AZ-305 Q&As

Designing Microsoft Azure Infrastructure Solutions

Pass Microsoft AZ-305 Exam with 100% Guarantee

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

https://www.geekcert.com/az-305.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

HOTSPOT

You have an Azure subscription. The subscription contains an Azure SQL managed instance that stores employee details, including social security numbers and phone numbers.

You need to configure the managed instance to meet the following requirements:

1.

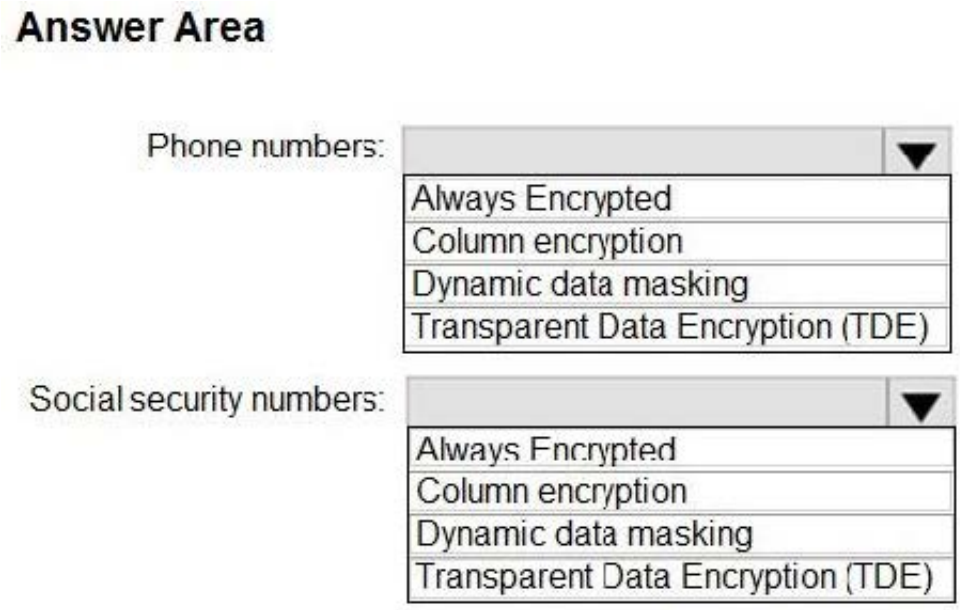
The helpdesk team must see only the last four digits of an employee\\'s phone number.

2.

Cloud administrators must be prevented from seeing the employee\\'s social security numbers.

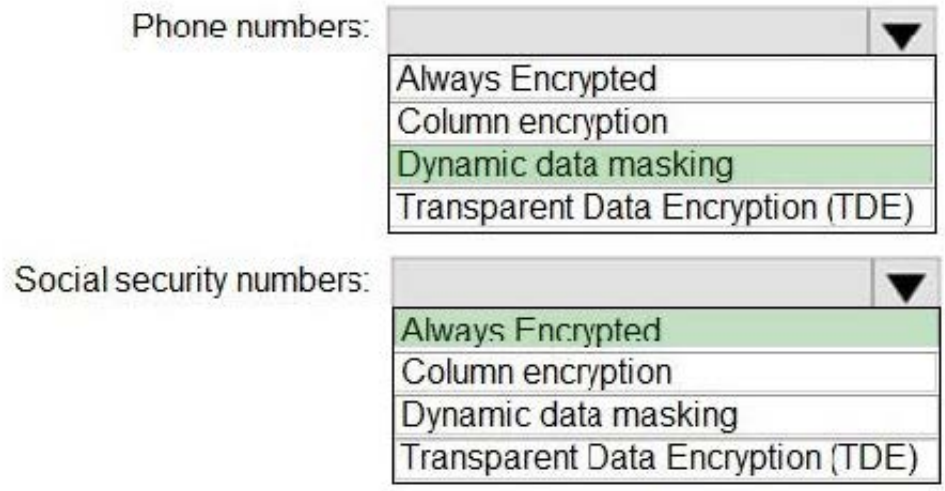
What should you enable for each column in the managed instance? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



Box 1: Dynamic data masking

The helpdesk team must see only the last four digits of an employee\\'s phone number.

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 effect on the application layer. It\\'s a policy-based security feature that hides

the sensitive data in the result set of a query over designated database fields, while the data in the database isn\\'t changed.

Masking functions: A set of methods that control the exposure of data for different scenarios.

* Credit card

Masking method, which exposes the last four digits of the designated fields and adds a constant string as a prefix in the form of a credit card.

XXXX-XXXX-XXXX-1234

Box 2: Always Encrypted

Cloud administrators must be prevented from seeing the employee\\'s social security numbers.

Always Encrypted is a feature designed to protect sensitive data, such as credit card numbers or national/regional identification numbers (for example, U.S. social security numbers), stored in Azure SQL Database, Azure SQL Managed

Instance, and SQL Server databases. Always Encrypted allows clients to encrypt sensitive data inside client applications and never reveal the encryption keys to the Database Engine. This provides a separation between those who own the

data and can view it, and those who manage the data but should have no access - on-premises database administrators, cloud database operators, or other high-privileged unauthorized users. As a result, Always Encrypted enables

customers to confidently store their sensitive data in the cloud, and to reduce the likelihood of data theft by malicious insiders.

Reference: https://learn.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine https://learn.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview

QUESTION 2

You need to deploy resources to host a stateless web app in an Azure subscription. The solution must meet the following requirements:

1.

Provide access to the full .NET framework.

2.

Provide redundancy if an Azure region fails.

3.

Grant administrators access to the operating system to install custom application dependencies.

Solution: You deploy a Azure virtual machine scale set that uses autoscaling.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead, you should deploy two Azure virtual machines to two Azure regions, and you create a Traffic Manager profile.

QUESTION 3

HOTSPOT

You are designing a software as a service (SaaS) application that will enable Azure Active Directory (Azure AD) users to create and publish online surveys. The SaaS application will have a front-end web app and a back-end web API. The web app will rely on the web API to handle updates to customer surveys.

You need to design an authorization flow for the SaaS application. The solution must meet the following requirements:

1.

To access the back-end web API, the web app must authenticate by using OAuth 2 bearer tokens.

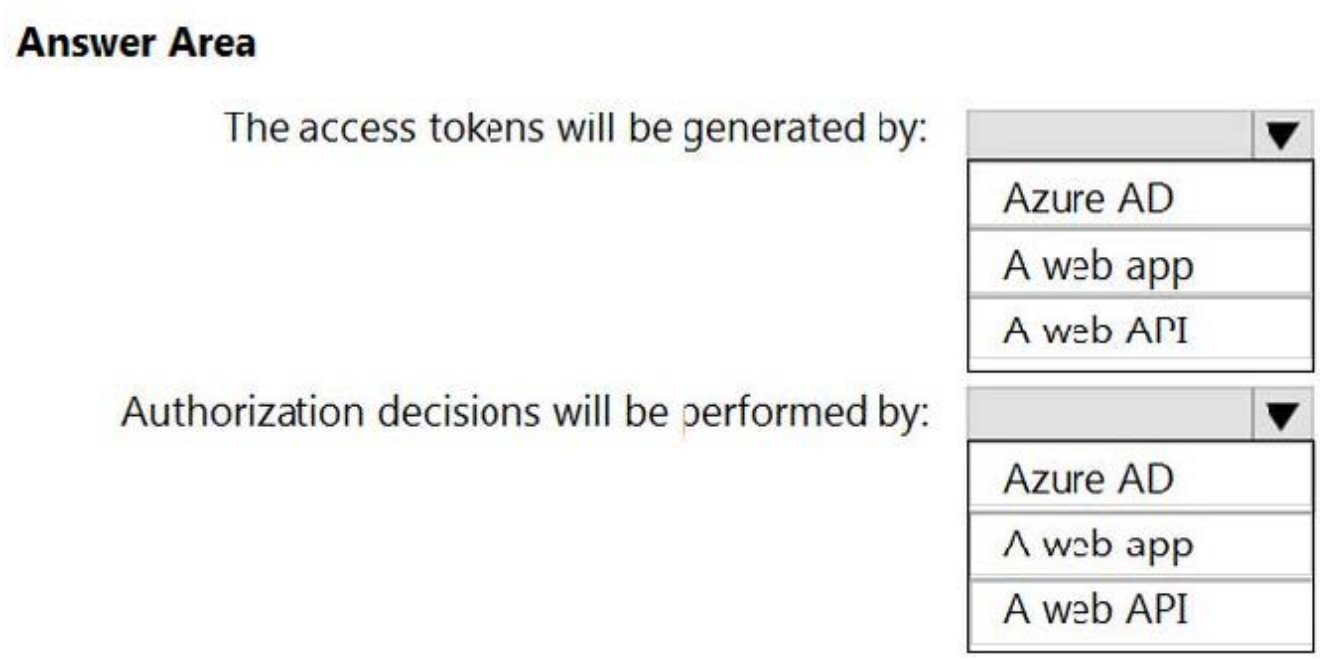
2.

The web app must authenticate by using the identities of individual users.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Reference: https://docs.microsoft.com/lb-lu/azure/architecture/multitenant-identity/web-api https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-v1-dotnet-webapi

QUESTION 4

HOTSPOT

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

Name	Type
storage1	General purpose v2 storage account
container1	Blob container
blob1	Blob
blob2	Blob

You need to recommend an authorization mechanism for controlling access to blob1. The solution must ensure that access to blob1 can be configured without affecting the other resources in storage1. What should you recommend? To answer, select the appropriate options in the answer area.

Hot Area:

Answer Area

To grant access to blob1, use:
- A stored access policy and a service shared access signature (SAS)
- A stored access policy and an account shared access signature (SAS)
- Azure role-based access control (Azure RBAC)

To revoke access to blob1:
- Modify the stored access policy
- Recreate the shared access signature (SAS)
- Modify the Access control (IAM) settings to container1

Correct Answer:

Answer Area

To grant access to blob1, use:
- A stored access policy and a service shared access signature (SAS)
- A stored access policy and an account shared access signature (SAS)
- Azure role-based access control (Azure RBAC)

To revoke access to blob1:
- Modify the stored access policy
- Recreate the shared access signature (SAS)
- Modify the Access control (IAM) settings to container1

Box 1: A stored access policy and a service shared access signature (SAS)

A stored access policy provides an additional level of control over service-level shared access signatures (SAS) on the server side. Establishing a stored access policy serves to group shared access signatures and to provide additional

restrictions for signatures that are bound by the policy.

The following storage resources support stored access policies:

1.

Blob containers

2.

File shares

3.

Queues

4.

Tables

Box 2: Modify the stored access signature (SAS)

You can use a stored access policy to change the start time, expiry time, or permissions for a signature, or to revoke it after it has been issued.

Reference:

https://docs.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy

QUESTION 5

Your company has an Azure Web App that runs via the Premium App Service Plan. A development team will be using the Azure Web App. You have to configure the Azure Web app so that it can fulfil the below requirements. Provide the ability to switch the web app from the current version to a newer version Provide developers with the ability to test newer versions of the application before the switch to the newer version occurs Ensure that the application version can be rolled back Minimize downtime Which of the following can be used for this requirement?

A. Create a new App Service Plan

B. Make use of deployment slots

C. Map a custom domain

D. Backup the Azure Web App

Correct Answer: B