed.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
Device1 routes messages to /messages/modules/MyModule1/outputs/seattle2.	○	○
Device2 has the MyModule1B route deployed.	○	○
Device3 has the MyModule2 route deployed.	○	○

QUESTION 8

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

Correct Answer: ACE

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

QUESTION 9

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 Message Queuing Telemetry Transport (MQTT) protocol and authenticate to the IoT hub by using symmetric keys

You need to configure the username and password for the MQTT connection.

What should you use? To answer, drag the appropriate components to the correct targets. Each component 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.

Select and Place:

Components

The device ID
The MAC address
The X.509 public key
The symmetric key of the device
The shared access signature (SAS) token

Answer Area

Username: {IoThubhostname}/ [   ]

Password: [   ]

Correct Answer:

Components

The MAC address
The X.509 public key
The symmetric key of the device

Answer Area

Username: {IoThubhostname}/ | The device ID

Password: | The shared access signature (SAS) token

QUESTION 10

DRAG DROP

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.

Select and Place:

Actions

Sign the CA1 certificate by using the intermediate CA certificate.

Sign the intermediate CA certificate by using the CA1 certificate.

Sign the device certificate by using the intermediate CA certificate.

Sign the device certificate by using the CA1 certificate.

Deploy the certificate chain to the device.

Answer Area

Correct Answer:

Actions

Sign the CA1 certificate by using the intermediate CA certificate.

Sign the device certificate by using the CA1 certificate.

Answer Area

Sign the intermediate CA certificate by using the CA1 certificate.

Sign the device certificate by using the intermediate CA certificate.

Deploy the certificate chain to the device.

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

QUESTION 11

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.

Correct Answer: C

QUESTION 12

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
Hub1	Azure IoT Hub
DPS1	Azure IoT Hub Device Provisioning service (DPS)
CA1	Certification authority (CA)

You create a group enrollment in DPS1 and enroll 100 IoT devices. Each device is issued a leaf certificate from CAT.

You need to deprovision a single IoT device from the group enrollment. The solution must not affect the other devices.

Solution: You create a disabled individual enrollment by using the X.509 certificate of the device.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

QUESTION 13

From the Device Provisioning Service, you create an enrollment as shown in the exhibit.

☐ ✕

enrollment1
Enrollment Group Details

🖫 Save   ↻ Refresh   ⤾ Regenerate keys

Settings   **Registration Records**

⊙ You can view and update attestation information, set how you want to assign devices to hubs, define the re-provisioning policy and set the initial twin state of provisioning devices.

Attestation Type
Symmetric Key

Primary Key

`**************************************************************`   👁 ⧉

Secondary Key

`**************************************************************`   👁 ⧉

IoT Edge device ⓘ

| True | **False** |

Select how you want to assign devices to hubs

| Evenly weighted distribution | ⌄ |

Select the IoT hubs this group can be assigned to: ⓘ

| iothub-contoso.azure-devices.net | ⌄ |

Link a new IoT hub

Select how you want device data to be handled on re-provisioning * ⓘ

| Re-provision and migrate data | ⌄ |

Enable entry ⓘ

| **Enable** | Disable |

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 HMAC-SHA256 hash of the device\\\'s registration ID

D. the endorsement key of the device\\\'s Trusted Platform Module (TPM)

Correct Answer: C

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

---

QUESTION 14

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

Correct Answer: D

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

---

QUESTION 15

HOTSPOT

You have an Azure 10T hub and an I0T device.

You are developing an IoT solution that will generate an alert when the IoT device leaves a geofenced area. The device sends telemetry in the following format.

```
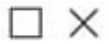{
    "location": {
        "type":"Point",
        "coordinates": [76.6, 10.1]
    }
}
```

You create an Azure Stream Analytics job that uses telemetry input from the IoT hub and a reference input that contains the data shown in the following table.

DeviceID	DeviceName	Geofence
"Device1"	"Device1"	"POLYGON((-122.13301696018573 47.63764925180358, -122.13272728161212 47.63764925180358, -122.1327487392842447.63784082716388,-122.13373579220172 47.63782998329432))"

How should you complete the Stream Analytics query? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
SELECT ReferenceInput.DeviceName, TelemetryInput.Location
INTO Output
FROM TelemetryInput JOIN ReferenceInput ON
        TelemetryInput.[_____ A _____ ▼]


WHERE st_within (


    WHERE st_within (  [____ B ____ ▼]   [____ C ____ ▼]
```

A ▼
DeviceID = ReferenceInput.DeviceID
ConnectionDeviceID = Referenceinput.DeviceID
loTHub.ConnectionDeviceid = Referenceinput.DeviceID
loTHub.ConnectionDeviceGenerationid = Referenceinput.DeviceID

B ▼
TelemetryInput.Location.
Referenceinput.Geofence.
TelemetryInput.Partitonid.
ReferenceInput.DeviceID

C ▼
TelemetryInput.Location)!=0
ReferenceInput.Geofence)!=0
TelemetryInput.PartitionID)!=0
ReferenceInput.DeviceID)!=0

Correct Answer:

Answer Area

SELECT ReferenceInput.DeviceName, TelemetryInput.Location
INTO Output
FROM TelemetryInput JOIN ReferenceInput ON

    TelemetryInput.[**A** ▼]

WHERE st_within (

    WHERE st_within ([**B** ▼] [**C** ▼]

A ▼
DeviceID = ReferenceInput.DeviceID
ConnectionDeviceID = ReferenceInput.DeviceID
IoTHub.ConnectionDeviceid = ReferenceInput.DeviceID
IoTHub.ConnectionDeviceGenerationid = ReferenceInput.DeviceID

B ▼
TelemetryInput.Location.
ReferenceInput.Geofence.
TelemetryInput.Partitonid.
ReferenceInput.DeviceID

C ▼
TelemetryInput.Location)!=0
ReferenceInput.Geofence)!=0
TelemetryInput.PartitionID)!=0
ReferenceInput.DeviceID)!=0