

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.pass2lead.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

Your company plans to use a separate Azure subscription for each of its business units. You identify the following governance requirements:

1.
Each business unit will analyze costs for different workloads such as production, development, and testing.
2.
The company will analyze costs by business unit and workload. What should you use to meet the governance requirements?
 - A. Azure Advisor alerts and Azure Logic Apps
 - B. Microsoft Intune and compliance policies
 - C. Azure management groups and RBAC
 - D. tags and Azure Policy

Correct Answer: D

QUESTION 2

You are designing an Azure Cosmos DB solution that will host multiple writable replicas in multiple Azure regions.

You need to recommend the strongest database consistency level for the design.

The solution must meet the following requirements:

1.
Provide a latency-based Service Level Agreement (SLA) for writes.
2.
Support multiple regions.

Which consistency level should you recommend?

- A. bounded staleness
- B. strong
- C. session
- D. consistent prefix

Correct Answer: A

Reference:

https://azure.microsoft.com/en-us/support/legal/sla/cosmos-db/v1_3/

<https://docs.microsoft.com/en-us/azure/cosmos-db/consistency-levels#consistency-levels- and-latency>

QUESTION 3

HOTSPOT

You need to design an authentication solution that will integrate on-premises Active Directory and Azure Active Directory (Azure AD). The solution must meet the following requirements:

1.
Active Directory users must not be able to sign in to Azure AD-integrated apps outside of the sign-in hours configured in the Active Directory user accounts.
2.
Active Directory users must authenticate by using multi-factor authentication (MFA) when they sign in to Azure AD-integrated apps.
3.
Administrators must be able to obtain Azure AD-generated reports that list the Active Directory users who have leaked credentials.
4.
The infrastructure required to implement and maintain the solution must be minimized.

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:

Integrate Active Directory and Azure AD by using:

<input type="checkbox"/>	Active Directory Federation Services
<input type="checkbox"/>	Pass-through authentication with Azure AD Seamless SSO
<input type="checkbox"/>	Pass-through authentication with Azure AD Seamless SSO and password hash synchronization
<input type="checkbox"/>	Password hash synchronization with Azure AD Seamless SSO

Implement MFA by using:

<input type="checkbox"/>	A third-party authentication solution
<input type="checkbox"/>	Azure MFA
<input type="checkbox"/>	The Active Directory Federation Services (AD FS) Azure MFA adapter

Correct Answer:

Integrate Active Directory and Azure AD by using:

Active Directory Federation Services
Pass-through authentication with Azure AD Seamless SSO
Pass-through authentication with Azure AD Seamless SSO and password hash synchronization
Password hash synchronization with Azure AD Seamless SSO

Implement MFA by using:

A third-party authentication solution
Azure MFA
The Active Directory Federation Services (AD FS) Azure MFA adapter

Box 1: Pass-through Authentication with Azure AD Seamless SSO

Azure AD Seamless SSO versus Active Directory Federation Services

Companies with a security requirement to immediately enforce on-premises user account states, password policies, and sign-in hours might use Azure AD Pass-through Authentication.

You can combine Pass-through Authentication with the Seamless Single Sign-On feature.

Note: Azure AD supports the following authentication methods for hybrid identity solutions.

Azure AD password hash synchronization

Azure AD Pass-through Authentication

Box 2: Azure MFA

One key benefit with Azure AD Pass-through Authentication is that it works seamlessly with Azure MFA.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

QUESTION 4

After you migrate App1 to Azure, you need to enforce the data modification requirements to meet the security and compliance requirements. What should you do?

- A. Create an access policy for the blob service.
- B. Implement Azure resource locks.

C. Create Azure RBAC assignments.

D. Modify the access level of the blob service.

Correct Answer: A

Scenario: Once App1 is migrated to Azure, you must ensure that new data can be written to the app, and the modification of new and existing data is prevented for a period of three years.

As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources>

QUESTION 5

You are designing a solution that will include containerized applications running in an Azure Kubernetes Service (AKS) cluster.

You need to recommend a load balancing solution for HTTPS traffic.

The solution must meet the following requirements:

1.

Automatically configure load balancing rules as the applications are deployed to the cluster.

2.

Support Azure Web Application Firewall (WAF).

3.

Support cookie-based affinity.

4.

Support URL routing.

What should you include in the recommendation?

A. an NGINX ingress controller

B. Application Gateway Ingress Controller (AGIC)

C. an HTTP application routing ingress controller

D. the Kubernetes load balancer service

Correct Answer: B

Much like the most popular Kubernetes Ingress Controllers, the Application Gateway Ingress Controller provides several features, leveraging Azure's native Application Gateway L7 load balancer. To name a few: URL routing Cookie-based

affinity Secure Sockets Layer (SSL) termination End-to-end SSL Support for public, private, and hybrid web sites
Integrated support of Azure web application firewall

Application Gateway redirection support isn't limited to HTTP to HTTPS redirection alone. This is a generic redirection mechanism, so you can redirect from and to any port you define using rules. It also supports redirection to an external site as well.

Reference: <https://docs.microsoft.com/en-us/azure/application-gateway/features>

[AZ-305 PDF Dumps](#)

[AZ-305 Practice Test](#)

[AZ-305 Braindumps](#)