DUMPSBOSS.

# Developing Solutions for Microsoft Azure

## Microsoft AZ-203

## Version Demo

**Total Demo Questions: 10**

**Total Premium Questions: 70**

**Buy Premium PDF**

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

# Topic Break Down

| Topic | No. of Questions |
|---|---|
| Topic 1, Case Study 1 | 1 |
| Topic 2, Case Study 2 | 2 |
| Topic 3, Case Study 3 | 1 |
| Topic 4, Case Study 4 | 0 |
| Topic 5, Case Study 5 | 3 |
| Topic 6, Case Study 6 | 6 |
| Topic 7, Case Study 7 | 1 |
| Topic 8, Case Study 8 | 2 |
| Topic 9, Case Study 9 | 3 |
| Topic 10, Case Study 10 | 0 |
| Topic 11, Case Study 11 | 4 |
| Topic 12, Mixed Questions | 47 |
| Total | 70 |

## QUESTION NO: 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 need to ensure that the SecurityPin security requirements are met.

Solution: Configure the web application to connect to the database using the WebAppIdentity security principal. Using the Azure Portal, add Data Masking to the SecurityPin column and exclude the WebAppIdentity service principal.

Does the solution meet the goal?

**A.** Yes

**B.** No

## ANSWER: B

**Explanation:**

Instead of DataMasing, enable Always Encrypted for the SecurityPin column.

Scenario: Users' SecurityPin must be stored in such a way that access to the database does not allow the viewing of SecurityPins. The web application is the only system that should have access to SecurityPins.

All certificates and secrets used to secure data must be stored in Azure Key Vault.

## QUESTION NO: 3

You provide an Azure API Management managed web service to clients. The back-end web service implements HTTP Strict Transport Security (HSTS).

Every request to the backend service must include a valid HTTP authorization header.

You need to configure the Azure API Management instance with an authentication policy.

Which two policies can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

**A.** OAuth Client Credential Grant

**B.** Basic Authentication

**C.** Certificate Authentication

**D.** Digest Authentication

**ANSWER: A C**

## QUESTION NO: 5

You develop a serverless application that includes Azure Functions by using Visual Studio. These functions connect to data from within the code. You deploy the functions to Azure.

You want to configure tracing for an Azure Function App project.

You need to change configuration settings in the host.json file.

Which tool should you use?

**A.** Visual Studio

**B.** Azure portal

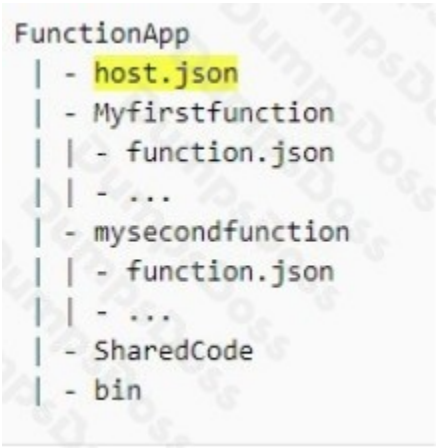
**C.** Azure PowerShell

**D.** Azure Functions Core Tools (Azure CLI)

**ANSWER: B**

**Explanation:**

The function editor built into the Azure portal lets you update the function.json file and the code file for a function. The host.json file, which contains some runtime-specific configurations, is in the root folder of the function app.




References: https://docs.microsoft.com/en-us/azure/azure-functions/functions-reference#fileupdate

## QUESTION NO: 6

You need to secure the Shipping Logic App.

What should you use?

**A.** Azure App Service Environment (ASE)

**B.** Azure AD B2B integration

**C.** Integration Service Environment (ISE)

**D.** VNet service endpoint

**ANSWER: C**

**Explanation:**

Scenario: The Shipping Logic App requires secure resources to the corporate VNet and use dedicated storage resources with a fixed costing model.

You can access to Azure Virtual Network resources from Azure Logic Apps by using integration service environments (ISEs).

Sometimes, your logic apps and integration accounts need access to secured resources, such as virtual machines (VMs) and other systems or services, that are inside an Azure virtual network. To set up this access, you can create an integration service environment (ISE) where you can run your logic apps and create your integration accounts.

References: https://docs.microsoft.com/en-us/azure/logic-apps/connect-virtual-network-vnet-isolated-environment-overview

**QUESTION NO: 8**

A company uses Azure SQL Database to store data for an app. The data includes sensitive information in a column named CustDetails.

You need to implement measures that allow only members of the managers group to see sensitive information.

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

NOTE: Each correct selection is worth one point.

**A.** Include the managers group.

**B.** Exclude the managers group.

**C.** Exclude the administrators group.

```
PUT https://management.azure.com/subscriptions/00000000-1111-2222-3333-444444444444
/resourceGroups/rg01/providers/Microsoft.Sql/servers/server01/databases/customers
/transparentDataEncryption/current?api-version=2014-04-01
```

```
New-AzureRmSqlDatabaseDataMaskingRule -SchemaName "dbo" -TableName "customers" `
  -ColumnName "CustDetails" -MaskingFunction "Default"
```

**ANSWER: B E**

**Explanation:**

Dynamic data masking helps prevent unauthorized access to sensitive data by enabling customers to designate how much of the sensitive data to reveal with minimal impact on the application layer.

SQL users excluded from masking - A set of SQL users or AAD identities that get unmasked data in the SQL query results.

Note: The New-AzureRmSqlDatabaseDataMaskingRule cmdlet creates a data masking rule for an Azure SQL database.

References: https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/new-azurermsqldatabasedatamaskingrule?view=azurermps-6.13.0

**QUESTION NO: 10**

You are preparing to deploy an ASP.NET Core website to an Azure Web App from a GitHub repository. The website includes static content generated by a script.

You plan to use the Azure Web App continuous deployment feature.

You need to run the static generation script before the website starts serving traffic.

What are two possible ways to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

**A.** Create a file named .deployment in the root of the repository that calls a script which generates the static content and deploys the website.

**B.** Add a PreBuild target in the websites csproj project file that runs the static content generation script.

**C.** Create a file named run.cmd in the folder /run that calls a script which generates the static content and deploys the website.

**D.** Add the path to the static content generation tool to WEBSITE_RUN_FROM_PACKAGE setting in the host.json file.

**ANSWER: A D**

**Explanation:**

A: To customize your deployment, include a .deployment file in the repository root.

You just need to add a file to the root of your repository with the name .deployment and the content:

[config]

command = YOUR COMMAND TO RUN FOR DEPLOYMENT

this command can be just running a script (batch file) that has all that is required for your deployment, like copying files from the repository to the web root directory for example.

D: In Azure, you can run your functions directly from a deployment package file in your function app. The other option is to deploy your files in the d: \home\site\wwwroot directory of your function app (see A above).

To enable your function app to run from a package, you just add a WEBSITE_RUN_FROM_PACKAGE setting to your function app settings.

Note: The host.json metadata file contains global configuration options that affect all functions for a function app.

References:

https://github.com/projectkudu/kudu/wiki/Custom-Deployment-Script https://docs.microsoft.com/bs-latn-ba/azure/azure-functions/run-functions-from-deployment-package