DUMPSQUEEN

Microsoft Azure IoT Developer

Microsoft AZ-220

Version Demo

Total Demo Questions: 15

Total Premium Questions: 271

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

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 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: 2

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 delete the device entry from the device registry of Hub1. Does this meet the goal?

A. Yes

B. No

ANSWER: B

QUESTION NO: 3

You have an Azure IoT Edge module named SampleModule that runs on a device named Device1.

You make changes to the code of SampleModule by using Microsoft Visual Studio Code.

You need to push the code to the container registry and then deploy the module to Device1.

Which two actions should you perform from Visual Studio Code? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Build and push the SampleModule code to the registry.

B. Create a deployment for a single device.

C. Generate a deployment manifest.

D. Build an IoT Edge solution.

E. Generate a shared access signature (SAS) token for Device1.

ANSWER: B C

Explanation:

C: Configure a deployment manifest. A deployment manifest is a JSON document that describes which modules to deploy, how data flows between the modules, and desired properties of the module twins.

B: You deploy modules to your device by applying the deployment manifest that you configured with the module information.
Reference:

https://docs.microsoft.com/en-us/azure/iot-edge/how-to-deploy-modules-vscode

QUESTION NO: 4 - (DRAG DROP)

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.

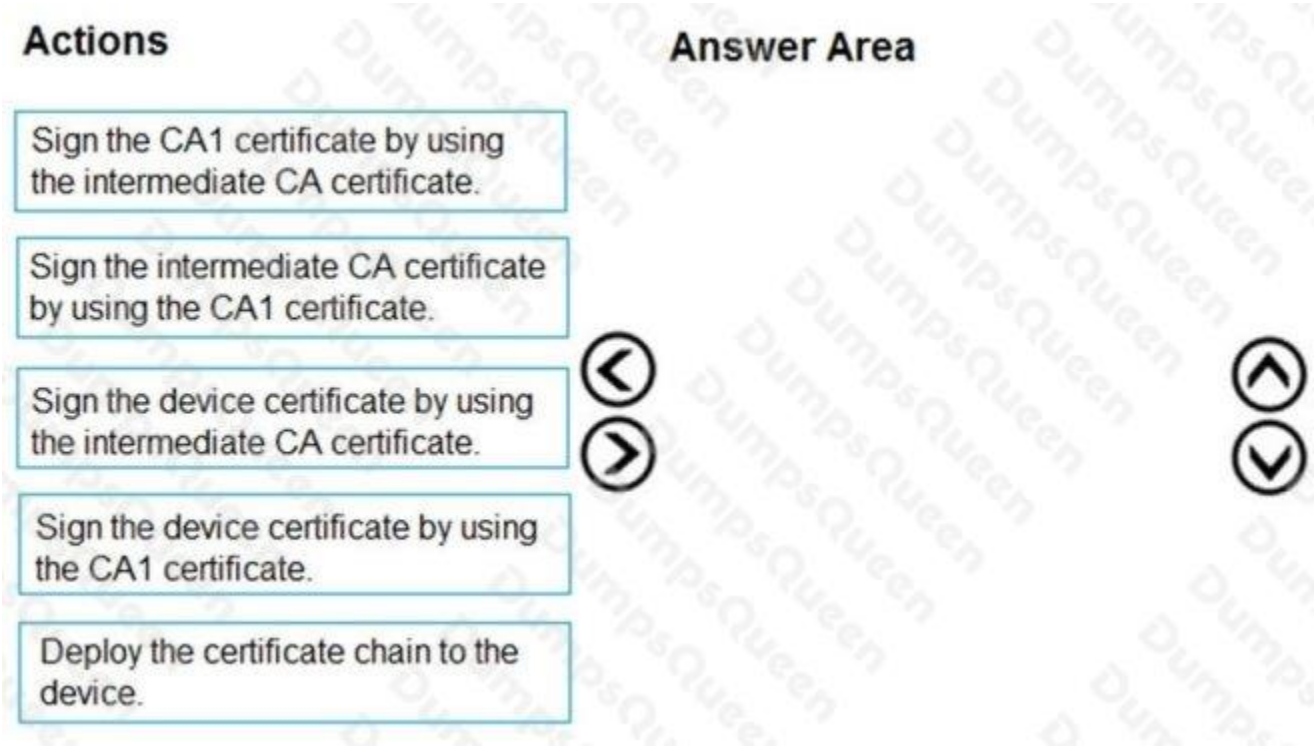
You and a custom manufacturing partner complete a proof of possession flow.

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.

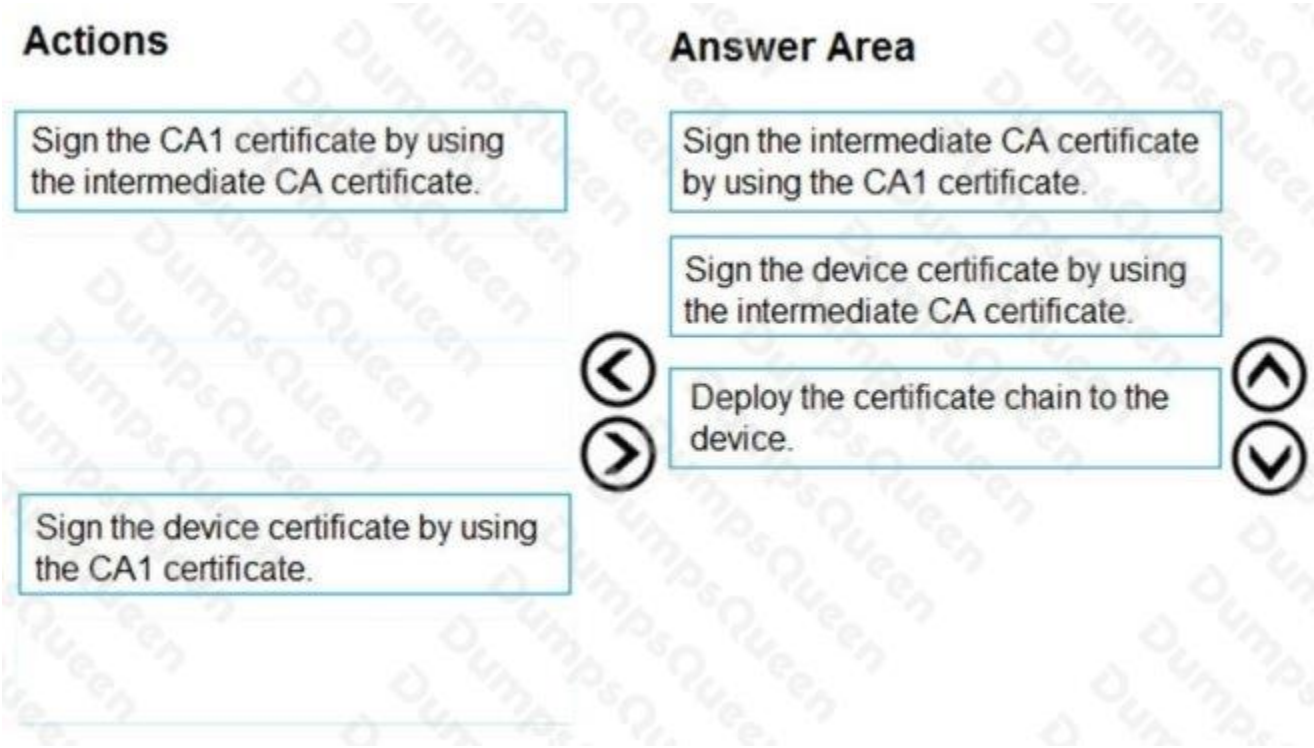
You need to ensure that the custom devices can connect successfully to Hub1.

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:



ANSWER:



Explanation:

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 NO: 5

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 section, 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 connecting to the IoT hub.

Solution: You disconnect the Device Provisioning Service from the IoT hub.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

Explanation:

Instead, from the Device Provisioning Service, you disable the enrollment group, and you disable device entries in the identity registry of the IoT hub to which the IoT devices are provisioned.

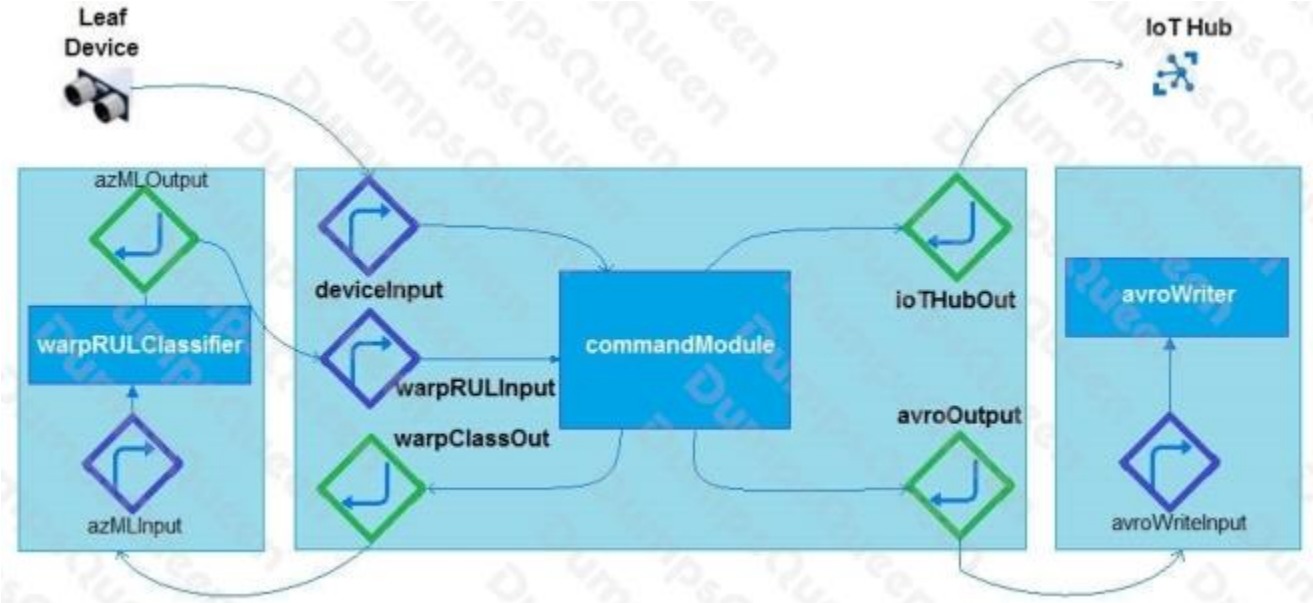
Reference:

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

QUESTION NO: 6 - (HOTSPOT)

HOTSPOT

You need to configure Azure IoT Edge module routing to ensure that modules route traffic as shown in the following exhibit.



How should you complete the IoT Edge module routes? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
"schemaVersion": "1.0",
"routes": {
    "deviceToCommand": "FROM /messages/" WHERE NOT IS_DEFINED( [ ] )
                                                  commandModule
                                                  $connectionModuled
                                                  $upstream

  INTO BrokeredEndpoint(\"
modules/commandModule/inputs/deviceInput\")",
    "warpClassifierToCommand": "FROM
/messages/modules/warpRULClassifier/outputs/azmlOutput
      INTO BrokeredEndpoint
(\"/modules/commandModule/inputs/warpRULInput\")",
    "commandToWarpClassifer": "FROM
/messages/modules/commandModule/outputs/warpClassOut
      INTO BrokeredEndpoint(\
" /modules/warpRULClassifier/inputs/azmlInput\")",
    "commandToAvroWriter": "FROM
/messages/modules/commandModule/outputs/avroOutput
     INTO BrokeredEndpoint
(\"/modules/avroWriter/inputs/avroWriterInput\")",
    "commandToCloud": "FROM
/messages/modules/commandModule/outputs/iotHubOut INTO [ ] *
                                                  commandModule
                                                  $connectionModuled
                                                  $upstream

  },
    "storeAndForwardConfiguration": {
      "timeToLiveSecs": 7200
      }
    }
  }
```

ANSWER:

Answer Area

Explanation:

Box 1: $connectionModuled

Add a route that tells the edge hub to route any message received by the IoT Edge device that was not sent by an IoT Edge module.

Box 2: $upstream

Send messages to $upstream, which passes the messages to the connected IoT Hub.

Reference:

https://docs.microsoft.com/en-us/azure/iot-edge/tutorial-machine-learning-edge-06-custom-modules

QUESTION NO: 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 name

C. Scope ID

D. Application Name

E. Device ID

ANSWER: A C

Explanation:

Required connection information:

▪ Group primary key: In your IoT Central application, navigate to Administration > Device Connection > SAS-IoT-Devices. Make a note of the shared access signature Primary key value. ▪ ID scope: In your IoT Central application, navigate to Administration > Device Connection. Make a note of the ID scope value.

Reference: https://docs.microsoft.com/bs-cyrl-ba/azure/iot-central/core/tutorial-connect-device-python

QUESTION NO: 8

You have an Azure IoT solution that includes an Azure IoT hub named hub1.

You plan to deploy an Azure Time Series Insights Gen 2 environment and connect the environment to hub1.

You need to use the device ID from hub1 as the Time Series ID.

What should you set as the Time Series ID when creating the environment?

A. device-id

B. connection-device-id

C. iothub-connection-device-id

D. deviceId

ANSWER: C

Explanation:

Your Time Series ID property is iothub-connection-device-id, dt-subject.

As an IoT Plug and Play user, for your Time Series ID, specify a composite key that consists of iothub-connection-device-id and dt-subject. The IoT hub adds these system properties that contain your IoT Plug and Play device ID and your device component names, respectively. Reference:

https://docs.microsoft.com/en-us/azure/iot-develop/tutorial-configure-tsi

QUESTION NO: 9

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: 10

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.

ANSWER: A C

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 NO: 11

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.

ANSWER: C E

Explanation:

In general, deprovisioning a device involves two steps:

- 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.

- 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/en-us/azure/iot-dps/how-to-unprovision-devices

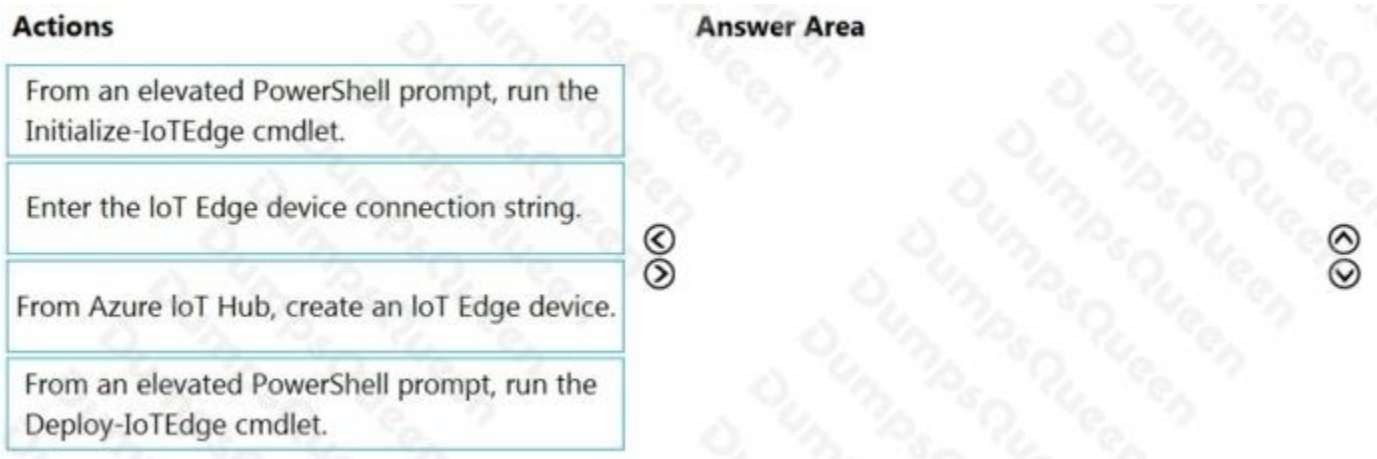
QUESTION NO: 12 - (DRAG DROP)

DRAG DROP

You need to install the Azure IoT Edge runtime on a new device that runs Windows 10 IoT Enterprise.

In which order should you perform the actions? 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:

Step 1: From Azure IoT hub, create an IoT Edge device

In the Azure Cloud Shell, enter the following command to create a device named myEdgeDevice in your hub. az iot hub device-identity create --device-id myEdgeDevice --edge-enabled --hub-name {hub_name}

View the connection string for your device, which links your physical device with its identity in IoT Hub. Copy the value of the connectionString key from the JSON output and save it. This value is the device connection string. You'll use this connection string to configure the IoT Edge runtime in the step 3.

Step 2: From an elevated PowerShell prompt, run the Deploy-IoTEdge cmdlet.

Install the Azure IoT Edge runtime on your IoT Edge device.

1. Run PowerShell as an administrator.

2. Run the Deploy-IoTEdge command, which performs the following tasks:

- Checks that your Windows machine is on a supported version.

- Turns on the containers feature.

- Downloads the moby engine and the IoT Edge runtime.

Step 3: From an elevated PowerShell prompt, run the Initialize-IoTEdge cmdlet

Step 4: Enter the IoT Edge device connection string.

Configure the IoT Edge device with a device connection string.

Reference: https://docs.microsoft.com/en-us/azure/iot-edge/quickstart

QUESTION NO: 13

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 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 targetCondition to "tags.floor='second'".

Does this meet the goal?

A. Yes

B. No

ANSWER: A

Explanation:

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 NO: 14

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

Does this meet the goal?

A. Yes

B. No

ANSWER: B

QUESTION NO: 15 - (HOTSPOT)

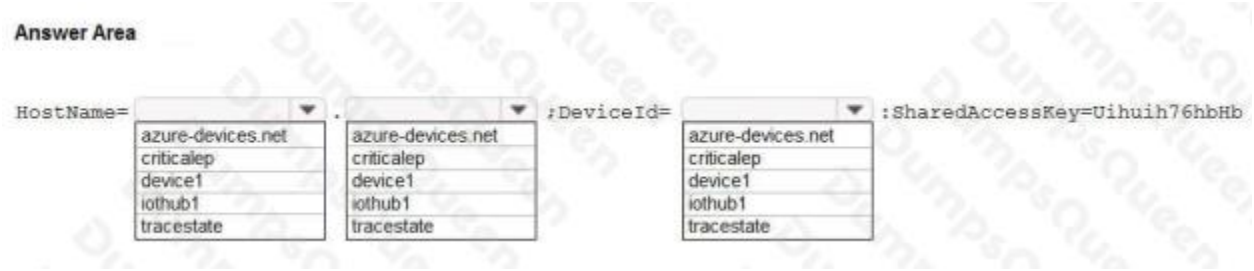
HOTSPOT

You create a new IoT device named device1 on iothub1. Device1 has a primary key of Uihuih76hbHb.

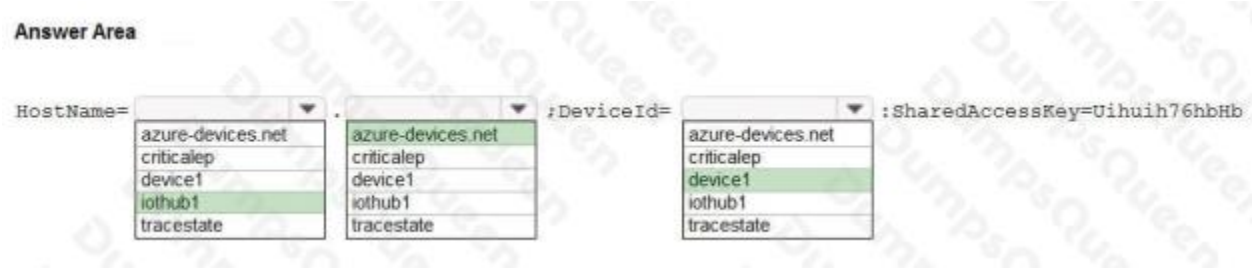
How should you complete the device connection string? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:



Explanation:

Box 1: iothub1

The Azure IoT hub is named iothub1.

Box 2: azure-devices.net

The format of the device connection string looks like:

HostName={YourIoTHubName}.azure-devices.net;DeviceId=MyNodeDevice;SharedAccessKey={YourSharedAccessKey}

Box 1: device1

Device1 has a primary key of Uihuih76hbHb.

Reference:

https://docs.microsoft.com/en-us/azure/iot-hub/quickstart-control-device-dotnet

Implement the IoT solution infrastructure