AZ-220

Number: AZ-220
Passing Score: 800
Time Limit: 120 min
File Version: 1

AZ-220

Implement the IoT solution infrastructure

Testlet 1

Case Study

This is a case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case**. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question on this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

Existing Environment. Current State of Development

Contoso produces a set of Bluetooth sensors that read the temperature and humidity. The sensors connect to IoT gateway devices that relay the data.

All the IoT gateway devices connect to an Azure IoT hub named iothub1.

Existing Environment. Device Twin

You plan to implement device twins by using the following JSON sample.

```
{
  "deviceId": "device_n",
  "etag": "AAAAAAAAAAQ=",
  "deviceEtag": "NDcwMTU4Mzk=",
  "status": "enabled",
  "statusUpdateTime": "0001-01-01T00:00:00Z",
  "connectionState": "Disconnected",
  "lastActivityTime": "0001-01-01T00:00:00Z",
  "cloudToDeviceMessageCount": 0,
  "authenticationType": "sas",
  "x509Thumbprint": {
    "primaryThumbprint": null,
    "secondaryThumbprint": null
  },
  "version": 11,
  "properties": {
    "desired": {
      "fanSpeed": 70,
      "$metadata": {
        "$lastUpdated": "2019-10-16T09:43:42.2944169Z",
        "$lastUpdatedVersion": 4,
        "fanSpeed": {
          "$lastUpdated": "2019-10-16T09:43:42.2944169Z",
          "$lastUpdatedVersion": 4
        }
      },
      "$version": 4
    },
    "reported": {
      "fanSpeed": 80,
      "metadata": {
        "$lastUpdated": "2019-10-16T09:43:42.4035171Z",
        "fanSpeed": {
        "$lastUpdated": "2019-10-16T09:43:42.4035171Z"
        }
      },
```

Existing Environment. Azure Stream Analytics

Each room will have between three to five sensors that will generate readings that are sent to a single IoT gateway device. The IoT gateway device will forward all the readings to iothub1 at intervals of between 10 and 60 seconds.

You plan to use a gateway pattern so that each IoT gateway device will have its own IoT Hub device identity.

You draft the following query, which is missing the `GROUP BY` clause.

```
SELECT
    AVG(temperature),
        System.TimeStamp() AS AsaTime
FROM
    Iothub
```

You plan to use a 30-second period to calculate the average temperature reading of the sensors.

You plan to minimize latency between the condition reported by the sensors and the corresponding alert issued by the Stream Analytics job.

Existing Environment. Device Messages

The IoT gateway devices will send messages that contain the following JSON data whenever the temperature exceeds a specified threshold.

```
{
  "event": {
    "payload": "Temperature = 26.23 Humidity = 78.70597746416186 Button = 0",
    "properties": {
      "application": {
        "level": "critical"
      }
    }
  }
}
```

The `level` property will be used to route the messages to an Azure Service Bus queue endpoint named criticalep.

Existing Environment. Issues

You discover connectivity issues between the IoT gateway devices and iothub1, which cause IoT devices to lose connectivity and messages.

Requirements. Planning Changes Contoso

plans to make the following changes:

- Use Stream Analytics to process and view data.
- Use Azure Time Series Insights to visualize data.
- Implement a system to sync device statuses and required settings.
- Add extra information to messages by using message enrichment.
- Create a notification system to send an alert if a condition exceeds a specified threshold.
- Implement a system to identify what causes the intermittent connection issues and lost messages.

Requirements. Technical Requirements

Contoso must meet the following requirements:

- Use the built-in functions of IoT Hub whenever possible.
- Minimize hardware and software costs whenever possible.
- Minimize administrative effort to provision devices at scale.
- Implement a system to trace message flow to and from iothub1.
- Minimize the amount of custom coding required to implement the planned changes.
- Prevent read operations from being negatively affected when you implement additional services.

Implement the IoT solution infrastructure

Question Set 2

QUESTION 1
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.

https://vceplus.com Does the solution meet the goal?

A. Yes
B. No

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 2

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 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 IoT hub, you change the credentials for the shared access policy of the IoT devices.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 4
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

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
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/

QUESTION 5
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.

NOTE: Each correct selection is worth one point.

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.

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
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}"
}
```

Incorrect Answers:
D: Deprecated: initialize a file upload with a GET. Use the POST method instead.

Reference: https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/iot-hub/iot-hub-configure-file-upload.md

QUESTION 6
You plan to deploy an Azure IoT hub.

The IoT hub must support the following:

- Three Azure IoT Edge devices
- 2,500 IoT devices

Each IoT device will spend a 6 KB message every five seconds.

You need to size the IoT hub to support the devices. The solution must minimize costs.

What should you choose?

A. one unit of the S1 tier
B. one unit of the B2 tier
C. one unit of the B1 tier
D. one unit of the S3 tier

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
2500* 6 KB * 12 = 180,000 KB/minute = 180 MB/Minute.

B3, S3 can handle up to 814 MB/minute per unit.

Incorrect Answers:
A, C: B1, S1 can only handle up to 1111 KB/minute per unit
B: B2, S2 can only handle up to 16 MB/minute per unit.

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

QUESTION 7
You create an Azure IoT hub by running the following command.

```
az iot hub create --resource-group MyResourceGroup --name MyIotHub --sku B1 --location westus --partition-count 4
```


What does MylotHub support?

A. Device Provisioning Service
B. cloud-to-device messaging
C. Azure IoT Edge
D. device twins

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The Device Provisioning Service is included in the Basic Tiers (such as B1).

Incorrect Answers:
B, C, D: The Standard tier is needed for cloud-to-device messaging, Azure IoT Edge, and device twins.

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

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
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 9
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.

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:
Explanation:
MQTT over WebSockets uses port 443.

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

Provision and manage devices

Testlet 1

Case Study

This is a case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case**. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question on this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

Existing Environment. Current State of Development
Contoso produces a set of Bluetooth sensors that read the temperature and humidity. The sensors connect to IoT gateway devices that relay the data.

All the IoT gateway devices connect to an Azure IoT hub named iothub1.

Existing Environment. Device Twin

You plan to implement device twins by using the following JSON sample.

```
{
  "deviceId": "device_n",
  "etag": "AAAAAAAAAAQ=",
  "deviceEtag": "NDcwMTU4Mzk=",
  "status": "enabled",
  "statusUpdateTime": "0001-01-01T00:00:00Z",
  "connectionState": "Disconnected",
  "lastActivityTime": "0001-01-01T00:00:00Z",
  "cloudToDeviceMessageCount": 0,
  "authenticationType": "sas",
  "x509Thumbprint": {
    "primaryThumbprint": null,
    "secondaryThumbprint": null
  },
  "version": 11,
  "properties": {
    "desired": {
      "fanSpeed": 70,
      "$metadata": {
        "$lastUpdated": "2019-10-16T09:43:42.2944169Z",
        "$lastUpdatedVersion": 4,
        "fanSpeed": {
          "$lastUpdated": "2019-10-16T09:43:42.2944169Z",
          "$lastUpdatedVersion": 4
        }
      },
      "$version": 4
    },
    "reported": {
      "fanSpeed": 80,
      "metadata": {
        "$lastUpdated": "2019-10-16T09:43:42.4035171Z",
        "fanSpeed": {
        "$lastUpdated": "2019-10-16T09:43:42.4035171Z"
        }
      },
```

Existing Environment. Azure Stream Analytics

Each room will have between three to five sensors that will generate readings that are sent to a single IoT gateway device. The IoT gateway device will forward all the readings to iothub1 at intervals of between 10 and 60 seconds.

You plan to use a gateway pattern so that each IoT gateway device will have its own IoT Hub device identity.

You draft the following query, which is missing the `GROUP BY` clause.

```
SELECT
    AVG(temperature),
        System.TimeStamp() AS AsaTime
FROM
    Iothub
```

You plan to use a 30-second period to calculate the average temperature reading of the sensors.

You plan to minimize latency between the condition reported by the sensors and the corresponding alert issued by the Stream Analytics job.

Existing Environment. Device Messages

The IoT gateway devices will send messages that contain the following JSON data whenever the temperature exceeds a specified threshold.

```
{
  "event": {
    "payload": "Temperature = 26.23 Humidity = 78.70597746416186 Button = 0",
    "properties": {
      "application": {
        "level": "critical"
      }
    }
  }
}
```

The `level` property will be used to route the messages to an Azure Service Bus queue endpoint named criticalep.

Existing Environment. Issues

You discover connectivity issues between the IoT gateway devices and iothub1, which cause IoT devices to lose connectivity and messages.

Requirements. Planning Changes

Contoso plans to make the following changes:

- Use Stream Analytics to process and view data.
- Use Azure Time Series Insights to visualize data.
- Implement a system to sync device statuses and required settings.
- Add extra information to messages by using message enrichment.
- Create a notification system to send an alert if a condition exceeds a specified threshold.
- Implement a system to identify what causes the intermittent connection issues and lost messages.

Requirements. Technical Requirements

Contoso must meet the following requirements:

- Use the built-in functions of IoT Hub whenever possible.
- Minimize hardware and software costs whenever possible.
- Minimize administrative effort to provision devices at scale.
- Implement a system to trace message flow to and from iothub1.
- Minimize the amount of custom coding required to implement the planned changes.
- Prevent read operations from being negatively affected when you implement additional services.

QUESTION 1
What should you do to identify the cause of the connectivity issues?

A. Send cloud-to-device messages to the IoT devices.
B. Use the heartbeat pattern to send messages from the IoT devices to iothub1.
C. Monitor the connection status of the device twin by using an Azure function.
D. Enable the collection of the Connections diagnostics logs and set up alerts for the connected devices count metric.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Scenario: You discover connectivity issues between the IoT gateway devices and iothub1, which cause IoT devices to lose connectivity and messages.

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. Step 1:

1. Sign in to the Azure portal.
2. Browse to your IoT hub.
3. Select Diagnostics settings.
4. Select Turn on diagnostics.
5. Enable Connections logs to be collected.
6. For easier analysis, turn on Send to Log Analytics (see pricing).

Step 2:
Set up alerts for device disconnect at scale
To get alerts when devices disconnect, configure alerts on the Connected devices (preview) metric.

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

Provision and manage devices

Question Set 2

QUESTION 1
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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/

QUESTION 2

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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/

QUESTION 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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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/

QUESTION 4
You have three Azure IoT hubs named Hub1, Hub2, and Hub3, a Device Provisioning Service instance, and an IoT device named Device1.

Each IoT hub is deployed to a separate Azure region.

Device enrollment uses the Lowest latency allocation policy.

The Device Provisioning Service uses the Lowest latency allocation policy.

Device1 is auto-provisioned to Hub1 by using the Device Provisioning Service.

Device1 regularly moves between regions.

You need to ensure that Device1 always connects to the IoT hub that has the lowest latency.

What should you do?

A. Configure device attestation that uses X.509 certificates.
B. Implement device certificate rolling.
C. Disenroll and reenroll Device1.
D. Configure the re-provisioning policy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Automated re-provisioning support.
Microsoft added first-class support for device re-provisioning which allows devices to be reassigned to a different IoT solution sometime after the initial solution assignment. Re-provisioning support is available in two options:
- Factory reset, in which the device twin data for the new IoT hub is populated from the enrollment list instead of the old IoT hub. This is common for factory reset scenarios as well as leased device scenarios.
- Migration, in which device twin data is moved from the old IoT hub to the new IoT hub. This is common for scenarios in which a device is moving between geographies.

Reference: https://azure.microsoft.com/en-us/blog/new-year-newly-available-iot-hub-device-provisioning-service-features/

QUESTION 5
You have an Azure subscription that contains a resource group named RG1.

You need to deploy the Device Provisioning Service. The solution must ensure that the Device Provisioning Service can accept new device enrollments.

You create a Device Provisioning Service instance.

Which two actions should you perform next? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From the **Linked IoT hubs** blade of the Device Provisioning Service, link an Azure IoT hub.
B. From the Azure portal, create a new Azure IoT hub.
C. From the Manage allocation policy blade of the Device Provisioning Service, configure an allocation policy.
D. From the Certificates blade of the Device Provisioning Service, upload an X.509 certificate to the Device Provisioning Service.

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
Explanation:
A: The Device Provisioning Service can only provision devices to IoT hubs that have been linked to it.

C: Allocation policy. The service-level setting that determines how Device Provisioning Service assigns devices to an IoT hub. There are three supported allocation policies:
- Lowest latency: devices are provisioned to an IoT hub with the lowest latency to the device.
- Evenly weighted distribution
- Static configuration via the enrollment list

Reference: https://docs.microsoft.com/bs-latn-ba/azure/iot-dps/concepts-service

QUESTION 6
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.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 7
You have an Azure IoT Central application.

You need to connect an IoT device to the application.

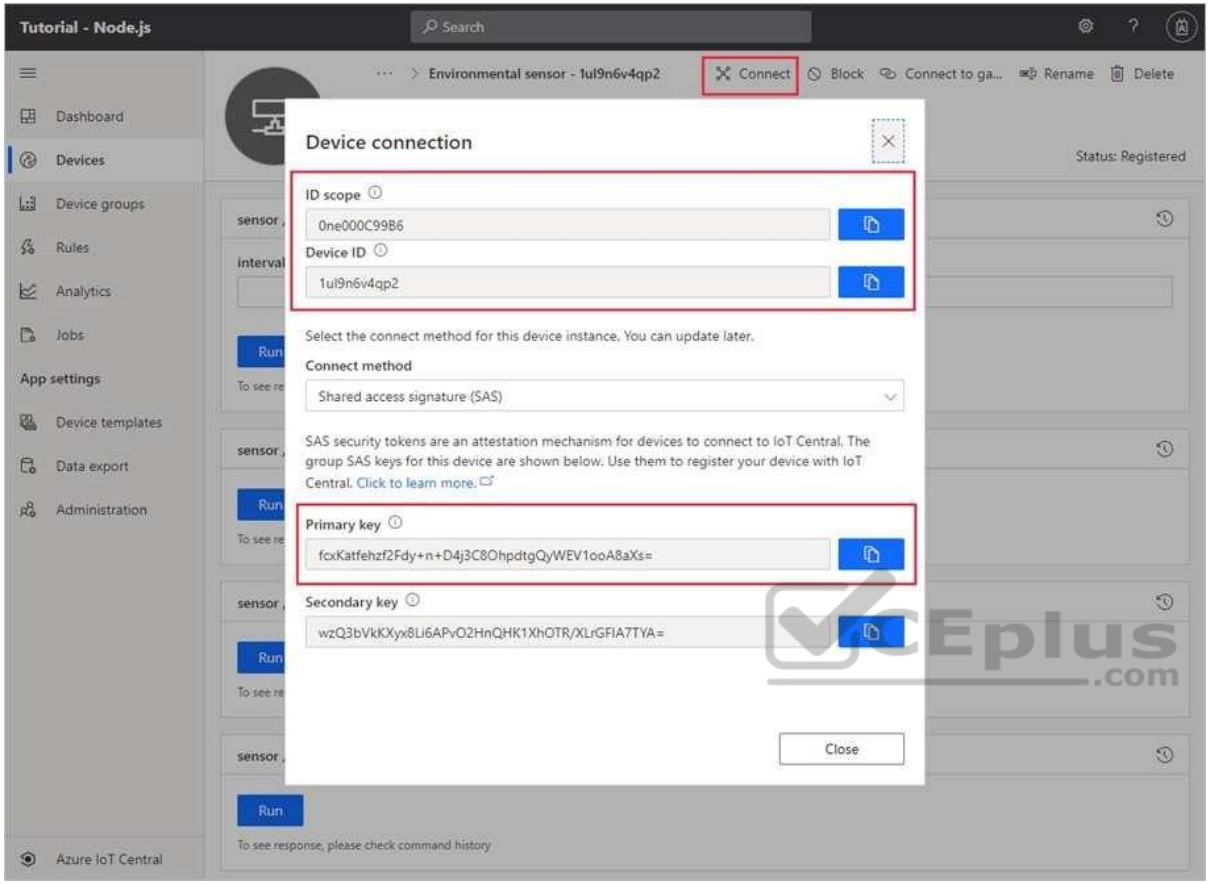
Which two settings do you require in IoT Central to configure the device? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Group SAS Primary Key
B. the IoT hub nameC. Scope ID
D. Application Name E.
Device ID

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
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

QUESTION 8
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.

Correct Answer: BCF
Section: (none)
Explanation

Explanation/Reference:
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 9
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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 10
You have an Azure IoT hub that uses a Device Provisioning Service instance.

You create a new individual device enrollment that uses symmetric key attestation.

Which detail from the enrollment is required to auto provision the device by using the Device Provisioning Service?

A. the registration ID of the enrollment
B. the primary key of the enrollment
C. the device identity of the IoT hub
D. the hostname of the IoT hub

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
An enrollment is the record of devices or groups of devices that may register through auto-provisioning. The enrollment record contains information about the device or group of devices, including:
▪ the attestation mechanism used by the device ▪
the optional initial desired configuration
▪ desired IoT hub
the desired device ID

Note: Azure IoT auto-provisioning can be broken into three phases:
1. Service configuration - a one-time configuration of the Azure IoT Hub and IoT Hub Device Provisioning Service instances, establishing them and creating linkage between them.

2. Device enrollment - the process of making the Device Provisioning Service instance aware of the devices that will attempt to register in the future. Enrollment is accomplished by configuring device identity information in the provisioning service, as either an "individual enrollment" for a single device, or a "group enrollment" for multiple devices.
3. Device registration and configuration

Reference:
https://docs.microsoft.com/en-us/azure/iot-dps/concepts-service#enrollment

QUESTION 11
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
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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

Implement Edge

Question Set 1

QUESTION 1

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`

Correct Answer: BDE
Section: (none)
Explanation

Explanation/Reference:
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 **QUESTION 2**

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 C:\deploymentMan1.json`
B. Create an IoT Edge deployment manifest that specifies the temperature module and the route to `$upstream`. From a Bush prompt, run the following command: `az iot hub monitor-events-device-id Edge1 -hub-name Hub1`
C. From the Azure portal, navigate to Hub1 and select IoT Edge. Select **Edge1**, select **Device Twin**, and then set the deployment manifest as a desired property. From a Bash prompt, run the following command `az iot hub monitor-events-device-id Edge1 -hub-name Hub1`
D. Create an IoT Edge deployment manifest that specifies the temperature module and the route to `$upstream`. From a Bush prompt, run the following command: `az iot edge set-modules -device-id Edge1 -hub-name Hub1 -content C:\deploymentMan1.json`

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 3
You have the devices shown in the following table.

Name	Type	Hardware configuration
Device1	Azure Sphere microcontroller unit (MCU)	4 MB of RAM ARM processor
Device2	Raspberry Pi single board computer (SBC)	1 GB of RAM ARM processor
Device3	Desktop computer	8 GB of RAM x64 processor
Device4	Apple iPhone	4 GB of RAM ARM processor

You are implementing a proof of concept (POC) for an Azure IoT solution.

You need to deploy an Azure IoT Edge device as part of the POC.

On which two devices can you deploy IOT Edge? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Device1
B. Device2
C. Device3
D. Device4

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Azure IoT Edge runs great on devices as small as a Raspberry Pi3 to server grade hardware.

Tier 1.
The systems listed in the following table are supported by Microsoft, either generally available or in public preview, and are tested with each new release.

Operating System	AMD64	ARM32v7	ARM64
Raspbian Stretch		✓	
Ubuntu Server 16.04	✓		Public preview
Ubuntu Server 18.04	✓		Public preview
Windows 10 IoT Core, build 17763	✓		
Windows 10 IoT Enterprise, build 17763	✓		
Windows Server 2019, build 17763	✓		
Windows Server IoT 2019, build 17763	✓		

Reference:
https://docs.microsoft.com/en-us/azure/iot-edge/support **Process and manage data**

Testlet 1

Case Study

This is a case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case**. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

To start the case study
To display the first question on this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

Existing Environment. Current State of Development

Contoso produces a set of Bluetooth sensors that read the temperature and humidity. The sensors connect to IoT gateway devices that relay the data.

All the IoT gateway devices connect to an Azure IoT hub named iothub1.

Existing Environment. Device Twin

You plan to implement device twins by using the following JSON sample.

```
{
  "deviceId": "device_n",
  "etag": "AAAAAAAAAAQ=",
  "deviceEtag": "NDcwMTU4Mzk=",
  "status": "enabled",
  "statusUpdateTime": "0001-01-01T00:00:00Z",
  "connectionState": "Disconnected",
  "lastActivityTime": "0001-01-01T00:00:00Z",
  "cloudToDeviceMessageCount": 0,
  "authenticationType": "sas",
  "x509Thumbprint": {
    "primaryThumbprint": null,
    "secondaryThumbprint": null
  },
  "version": 11,
  "properties": {
    "desired": {
      "fanSpeed": 70,
      "$metadata": {
        "$lastUpdated": "2019-10-16T09:43:42.2944169Z",
        "$lastUpdatedVersion": 4,
        "fanSpeed": {
          "$lastUpdated": "2019-10-16T09:43:42.2944169Z",
          "$lastUpdatedVersion": 4
        }
      },
      "$version": 4
    },
    "reported": {
      "fanSpeed": 80,
      "metadata": {
        "$lastUpdated": "2019-10-16T09:43:42.4035171Z",
        "fanSpeed": {
        "$lastUpdated": "2019-10-16T09:43:42.4035171Z"
        }
      },
```

Existing Environment. Azure Stream Analytics

Each room will have between three to five sensors that will generate readings that are sent to a single IoT gateway device. The IoT gateway device will forward all the readings to iothub1 at intervals of between 10 and 60 seconds.

You plan to use a gateway pattern so that each IoT gateway device will have its own IoT Hub device identity.

You draft the following query, which is missing the `GROUP BY` clause.

```
SELECT
    AVG(temperature),
        System.TimeStamp() AS AsaTime
FROM
    Iothub
```

You plan to use a 30-second period to calculate the average temperature reading of the sensors.

You plan to minimize latency between the condition reported by the sensors and the corresponding alert issued by the Stream Analytics job.

Existing Environment. Device Messages

The IoT gateway devices will send messages that contain the following JSON data whenever the temperature exceeds a specified threshold.

```
{
  "event": {
    "payload": "Temperature = 26.23 Humidity = 78.70597746416186 Button = 0",
    "properties": {
      "application": {
        "level": "critical"
      }
    }
  }
}
```

The `level` property will be used to route the messages to an Azure Service Bus queue endpoint named criticalep.

Existing Environment. Issues

You discover connectivity issues between the IoT gateway devices and iothub1, which cause IoT devices to lose connectivity and messages.

Requirements. Planning Changes

Contoso plans to make the following changes:

- Use Stream Analytics to process and view data.
- Use Azure Time Series Insights to visualize data.
- Implement a system to sync device statuses and required settings.
- Add extra information to messages by using message enrichment.
- Create a notification system to send an alert if a condition exceeds a specified threshold.
- Implement a system to identify what causes the intermittent connection issues and lost messages.

Requirements. Technical Requirements

Contoso must meet the following requirements:

- Use the built-in functions of IoT Hub whenever possible.
- Minimize hardware and software costs whenever possible.
- Minimize administrative effort to provision devices at scale.
- Implement a system to trace message flow to and from iothub1.
- Minimize the amount of custom coding required to implement the planned changes.
- Prevent read operations from being negatively affected when you implement additional services.

QUESTION 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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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