Free Questions for AZ-220 by ebraindumps

Shared by Gilliam on 20-10-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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?

Options:

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.

https://docs.microsoft.com/en-us/azure/digital-twins/troubleshoot-error-403

Question 2

Question Type: MultipleChoice

You have an Azure IoT solution that contains an Azure IoT hub and 100 IoT devices. The devices run Windows Server 2016.

You need to deploy the Azure Defender for IoT C#-based security agent to the devices.

What should you do first?

Options:

A- On the devices, initialize Trusted Platform Module (TPM).

B- From the IoT hub. create a system-assigned managed identity.

C- From the IoT hub. create a security module for the devices.

D- On the devices, set the PowerShell execution policy to Restricted.

Answer:

C

Explanation:

The IoT Edge security manager provides a safe framework for security service extensions through host-level modules. The IoT Edge security manager include

Ensure safe operation of client agents for services including Device Update for IoT Hub and Azure Defender for IoT.

https://docs.microsoft.com/en-us/azure/iot-edge/iot-edge-security-manager

Question 3

Question Type: MultipleChoice

You have an Azure subscription that contains an Azure IoT hub and two Azure IoT Edge devices named Device1 and Device2.

You need to ensure that the IoT hub only accepts connections from Device1 and Device2.

What should you configure?

Options:

A- a private endpoint connection

B- Azure API Management

C- Azure Active Directory (Azure AD) Identity Protection

D- a gateway device

Answer:

A

Explanation:

Ingress connectivity to IoT Hub using Azure Private Link.

A private endpoint is a private IP address allocated inside a customer-owned VNet via which an Azure resource is reachable. Through Azure Private Link, you can set up a private endpoint for your IoT hub to allow services inside your VNet to reach IoT Hub without requiring traffic to be sent to IoT Hub's public endpoint. Similarly, your on-premises devices can use Virtual Private Network (VPN) or ExpressRoute peering to gain connectivity to your VNet and your IoT Hub (via its private endpoint). As a result, you can restrict or completely block off connectivity to your IoT hub's public endpoints by using IoT Hub IP filter or the public network access toggle. This approach keeps connectivity to your Hub using the private endpoint for devices.

https://docs.microsoft.com/en-us/azure/iot-hub/virtual-network-support

Question 4

Question Type: **MultipleChoice**

You have an Azure IoT hub.

You need to enable Azure Defender for IoT on the IoT hub.

What should you do?

Options:

A- From the Security settings of the IoT hub, select Secure your IoT solution.

B- From the Diagnostics settings of the IoT hub, select Add diagnostic setting.

C- From Defender, add a security policy.

D- From Defender, configure security alerts.

Answer:

A

Explanation:

https://docs.microsoft.com/en-us/azure/defender-for-iot/device-builders/quickstart-onboard-iot-hub

Question 5

Question Type: MultipleChoice

You have an Azure IoT solution that contains an Azure IoT hub.

You need to ensure that the IoT hub configuration is compliant with the Health Insurance Portability and Accountability Act (HIPAA) audit logging requirements.

What should you use?

Options:

A- Azure Advisor recommendations

B- an Azure Policy definition

C- Azure Monitor alerts

D- an Azure Sentinel workspace

Answer:

B

Explanation:

Regulatory Compliance in Azure Policy provides Microsoft created and managed initiative definitions, known as built-ins, for the compliance domains and security controls related to different compliance standards, including HIPAA auditing logging.

https://docs.microsoft.com/en-us/azure/iot-hub/security-controls-policy

Question 6

Question Type: MultipleChoice

You have an Azure IoT hub and 15,000 IoT devices that monitor temperature. The IoT hub has four partitions. Each IoT device sends a 1-KB message every five seconds.

You plan to use Azure Stream Analytics to process the telemetry stream and generate an alert when temperatures exceed a defined threshold.

You need to recommend the minimum number of streaming units to configure for Stream Analytics.

What should you recommend?

Options:

A- 1

B- 3

C- 6

D- 12

Answer:

D

Explanation:

https://docs.microsoft.com/en-us/azure/stream-analytics/stream-analytics-parallelization#calculate-the-maximum-streaming-units-of-a-job