



AZ-305: Designing Microsoft Azure Infrastructure Solutions

Full Exam Pack – 5 Integrated Practice Exams

💡 This exam pack is shared for FREE as part of my commitment to high-quality, accessible tech education through Nokhba Academy.

Designed for candidates preparing for the Microsoft Certified: Azure Solutions Architect Expert exam.

You are free to use this for personal learning purposes.

📲 Stay Connected

Done by Ahmed Fouad

LinkedIn: <https://www.linkedin.com/in/ahmed-fouad-270200/>

Facebook Page (Nokhba Academy): <https://shorturl.at/UUDf2>

YouTube Channel: https://www.youtube.com/@nokhba_learning

For more resources, follow Nokhba Academy on social media or visit our official website at <https://nokhba-academy.online>

--- START OF EXAM CONTENT ---

Exam1

- Contoso, your employer, maintains several Azure Logic Apps integrated with an on-premises web service via HTTP triggers. A strategic alliance arises between Contoso and Fabrikam, whereby Fabrikam developers aspire to connect their applications with Contoso's web service through a selection of Logic Apps. Craft a solution that observes these restrictions:

- Impose usage limits on Fabrikam developers accessing the Logic Apps, distinguishing them from Contoso users.

- Empower Fabrikam developers to carry on using their prevailing OAuth 2.0 system for authentication purposes.
- Abstain from updating the Logic Apps during the implementation.
- Evade employing Azure AD guest accounts.

Identify the most fitting tool to compose the solution:

- A) Azure AD business-to-business (B2B)
- B) Azure AD Application Proxy
- C) Azure Front Door
- D) Azure API Management

Answer: D

Feedback(if correct):-

Azure API Management allows organizations to release APIs to external, partner, and internal developers, empowering them to extract the utmost value from their data and services. By safeguarding API Management with OAuth 2.0 client credentials flow, you can confidently meet the requirements laid out in the scenario.

Feedback(if wrong):-

- A) Azure AD business-to-business (B2B) - Not compatible with third-party OAuth 2.0 providers.
- B) Azure AD Application Proxy - Designed for exposing on-premises applications, not for controlling request frequencies nor interacting with third-party OAuth 2.0 systems.
- C) Azure Front Door - Specializes in global load balancing, failover, and SSL offloading, not managing request frequencies or dealing with third-party OAuth 2.0 providers.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305



Subskills: Designing Identity and Security Solutions

Competencies: Identity and Access Management, Security, Authentication, Authorization

Difficulty Level: Expert

Bloom's Taxonomy Level: Evaluation

2. Your company operates a hybrid Azure Active Directory (Azure AD) tenant with the Free edition. The tenant employs password hash synchronization. You're tasked with recommending solutions to meet specific requirements:

Requirement 1:

Prevent Active Directory domain user accounts from being locked out due to brute force attacks targeting Azure AD user accounts.

Requirement 2:

Block legacy authentication attempts to Azure AD integrated apps.

Which solution should you recommend for each requirement?

- A) For Requirement 1: Azure AD Password Protection, For Requirement 2: Azure AD Application Proxy
- B) For Requirement 1: Conditional access policies, For Requirement 2: Azure AD Password Protection
- C) For Requirement 1: Pass-through authentication, For Requirement 2: Conditional access policies
- D) For Requirement 1: Smart lockout, For Requirement 2: Enable Security defaults

Answer: B, D

Feedback (if correct):

B) Conditional Access Policies: Conditional Access Policies in Azure AD allow you to control access to your applications based on specific conditions. By configuring Conditional Access Policies, you can block legacy authentication attempts to Azure AD-integrated apps, ensuring that only modern authentication methods are allowed. This helps enhance security by preventing the use of less secure authentication protocols.

D) Enable Security Defaults: Enabling Security Defaults is a quick and easy way to help protect your organization's Azure AD tenant. Security Defaults enforce a set of predefined security configurations, including blocking legacy authentication. By enabling Security Defaults, you automatically implement security measures recommended by Microsoft, reducing the risk of unauthorized access and minimizing administrative effort and costs associated with managing security settings individually.

Feedback (if wrong):

Option A) Azure AD Password Protection:

For Requirement 1, Azure AD Password Protection is not directly related to preventing Active Directory domain user accounts from being locked out due to brute force attacks targeting Azure AD user accounts. Instead, it focuses on enforcing strong password policies and preventing the use of commonly used or easily guessed passwords.

For Requirement 2, Azure AD Password Protection does not address blocking legacy authentication attempts to Azure AD integrated apps. Its primary purpose is to enhance password security by preventing the use of weak passwords.

Option D) Azure AD Application Proxy:

For Requirement 2, Azure AD Application Proxy allows secure remote access to on-premises web applications hosted behind Azure AD. However, it does not directly address the need to block legacy authentication attempts to Azure AD-integrated apps. Its primary function is to provide secure access to on-premises applications through Azure AD, rather than controlling authentication methods.

Therefore, neither option A nor option D fully meets the requirements provided in the scenario. The correct combination of solutions would be Smart Lockout for Requirement 1 and Conditional Access Policies for Requirement 2.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Secure authentication and authorization in Azure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

3. Your organization hosts numerous applications on Azure App Service Web and API. These applications depend on Azure Key Vault to manage various authentication, storage accounts, and data encryption keys. Different departments have raised requests to support these applications:

Department Request

Security:

Review membership of administrative roles and demand justifications for continuous membership

Get alerts regarding changes in administrator assignments

See a history of administrator activity, including amendments to Azure resources

Development:

Enable applications to access Azure Key Vault and fetch keys for use in code

Quality Assurance:

Obtain temporary administrator access to establish and finetune supplementary Web and API applications in the testing setting

To accommodate these requests, you must suggest the appropriate Azure service.

What should you recommend for the Security department?

- A. Azure AD Privileged Identity Management
- B. Azure AD Managed Service Identity
- C. Azure AD Identity Protection
- D. Azure AD Connect

Answer: A

Feedback(if correct):- Azure AD Privileged Identity Management (PIM) enables organizations to manage, control, and monitor access within Azure AD. It allows for the review and justification of administrative roles, provides alerts for changes in assignments, and maintains a history of administrator activity, fulfilling the security department's requirements for role management and monitoring.

Feedback(if wrong):- B. Azure AD Managed Service Identity: Managed Service Identity is not designed to address the specific requirements mentioned for the Security department, such as role review, alerting, and activity tracking.

C. Azure AD Identity Protection: Azure AD Identity Protection primarily focuses on detecting and preventing identity-based attacks, such as account compromise and insider threats, rather than providing role management and monitoring capabilities.

D. Azure AD Connect: Azure AD Connect is a tool used for integrating on-premises directories with Azure AD but does not offer the role review, alerting, and activity tracking features required by the Security department.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Secure authentication and authorization in Azure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

4. Your organization hosts numerous applications on Azure App Service Web and API. These applications depend on Azure Key Vault to manage various authentication, storage accounts, and data encryption keys. Different departments have raised requests to support these applications:

Department Request

Security:

Review membership of administrative roles and demand justifications for continuous membership

Get alerts regarding changes in administrator assignments

See a history of administrator activity, including amendments to Azure resources

Development:

Enable applications to access Azure Key Vault and fetch keys for use in code

Quality Assurance:

Obtain temporary administrator access to establish and finetune supplementary Web and API applications in the testing setting

To accommodate these requests, you must suggest the appropriate Azure service.

To enable applications to securely access Azure Key Vault and fetch keys for use in code, which Azure service is most suitable to use for the Development department?



- A. Azure AD Privileged Identity Management
- B. Azure AD Managed Service Identity
- C. Azure AD Connect
- D. Azure AD Identity Protection

Answer: B

Feedback (if correct):

MSIs are tied to individual Azure resources, such as virtual machines or Azure App Services. When enabled, the MSI authenticates to Azure services, such as Azure Key Vault, using a managed identity in Azure AD instead of using certificates or secrets stored within the application or service configuration.

Using MSIs simplifies the management of cryptographic keys and secrets, as there is no need to manage, rotate, or securely store the credentials. Azure takes care of assigning the rights needed for the MSI to perform tasks in Azure Key Vault or other Azure services, and revoking them when the MSI is deleted.

Feedback (if wrong):

- A) Azure AD Privileged Identity Management (PIM): PIM deals with just-in-time and just enough administration for resources in Azure AD and Azure subscription administrators. It is not related to granting applications access to Azure Key Vault.
- C) Azure AD Connect: This service is used to join Azure AD with on-premises Active Directory. It is not related to granting applications access to Azure Key Vault either.
- D) Azure AD Identity Protection: This service helps protect user identities by identifying risk events and taking appropriate actions based on organizational policies. But again, it is not related to granting applications access to Azure Key Vault.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Secure authentication and authorization in Azure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

5. Your organization hosts numerous applications on Azure App Service Web and API. These applications depend on Azure Key Vault to manage various authentication, storage accounts, and data encryption keys. Different departments have raised requests to support these applications:

Department Request

Security:

Review membership of administrative roles and demand justifications for continuous membership

Get alerts regarding changes in administrator assignments

See a history of administrator activity, including amendments to Azure resources

Development:

Enable applications to access Azure Key Vault and fetch keys for use in code

Quality Assurance:

Obtain temporary administrator access to establish and finetune supplementary Web and API applications in the testing setting

To accommodate these requests, you must suggest the appropriate Azure service.

To provide Quality Assurance with temporary administrator access for creating and testing Web/API applications, which Azure service best meets their needs?

- A. Azure AD Privileged Identity Management
- B. Azure AD Managed Service Identity
- C. Azure AD Connect
- D. Azure AD Identity Protection

Answer: A

Feedback(if correct):

Azure AD Privileged Identity Management (PIM) is the appropriate Azure service to recommend for the Quality Assurance department's request. Azure AD PIM enables organizations to manage, control, and monitor access to Azure resources, including providing just-in-time privileged access to users who need it for specific tasks. By using Azure AD PIM, the Quality Assurance department can grant temporary administrator access to establish and fine-tune supplementary Web and API applications in the testing environment, ensuring security and accountability.

Feedback(if wrong):

Option B: Azure AD Managed Service Identity (MSI) is used for securely authenticating applications to Azure services without the need to manage credentials explicitly. However, it is not suitable for providing temporary administrator access to users for creating and testing Web/API applications.

Option C: Azure AD Connect is used for integrating on-premises directories with Azure Active Directory (AAD) and is not relevant to providing temporary administrator access for establishing and fine-tuning supplementary applications in a testing environment.

Option D: Azure AD Identity Protection is a feature within Azure AD that helps organizations prevent, detect, and investigate identity-based risks, but it is not related to providing temporary administrator access for creating and testing Web/API applications.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Secure authentication and authorization in Azure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

6. Which Azure service should App1 utilize to obtain an access token to meet authentication and authorization requirements during migration to Azure?

- A. Azure Active Directory (Azure AD)
- B. Azure Key Vault
- C. Azure Traffic Manager

D. Azure Cosmos DB

Answer: A

Feedback(if correct):-

A. Azure Active Directory (Azure AD). Azure AD is the identity and access management service in Azure, providing secure authentication and authorization capabilities for applications and services. It is the appropriate endpoint for obtaining access tokens to meet authentication and authorization requirements during migration to Azure.

Feedback(if wrong):-

B. Azure Key Vault: Azure Key Vault is a secure secrets management service, not an endpoint for obtaining access tokens for authentication and authorization.

C. Azure Traffic Manager: Azure Traffic Manager is a DNS-based traffic load balancer, not an endpoint for obtaining access tokens for authentication and authorization.

D. Azure Cosmos DB: Azure Cosmos DB is a globally distributed, multi-model database service, not an endpoint for obtaining access tokens for authentication and authorization.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Secure authentication and authorization in Azure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

7. You are tasked with deploying an application named App1 on five Azure virtual machines, with the possibility of additional virtual machines being deployed later to run App1. You need to recommend a solution to meet the following requirements for the virtual machines running App1:

Ensure the virtual machines can authenticate to Azure Active Directory (Azure AD) for access to an Azure Key Vault, Azure Logic Apps instances, and an Azure SQL database.

Avoid assigning new roles and permissions for Azure services when deploying additional virtual machines.

Prevent storing secrets and certificates on virtual machines.

Which type of identity should you recommend?

- A) A service principal configured to use a certificate
- B) A system-assigned managed identity
- C) A service principal configured to use a client's secret
- D) A user-assigned managed identity

Answer: B

Feedback(if correct):

The correct answer is B) A system-assigned managed identity. System-assigned managed identities are automatically created and assigned to Azure resources, such as virtual machines in this scenario, allowing them to authenticate to Azure AD without the need for storing credentials or certificates on the virtual machines. This solution also ensures consistency in access control across all instances of the virtual machines running App1.

Feedback(if wrong):

Option A) A service principal configured to use a certificate: Incorrect because using a service principal with a certificate would require managing and storing the certificate securely on each virtual machine, which contradicts the requirement to avoid storing secrets and certificates on the virtual machines.

Option C) A service principal configured to use a client secret: Incorrect because using a service principal with a client secret would also involve storing the secret securely on each virtual machine, which violates the requirement to avoid storing secrets on the virtual machines.

Option D) A user-assigned managed identity: Incorrect because user-assigned managed identities are manually created and assigned to specific Azure resources, and they do not meet the requirement to avoid assigning new roles and permissions for Azure services when deploying additional virtual machines. Additionally, they do not provide a solution for avoiding storing secrets and certificates on virtual machines.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Plan and implement authentication and access control

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

8. Users managing the production environment in Azure need to be registered for Azure Multi-Factor Authentication (MFA) and must authenticate using Azure MFA when they sign in to the Azure portal. The solution must meet authentication and authorization requirements. What should you do to register users for Azure Multi-Factor Authentication (MFA) to meet the authentication and authorization requirements for managing the production environment in Azure?
- A. Configure Azure AD Identity Protection
 - B. Enable Security defaults in Azure AD
 - C. Utilize Per-user MFA in the MFA management UI
 - D. Implement Grant control

Answer: C.

Feedback(if correct):

This option enables the registration of users for Azure Multi-Factor Authentication (MFA) on a per-user basis, ensuring that users managing the production environment in Azure are registered for MFA as required. It meets the authentication and authorization requirements by enforcing MFA for specific users.

Feedback(if wrong):

Option A: Configuring Azure AD Identity Protection focuses on managing security risks but does not directly address the registration of users for MFA.

Option B: Enabling Security defaults in Azure AD provides basic security settings but does not specifically enable the registration of users for MFA.

Option D: Implementing Grant control is a vague option that does not specify how it relates to registering users for MFA.

Skill Mapping:



Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing authentication and authorization mechanisms, Configuring security policies and procedures

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Comprehension

9. Users managing the production environment in Azure need to be registered for Azure Multi-Factor Authentication (MFA) and must authenticate using Azure MFA when they sign in to the Azure portal. The solution must meet authentication and authorization requirements.

What should you do to enforce Azure Multi-Factor Authentication (MFA) authentication for users managing the production environment in Azure, meeting the authentication and authorization requirements?

- A. Configure Azure AD Identity Protection
- B. Enable Security defaults in Azure AD
- C. Utilize Per-user MFA in the MFA management UI
- D. Implement a Sign-in risk policy in Azure AD Identity Protection for the tenant

Answer: C

Feedback(if correct):

C. Utilize Per-user MFA in the MFA management UI. This option aligns with the requirement to enforce Azure Multi-Factor Authentication (MFA) authentication for users managing the production environment in Azure, meeting the authentication and authorization requirements. It demonstrates comprehension of the scenario and applies the appropriate solution to address the security need.

Feedback(if wrong):

Option A: Configuring Azure AD Identity Protection does not directly enforce MFA authentication for users. It provides security features related to risk management but does not meet the specific requirements outlined in the scenario.

Option B: Enabling Security defaults in Azure AD is a general security measure but does not specifically address the need to enforce MFA authentication for users in the production environment.



Option D: Implementing a Sign-in risk policy in Azure AD Identity Protection focuses on risk management but does not directly enforce MFA authentication for users.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing authentication and authorization mechanisms, Configuring security policies and procedures

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Comprehension

10. In an organization's Azure environment, the IT department manages various infrastructure components, including network connectivity, user authentication, and system health monitoring. The IT Support distribution group is responsible for receiving notifications related to system health and performance issues to ensure timely resolution and minimize downtime.

Requirements for the Notification Solution:

1. Timely Notifications: The solution should provide real-time notifications to the IT Support distribution group whenever system health or performance issues arise.
2. Customization: The solution should allow customization of notification settings and content based on the specific needs and preferences of the IT Support team.
3. Integration with Azure Environment: The solution should seamlessly integrate with the organization's existing Azure environment to leverage Azure services and resources effectively.

A. Azure Network Watcher:

B. An Action Group:

C. A SendGrid Account with Advanced Reporting:

D. Azure AD Connect Health:

Answer: B.

Feedback(if correct):-

An action group in Azure allows for customized notifications and actions based on specific events, making it suitable for providing real-time alerts to the IT Support distribution group regarding system health and performance issues.

Feedback(if wrong):-

- A. Azure Network Watcher: While Azure Network Watcher provides network monitoring and diagnostics, it does not offer direct notification capabilities for the IT Support distribution group.
- C. A SendGrid account: SendGrid is primarily used for sending transactional and marketing emails, not for real-time alerts related to system health.
- D. Azure AD Connect Health: Azure AD Connect Health monitors the health and performance of Azure AD Connect but is not designed to notify the IT Support distribution group about system health and performance issues.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Designing effective solutions for securing Azure infrastructure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

11. You need to recommend a solution to ensure that App1 can access the third-party credentials and access strings. The solution must meet the security requirements. What should you include in the recommendation? Select the appropriate options

- A) Authenticate App1 by using a certificate.
- B) Authenticate App1 by using a service principal.
- C) Authenticate App1 by using a system-assigned managed identity.
- D) Authorize App1 to retrieve Key Vault secrets by using an access policy.

Answer: B, D

Feedback(if correct):

By recommending the use of a service principal (Option B) for authenticating App1 and setting an access policy (Option D) for Key Vault secrets, you ensure secure credential management. This combo maintains

security requirements while enabling App1 to access necessary third-party credentials and access strings.

Feedback(if wrong):-

- A) Authenticating App1 using a certificate is not a suitable solution in this case since it introduces additional overhead, like certificate issuing, renewal, and rotation, which increases operational complexity and maintenance burden. Besides, it does not solve the challenge of safely managing third-party credentials and access strings.
- C) Authenticating App1 using a system-assigned managed identity is restricted to the lifecycle of the resource it belongs to, limiting its utility across multiple resources. This limitation hinders sharing credentials and access strings across applications, resulting in ineffective access control and management.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Analyzing requirements and designing efficient solutions

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Synthesis

12. A company named Contoso is planning to migrate its legacy on-premises SQL Server workload to Azure. They need a highly available, scalable, and secure platform to host their line-of-business (LoB) applications and reporting services. The solution should meet stringent disaster recovery requirements with minimal downtime.

As a seasoned Azure engineer, which of the following designs would you propose to fulfill the customer's requirements?

- A) Deploy the workload on Azure Virtual Machines (IaaS) backed by Azure Site Recovery (DRaaS) and load balancer.

- B) Implement an Azure Synapse Analytics workspace integrated with Azure DevOps for automated release pipelines.
- C) Migrate the SQL Server estate to Azure SQL Managed Instance with read replicas for global distribution and failover groups.
- D) Create a Cosmos DB account with multi-region writes and continuously synchronize data with on-premises SQL Servers using Change Feed Processor.

Answer: C

Feedback(if correct): This option leverages Azure SQL Managed Instance to provide a highly available, scalable, and secure platform for hosting the SQL Server workload. It offers built-in disaster recovery capabilities with failover groups for minimal downtime and read replicas for global distribution, aligning perfectly with the customer's requirements.

Feedback(if wrong): Option A relies on Azure Virtual Machines, which may not provide the same level of scalability and availability as Azure SQL Managed Instance. Option B focuses on analytics and automated release pipelines, which are not directly related to hosting the SQL Server workload. Option D involves Cosmos DB, which may not be the best fit for hosting SQL Server workloads with stringent disaster recovery requirements.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Designing effective solutions for securing Azure infrastructure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

13. You need to configure an Azure policy to ensure that the Azure SQL databases have Transparent Data Encryption (TDE) enabled. The solution must meet the security and compliance requirements. Which actions should you perform in sequence?

- A) Create an Azure policy definition that uses the deployIfNotExists effect.

- B) Create a user-assigned managed identity.
- C) Invoke a remediation task then Create an Azure policy assignment.
- D) Invoke an encryption policy task then Create an Azure Config assignment.

Answers: A, C

Feedback(if correct):

The correct sequence of actions is: A) Create an Azure policy definition that uses the deployIfNotExists effect, followed by C) Invoke a remediation task then Create an Azure policy assignment. This ensures that the policy is defined to check for TDE and then invoked for remediation and assignment to Azure SQL databases.

Feedback(if wrong):

Option B is not relevant to enabling TDE for Azure SQL databases. Option D involves invoking an encryption policy task, which is not directly related to TDE for Azure SQL databases. Therefore, it is not part of the correct sequence.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Analyzing requirements and designing efficient solutions

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Synthesis

14. Suppose you are tasked with loading a substantial amount of data from an Azure Data Lake Storage account into an Azure Synapse Analytics dedicated SQL pool. More precisely, imagine you possess 1,000 CSV files, each having a size of approximately 10 megabytes, located in your Data Lake Storage. Moreover, envision you have already designated an Azure Synapse Analytics dedicated SQL pool referred to as 'sqlpool1'. How would you effectively upload the sizable CSV

files from the Data Lake Storage to 'sqlpool1', ensuring maximum data load efficiency while simultaneously avoiding the necessity to establish external tables beforehand? Kindly select the optimum technique from the subsequent alternatives:

- A. Leveraging the COPY command integrated into the Azure Synapse Analytics system.
- B. Employing PolyBase in conjunction with the Azure Synapse Analytics environment.
- C. Utilizing the bulk copy program (BCP).
- D. Exploiting the SqlBulkCopy class native to .NET Framework.

Answer: B

Feedback (if correct):

The correct answer is PolyBase, which allows you to load data from Azure Data Lake Storage into Azure Synapse Analytics quickly and efficiently without needing to define external tables ahead of time, thus fulfilling the given requirements.

Feedback (if wrong):

The COPY statement is used mainly for copying data within Azure Storage accounts, not between Azure Data Lake Storage and Azure Synapse Analytics.

The SQLBulkcopy object is not specifically designed for loading data from Azure Data Lake Storage into Azure Synapse Analytics.

BCP is mostly used for importing/exporting data to/from SQL Server instances or Azure SQL databases, not between Azure Data Lake Storage and Azure Synapse Analytics.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Designing Data Platforms

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

15. Two applications, App1 and App2, require Azure storage solutions tailored to their specific needs. App1 necessitates data lifecycle management, while App2 demands data storage in an Azure file share. Identify the appropriate blend of Azure storage services catering to both applications' requirements. Considering the following Azure Storage services, mark the correct combination:

- General Purpose v2
- BlockBlobStorage
- FileShare
- Cool Access Tier

App1 requires lifecycle management for its data. App2 needs Azure file share for its storage.

Which combination of Azure Storage services should you choose?

- A) General Purpose v2 and Cool Access Tier only
- B) General Purpose v2 and BlockBlobStorage only
- C) General Purpose v2, BlockBlobStorage, and FileShare only
- D) General Purpose v2, BlockBlobStorage, FileShare, and Cool Access Tier

Feedback (if correct):

The correct combination of Azure storage services ensures that App1 obtains the necessary lifecycle management while App2 acquires the sought-after Azure file share storage. Specifically, the General Purpose v2 storage account offers flexible and economical storage options, including lifecycle management policies. Simultaneously, the FileShare component grants App2 access to Azure file shares, fulfilling its storage requirements. Together, these elements strike the perfect balance between cost-efficiency and functionality, making them the ideal solution for App1 and App2.

Feedback (if wrong):

- A) General Purpose v2 and Cool Access Tier only

Addresses the lifecycle management requirement but misses the Azure file share storage.

- B) General Purpose v2 and BlockBlobStorage only

Focuses primarily on object storage, lacking the Azure file share storage.

D) General Purpose v2, BlockBlobStorage, FileShare, and Cool Access Tier

Contains redundant services, introducing unnecessary complexity for the given requirements.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Applying the necessary Azure storage services and features to satisfy various application requirements

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

16. You manage an on-premises file server hosting 2 TB of data files. Your task is to migrate these data files to Azure Blob Storage located in the West Europe Azure region. To ensure a seamless transition, you must recommend the appropriate storage account type and replication solution, considering the specific requirements:

- The solution should remain available even if a single Azure datacenter experiences a failure.
- It should support storage tiers.
- The overall cost should be minimized.

Which combination of options should you recommend?

- A) General-purpose v2 storage account with read-access geo-redundant storage (RA-GRS) replication
- B) Blob storage account with geo-redundant storage (GRS) replication
- C) Premium Blob storage account with zone-redundant storage (ZRS) replication
- D) BlockBlobStorage storage account with locally redundant storage (LRS) replication

Answer: A

Feedback (if correct):

General-purpose v2 storage accounts support storage tiers, which can reduce costs depending on the accessed data patterns. Furthermore, RA-GRS replication keeps six copies of your data in two Azure regions, ensuring availability even if a single datacenter fails. Although RA-GRS is slightly more expensive than LRS, the enhanced availability compensates for the slight increase in cost.

Feedback (if wrong):

Option B suggests a Blob storage account with geo-redundant storage (GRS) replication, which might provide redundancy but may not optimize costs effectively.

Option C proposes a Premium Blob storage account with zone-redundant storage (ZRS) replication, which may not be the most cost-effective choice for large-scale data storage.

Option D recommends a BlockBlobStorage storage account with locally redundant storage (LRS) replication, which lacks the necessary redundancy for ensuring availability in case of a single Azure datacenter failure.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Designing Azure Storage Strategies, Configuring Azure Storage Replication, Cost optimization in Azure Storage Solutions

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

17. You are leading the design of an Azure infrastructure solution for a company's transaction-intensive applications that will access file shares from on-premises environments. The solution requires minimizing latency and ensuring high resiliency.

Which combination of storage tier and resiliency option would best meet the company's requirements?

- A) Premium tier with Geo-redundant storage (GRS)
- B) Standard tier with Locally-redundant storage (LRS)
- C) Premium tier with Zone-redundant storage (ZRS)
- D) Standard tier with Geo-redundant storage (GRS)

Answer: A

Feedback(if correct):

This option aligns with the requirement to minimize latency and ensure high resiliency for transaction-intensive applications accessing file shares from on-premises environments. The Premium storage tier offers solid-state drives (SSDs) for high performance, while Geo-redundant storage (GRS) provides data replication to a secondary region, ensuring availability and durability.

Feedback(if wrong):

Option B) Standard tier with Locally-redundant storage (LRS): Incorrect because the Standard tier may not offer the required performance for transaction-intensive workloads, and Locally-redundant storage (LRS) does not provide the same level of resiliency as Geo-redundant storage (GRS).

Option C) Premium tier with Zone-redundant storage (ZRS): Incorrect because while the Premium tier offers high performance, Zone-redundant storage (ZRS) replicates data within a single region, which may not meet the resiliency requirement for disaster recovery across regions.

Option D) Standard tier with Geo-redundant storage (GRS): Incorrect because although Geo-redundant storage (GRS) provides resiliency by replicating data to a secondary region, the Standard tier may not offer the required performance for transaction-intensive workloads.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskill: Designing Compute and Network Infrastructure

Competency: Solution Design

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

18. Your company has recently migrated its data platform to Microsoft Azure. As part of the migration, you need to ensure efficient monitoring of network traffic for the Azure-based data platform.

Which solution should you recommend to achieve this objective?

- A. Install and configure Azure Network Watcher to monitor network traffic.
- B. Deploy Azure Security Center to analyze network traffic and identify potential threats.
- C. Utilize Azure Data Lake Storage to store and analyze network traffic data.
- D. Implement Azure Data Factory to orchestrate data flows and monitor network usage.



Answer: A

Feedback(if correct):

Installing and configuring Azure Network Watcher allows for efficient monitoring of network traffic in Azure, aligning with the requirement to monitor the Azure-based data platform.

Feedback(if wrong):

Option B is incorrect because Azure Security Center primarily focuses on security posture management and threat protection, rather than network traffic monitoring.

Option C is incorrect because Azure Data Lake Storage is designed for storing and analyzing large volumes of data, not specifically for monitoring network traffic.

Option D is incorrect because Azure Data Factory is a data integration service for orchestrating data workflows and does not provide network traffic monitoring capabilities.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Plan and implement monitoring and logging solutions

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

19. Your company has implemented an Azure Synapse Analytics instance (ASI) and an Azure Cosmos DB SQL API account (COSMOSDB54). COSMOSDB54 hosts a container that stores continuously updated operational data. You are tasked with designing a solution to analyze this operational data daily using ASI. What solution should you recommend to analyze the data without affecting the performance of the operational data store?

- A. Azure Cosmos DB remote procedure
- B. Azure Synapse Link for Azure Cosmos DB
- C. Azure Web App with Azure MS SQL DB
- D. Azure Synapse Analytics with Active Data Loading

Answer: D

Feedback(if correct):-

Azure Synapse Link for Azure Cosmos DB is the most appropriate solution for analyzing the operational data stored in Azure Cosmos DB without affecting its performance. It provides seamless integration between Azure Synapse Analytics and Cosmos DB, enabling real-time analytics on operational data.

Feedback(if wrong):-

- A. Azure Cosmos DB remote procedure: This option is incorrect because remote procedure calls in Cosmos DB are used for executing server-side logic within the database, not for analyzing data in Azure Synapse Analytics.
- C. Azure Web App with Azure MS SQL DB: This option is incorrect as it involves using a web app and SQL database, which are not directly related to analyzing operational data stored in Cosmos DB using Azure Synapse Analytics.
- D. Azure Synapse Analytics with Active data loading: This option is incorrect because active data loading in Azure Synapse Analytics is used for loading data from various sources into Synapse Analytics, not specifically for analyzing operational data stored in Cosmos DB.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Plan and implement data storage solutions

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

20. Your company has implemented a new Azure SQL Database named "DB4" to store critical data. The database is expected to experience varying workload demands. You need to recommend two parameters to set up to ensure that the "DB4" database can scale effectively to meet these workload demands. What two parameters would you recommend setting up to ensure that the new "DB4" database will scale to meet the workload demands?

- A. Define the maximum size for a database**
- B. Define the minimum resource limit per group of databases**

- C. Define the maximum of Database Transaction Units
- D. Define the maximum of the allocated memory

Answer: A, C

Feedback(if correct):

Setting the maximum size for the database (Option A) allows for scalability by ensuring that the database can grow to accommodate increasing data volumes. Additionally, defining the maximum number of Database Transaction Units (DTUs) (Option C) ensures that the database can handle varying workload demands by dynamically allocating resources.

Feedback(if wrong):

Option B is incorrect because defining the minimum resource limit per group of databases does not directly contribute to the scalability of an individual database like "DB4".

Option D is incorrect because defining the maximum of the allocated memory is not specific to Azure SQL Database scalability and may not directly address varying workload demands.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platform, Designing Compute and Network Infrastructure

Competencies: Architecting for Business Continuity and Disaster Recovery

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

21. You plan to migrate App1 to Azure, requiring an estimation of compute costs while ensuring security and compliance. What methods should you use to estimate the costs, and what strategies should you implement to minimize these costs? Choose the appropriate options from the list below.

- A. Use Azure AD
- B. Implement Azure Reserved Instances to minimize costs
- C. Utilize Azure Hybrid Benefit to reduce licensing costs
- D. Apply Azure Groups

Answer: B, C

Feedback(if correct):

The correct answers are B and C. Option B recommends implementing Azure Reserved Instances to minimize costs, which is an effective strategy for optimizing compute costs. Option C suggests utilizing Azure Hybrid Benefit to reduce licensing costs, which is another cost-saving measure relevant to the scenario.

Feedback(if wrong):

Option A (Use Azure AD) is incorrect because Azure AD (Active Directory) is not directly related to estimating compute costs or implementing cost-saving measures for Azure services.

Option D (Apply Azure Groups) is incorrect as Azure Groups is not a relevant tool for estimating costs or implementing cost-saving measures in Azure.

skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Cost Estimation and Optimization, Security and Compliance Implementation

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

22. In an organization's Azure environment, two critical databases, DB1 and DB2, are being migrated to the cloud platform. These databases are pivotal for the organization's operations, and their availability is paramount. Once migrated to Azure, DB1 and DB2 must adhere to specific requirements to ensure seamless operation and reliability.

Requirements for DB1 and DB2 after migration:

1. **Maintain Availability:** DB1 and DB2 must remain accessible even in the event of a failure in two availability zones within the local Azure region. This requirement emphasizes the need for robust fault tolerance to ensure uninterrupted access to the databases.
2. **Automatic Failover:** The databases should have the capability to automatically failover in case of any disruption or failure. This feature ensures continuity of operations and minimizes downtime, which is crucial for critical production environments.

3. Minimize I/O Latency: To optimize performance and responsiveness, DB1 and DB2 should minimize input/output (I/O) latency. This requirement aims to ensure that database operations are executed efficiently and with minimal delay, enhancing user experience and application responsiveness.

Additionally, select the appropriate service tier for the chosen database implementation(s):

- A. Adopt an Azure SQL Managed Instance for DB1 and DB2:
- B. Place DB1 and DB2 in an Azure SQL Database Elastic Pool:
- C. Business Critical Service tier
- D. General Purpose service tier

Answers: A, C.

Feedback(if correct):

A. Adopt an Azure SQL Managed Instance for DB1 and DB2: Azure SQL Managed Instance provides high availability and automatic failover capabilities, making it suitable for critical production environments. It also offers robust performance with minimal I/O latency, meeting all the specified requirements for DB1 and DB2.

C. Business Critical service tier: Azure SQL Managed Instance offers a Business Critical service tier, which is specifically designed for applications with low I/O latency requirements and minimal impact of underlying maintenance operations on the workload. This service tier aligns with the requirement to minimize I/O latency for DB1 and DB2.

Feedback(if wrong):

B. Place DB1 and DB2 in an Azure SQL Database Elastic Pool: Azure SQL Database Elastic Pool is designed for managing and scaling multiple databases with varying and unpredictable usage demands. It does not inherently provide the necessary fault tolerance and automatic failover capabilities required for DB1 and DB2.

D. General Purpose service tier: Azure SQL Managed Instance offers a General Purpose service tier, which may not meet the specific requirements for low I/O latency and high availability as outlined in the scenario.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms, Designing Identity and Security Solutions, Architecting for Business Continuity and Disaster Recovery

Competencies: Designing Azure Infrastructure Solutions, Implementing and Managing Azure Solutions, Monitoring and Optimizing Azure Solutions, Connecting and Securing Azure Solutions

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

23. You are tasked with migrating App1 to Azure. As part of this migration, you must ensure that the data storage for App1 meets the security and compliance requirements. What is the most appropriate action to take?

- A. Configure access policies for the blob storage.
- B. Adjust the access level of the blob service.
- C. Implement Azure resource locks.
- D. Create Azure RBAC assignments.

Answer: A.

Feedback(if correct):-

Create an access policy for the blob (Option A). This aligns with the requirement to ensure that the data storage for App1 meets security and compliance requirements by controlling who can access the blob data and under what conditions.

Feedback(if wrong):-

Option B, which suggests modifying the access level of the blob service, is incorrect because it focuses on adjusting the overall access level of the blob service rather than specifically creating access policies for individual blobs. This approach might not provide the granularity needed to meet specific security and compliance requirements.

Option C proposes implementing Azure resource locks, which are used to prevent accidental deletion or modification of Azure resources. While resource locks can enhance security by safeguarding critical resources, they do not directly address the requirement of creating access policies for blob storage to ensure security and compliance.

Option D suggests creating Azure RBAC assignments, which involve assigning specific roles to users or groups to control access to Azure resources. While RBAC is crucial for managing access permissions in Azure environments, it does not specifically address the requirement of creating access policies for blob storage, which is essential for ensuring security and compliance.

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Designing Azure Infrastructure Solutions, Implementing and Managing Azure Solutions, Monitoring and Optimizing Azure Solutions, Connecting and Securing Azure Solutions

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis:

24. WebApp1 requires a robust data storage solution meeting stringent security and performance requirements. Which storage option should you recommend?

- A) Azure SQL Database elastic pool
- B) vCore-based Azure SQL database
- C) Virtual Machine hosting MySQL
- D) Blob Storage

Answer: B

Feedback (if correct):

Well done! A vCore-based Azure SQL database provides greater flexibility, higher performance, and improved scalability for WebApp1's evolving data storage demands while adhering to security and compliance requirements.

Feedback (if wrong):

Option A, Azure SQL Database elastic pool, is suitable for managing and scaling multiple databases with varying and unpredictable usage patterns, not necessarily for stringent security and performance requirements. Option C, Virtual Machine hosting MySQL, might provide flexibility but lacks the built-in features and management capabilities of Azure SQL Database. Option D, Blob Storage, is primarily used for unstructured data such as files, images, and videos, and may not be the best choice for structured data storage with specific security and performance requirements.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskill: Designing Data Platforms

Competency: Solution Design

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

25. A healthcare provider, Blue Cross, wishes to modernize their legacy data warehouse and implement a highly available, secure, and easy-to-manage solution in Azure. The solution should support ETL workloads, provide consistent performance, and allow rapid query processing. Which Azure service(s) should you recommend to fulfill these requirements?

- A) Azure Databricks
- B) Azure Cosmos DB
- C) Azure SQL Database
- D) Azure Synapse Analytics

Answer: D

Feedback (if correct):

Azure Synapse Analytics is an ideal solution for modernizing data warehouses, offering limitless scalability, lightning-fast query processing, and native integration with various data formats.

Feedback (if incorrect):

Azure Databricks and Azure Cosmos DB are not ideally suited for this scenario. Azure Databricks is an Apache Spark-based analytics service, while Azure Cosmos DB is a globally distributed, horizontally partitioned multi-model database service. On the contrary, Azure SQL Database is a relational database service, but it may face performance limitations when handling heavy ETL workloads. Azure Synapse Analytics, formerly SQL Data Warehouse, is the most appropriate solution as it can handle massive amounts of structured and semi-structured data, efficiently execute parallel queries, and provide a unified experience for data engineers, data scientists, and business analysts. Revise your understanding and continue practicing to sharpen your solution design skills.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskill: Designing Data Platforms

Competency: Solution Design

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

26. A pharmaceutical company is moving its research and development data platform to Azure. Due to the nature of the industry, data integrity and durability are of utmost importance, while cost optimization remains a major factor. The company expects millions of transactions daily, and the data size will grow exponentially over time.

Propose a storage solution with the appropriate storage tier, replication strategy, and cost optimization techniques to meet the company's requirements.

- A) Store data in premium block blob storage, implement zone-redundant storage (ZRS) replication and leverage storage lifecycle management policies for cost optimization.
- B) Store data in cool object storage, apply geo-redundant storage (GRS) replication and utilize Azure Archive Blobs for long-term archival storage to minimize costs.
- C) Store data in hot general-purpose v2 storage, use read-access geo-zone-redundant storage (RA-GZRS) replication and enable soft delete for deleted blobs for extra protection and cost reduction.
- D) Store data in archive block blob storage, apply geo-redundant storage (GRS) replication and employ Azure Backup to protect older data sets while cutting expenses.

Answer: C

Feedback (if correct):

Great choice! Hot general-purpose v2 storage is ideal for frequent read/write operations and quick access to data. RA-GZRS replication provides the highest resiliency, spanning three regions for ultimate durability. Soft deletion reduces accidental deletion costs and improves overall data management.

Feedback (if wrong):

- A) Premium block blob storage targets IO-intensive operations and may not be the most cost-efficient solution for this scenario. ZRS replication provides resiliency within a single region.
- B) Cool object storage and GRS are tailored for infrequent access and lowest-cost storage. Archive Blobs lock data for longer periods and introduce delayed restores.
- D) Archive block blob storage is for seldom-used data, introducing slow restoration speeds. GRS replication is not the optimal solution for high transaction volume and resiliency. Azure Backup does not directly relate to cost optimization in this context.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Designing Azure Storage Strategies, Configuring Azure Storage Replication, Cost optimization in Azure Storage Solutions

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

27. You plan to deploy multiple instances of an Azure web app across several Azure regions.

You need to design an access solution for the app. The solution must meet the following replication requirements:

- Support rate limiting
- Balance requests between all instances

Does using Azure Load Balancer combined with Azure Application Gateway meet these goals?

A. Yes

B. No

Answer: A

Feedback (if correct):

Using Azure Load Balancer in tandem with Azure Application Gateway indeed satisfies the replication requirements—supporting rate limiting and distributing requests amongst all instances. Azure Load

Balancer can evenly spread traffic across instances, whereas Azure Application Gateway enables rate limiting through its Web Application Firewall feature.

Feedback (if wrong):

both Azure Load Balancer and Azure Application Gateway play crucial roles in achieving the replication requirements. Azure Load Balancer excels in spreading traffic equally across instances, while Azure Application Gateway shines in enforcing rate limiting and offering Web Application Firewall protection. Employing both in concert delivers a robust and adaptable solution.

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Scaling Applications & Services

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

28. You plan to deploy multiple instances of an Azure web app across several Azure regions.

You need to design an access solution for the app. The solution must meet the following replication requirements:

- Support rate limiting
- Balance requests between all instances

Does using Azure Load Balancer combined with Azure Application Gateway meet these goals?

A. Yes

B. No

Answer: A

Feedback (if correct):

Azure Load Balancer combined with Azure Application Gateway indeed meets the replication requirements of supporting rate limiting and balancing requests between all instances. Azure Load Balancer efficiently distributes network traffic across multiple instances, while Azure Application

Gateway can be configured with a Web Application Firewall (WAF) to enforce rate limiting and ensure seamless balancing of requests.

Feedback (if wrong):

Even though your answer is not correct, let's examine the components involved. Azure Load Balancer is responsible for distributing network traffic across various instances, while Azure Application Gateway plays a pivotal role in handling application-specific traffic distribution and enforcing security policies, such as rate limiting through its Web Application Firewall (WAF) feature. It's essential to leverage both services to achieve a holistic and effective solution.

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Scaling Applications & Services

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

Scenario:

You are tasked with recommending a deployment and resiliency solution for migrating on-premises Microsoft SQL Server databases to Azure. The solution must meet specific requirements related to user-initiated backups, automatic replication across Azure regions, and minimizing administrative effort for business continuity.

29. You are tasked with recommending a solution for delivering large files from Azure Blob storage to end users accessing two instances of an Azure web app deployed in different Azure regions. The solution must ensure that users receive files from the same region as the web app they access, ensure file updates are only performed once, and minimize costs. You deploy two instances of an Azure web app. One instance is in the East US Azure region and the other instance is in the West US Azure region. The web app uses Azure Blob storage to deliver large files to end users.

You need to recommend a solution for delivering the files to the users. The solution must meet the following requirements:



- Ensure that the users receive files from the same region as the web app that they access.
- Ensure that the files only need to be updated once.
- Minimize costs.

What should you include in the recommendation?

- A) Azure File Sync
- B) Distributed File System (DFS)
- C) Read-access geo-redundant storage (RA-GRS)
- D) Geo-redundant storage (GRS)

Answer: C

Feedback(if correct):

The correct answer is option C) Read-access geo-redundant storage (RA-GRS). RA-GRS provides read access to data from the nearest geographical location, ensuring users receive files from the same region as the web app they access, minimizing costs by avoiding data transfer between regions, and ensuring file updates only need to be performed once.

Feedback(if wrong):

Option A) Azure File Sync is incorrect because it is used for syncing on-premises file servers with Azure File shares, not for delivering files to end users from Blob storage. Option B) Distributed File System (DFS) is incorrect as it's a Windows feature for replicating files across servers, not for delivering files from Azure Blob storage to end users. Option D) Geo-redundant storage (GRS) is incorrect because while it provides redundancy by replicating data to a secondary region, it does not ensure users receive files from the same region as the web app they access, and it may incur higher costs due to data replication across regions.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Architecting for Business Continuity and Disaster Recovery

Difficulty Level: Expert

Bloom's Taxonomy Level: Evaluation

30. You manage an app named App1 that currently utilizes two on-premises Microsoft SQL Server databases named DB1 and DB2. You are tasked with migrating DB1 and DB2 to Azure. Your solution must support server-side transactions across both databases and minimize administrative effort for updates.

You need to recommend an Azure solution to host DB1 and DB2. The solution must meet the following requirements:

- Support server-side transactions across DB1 and DB2.
- Minimize administrative effort to update the solution.

What should you recommend?

- A) Two SQL Server databases on an Azure virtual machine
- B) Two Azure SQL databases on different Azure SQL Database servers
- C) Two Azure SQL databases in an elastic pool
- D) Two Azure SQL databases on the same Azure SQL Database managed instance

Answer: A

Feedback(if correct):

The correct answer is option A) Two SQL Server databases on an Azure virtual machine. This solution aligns with the requirement of supporting server-side transactions across both DB1 and DB2 while minimizing administrative effort for updates, as it maintains the current setup and provides control over configuration and management.

Feedback(if wrong):

Option B) Two Azure SQL databases on different Azure SQL Database servers is incorrect as it may not support server-side transactions across both databases and can increase administrative effort for managing two separate instances. Option C) Two Azure SQL databases in an elastic pool are incorrect because elastic pools are used for managing and scaling multiple databases with varying usage patterns, but they do not directly support server-side transactions across separate databases. Option D) Two Azure SQL databases on the same Azure SQL Database managed instance is incorrect because while it provides a shared environment, it may not guarantee transactional consistency across the separate databases.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms, Designing Compute and Network Infrastructure

Competencies: Architecting for Business Continuity and Disaster Recovery

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Evaluation

31. You have an on-premises application named App1. Customers use App1 to manage digital images. You plan to migrate App1 to Azure. You need to recommend a data storage solution for App1. The solution must meet the following image storage requirements:

Encrypt images at rest.

Allow files up to 50 MB.

What should you recommend for image storage?

- A) Azure Blob storage
- B) Azure Cosmos DB
- C) Azure SQL Database
- D) Azure Table storage

Answer: A.

Feedback (if correct):

You have recommended Azure Blob Storage as the data storage solution for the on-premises application App1, which manages digital images. Azure Blob Storage supports encrypting images at rest, allowing files up to 50 MB, and is a perfect fit for storing large binary files like images. Good job!

Feedback (if wrong):

Azure Cosmos DB, Azure SQL Database, and Azure Table storage do not serve as optimal data storage solutions for image files due to the following reasons:

Azure Cosmos DB is a globally distributed, multi-model database service that targets mission-critical applications demanding guaranteed uptime, low latency, and blazing-fast reads and writes. As a NoSQL database service, it is less suitable for image storage compared to Azure Blob storage.

Azure SQL Database is a relational database-as-a-service (DBaaS) offered by Microsoft Azure, mainly used for storing structured data and performing complex queries. Images usually qualify as unstructured data, and Azure SQL Database is not the best option for storing large binary files, especially ones larger than 50 MB.

Azure Table storage is a NoSQL key-value store suitable for storing large amounts of structured data. Due to its limitation of supporting only 1-MB maximum blob size, it is not an appropriate option for storing images, particularly those exceeding 50 MB.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Cloud Storage Solutions

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

32. You plan to migrate a web application named App1 from an on-premises data center to Azure. App1 relies on a custom COM component installed on the host server. You need to recommend a solution to host App1 in Azure, ensuring availability if an Azure data center becomes unavailable while minimizing costs. What should you recommend?

- A) In two Azure regions, deploy a load balancer and a virtual machine scale set.
- B) In two Azure regions, deploy a Traffic Manager profile and a web app.
- C) In two Azure regions, deploy a load balancer and a web app.
- D) Deploy a load balancer and a virtual machine scale set across two availability zones.

Answer: D

Feedback(if correct):

The correct answer is option D) Deploy a load balancer and a virtual machine scale set across two availability zones. This solution aligns with the requirement of ensuring high availability of the web

application (App1) by deploying across two availability zones, providing redundancy and fault tolerance while minimizing costs.

Feedback(if wrong):

Option A) Deploying a load balancer and a virtual machine scale set in two Azure regions may provide high availability, but it may increase costs significantly compared to deploying in availability zones within a single region. Option B) Deploying a Traffic Manager profile and a web app in two Azure regions may provide geographic redundancy but may not offer fault tolerance within a single region. Option C) Deploying a load balancer and a web app in two Azure regions may provide redundancy but may not offer fault tolerance within a single region, and it may increase costs compared to deploying in availability zones.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure, Architecting for Business Continuity and Disaster Recovery

Competencies: Availability and Fault Tolerance

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Evaluation

33. Your company plans to deploy various Azure App Service instances that will use Azure SQL databases. The App Service instances will be deployed at the same time as the Azure SQL databases. The company has a regulatory requirement to deploy the App Service instances only to specific Azure regions. The resources for the App Service instances must reside in the same region.

You need to recommend a solution to meet the regulatory requirements.

Solution: You recommend using Azure API Management to specify the desired Azure regions for deploying the App Service instances.

Does this meet the goal?

A) Yes

B) No

Feedback(if correct):

The correct answer is B) No. Azure API Management is not suitable for specifying Azure regions for deploying App Service instances. It is primarily used for managing and securing APIs. Therefore, this solution does not meet the regulatory requirement of deploying App Service instances only to specific Azure regions.

Feedback(if wrong):

All other options are incorrect because they suggest using solutions that are not designed for specifying Azure regions for deploying App Service instances. Therefore, they do not meet the regulatory requirements stated in the scenario.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure, Architecting for Business Continuity and Disaster Recovery

Competencies: Compliance and Regulatory Requirements

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Evaluation

34. Your company plans to deploy various Azure App Service instances that will use Azure SQL databases. The App Service instances will be deployed at the same time as the Azure SQL databases. The company has a regulatory requirement to deploy the App Service instances only to specific Azure regions. The resources for the App Service instances must reside in the same region. You need to recommend a solution to meet the regulatory requirements.

Solution: You recommend using Azure Resource Manager templates with location constraints to specify the desired Azure regions for deploying the App Service instances.

Does this meet the goal?

A) Yes

B) No

Answer: A

Feedback(if correct):

The correct answer is A) Yes. Using Azure Resource Manager templates with location constraints allows for specifying the desired Azure regions for deploying the App Service instances, ensuring compliance with regulatory requirements to deploy resources in specific regions. Therefore, this solution meets the goal.

Feedback(if wrong):

Option B) No is incorrect because using Azure Resource Manager templates with location constraints is an appropriate solution to meet the regulatory requirement of deploying resources only to specific Azure regions, thus making the answer "No" inaccurate.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure.

Competencies: Compliance and Regulatory Requirements

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Evaluation

35. Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is being deployed and configured for on-premises to Azure connectivity. Several virtual machines exhibit network connectivity issues.

You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.

Solution: Use Azure Network Watcher with flow logs enabled to analyze the network traffic.

Does this meet the goal?

A) Yes

B) No

Answer: A

Feedback(if correct):

The correct answer is A) Yes. Using Azure Network Watcher with flow logs enabled allows for analyzing network traffic, including identifying whether packets are being allowed or denied to the virtual machines. Therefore, this solution meets the goal of analyzing network traffic to troubleshoot connectivity issues.

Feedback(if wrong):

Option B) No is incorrect because using Azure Network Watcher with flow logs enabled is an appropriate solution for analyzing network traffic and identifying packet issues, thereby meeting the goal of the scenario.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Troubleshooting and Analysis

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

36. Your organization requires a solution to empower developers to provision Azure virtual machines while adhering to specific guidelines. The solution should ensure that virtual machines are only created in designated regions and with specific sizes. Which recommendation should you propose?

- A. Conditional Access policies
- B. Role-based access control (RBAC)
- C. Azure Resource Manager (ARM) templates
- D. Azure Policy

Answer: D

Feedback(if correct):-

Correct Answer (D - Azure Policy): Azure Policy enables organizations to enforce compliance with specific rules and conditions across Azure resources, making it the appropriate solution for ensuring that virtual machines are provisioned according to specified regions and sizes. It allows the implementation of governance standards, ensuring adherence to organizational policies and standards.

Feedback(if wrong):-

A - Conditional Access policies: Conditional Access policies primarily focus on controlling access to Azure resources based on certain conditions such as user identity, device health, or location. They are not designed to manage the provisioning of virtual machines in specific regions or sizes.

B - Role-based access control (RBAC): RBAC is used to manage user access to Azure resources based on their roles within the organization. While it controls who can access what resources, it does not address the requirement of restricting virtual machine provisioning to specific regions or sizes.

C - Azure Resource Manager (ARM) templates: ARM templates are used for deploying and managing Azure resources through declarative JSON templates. While they facilitate consistent resource deployments, they do not inherently enforce policies regarding virtual machine provisioning in specific regions or sizes.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Leveraging Azure Policy for Infrastructure Governance

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

37. You are tasked with deploying an Azure web app across multiple Azure regions to ensure high availability and fault tolerance. The solution must meet the following requirements:

- Support rate limiting.
- Distribute requests evenly across all instances.
- Ensure continuous access to the app in case of a regional outage.



Which Azure service should you use to fulfill these requirements?

- A) Azure IoT Manager
- B) Azure Web App
- C) Azure Front Door
- D) Azure Load Balancer

Answer: C

Feedback (if correct):

Azure Front Door is the right choice for supporting rate limiting, distributing requests evenly, and ensuring continuous access to the app during a regional outage. It offers global load balancing and traffic management capabilities, as well as SSL termination, WAF, CDN, and reverse proxy functionalities.

Feedback (if wrong):

Azure IoT Hub (Option A) is not the appropriate choice for deploying a web app across multiple Azure regions. Azure Web App (Option B) is a PaaS offering for hosting web applications, but it does not support multi-region deployments and traffic management. Azure Load Balancer (Option D) is a layer 4 load balancer that handles traffic within a single region or availability zone, lacking global load balancing and traffic management features for multi-region deployments.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Architecting for Global Distribution and Resiliency

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

38. Your company intends to deploy a High Performance Computing (HPC) cluster on Azure, leveraging a third-party scheduler for job orchestration. Which solution should you recommend to efficiently provision and manage the HPC cluster nodes?

A) Azure Lighthouse

B) Azure AD

C) Azure Sentinel

D) Azure CycleCloud

Answer: D

Feedback (if correct):

- Azure CycleCloud perfectly fits the description, as it caters to efficiently deploying, scaling, and controlling HPC clusters on Azure.

Feedback (if wrong):

Azure Lighthouse deals with multi-tenant environments, Azure AD oversees identity and access management, whereas Azure Sentinel concentrates on threat detection.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskill: Designing Compute and Network Infrastructure

Competency: Intermediate

Bloom's Taxonomy Level: Application

39. Your company uses an Azure Web App deployed on a Premium App Service Plan. Developers need a solution to manage version updates while minimizing downtime and ensuring rollback capabilities.

Requirements:

Seamless version switching: Ability to switch from the current version to a new one without service interruptions.

Pre-deployment testing: Offer developers a dedicated environment to test new versions before deployment.

Rollback: Provide the option to revert to the previous version if necessary.

Which Azure service best meets these requirements for managing version updates on your Azure Web App?

- A. Azure Traffic Manager
- B. Azure App Service Deployment Slots
- C. Azure Storage Blobs
- D. Azure Backup

Answer: B

Feedback(if correct):-

Deployment slots allow you to create isolated testing environments where you can deploy newer versions of your app and perform rigorous testing before switching to production. This ensures minimal downtime and avoids impacting live users. Rollback is then simply achieved by switching back to the previous slot.

Feedback(if wrong):-

- A. Azure Traffic Manager: While it can distribute traffic across different instances, it doesn't provide testing or rollback capabilities.
- C. Azure Storage Blobs: Mainly for storing app content, not ideal for version management.
- D. Azure Backup: Useful for disaster recovery, not specifically designed for version switching.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Plan and implement application infrastructure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

40. Your task is to recommend a solution for deploying containers that host a two-tier application, with each tier implemented as a separate Docker Linux-based image. The solution must fulfill the following requirements:

- The front-end tier must be accessible via a public IP address on port 80.
- Access to the backend tier should be restricted to port 8080 and only accessible from the front-end tier.
- Both containers must have access to the same Azure file share.
- Automatic restart of the application in case of container failure.
- Minimization of costs.

Which option would you recommend for hosting the application?

- A) Azure Web App
- B) Azure Groups
- C) Azure Kubernetes Service (AKS)
- D) Azure Container Instances

Answer: D

Feedback(if correct): Azure Container Instances (ACI) allow for easy deployment of containers with minimal management overhead, automatic restart on failure, and low cost, making it the ideal solution for this scenario.

Feedback(if wrong):

Option A) Azure Web App: While Azure Web App can host applications, it does not support containerized applications with specific requirements for Docker Linux-based images and port access restrictions.

Option B) Azure Groups: Azure Groups is not a service for hosting containers or managing containerized applications. It is primarily used for organizing resources and managing access control.

Option C) Azure Kubernetes Service (AKS): While AKS is a powerful tool for managing containerized applications and orchestrating containers at scale, it may introduce unnecessary complexity and cost for this scenario, where the requirements are relatively simple and cost minimization is emphasized.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Designing Compute and Network Infrastructure
- Competencies: Architecting for Business Continuity and Disaster Recovery
- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Synthesis

41. You are tasked with deploying 20 applications to Azure, distributed across four Azure Kubernetes Service (AKS) clusters, with each cluster located in a separate Azure region. The deployment must satisfy the following requirements:

- Ensure high availability of the applications even if one AKS cluster fails.
- Encrypt internet traffic using SSL without configuring SSL on each container.

Which service should you include in the recommendation?

- A) Azure Application Gateway
- B) Azure Container Web App
- C) Azure Front Door
- D) AKS Ingress Controller

Feedback(if correct):

The correct answer is D) AKS Ingress Controller. By utilizing an Ingress Controller in Azure Kubernetes Service (AKS), you can achieve high availability by distributing traffic across multiple clusters and ensuring SSL encryption for internet traffic without configuring SSL on each container.

Feedback(if wrong): Option A) Azure Application Gateway: Incorrect because Azure Application Gateway is not specifically designed for managing traffic across multiple AKS clusters and does not directly address the requirement for SSL encryption without configuring SSL on each container.

Option B) Azure Container Web App: Incorrect because Azure Container Web App does not provide the necessary capabilities for managing traffic across AKS clusters or handling SSL encryption at the cluster level.

Option C) Azure Front Door: Incorrect because Azure Front Door primarily focuses on global load balancing and routing for web applications, but it does not directly integrate with AKS clusters or provide SSL encryption for traffic between clusters and the internet without configuring SSL on each container.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Architecting for Business Continuity and Disaster Recovery
- Competencies: Plan and implement disaster recovery strategies, Design and implement business continuity and high availability
- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Application

42. Your company has deployed several virtual machines (VMs) both on-premises and in Azure. Azure ExpressRoute has been established to facilitate connectivity between the on-premises environment and Azure. However, some VMs are experiencing network connectivity issues.

You are tasked with analyzing the network traffic to determine whether packets are being allowed or denied to the VMs.

Which solution should you recommend to meet this goal?

- A. Install and configure the Microsoft Monitoring Agent and the Dependency Agent on all VMs. Use the Wire Data solution in Azure Monitor to analyze the network traffic.
- B. Use Azure Network Watcher to run IP flow verification to analyze the network traffic.
- C. Configure Azure Security Center to monitor network traffic and identify any issues.
- D. Set up Azure Traffic Manager to route network traffic efficiently to the VMs.

Answer: B

Feedback(if correct):

Azure Network Watcher provides tools for analyzing network traffic, including IP flow verification, which can be used to troubleshoot connectivity issues and determine if packets are being allowed or denied to the VMs.

Feedback(if wrong):

Option A is incorrect because while installing and configuring the Microsoft Monitoring Agent and Dependency Agent may help with monitoring VMs, the Wire Data solution in Azure Monitor is not designed specifically for analyzing network traffic at the transport layer.

Option C is incorrect because Azure Security Center primarily focuses on security posture management, threat protection, and security monitoring, rather than network traffic analysis.

Option D is incorrect because Azure Traffic Manager is a DNS-based traffic load balancer and does not provide the tools needed to analyze network traffic for troubleshooting connectivity issues.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Architecting for Business Continuity and Disaster Recovery
- Competencies: Plan and implement disaster recovery strategies, Design and implement business continuity and high availability
- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Application

43. You are tasked with designing a monitoring solution for an Azure Load Balancer named LB1, which balances requests to five Azure virtual machines. Your solution must generate an alert under specific conditions. You have an Azure Load Balancer named LB1 that balances requests to five Azure virtual machines. You need to develop a monitoring solution for LB1. The solution must generate an alert when any of the following conditions are met:

1. A virtual machine is unavailable.
2. Connection attempts exceed 50,000 per minute.

Which signal should you include in the solution for each condition? Choose the correct options from the list below:

A) An unavailable virtual machine: Data Path Availability

More than 50,000 connection attempts per minute: Packet Count

B) An unavailable virtual machine: Health Probe Status

More than 50,000 connection attempts per minute: SYN Count

C) An unavailable virtual machine: Health Probe Status

More than 50,000 connection attempts per minute: Packet Count

D) An unavailable virtual machine: Data Path Availability

More than 50,000 connection attempts per minute: SYN Count

Answer: C

Feedback (if correct):

Including "Health Probe Status" for detecting an unavailable virtual machine and "Packet Count" for tracking more than 50,000 connection attempts per minute in the monitoring solution is the correct approach. This setup allows administrators to receive timely alerts to mitigate potential issues.

Feedback (if wrong):

- a. Data Path Availability: While this metric indicates whether the data path is operational, it may not pinpoint specific virtual machine failures.
- b. SYN Count: Although this metric counts the synchronized packets, it doesn't represent the total number of connection attempts, especially when it comes to limiting the rate of incoming requests.
- c. Packet Count: This metric shows the number of packets sent and received via the load balancer, offering insight into excessive connection attempts.

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Architecting for Business Continuity and Disaster Recovery

Difficulty Level: Expert

Bloom's Taxonomy Level: Application

44. You are tasked with automating the deployment of resources to Azure subscriptions. What is the key difference between using Azure Blueprints and Azure Resource Manager templates?

A) Azure Resource Manager templates remain connected to the deployed resources.

B) Only Azure Resource Manager templates can contain policy definitions.

- C) Azure Blueprints remain connected to the deployed resources.
- D) Only Azure Blueprints can contain policy definitions.

Answer: C

Feedback(if correct):- With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved. This connection supports improved tracking and auditing of deployments. Azure Blueprints can also upgrade several subscriptions at once that are governed by the same blueprint.

Feedback(if wrong):

- A) Azure Resource Manager templates - While Azure Resource Manager templates define the infrastructure and configuration of Azure resources, they do not maintain a connection to the deployed resources like Azure Blueprints.
- B) Only Azure Resource Manager templates - Azure Blueprints also support policy definitions, allowing organizations to define and enforce standards and compliance requirements across their Azure environments.
- D) Only Azure Blueprints - Azure Resource Manager templates can also contain policy definitions, enabling organizations to define policies for resources deployed using templates.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Azure Governance

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

45. You plan to deploy multiple instances of an Azure web app across several Azure regions.

You need to design an access solution for the app. The solution must meet the following replication requirements:

- Ensure that users can access the app in the event of a regional outage
- Balance requests between all instances



Can Azure Availability Zones solve this challenge?

- A. Yes
- B. No

Answer: A

Feedback (if correct):

Azure Availability Zones certainly can address this challenge. They ensure high availability and resiliency by distributing your web app instances across physically separate zones within an Azure region, thus mitigating the impact of regional outages and maintaining consistent access to your application. Moreover, Azure Load Balancer or Azure Application Gateway can be employed to balance requests between all instances.

Feedback (if wrong):

The correct answer is "Yes." Azure Availability Zones provide redundancy and fault tolerance within a single Azure region, ensuring high availability for services deployed within that region. However, selecting "No" is incorrect because although Azure Availability Zones don't directly address the requirement to balance requests between instances deployed across different regions, they still contribute to the overall availability and resilience of the application within each region. For ensuring access to the app in the event of a regional outage and balancing requests between instances deployed across multiple regions, other Azure services like Azure Traffic Manager or Azure Front Door would be more appropriate.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Resiliency and High Availability

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

46. From the list below, select the best deployment and resiliency solution for migrating on-premises Microsoft SQL Server databases to Azure. The solution must:

Support user-initiated backups

Support multiple automatically replicated instances across Azure regions

Minimize administrative efforts to implement and maintain business continuity

Choose the correct options:

A) Deployment solution: Azure SQL Managed Instance

Resiliency solution: Auto-failover group

B) Deployment solution: SQL Server on Azure Virtual Machines

Resiliency solution: Active geo-replication

C) Deployment solution: An Azure SQL Database single database

Resiliency solution: Zone-redundant deployment

D) Deployment solution: Azure SQL Managed Instance

Resiliency solution: Active geo-replication

Answer:D

Feedback (if correct):

Azure SQL Managed Instance and Auto-failover group. This combination meets all the requirements: it supports user-initiated backups, automatically replicates instances across Azure regions, and minimizes administrative efforts for business continuity.

Auto-failover groups provide automated failover and automatic replication, reducing manual intervention and administration overhead. Azure SQL Managed Instance is a fully managed SQL Server service, eliminating much of the administrative burden compared to running SQL Server on traditional virtual machines.

Feedback (if incorrect):

A) SQL Server on Azure Virtual Machines – This solution involves manually creating and managing highly available VMs, leading to increased administrative effort. While Azure Backup can be used for user-initiated backups, active geo-replication isn't supported for SQL Server on Azure Virtual Machines.

B) An Azure SQL Database single database – This option lacks support for user-initiated backups as backup and restore options are controlled by Azure, rather than the user. Additionally, zone-redundant deployment is a HA strategy, not DR, and does not cover cross-region automatic replication.

C) Azure SQL Managed Instance with Active Geo-Replication – Though this option meets the majority of the requirements, Active Geo-Replication imposes limitations on the number of secondary replicas, increasing administrative overhead and costs.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Plan and implement disaster recovery strategies, Design and implement business continuity and high availability

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

47. You are tasked with recommending an Azure Storage Account configuration for two applications named Application1 and Application2. The configuration must meet specific requirements for each application. For Application1, the storage solution must provide the highest possible transaction rates and the lowest possible latency. For Application2, the storage solution must offer the lowest possible storage costs per GB. Both solutions need to be optimized for uploads and downloads and must remain available in the event of a datacenter failure. Which Azure Storage Account configuration should you recommend for each application?

- A. Application1: BlobStorage with Standard performance, Hot access tier, and Read-access geo-redundant storage (RA-GRS) replication; Application2: BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication
- B. Application1: General purpose v2 with Premium performance and Locally-redundant storage (LRS) replication; Application2: General purpose v1 with Standard performance and Read-access geo-redundant storage (RA-GRS) replication
- C. Application1: BlobStorage with Premium performance and Zone-redundant storage (ZRS) replication; Application2: General purpose v2 with Standard performance, Cool access tier, and Read-access geo-redundant storage (RA-GRS) replication
- D. Application1: BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication; Application2: BlobStorage with Standard performance, Cool access tier, and Geo-redundant storage (GRS) replication

Answer: A

Feedback (if correct): Option A is the correct choice for the given requirements. For Application1, BlobStorage with Standard performance, Hot access tier, and RA-GRS replication provides the highest transaction rates, low latency, and read-access geo-redundancy. For Application2, BlockBlobStorage with Premium performance and ZRS replication offers the lowest storage costs per GB and ensures availability in the event of a datacenter failure.

Feedback (if wrong):

Option B does not meet the requirements. General purpose v2 with Premium performance and LRS replication for Application1 does not provide the highest transaction rates and lowest latency. General purpose v1 with Standard performance and RA-GRS replication for Application2 does not offer the lowest storage costs per GB.

Option C does not meet the requirements. BlobStorage with Premium performance and ZRS replication for Application1 does not provide the highest transaction rates and lowest latency. General purpose v2 with Standard performance, Cool access tier, and RA-GRS replication for Application2 does not offer the lowest storage costs per GB.

Option D does not meet the requirements. BlockBlobStorage with Premium performance and ZRS replication for Application1 does not provide the highest transaction rates and lowest latency. BlobStorage with Standard performance, Cool access tier, and GRS replication for Application2 does not offer the lowest storage costs per GB.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms, Designing Compute and Network Infrastructure

Competencies: Plan and implement disaster recovery strategies, Design and implement business continuity and high availability

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

48. Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity. However, some VMs are experiencing network connectivity issues. You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs. Which solution should you recommend to meet this goal?

A. Install and configure the Microsoft Monitoring Agent and the Dependency Agent on all VMs. Use the Wire Data solution in Azure Monitor to analyze the network traffic.

- B. Use Azure Network Watcher to run IP flow verification to analyze the network traffic.
- C. Configure Azure Security Center to monitor network traffic and identify any issues.
- D. Set up Azure Traffic Manager to route network traffic efficiently to the VMs.

Answer: B

Feedback(if correct):

Using Azure Network Watcher to run IP flow verification is the correct solution for analyzing network traffic and determining whether packets are being allowed or denied to the VMs.

Feedback(if wrong):

Option A is incorrect because while the Microsoft Monitoring Agent and Dependency Agent along with the Wire Data solution in Azure Monitor can provide insights into network traffic, they do not specifically allow for the analysis of packet allowance or denial.

Option C is incorrect as Azure Security Center is primarily focused on security posture management and threat protection, not specifically on analyzing network traffic for connectivity issues.

Option D is incorrect because Azure Traffic Manager is used for traffic routing and load balancing across different endpoints, not for analyzing network traffic to determine packet allowance or denial.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Plan and implement disaster recovery strategies, Design and implement business continuity and high availability

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

49. Your company has an on-premises file server named "fs01" that runs Windows Server 2019. Windows Admin Center is used to manage this server. The company also owns an Azure subscription. You need to propose an Azure solution to ensure data protection in case the file server experiences a failure. Solution: You plan to create an Azure Recovery Services vault and install the Azure Backup agent on "fs01" to schedule regular backups. Would this solution meet the requirement?

- A. Yes
- B. No

Answer: A

Feedback(if correct):

Yes, the proposed solution meets the requirement. Creating an Azure Recovery Services vault and installing the Azure Backup agent on "fs01" to schedule regular backups would ensure data protection in case the file server experiences a failure. This aligns with the competency of designing Microsoft Azure infrastructure solutions by implementing a reliable backup and recovery strategy.

Feedback(if wrong):

Option B is incorrect because the proposed solution of creating an Azure Recovery Services vault and installing the Azure Backup agent on "fs01" to schedule regular backups would indeed meet the requirement of ensuring data protection in case the file server experiences a failure. This aligns with the competency of designing Microsoft Azure infrastructure solutions by implementing a reliable backup and recovery strategy. Therefore, Option A is the correct answer.

skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Implementing Azure Backup and Recovery Solutions

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

50. Your organization is planning to implement a disaster recovery (DR) strategy for its critical applications hosted in Azure. As part of the Azure AZ-305 exam preparation, you are tasked with designing a robust DR solution that meets the organization's requirements for business continuity and high availability. Given the scenario, devise a comprehensive DR strategy by selecting the most appropriate Azure services and configurations.

1. RTO and RPO: The RTO (Recovery Time Objective) for critical applications should be less than 4 hours, and the RPO (Recovery Point Objective) should be less than 1 hour.

2. **Regional Failover:** The DR solution must support failover to an alternate Azure region in the event of a regional outage.
3. **Automated Failover:** Failover should be automated to minimize downtime and ensure seamless continuity of operations.
4. **Cost Optimization:** Implement cost-effective solutions while maintaining high availability and disaster recovery capabilities.

Select the Azure services and configurations that best meet these requirements from the options provided:

- A) Azure Site Recovery (ASR) with Azure Traffic Manager for DNS-based failover.
- B) Azure Backup with Azure File Sync for data replication and Azure Traffic Manager for DNS-based failover.
- C) Azure Site Recovery (ASR) with Azure Traffic Manager for DNS-based failover and Azure Automation for automated failover.
- D) Azure Backup with Azure File Sync for data replication and Azure Automation for automated failover.

Answer: C

Feedback(if correct):-

Option C is the correct answer as it combines Azure Site Recovery (ASR) for automated failover, Azure Traffic Manager for regional failover, and Azure Automation for orchestrating failover processes, fulfilling all specified requirements.

Feedback(if wrong):-

Option A is incorrect because it lacks automated failover capabilities, which are crucial for meeting the RTO and RPO requirements.

Option B is incorrect as Azure Backup is primarily for data backup and not suitable for achieving rapid failover objectives.

Option D does not include a solution for automated failover, making it less suitable for meeting the RTO and RPO requirements.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Plan and implement disaster recovery strategies, Design and implement business continuity and high availability

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

51. TrenTop Corporation, a multinational financial institution, is seeking to design comprehensive and highly resilient disaster recovery solutions for its critical systems in Azure. They require a solution that can handle various disaster scenarios and minimize downtime and data loss to meet strict regulatory requirements.

Which of the following considerations should be given the highest priority when designing disaster recovery solutions in Azure for XYZ Corporation, considering the complexity and criticality of their systems?

- A) Recovery Point Objective (RPO): The maximum acceptable data loss in the event of a disaster, which influences the frequency of data replication and backup to ensure minimal data loss.
- B) Recovery Time Objective (RTO): The maximum acceptable downtime for recovering critical systems, which drives the choice of disaster recovery strategies and technologies to minimize downtime.
- C) Geographical Redundancy: The use of Azure regions and paired regions to replicate and distribute resources across multiple locations, ensuring resilience and minimizing the impact of regional disasters.
- D) Automated Failover and Testing: Implementing automated failover mechanisms and conducting regular disaster recovery tests to validate the effectiveness and reliability of the solutions, reducing manual intervention and ensuring readiness.

Answer: B

Feedback (if correct): The correct answer is B) Recovery Time Objective (RTO). This is because RTO defines the maximum acceptable downtime for recovering critical systems, which directly impacts the choice of disaster recovery strategies and technologies to minimize downtime.

Feedback (if wrong):

- A) Recovery Point Objective (RPO): This is incorrect because while RPO is important for minimizing data loss, it does not directly address minimizing downtime, which is the primary concern in disaster recovery.
- C) Geographical Redundancy: This is incorrect because while geographical redundancy is important for resilience and minimizing the impact of regional disasters, it may not address the immediate need to minimize downtime for critical systems.
- D) Automated Failover and Testing: This is incorrect because while automated failover mechanisms and regular testing are essential for ensuring readiness and reliability, they do not directly address the priority of minimizing downtime, which is crucial in disaster recovery scenarios.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskill: Architecting for Business Continuity and Disaster Recovery

Competencies: Designing business continuity solutions, Designing infrastructure solutions

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

52. Top4 Corporation is migrating its applications to Microsoft Azure and needs to ensure secure access to Azure resources. Which of the following considerations should be given the highest priority when recommending solutions to allow applications to access Azure resources, ensuring secure storage of passwords and secrets?

- A) Implementing Multi-Factor Authentication (MFA) for application access to Azure resources, and utilizing Azure Key Vault for secure storage of passwords and secrets.
- B) Utilizing Azure Active Directory (Azure AD) Application Proxy for application access to Azure resources, and storing passwords and secrets in Azure Blob Storage.
- C) Configuring Azure Virtual Network Service Endpoints for application access to Azure resources, and storing passwords and secrets in Azure SQL Database.
- D) Deploying Azure Application Gateway for application access to Azure resources, and managing passwords and secrets locally within the application codebase.

Answer: A

Feedback (if correct):

A) Implementing Multi-Factor Authentication (MFA) for application access to Azure resources, and utilizing Azure Key Vault for secure storage of passwords and secrets. This is because MFA adds an extra layer of security for application access, and Azure Key Vault provides a secure and centralized solution for storing and managing passwords and secrets.

Feedback (if wrong):

- B) Utilizing Azure Active Directory (Azure AD) Application Proxy for application access to Azure resources, and storing passwords and secrets in Azure Blob Storage: This is incorrect because Azure Blob Storage is not specifically designed for secure storage of passwords and secrets, and Azure AD Application Proxy is primarily used for secure remote access to on-premises applications.
- C) Configuring Azure Virtual Network Service Endpoints for application access to Azure resources, and storing passwords and secrets in Azure SQL Database: This is incorrect because Azure SQL Database may not be the most appropriate solution for storing passwords and secrets securely, and Azure Virtual Network Service Endpoints are used to secure connections to Azure services but do not directly address the secure storage of passwords and secrets.
- D) Deploying Azure Application Gateway for application access to Azure resources, and managing passwords and secrets locally within the application codebase: This is incorrect because managing passwords and secrets locally within the application codebase is not a secure practice, and Azure Application Gateway is primarily used for load balancing and secure reverse proxy functionality, not for securing access to Azure resources or managing passwords and secrets.

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Design identities and access for applications

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Evaluation

az305 final exam2

1. ABC Corporation is transitioning its applications to Microsoft Azure and needs to ensure secure access to Azure resources while designing identity and security solutions.

Question: Which of the following considerations should be given the highest priority when designing identity and security solutions to allow applications secure access to Azure resources, including securely storing passwords and secrets?

- A) Implementing Multi-Factor Authentication (MFA) for application access to Azure resources, and utilizing Azure Key Vault for secure storage of passwords and secrets.
- B) Utilizing Azure Active Directory (Azure AD) Application Proxy for application access to Azure resources, and storing passwords and secrets in Azure Blob Storage.
- C) Configuring Azure Virtual Network Service Endpoints for application access to Azure resources, and storing passwords and secrets in Azure SQL Database.
- D) Deploying Azure Application Gateway for application access to Azure resources, and managing passwords and secrets locally within the application codebase.

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Designing identities and access for applications

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Evaluation

Feedback (if correct):

The correct answer is A) Implementing Multi-Factor Authentication (MFA) for application access to Azure resources, and utilizing Azure Key Vault for secure storage of passwords and secrets. This is because MFA adds an extra layer of security for application access, and Azure Key Vault provides a secure and centralized solution for storing and managing passwords and secrets, aligning with the subskill of designing identities and access for applications.

Feedback (if wrong):

- B) Utilizing Azure Active Directory (Azure AD) Application Proxy for application access to Azure resources, and storing passwords and secrets in Azure Blob Storage: This is incorrect because Azure Blob Storage is not specifically designed for secure storage of passwords and secrets, and Azure AD Application Proxy is primarily used for secure remote access to on-premises applications, not for securing access to Azure resources.
- C) Configuring Azure Virtual Network Service Endpoints for application access to Azure resources, and storing passwords and secrets in Azure SQL Database: This is incorrect because Azure SQL Database may not be the most appropriate solution for storing passwords and secrets securely, and Azure Virtual Network Service Endpoints are used to secure connections to Azure services but do not directly address the secure storage of passwords and secrets for applications.
- D) Deploying Azure Application Gateway for application access to Azure resources, and managing passwords and secrets locally within the application codebase: This is incorrect because managing passwords and secrets locally within the application codebase is not a secure practice, and Azure Application Gateway is primarily used for load balancing and secure reverse proxy functionality, not for securing access to Azure resources or managing passwords and secrets.

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Designing identities and access for applications

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Evaluation

2. Fabrikam, a rapidly growing tech startup, plans to scale its operations and consolidate its authentication infrastructure in Azure Active Directory (Azure AD). Their main priority lies in ensuring strong authentication and authorization protocols for their employees, customers, and partners alike. Moreover, they aspire to benefit from Azure AD's rich features and seamless integration with Office 365 and countless other SaaS applications.

To achieve these objectives, the Fabrikam IT Team has reached out to you, an expert in Azure AD, to assist in determining the necessary components for a robust and secure authentication solution. Your guidance will play a crucial role in helping Fabrikam meet the following essential requirements:

1. Strengthen authentication procedures for increased security and regulatory compliance.
2. Streamline user access and eliminate friction in their everyday workflows.
3. Reinforce conditional access controls based on location, device, and user risk levels.
4. Equip Fabrikam with an extensible architecture capable of supporting upcoming growth and acquisitions.

As you collaborate with the Fabrikam IT Team, you find yourself having to balance competing priorities and making strategic tradeoffs to arrive at the most practical and forward-looking solution. Through careful deliberation and informed decision-making, you settle on a series of recommendations that strike an optimal balance between security, convenience, and scalability.

Now, it's your turn to select the correct components for Fabrikam's Azure AD authentication solution from the options provided earlier.

To meet Fabrikam's authentication requirements in Azure AD, consider the following configurations. Choose the most appropriate answer from the options below.

- A) Minimum Number of Azure AD tenants: 1 tenant, complemented with zero custom domains and a single conditional access policy.
- B) Minimum Number of Azure AD tenants: Two tenants, accompanied by 1 custom domain and 2 conditional access policies
- C) Minimum Number of Azure AD tenants: Three tenants, accompanied by 2 custom domains and 4 conditional access policies
- D) Minimum Number of Azure AD tenants: 5 tenants, accompanied by 3 custom domains and 1 conditional access policy

Answer: A

Feedback(if correct):-

Option A recommends a single Azure AD tenant, which aligns with Fabrikam's goal of consolidating its authentication infrastructure, ensuring simplicity, and minimizing administrative overhead. It provides a practical and efficient solution that meets Fabrikam's requirements while maintaining security and compliance.

Feedback(if wrong):-

B) Minimum Number of Azure AD tenants: Two tenants, accompanied by 1 custom domain and 2 conditional access policies

This option suggests using two Azure AD tenants, which may not be necessary for Fabrikam's requirements. Having multiple tenants can introduce complexity and administrative overhead, especially for a growing organization. It is more practical to have a single Azure AD tenant to consolidate the authentication infrastructure and simplify management.

C) Minimum Number of Azure AD tenants: Three tenants, accompanied by 2 custom domains and 4 conditional access policies

This option suggests using three Azure AD tenants, which is again unnecessary for Fabrikam's requirements. Multiple tenants can lead to increased complexity and administrative overhead. It is more efficient to have a single Azure AD tenant to consolidate the authentication infrastructure and streamline management.

D) Minimum Number of Azure AD tenants: 5 tenants, accompanied by 3 custom domains and 1 conditional access policy

This option suggests using five Azure AD tenants, which is excessive for Fabrikam's needs. Managing multiple tenants can be complex and time-consuming. It is more practical to have a single Azure AD tenant to consolidate the authentication infrastructure and simplify management.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Analyzing requirements and designing efficient solutions

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Synthesis

3. Your on-premises network contains a server named Server1 that runs an ASP.NET application named App1. You have a hybrid deployment of Azure Active Directory (Azure AD). You need to recommend a solution to ensure that users sign in by using their Azure AD account and Azure Multi-Factor Authentication (MFA) when they connect to App1 from the internet. You need to recommend three Azure services to be deployed and configured in sequence. Which three Azure services should you recommend, and in what order should they be arranged?

- A) Azure AD Application Proxy
- B) Azure AD Enterprise Application
- C) Azure AD Conditional Access Policy
- D) Azure AD Managed Identity

Answer: A, B, C

Feedback (if correct):

By recommending the sequential arrangement of Azure AD Application Proxy, Azure AD Enterprise Application, and Azure AD Conditional Access Policy, you have demonstrated a deep comprehension of the essential components required for authenticating users with Azure AD and MFA when accessing App1. Your synthesis of knowledge illustrates your capability to craft a cohesive, practical solution.

Feedback (if wrong):

Azure AD Managed Identity is not a fitting solution for the provided scenario because it is focused on managing identities for automated processes and applications rather than human users. It does not inherently support Multi-Factor Authentication (MFA), which is explicitly required in the scenario.

Additionally, Azure AD Managed Identity is aimed at simplifying the management of application secrets and granting permissions to services without exposing explicit credentials. Its core strength lies in automating the acquisition and renewal of access keys and tokens for communication with Azure APIs and services. Hence, it wouldn't contribute much to enforcing authentication mechanisms for human users trying to access App1 over the internet.

Feedback (if correct):

You have selected the correct solution, Azure API Management. This choice allows for rate limiting, external OAuth 2.0 authentication, and proxy functionality without changing the Logic Apps themselves or leveraging Azure AD guest accounts.

Feedback (if wrong):

Unfortunately, the other options fall short of meeting the requirements. Azure AD business-to-business (B2B) would require Azure AD guests, violating the fourth constraint. Azure AD Application Proxy is meant for on-premises apps and couldn't accomplish the necessary external OAuth 2.0 integration. Azure Front Door is primarily focused on global load balancing and failover, failing to provide the required throttling and authentication features.

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Meeting accessibility and authentication requirements for partner companies while abiding by imposed constraints

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

4. Your company, Contoso Ltd., has implemented several Azure Logic Apps with HTTP triggers to provide access to an on-premises web service. Recently, Contoso established a partnership with Fabrikam Inc. Fabrikam does not have an existing Azure Active Directory (Azure AD) tenant and uses third-party OAuth 2.0 identity management to authenticate its users. Fabrikam developers plan to utilize a subset of the Logic Apps to integrate with Contoso's on-premises web service. Your task is to design a solution that allows Fabrikam developers access to the Logic Apps while meeting the following requirements:

- Requests from Fabrikam developers to the Logic Apps must be limited to lower rates than those from Contoso users.
- Fabrikam developers should rely on their existing OAuth 2.0 provider for accessing the Logic Apps.
- The solution must not require modifications to the Logic Apps.
- Azure AD guest accounts must not be utilized in the solution.

What should you include in the solution?

- A) Azure AD business-to-business (B2B)
- B) Azure AD Application Proxy
- C) Azure Front Door
- D) Azure API Management

Answer: D

Feedback(if correct):

Azure API Management because it allows organizations to publish APIs securely and provides OAuth 2.0 integration for authentication. It also offers rate-limiting capabilities to control access to the Logic Apps, meeting all the specified requirements in the scenario.

Feedback(if wrong):

Option A (Azure AD business-to-business): This option involves collaborating with users from other organizations through Azure AD, but it doesn't meet the requirement of rate limiting or relying on Fabrikam's existing OAuth 2.0 provider.

Option B (Azure AD Application Proxy): While Azure AD Application Proxy allows organizations to securely publish internal web applications, it doesn't provide rate limiting or integration with Fabrikam's OAuth 2.0 provider.

Option C (Azure Front Door): Azure Front Door provides fast and secure delivery of web applications but lacks the necessary rate limiting and OAuth 2.0 integration required in the scenario.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Identity and Access Management, Security, Authentication, Authorization

Difficulty Level: Expert

Bloom's Taxonomy Level: Evaluation

5. You are designing a solution to ensure that users can securely access an ASP.NET application named App1 from the internet using their Azure AD account and Azure MultiFactor Authentication (MFA). Which three Azure services should you recommend deploying and configuring in sequence?

- A) Azure AD conditional access policy
- B) Azure AD Application Proxy
- C) Azure AD enterprise application
- D) Azure AD managed identity

Answer: A, B, C

Feedback(if correct):

The correct sequence is:

1. Azure AD Application Proxy: It allows secure remote access to on-premises applications. By configuring Azure AD Application Proxy, you can publish the ASP.NET application App1 securely for access over the internet.
2. Azure AD conditional access policy: This policy can be configured to enforce MultiFactor Authentication (MFA) requirements based on conditions such as user location, device compliance, or risk level. By setting up a conditional access policy, you ensure that users are prompted for MFA when accessing the application.
3. Azure AD enterprise application: This represents the ASP.NET application (App1) within Azure AD. It allows you to manage single-sign-on (SSO) and access control policies for the application.

Feedback(if wrong):

Option A is incorrect because Azure AD conditional access policy should be configured after setting up Azure AD Application Proxy. The conditional access policy enforces additional security requirements, such as MFA, which should be applied after ensuring secure remote access using Azure AD Application Proxy.

Option D is incorrect because Azure AD managed identity is not relevant to the scenario of enabling secure access to an ASP.NET application from the internet using Azure AD and MFA.

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Analyzing: Evaluating the requirements and determining the appropriate Azure services and configurations needed to secure access to the ASP.NET application, Applying: Implementing the recommended Azure services and configurations in the correct sequence to achieve the desired security objectives.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

6. You are tasked with securing access to an ASP.NET application named App1, ensuring that users can authenticate with their Azure AD accounts and utilize Azure MultiFactor Authentication (MFA) when accessing the application from the internet. Which sequence of Azure services should you recommend deploying and configuring to achieve this?

- A) Azure AD managed identity, Internal Azure Load Balancer, Azure AD conditional access policy
- B) Azure AD Application Proxy, Azure AD conditional access policy, Azure AD enterprise application

- C) Public Azure Load Balancer, Azure AD conditional access policy, Azure AD managed identity
- D) Azure AD Application Proxy, Public Azure Load Balancer, Azure AD enterprise application

Answer: B

Feedback(if correct):

Azure AD Application Proxy: It allows secure remote access to on-premises applications, such as ASP.NET applications, by providing reverse proxy functionality. Configuring Azure AD Application Proxy enables external users to access the application securely via Azure AD authentication.

Azure AD conditional access policy: This policy can be set up to enforce Azure MultiFactor Authentication (MFA) requirements based on various conditions, such as user location or device state. By configuring a conditional access policy, you ensure that users are prompted for MFA when accessing the application.

Azure AD enterprise application: This represents the ASP.NET application within Azure AD. Configuring the enterprise application allows you to manage single-sign-on (SSO) settings and access control policies for the application.

Feedback(if wrong):

Option A: Azure AD managed identity and Internal Azure Load Balancer is not necessary for securing access to an ASP.NET application with Azure AD authentication and MFA.

Option C: Public Azure Load Balancer is not typically used for securing access to application endpoints, and Azure AD managed identity is not relevant to this scenario.

Option D: While Azure AD Application Proxy is correctly included, Public Azure Load Balancer is not typically used for securing access to application endpoints, and Azure AD enterprise application should be configured after Azure AD Application Proxy and conditional access policies for proper authentication and access control.

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Analyzing: Evaluating the requirements and determining the appropriate Azure services and configurations needed to secure access to the ASP.NET application, Applying: Implementing the recommended Azure services and configurations in the correct sequence to achieve the desired security objectives.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

7. You are tasked with configuring authentication for a new web application named WebApp1 hosted on an on-premises server called Server1 but is not directly accessible over the internet. The application must allow users to sign in using their Azure AD accounts and utilize Azure Multi-Factor Authentication (MFA) when accessing it from external networks. What should you recommend as the initial step in configuring the authentication mechanism for WebApp1?

- A) Implement Azure AD Conditional Access Policies
- B) Configure Azure AD Application Proxy
- C) Set up Azure AD Enterprise Application for WebApp1
- D) Deploy Azure AD Managed Identity for Server1

Answer: B

Feedback(if correct): Configuring Azure AD Application Proxy is the recommended initial step because it enables secure remote access to on-premises applications like WebApp1 without requiring VPNs or opening up ports on firewalls. It also provides authentication and authorization capabilities, allowing users to sign in using their Azure AD accounts and enforcing Azure Multi-Factor Authentication (MFA) when accessing the application from external networks.

Feedback(if wrong): The other options are not the correct initial step for configuring the authentication mechanism for WebApp1. Here's why they are incorrect:

- A) Implementing Azure AD Conditional Access Policies: While conditional access policies are important for enforcing specific access rules based on conditions, they are not the first step in configuring the authentication mechanism for an on-premises application like WebApp1.
- C) Setting up Azure AD Enterprise Application for WebApp1: This step comes after configuring Azure AD Application Proxy and involves registering the on-premises application with Azure AD as an enterprise application. It is not the initial step in the configuration process.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Executing the deployment and configuration of Azure services to enable secure authentication mechanisms for the web application, ensuring compliance with organizational security policies and best practices.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

8. After deploying and configuring Azure AD Application Proxy, you need to proceed with configuring two additional Azure services to complete the authentication setup for the ASP.NET application. Which two Azure services should you recommend deploying and configuring next, in sequence?

- A) Azure AD Application Proxy
- B) Azure AD enterprise application
- C) Azure AD conditional access policy
- D) Azure AD managed identity

Answer: B, C

Feedback(if correct):

After deploying Azure AD Application Proxy to enable secure remote access to the ASP.NET application, the next step is to configure an Azure AD enterprise application. This enterprise application represents the ASP.NET application in Azure AD and defines how it interacts with users and other applications.

Once the enterprise application is configured, you need to set up a conditional access policy in Azure AD. This policy defines the conditions under which users can access the ASP.NET application, including requirements for Azure MultiFactor Authentication (MFA) and other security controls.

Feedback(if wrong):

A) Azure AD Application Proxy: This service has already been deployed and configured in the previous step, so it does not need to be repeated.

D) Azure AD managed identity: Managed identities are used for authenticating Azure services with other Azure resources and are not relevant to configuring access for the ASP.NET application.

Skill Mapping:



Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Executing the deployment and configuration of Azure services to enable secure authentication mechanisms for the web application, ensuring compliance with organizational security policies and best practices.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

9. You have an Azure App Service web app that utilizes a system-assigned managed identity. You need to recommend a solution to store its settings as secrets in an Azure Key Vault while minimizing changes to the app code and adhering to the principle of least privilege. Which integration method should you recommend for the Key Vault references?

- A) Key Vault references in Application settings
- B) Key Vault references in Appsettings.json
- C) Key Vault references in Web.config
- D) Key Vault references in Appsettings.yml

Feedback(if correct): Option A) Key Vault references in Application settings is the recommended integration method for storing settings as secrets in an Azure Key Vault for an Azure App Service web app. This method allows you to securely access Key Vault secrets without directly exposing sensitive information in the app's code. By configuring Key Vault references in the Application settings, you can easily manage secrets centrally in the Key Vault without requiring modifications to the app's codebase, thus minimizing potential security risks and adhering to the principle of least privilege.

Feedback(if wrong):

Option B) Key Vault references in Appsettings.json: While it is possible to reference Key Vault secrets in the appsettings.json file, this method involves modifying the app's code, which contradicts the requirement to minimize changes to the app code.

Option C) Key Vault references in Web.config: Similar to Option B, referencing Key Vault secrets directly in the Web.config file would require modifications to the app's code, which is not in line with the requirement to minimize changes.

Option D) Key Vault references in Appsettings.yml: This option is invalid as Azure App Service web apps typically use JSON (appsettings.json) for configuration settings, not YAML (appsettings.yml). Therefore, this

method is not applicable for storing settings as secrets in Azure Key Vault for an Azure App Service web app.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskills: Designing Identity and Security Solutions

Competencies: Azure Key Vault Integration, RoleBased Access Control (RBAC)

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

10. You're tasked with configuring an Azure App Service web app to securely access its settings stored as secrets in Azure Key Vault. To achieve this without extensive code changes and following the principle of least privilege, which integration method should be recommended for the Key Vault references? Additionally, what permissions should be assigned to the managed identity for secure access to Key Vault secrets? Choose the correct option(s) from the provided choices.

- A) Key Vault Secrets User
- B) Key Vault Secrets Officer
- C) Key Vault Contributor
- D) Key Vault Admin

Answer: A

Feedback(if correct):

A) Key Vault Secrets User Correct. Assigning the "Key Vault Secrets User" role to the managed identity allows it to retrieve secrets from Azure Key Vault, aligning with the principle of least privilege by providing only the necessary permissions for accessing secrets without granting unnecessary privileges.

Feedback(if wrong):

B) Key Vault Secrets Officer Incorrect. There is no such role as "Key Vault Secrets Officer" in Azure Key Vault. This option is incorrect.

C) Key Vault Contributor Incorrect. While the "Key Vault Contributor" role provides full access to manage Azure Key Vaults, it grants more privileges than necessary and does not adhere to the principle of least privilege.

D) Key Vault Admin Incorrect. The "Key Vault Admin" role does not exist in Azure Key Vault. This option is incorrect.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskills: Designing Identity and Security Solutions

Competencies: Azure Key Vault Integration, RoleBased Access Control (RBAC)

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

11. Your organization, TechSolutions, has implemented several Azure Functions that serve as HTTP triggers, providing access to an internal API. TechSolutions recently partnered with a startup named InnovateX. InnovateX does not have an Azure Active Directory (Azure AD) tenant and relies on a third-party OAuth 2.0 identity provider for user authentication. Developers at InnovateX need access to a subset of the Azure Functions to build applications that integrate with TechSolutions' internal API. You need to design a solution that allows InnovateX developers to access the Azure Functions while meeting the following requirements:

1. Limit requests from InnovateX developers to lower rates than those from TechSolutions users.
2. Enable InnovateX developers to use their existing OAuth 2.0 provider for access.
3. Avoid making changes to the Azure Functions.
4. Avoid using Azure AD guest accounts.

What solution should you recommend?

A) Azure AD (B2B)

B) Azure API Management

- C) Azure Front Door
- D) Azure AD Application Proxy

Answer: B

Feedback(if correct):

This solution aligns with the requirements by allowing InnovateX developers to access Azure Functions using their existing OAuth 2.0 provider while also enabling rate limiting to control request rates.

Feedback(if wrong):

Option A) Azure AD (B2B): This option involves Azure AD's business-to-business (B2B) collaboration, which allows external users to be invited to an organization's resources. However, it does not directly address the requirement for rate limiting or support the use of InnovateX's existing OAuth 2.0 provider.

Option C) Azure Front Door: Azure Front Door is a global, scalable entry point for web applications, but it is not primarily designed for managing access to APIs or enforcing rate limits.

Option D) Azure AD Application Proxy: Azure AD Application Proxy enables remote access to on-premises applications, but it does not support rate limiting or integrate with InnovateX's OAuth 2.0 provider.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskills: Designing Identity and Security Solutions

Competencies: design a solution that enables secure access to Azure resources while integrating with third-party identity providers and enforcing access controls

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

12. You manage several Azure SQL Database instances and are tasked with configuring the Diagnostics settings, as depicted in the following table:

Diagnostics settings:

Metric Category	Log Analytics Workspace
Performance Monitoring	ContosoAnalytics
Query Store Runtime Statistics	ContosoAnalytics
Query Store Wait Statistics	ContosoAnalytics

The retention period for Performance Monitoring data in the Log Analytics Workspace is set to 60 days. Determine the correct options for the following statements:

What is The duration that Performance Monitoring data will be stored in the Log Analytics Workspace?

- A) 30 days
- B) 60 days
- C) 90 days
- D) Indefinite

Answer: B

Feedback(if correct): Option B (60 days) is the correct selection because the Performance Monitoring data is configured to be stored in the Log Analytics Workspace for a retention period of 60 days, as indicated in the diagram.

Feedback(if wrong): Options A, C, and D are incorrect. Option A (30 days) is incorrect because the retention period specified in the diagram is 60 days, not 30 days. Option C (90 days) is incorrect as the specified retention period is 60 days, not 90 days. Option D (Indefinite) is incorrect because the retention period is explicitly set to 60 days, indicating a definite duration, not indefinite.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskills: Designing Identity and Security Solutions

Competencies: Designing Identity and Security Solutions, Designing Compute and Network Infrastructure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

13. You manage several Azure SQL Database instances and are tasked with configuring the Diagnostics settings, as depicted in the following table:

Diagnostics settings:

Metric Category	Log Analytics Workspace
Performance Monitoring	ContosoAnalytics
Query Store Runtime Statistics	ContosoAnalytics
Query Store Wait Statistics	ContosoAnalytics

The retention period for Performance Monitoring data in the Log Analytics Workspace is set to 60 days. Determine the correct options for the following statements:

What is The maximum storage duration for Query Store Runtime Statistics data in the Log Analytics Workspace?

- A) 60 days
- B) 90 days
- C) 180 days
- D) Indefinite

Answer: B

Feedback(if correct): The correct selection is B) 90 days because in the scenario, it is mentioned that the Query Store Runtime Statistics data is configured to be stored in Azure Log Analytics for 90 days.

Feedback(if wrong): If you chose any option other than B) 90 days, it's incorrect. The scenario clearly states that the data is configured to be stored for 90 days, not for any other duration provided in the options.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskills: Designing Identity and Security Solutions

Competencies: Designing Identity and Security Solutions, Designing Compute and Network Infrastructure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

14. You are designing a solution for a multinational corporation that requires a highly available and scalable database system for its global operations. The solution needs to support low-latency read and write operations across different geographical regions, and it should require minimal management effort.

Which Azure service would be the most suitable for this scenario?

- A. Azure SQL Database
- B. Azure SQL Managed Instance
- C. Azure Cosmos DB
- D. Azure Database for PostgreSQL

Answer: C

Feedback(if correct):

Azure Cosmos DB provides a globally distributed, multimodel database service with comprehensive SLAs for low latency reads and writes across multiple regions. It offers automatic and instant scalability, and it requires minimal management effort, making it the ideal choice for the specified requirements. Reference: Microsoft Azure documentation.

Feedback(if wrong):

Option A) Azure SQL Database:

Azure SQL Database is a fully managed relational database service that offers high availability, scalability, and security. However, it does not inherently support simultaneous write operations in multiple Azure regions with low latency. Additionally, while it supports indexing, managing indexes might require some development effort, which contradicts the requirement to minimize development effort.

Option B) Azure SQL Managed Instance:

Azure SQL Managed Instance is also a fully managed relational database service, but it operates more like an on-premises SQL Server instance. Like Azure SQL Database, it does not natively support simultaneous

write operations across multiple regions with low latency. Additionally, while it supports indexing, managing indexes may still require some development effort.

Option D) Azure Database for PostgreSQL:

Azure Database for PostgreSQL is a fully managed relational database service that is compatible with PostgreSQL, offering features like high availability, scalability, and security. However, it does not inherently support the requirement for simultaneous write operations in multiple Azure regions with low latency. Additionally, while it supports indexing, it may not provide the same level of automatic indexing as Azure Cosmos DB, potentially requiring more development effort to manage indexing.

Skill mapping:

Skill: Designing Data Platforms

Subskill: Designing Data Platforms

Competencies: Analyzing, Evaluating

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Synthesis

15. Your organization is migrating an on-premises application to Azure. The application, named App36, relies on data from multiple Microsoft SQL Server databases hosted locally. The databases and their respective sizes are outlined below:

DB1: 450 GB

DB2: 300 GB

DB3: 380 GB

DB4: 70 GB

App36 is utilized only on specific days of the month and is not expected to undergo significant data growth. As part of the migration, the company plans to transfer the databases to Azure SQL Database. Your task is to select the appropriate service tier to minimize costs. Which service tier should you recommend?

- A) DTUbased Business Critical
- B) DTUbased General Purpose
- C) DTUbased Standard
- D) DTUbased Basic

Answer: C

Feedback(if correct):

(if correct) The correct selection is "C) DTUbased Standard." This option is the most suitable because the scenario mentions that the data is not expected to grow significantly and the databases are used only on specific days of the month. DTUbased Standard tier provides a cost-effective solution for databases up to 1 TB in size, meeting the requirements while minimizing costs.

Feedback(if wrong):

Option A, DTUbased Business Critical, typically offers higher performance and is more suitable for critical workloads requiring high availability and performance. It is not necessary for this scenario, where the primary concern is cost optimization.

Option B, DTUbased General Purpose, also provides balanced performance for typical workloads but might be more than what is needed for an application used only on specific days of the month.

Option D, DTUbased Basic, offers the lowest cost but may not be suitable for larger databases or applications that require more resources.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ305)

Subskill: Designing Data Platforms

Competency: Selecting appropriate Azure SQL Database service tiers based on workload requirements and cost considerations.

Difficulty Level: Advanced

Bloom's Taxonomy Level: Application

16. Your organization is migrating an on-premises application, named AppY, to Azure. The application relies on data from multiple Microsoft SQL Server databases hosted locally. These databases and their sizes are as follows:

DB1: 500 GB

DB2: 350 GB

DB3: 420 GB

DB4: 80 GB

AppY is a critical application with demanding workloads and there are aims for significant data growth and require high availability and performance. As part of the migration plan, the company aims to transfer the databases to Azure SQL Database. Your task is to recommend the appropriate service tier to minimize costs. Which service tier should you suggest?

- A) DTU based Business Critical
- B) DTU based General Purpose
- C) DTU based Standard
- D) DTU based Basic

Answer: A

Feedback(if correct): The correct selection is A) DTU based Business Critical. This service tier is designed for critical applications with demanding workloads, requiring high availability and performance. It provides advanced features such as automatic backups, high availability, and performance enhancements, making it suitable for applications like AppY.

Feedback(if wrong):

- B) DTUbased General Purpose: While this service tier offers a balance between cost and performance for a wide range of database workloads, it may not provide the high availability and performance required for critical applications like AppY.
- C) DTUbased Standard: Although this service tier offers a cost-effective option for light to medium database workloads, it may not meet the high availability and performance demands of critical applications like AppY.

D) DTU-based Basic: This service tier is designed for light database workloads with minimal performance requirements. It may not provide the necessary features and performance levels required for critical applications like AppY.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ305)

Subskill: Designing Data Platforms

Competency: Selecting appropriate Azure SQL Database service tiers based on workload requirements and cost considerations.

Difficulty Level: Advanced

Bloom's Taxonomy Level: Application

17. You are managing an Azure storage account that contains sensitive documents. For the month of April, you need to grant temporary access to specific users in your organization's finance department to these documents. Which security solution should you recommend for providing temporary access?

- A) Azure Active Directory roles
- B) Azure AD conditional access policies
- C) Shared access signatures (SAS)
- D) Azure Role Based Access Control (RBAC)

Answer: C

Feedback:

C) Shared access signatures (SAS) Correct

Shared access signatures (SAS) are the appropriate solution for providing temporary access to specific users. They allow for limited time, and accurate access control to Azure Storage resources, making them suitable for granting temporary access to sensitive documents for the month of April. With SAS, you can specify the duration of access and revoke access once it's no longer needed.

A) Azure Active Directory roles Incorrect

Azure Active Directory (Azure AD) roles are used for managing access to Azure resources based on a user's role or group membership. While they are useful for managing longterm access permissions, they are not designed for providing temporary access for a specific time period.

B) Azure AD conditional access policies Incorrect

Azure AD conditional access policies are used to enforce organizational security policies based on conditions such as user location, device compliance, or application sensitivity. While they can help control access to resources, they are not intended to provide temporary access to specific documents for a limited time period.

D) Azure Role based access control (RBAC) Incorrect

Azure Role based access control (RBAC) is used to manage access to Azure resources by assigning roles to users, groups, or applications at a certain scope. While RBAC provides granular access control, it is not suitable for providing temporary access for a specific time period, as required in this scenario.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ305)

Subskill: Designing Data Platforms

Competency: Access Control and Security

Difficulty Level: Intermediate

18. You are in charge of managing access to a blob container in your Azure subscription. Ten users in the finance department need to access the blobs during the month of April only. What security solution should you recommend to enable this limited-time access?

A) Shared access signatures (SAS)

B) Access keys

C) Conditional access policies

D) Certificates

Answer: A

Feedback(if correct):

A) Shared access signatures (SAS)

Shared access signatures (SAS) are the appropriate solution for providing limited-time access to resources in Azure Storage, such as blob containers. With SAS, you can generate a token with specific permissions and an expiration time, allowing the finance department users to access the blobs during April only.

Shared access signatures (SAS) provide granular control over the permissions and duration of access, making them suitable for scenarios where temporary access needs to be granted to specific users or applications for a limited time period.

Feedback(if wrong):

B) Access keys

Access keys are longterm credentials used for authenticating requests to Azure Storage accounts. They are not suitable for providing temporary access to specific users for a limited period of time.

C) Conditional access policies

Conditional access policies are used to enforce organizational security policies based on specific conditions such as user location, device state, or application sensitivity. They are not intended to provide temporary access to specific resources like blob containers for a limited duration.

D) Certificates

Certificates are used for authenticating and securing communications between different entities. However, they are not typically used for providing temporary access to specific resources like blob containers in Azure Storage.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ305)

Subskill: Designing Data Platforms

Competency: Access Control and Security

Difficulty Level: Intermediate

19. You have 50 servers running Windows Server 2016 hosting Microsoft SQL Server 2016 instances. These instances manage databases with the following characteristics:

- The largest database size is 2 TB, and none exceed 3 TB.
- CLR stored procedures are used extensively.

You're planning to migrate all the data from SQL Server to Azure. Your aim is to select an Azure service to host the databases while minimizing management overhead and the number of necessary database changes for migration. Additionally, you want to ensure that users can authenticate using their Active Directory credentials.

Which Azure SQL Database service should you recommend, considering workload requirements and cost considerations?

- A) Azure SQL Database single databases
- B) Azure SQL Database Managed Instance
- C) Azure SQL Database elastic pools
- D) SQL Server 2019 on Azure virtual machines

Answer: B

Feedback(if correct): Option B) Azure SQL Database Managed Instance is the correct choice for hosting the databases in Azure. It allows for minimal management overhead and requires fewer database changes during migration. Additionally, it offers PaaS capabilities such as automatic patching, version updates, and automated backups, which reduce management complexity and total cost of ownership (TCO).

Feedback(if wrong): Option A) Azure SQL Database single databases would not be the best choice in this scenario because it does not provide the same level of compatibility with existing SQL Server instances and CLR stored procedures. While it offers PaaS benefits, it may require more database changes for migration compared to Managed Instance. Options C and D are also incorrect because they do not align with the requirement for minimizing management overhead and database changes during migration.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ305)

Subskill: Designing Data Platforms

Competency: Selecting appropriate Azure SQL Database service tiers based on workload requirements and cost considerations.

Difficulty Level: Advanced

Bloom's Taxonomy Level: Application

20. You are tasked with designing a Data Engineering solution for your company, which currently holds an Azure subscription. The company's application data resides in an on-premises SQL Server database. The goal is to transfer transactional data from the on-premises SQL Server to a data warehouse in Azure, with data transferred nightly as a scheduled job. Additionally, a managed Spark cluster is required for data engineers to analyze the data in the SQL data warehouse using notebooks in Scala, R, and Python. Furthermore, a data lake store is needed for ingesting data from various sources. Which Azure service should be used to host the data warehouse?

- A) Azure AD
- B) Azure Synapse Analytics
- C) Azure Data Lake Gen2
- D) Azure Databricks

Answer: B

Feedback(if correct): Option B, Azure Synapse Analytics, is the correct choice. Azure Synapse Analytics is a powerful analytics service that brings together enterprise data warehousing and big data analytics. It allows for the seamless integration of on-premises and cloud data sources, enabling efficient data transfer from the on-premises SQL Server to the data warehouse in Azure. Additionally, it provides capabilities for data engineers to perform advanced analytics using tools like notebooks in Scala, R, and Python.

Feedback(if wrong):

Option A, Azure AD (Azure Active Directory), is incorrect. Azure AD is an identity and access management service, not a data warehousing solution.

Option C, Azure Data Lake Gen2, is incorrect. While Azure Data Lake Storage Gen2 is a highly scalable and cost-effective data lake solution, it is not designed specifically for data warehousing purposes.

Option D, Azure Databricks, is incorrect. Azure Databricks is a cloud-based big data analytics platform that provides Apache Spark-based analytics and collaborative capabilities. While it supports data engineering tasks, it is not a dedicated data warehouse solution.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ305)

Subskill: Designing Data Platforms



Competency: Choosing the right Azure service to host a data warehouse based on specific business needs and requirements.

Difficulty Level: Intermediate

21. You are designing a data platform on Azure for a financial institution that requires strict access control and robust security measures. The data platform will consist of an Azure Synapse Analytics workspace, Azure Databricks clusters, and Azure Data Lake Storage Gen2. To meet the security requirements, you need to recommend an appropriate access control mechanism that complies with regulatory standards. What should you recommend?

- A) Shared Access Signatures (SAS)
- B) Azure Active Directory (Azure AD) integration
- C) Azure Key Vault
- D) Azure Private Link

Answer: B

Feedback (if correct):

Azure Active Directory (Azure AD) integration is the recommended approach for access control and security in a data platform. It provides centralized identity and access management, ensuring secure access to your Azure Synapse Analytics workspace, Azure Databricks clusters, and Azure Data Lake Storage Gen2.

Feedback (if wrong):

Azure Active Directory (Azure AD) integration is the preferred method for access control and security in Azure data platforms. By integrating Azure AD, you can centrally manage access to your Azure Synapse Analytics workspace, Azure Databricks clusters, and Azure Data Lake Storage Gen2, ensuring a secure environment that adheres to regulatory standards.

Skill Map:

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ305)

Subskill: Designing Data Platforms



Competency: Access Control and Security

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

22. You manage an Azure Active Directory (Azure AD) tenant that syncs with an on-premises Active Directory domain. Your organization has developed a proprietary line-of-business (LOB) application.

You are tasked with implementing SAML single sign-on (SSO) for the LOB application and enforcing multi-factor authentication (MFA) when users attempt to access the application from an unknown location.

Which two features should you include in the solution? Select the appropriate options from the answer choices. (Note: Each correct selection is worth one point.)

- A. Azure AD enterprise applications
- B. Azure AD Identity Protection
- C. Azure Application Gateway
- D. Conditional Access policies

Answer: A, D

Feedback (if correct):

By selecting Azure AD enterprise applications (feature A) and Conditional Access policies (feature D), you've addressed the requirements for SAML single sign-on (SSO) and enforced multi-factor authentication (MFA) based on known vs. unknown locations.

Azure AD enterprise applications act as the SSO connector for your proprietary line-of-business (LOB) application, while Conditional Access policies let you define rules governing user authentication methods, such as multi-factor authentication, based on location and other properties.

Feedback (if wrong):

Incorrect selections imply that the solution does not address the requirements for SAML SSO and MFA enforcement. Here's why the other options wouldn't work:

- Azure AD Identity Protection (feature B) helps protect your organization from compromised identities, but it won't assist with implementing SAML SSO or MFA enforcement.

- Azure Application Gateway (feature C) acts as a reverse proxy, but it doesn't participate in SSO or MFA enforcement.

Make sure to thoroughly analyze the requirements and explore all possible features to find the best-suited solutions.

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ305)

Subskill: Designing Data Platforms

Competency: Access Control and Security

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

23. You are planning to create an Azure Storage account to host file shares. These file shares will be accessed from on-premises applications that are transaction-intensive. Your goal is to minimize latency when accessing the file shares while ensuring the highest level of resiliency for the selected storage tier. Which storage tier and resiliency options should you recommend? Select all that apply.

- A) Hot
- B) Premium
- C) Transaction optimized
- D) Zone-redundant storage (ZRS)

Answer: B, D

Feedback (if correct):

The Premium storage tier coupled with Zone-redundant storage (ZRS) offers the lowest latency for transaction-intensive on-premises applications while providing exceptional resiliency. The Premium storage tier caters to demanding IO-bound workloads, and ZRS ensures high durability by replicating data across multiple physical isolation zones within the same region.

Feedback (if wrong):

If the Hot storage tier had been chosen, the feedback would have explained that, although the Hot tier offers faster access than Cool or Archive tiers, it does not minimize latency for transaction-intensive on-premises applications as much as the Premium tier does.

If Transaction optimized had been chosen, the feedback would have pointed out that there is no such storage tier as Transaction optimized in Azure Storage. One should consider the Premium storage tier instead for transaction-intensive workloads.

Had Zone-redundant storage (ZRS) not been selected, the feedback would have highlighted that ZRS is the ideal choice for resiliency in conjunction with the Premium storage tier, as it maintains six replicas of your data across three availability zones for maximum durability.

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ305)

Subskill: Designing Data Platforms

Competency: Access Control and Security

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

24. You manage a database environment for a Microsoft Volume Licensing customer named Contoso, Ltd. Contoso uses License Mobility through Software Assurance.

You need to deploy 50 databases. The solution must meet the following requirements:

Support automatic scaling.

Minimize Microsoft SQL Server licensing costs.

Which purchase model and deployment option should you include in the solution? Select all that apply.

- A) DTU
- B) vCore
- C) Azure reserved virtual machine instances

- D) An Azure SQL Database elastic pool

Answer: B, D

Feedback(if correct):-

Option B (vCore) is correct because the vCore purchase model allows for automatic scaling and helps minimize Microsoft SQL Server licensing costs. With this model, you can choose the exact amount of computing resources needed for your workload, allowing for flexibility and cost optimization.

Option D (An Azure SQL Database elastic pool) is correct because deploying databases within an elastic pool provides support for automatic scaling and allows for cost-effective management of multiple databases within a shared set of resources. This option aligns with the requirement to support automatic scaling and helps minimize costs by sharing resources among multiple databases.

Feedback(if wrong):-

Option A (DTU) is incorrect. While DTU-based purchasing may support automatic scaling, it may not provide the flexibility and cost optimization benefits of the vCore model. DTU-based purchasing relies on a pre-defined set of resources, which may not be as efficient for scaling and cost management.

Option C (Azure reserved virtual machine instances) is incorrect. While reserved virtual machine instances may help reduce costs for Azure VMs, they are not directly related to minimizing Microsoft SQL Server licensing costs or supporting automatic scaling for SQL databases.

Skill mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ-305)

Subskill: Designing Data Platforms

Competency: Cost Optimization and Scalability

Difficulty Level: Intermediate

25. You manage a database environment for a Microsoft Volume Licensing customer named Contoso, Ltd. Contoso utilizes License Mobility through Software Assurance. You need to deploy 120 small databases with maximum SQL Server licensing costs. Choose the most appropriate definition for the following Azure SQL Database deployment options:

- A) Single database: Represents a fully managed, isolated database.
- B) Elastic pool: A collection of single databases with a shared set of resources, such as CPU or memory.
- C) SQL Server Always On availability group: A high availability and disaster recovery solution for databases.
- D) An Azure SQL managed instance: A fully managed, standalone SQL Server instance hosted in Azure.

Feedback(if correct):-

Elastic pools are an optimal choice for deploying multiple databases with varying usage patterns and workloads while minimizing SQL Server licensing costs. With an elastic pool, databases share a pool of resources, which helps in maximizing resource utilization and reducing overall costs. This option aligns with the requirement of deploying 120 databases with maximum licensing costs.

Feedback(if wrong):-

- A) Single database: Represents a fully managed, isolated database.

While single databases are fully managed and isolated, they are not the most cost-effective option for deploying a large number of databases as in this scenario. Each database in this model requires separate resources, which can lead to higher licensing costs compared to other deployment options.
- C) SQL Server Always On availability group: A high availability and disaster recovery solution for databases.

SQL Server Always On availability groups are primarily used for high availability and disaster recovery purposes, providing features like automatic failover and data replication. While important for ensuring database resilience, this option is not focused on minimizing licensing costs for deploying a large number of databases.

D) An Azure SQL managed instance: A fully managed, standalone SQL Server instance hosted in Azure.

Azure SQL-managed instances are suitable for scenarios where you need a dedicated instance of SQL Server with full compatibility and feature parity. However, they may not be the most cost-effective option for deploying a large number of databases, as each managed instance incurs its own set of costs and may not be as scalable as an elastic pool.

Skill mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ-305)

Subskill: Designing Data Platforms

Competency: Database Deployment and Management

Difficulty Level: Intermediate

26. You are tasked with deploying resources to host a stateless web app in an Azure subscription. The solution must provide access to the full .NET framework, offer redundancy in case of an Azure region failure, and allow administrators access to the operating system for installing custom application dependencies. You plan to deploy the stateless web app using Azure App Service in combination with Azure Traffic Manager. Does this solution meet the goal?

- A. Yes
- B. NO

Answer: A

Feedback(if correct): Yes, the solution meets the goal. Azure App Service provides access to the full .NET framework, and when combined with Azure Traffic Manager, it offers redundancy across Azure regions. Additionally, administrators can access the underlying operating system to install custom application dependencies.

Feedback(if wrong): The solution provided meets the specified requirements. Azure App Service, combined with Azure Traffic Manager, fulfills the need for the full .NET framework, redundancy across regions, and access for administrators to the operating system.

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskills: Designing Compute and Network Infrastructure

Competencies: Analyzing requirements and recommending appropriate Azure services

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

27. Your organization plans to deploy a highly available web application in Azure. The application requires access to the full .NET framework, redundancy across Azure regions, and the ability for administrators to install custom application dependencies. Which Azure service(s) should you recommend to meet these requirements?

- A) Azure Virtual Machine Scale Sets with autoscaling
- B) Azure App Service with Azure Traffic Manager
- C) Azure VM with Azure Load Balancer
- D) Azure Functions with Azure Front Door

Answer: B

Feedback(if correct): Option B is the correct answer. Azure App Service provides access to the full .NET framework, offers redundancy across Azure regions through Azure Traffic Manager, and allows administrators to install custom application dependencies.

Feedback(if wrong): Option A is incorrect because Azure Virtual Machine Scale Sets with autoscaling do not inherently provide redundancy across Azure regions. Option C is incorrect because Azure VMs with Azure Load Balancer do not offer Platform-as-a-Service (PaaS) features

like access to the full .NET framework. Option D is incorrect because Azure Functions is a serverless compute service and may not be suitable for hosting a highly available web application with access to the full .NET framework and custom dependencies.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskills: Designing Compute and Network Infrastructure

Competencies: Plan and implement solutions that meet high availability and redundancy requirements

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

28. You are tasked with designing an alerting strategy for security-related events in Azure Log Analytics. The subscription contains Azure virtual machines running Windows Server 2016 and Linux. Which Log Analytics tables should you query for each log type?

- A) AzureActivity for Events from Windows event logs and Syslog for Events from Linux system logging
- B) AzureDiagnostics for Events from Windows event logs and Syslog for Events from Linux system logging
- C) Event for Events from Windows event logs and Syslog for Events from Linux system logging
- D) AzureActivity for Events from Linux system logging and Event for Events from Windows event logs

Answer: A

Feedback(if correct): Option A is correct. AzureActivity is used for Windows event logs, while Syslog is used for Linux system logging.

Feedback(if wrong): Option B is incorrect because AzureDiagnostics typically contains diagnostic data from Azure resources, not security-related events. Option C is incorrect because the Event table is not typically used for Windows event logs; AzureActivity is more appropriate for this purpose. Option D is incorrect because AzureActivity is not used for Linux system logging; Syslog is the appropriate table for this type of logging.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Compute and Network Infrastructure

Competency: Selecting appropriate Azure services and features to meet specific requirements

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

29. You have an Azure subscription with Windows Server 2016 and Linux virtual machines. Your task is to create an alerting strategy for security-related events using Azure Log Analytics. Which Log Analytics tables should you query?

- A. Employ Azure Diagnostics for Windows event logs and Azure Activity for Linux system logging.
- B. Use Syslog for Windows event logs and the Event table for Linux system logging.
- C. Utilize the Azure Activity table for Windows event logs and Azure Diagnostics for Linux system logging.
- D. Use the Event table for Windows event logs and Syslog for Linux system logging.

Answer: D

Feedback(if correct): The answer is correct because the Event table in Azure Log Analytics is used for collecting Windows event logs, while Syslog is used for collecting logs from Linux systems. This ensures that security-related events from both Windows and Linux systems can be monitored and alerted effectively.

Feedback(if wrong):

Option A suggests using Azure Diagnostics for Windows event logs and Azure Activity for Linux system logging. This is incorrect because Azure Diagnostics is primarily used for monitoring Azure resources and collecting diagnostic data, not for capturing Windows event logs. Additionally, Azure Activity logs provide information about operations performed on Azure resources, which is unrelated to collecting logs from Linux systems.

Option B proposes using Syslog for Windows event logs and the Event table for Linux system logging. This is incorrect because the Syslog protocol is typically used for collecting logs from Linux systems, not for Windows event logs. Conversely, the Event table in Azure Log Analytics is designed to capture Windows event logs, not logs from Linux systems.

Option C suggests utilizing the Azure Activity table for Windows event logs and Azure Diagnostics for Linux system logging. This is incorrect because Azure Activity logs contain data related to operations performed on Azure resources, not Windows event logs. Similarly, Azure Diagnostics is primarily used for monitoring Azure resources and collecting diagnostic data, rather than capturing logs from Linux systems.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Compute and Network Infrastructure

Competency: Selecting appropriate Azure services and features to meet specific requirements

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

30. Your organization maintains an Azure subscription containing an Azure SQL database. You intend to utilize Azure reservations for the Azure SQL database. Which resource type will benefit from the reservation discount?

- A) Licensing
- B) Web App
- C) MS SQL
- D) Compute vCores

Answer: D

Feedback(if correct): The correct selection is D) Compute vCores. Azure reservations can be applied to compute resources such as vCores in the Azure SQL Database, allowing for cost savings through reserved capacity.

Feedback(if wrong): Azure reservations do not apply to licensing, web apps, or MS SQL. They are specifically used for reserving compute resources like vCores in Azure SQL Database.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Compute and Network Infrastructure

Competency: Understanding Azure pricing and cost management, Designing cost effective , Solutions using Azure reservations, Understanding Azure resource types and their billing models, Designing Azure infrastructure for optimized cost management

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

31. You are designing a cost-effective solution for your company's Azure environment. Which of the following statements about Azure reservations is true?

- A) Azure reservations are billed at the full price regardless of usage.
- B) Azure reservations provide flexibility in changing the resources they apply to.
- C) Azure reservations are only available for a fixed term of 1 year.
- D) Azure reservations apply only to specific Azure regions.

Answer: B

Feedback(if correct): Option B) Azure reservations do provide flexibility in changing the resources they apply to. This statement is true.

Feedback(if wrong): Option A) Azure reservations are not billed at the full price regardless of usage. They provide cost savings based on the reserved capacity. Option C) Azure reservations are available for both 1-year and 3-year terms, so it's not accurate to say they are only available for a fixed term of 1 year. Option D) Azure reservations can be applied to resources in any Azure region, not just specific ones.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Compute and Network Infrastructure

Competency: Understanding Azure pricing and cost management, Designing cost effective, Solutions using Azure reservations, Understanding Azure resource types and their billing models, Designing Azure infrastructure for optimized cost management

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

32. When purchasing an Azure reservation for SQL Databases, what is the significance of "quantity" in the context of vCore purchases?

- A. It determines the maximum number of databases that can be hosted.
- B. It specifies the maximum amount of storage available for the databases.
- C. It indicates the number of vCores being reserved and will receive the billing discount.
- D. It signifies the number of concurrent connections allowed to the databases.

Answer: C

Feedback(if correct): Option C) indicates the number of vCores being reserved and will receive the billing discount. This is the correct significance of "quantity" when purchasing an Azure reservation for SQL Databases.

Feedback(if wrong): Option A) Quantity does not determine the maximum number of databases that can be hosted. Option B) It does not specify the maximum amount of storage available for the databases. Option D) Quantity does not signify the number of concurrent connections allowed to the databases.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Compute and Network Infrastructure

Competency: Understanding Azure pricing and cost management, Designing cost effective , Solutions using Azure reservations, Understanding Azure resource types and their billing models, Designing Azure infrastructure for optimized cost management

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

33. Your company develops a web service deployed to an Azure virtual machine named VM1, allowing access to realtime data via an API. The virtual machine deployment is displayed as follows:

VM1:

Virtual Network: VNet1

Subnet: ProdSubnet



The chief technology officer (CTO) states that developers have ensured the API is accessible from VM1 and VM2. Partners must access the API over the Internet for their applications. You deploy an Azure API Management (APIM) service with the following configuration:

Location: West Europe

Virtual Network: VNet1

Subnet: ProdSubnet

For each statement below, select Yes if true. Otherwise, select No.

1. The API is available to partners over the Internet.
2. The APIM instance can access realtime data from VM1.
3. A VPN gateway is required for partner access.

Options:

- A) Yes, No, Yes
- B) Yes, Yes, No
- C) No, Yes, Yes
- D) No, No, No

Answer: B

Feedback(if correct):

1. The API is available to partners over the Internet because the APIM service is deployed in West Europe, which allows external access.
2. The APIM instance can access realtime data from VM1 as it is deployed within the same virtual network and subnet, enabling connectivity.
3. A VPN gateway is not required for partner access because the API is accessible over the Internet, eliminating the need for a VPN connection.

Feedback(if wrong):

- A) Licensing: Azure reservations are not applied to licensing but rather to compute resources such as virtual machines, databases, and other services that offer reserved capacity pricing models.
- C) MS SQL: Azure reservations do not directly apply to Microsoft SQL Server itself. Instead, reservations are applied to specific resources such as Azure SQL Database or SQL Server virtual machines.
- D) Web App: Azure reservations do not apply to Azure App Service resources like Web Apps. Reservations are primarily designed for computing resources such as virtual machines and databases.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ305)

Subskill: Designing Compute and Network Infrastructure

Competencies: Understanding network configurations, designing access control policies, deploying Azure services for connectivity

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

34. You manage an Azure subscription containing a Basic Azure virtual WAN named VirtualWAN1 and the virtual hubs listed below:

Name: Hub1, Azure region: US East Name: Hub2, Azure region: US West

An ExpressRoute circuit is available in the US East region. You are tasked with creating an ExpressRoute association to VirtualWAN1. What should be the initial step?

- A) Upgrade VirtualWAN1 to Standard.
- B) Create a gateway on Hub1.
- C) Establish a hub virtual network in the US East region.
- D) Enable the ExpressRoute premium addon.

Answer: A

Feedback(if correct): Upgrading VirtualWAN1 to the Standard tier is the correct initial step because ExpressRoute associations require the Standard tier for connectivity. By upgrading, VirtualWAN1 will have the necessary capabilities to establish the ExpressRoute association.

Feedback(if wrong): If you selected any option other than A, it is incorrect because VirtualWAN1 needs to be upgraded to the Standard tier to enable the establishment of an ExpressRoute association. Creating a gateway on Hub1 (Option B) or establishing a hub virtual network in the US East region (Option C) are not the correct initial steps for setting up an ExpressRoute association. Additionally, enabling the ExpressRoute premium addon (Option D) is not necessary for this scenario.

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskills: Designing Compute and Network Infrastructure

Competencies: Designing Compute and Network Infrastructure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

35. You are developing a sales application that will utilize several Azure cloud services to handle various components of a transaction. These services will process customer orders, billing, payment inventory, and shipping. To enable asynchronous communication of transaction information using XML messages, what solution should you recommend? Select all that apply.

- A) Azure CosmosDB
- B) Azure Blob Storage
- C) Azure Queue Storage
- D) Azure Service Fabric

Answer: C, D

Feedback(if correct):

Azure Queue Storage is suitable for asynchronous communication and can store messages in XML format, making it an appropriate choice for handling transaction information.

Azure Service Fabric supports the development of scalable, reliable microservices and can facilitate asynchronous communication between different components of the application, including handling XML messages.

Feedback(if wrong):

Azure CosmosDB is a NoSQL database service and may not be the best choice for storing and processing XML messages for asynchronous communication.

Azure Blob Storage is a general-purpose object storage solution and may not be the most suitable option for handling transaction information in XML format asynchronously.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskills: Designing Compute and Network Infrastructure

Competencies: Decision Making, Solution Design

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

36. Your organization maintains 100 virtual machines in a VMware environment on-premises. These virtual machines have varying sizes and utilization levels. You intend to migrate all these virtual machines to Azure. To recommend the required number and size of Azure virtual machines for the migration while minimizing administrative effort, what tool should you use?

- A) Azure Cost Explorer
- B) Azure Cognito
- C) Azure B2B

D) Azure Migrate

Answer: D

Feedback(if correct):

The correct selection is option D) Azure Migrate. Azure Migrate is the appropriate tool for assessing server readiness for migration to Azure, right-sizing servers, planning costs, and analyzing application dependencies. It streamlines the migration process efficiently by providing valuable metadata.

Feedback(if wrong):

Option C) Azure B2B is incorrect. Azure B2B (Business to Business) is a feature that enables secure access to your organization's applications and services for guest users from other organizations. It is not related to assessing server readiness for migration or right-sizing servers. Therefore, it is not the appropriate solution to recommend the required Azure virtual machines for migration while minimizing administrative effort.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ305)

Subskill: Designing Compute and Network Infrastructure

Competencies: Understanding network configurations, designing access control policies, deploying Azure services for connectivity

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

37. You have an Azure subscription with two SQL servers and two storage accounts distributed across different regions as follows:

SQL Servers:

Name	Resource Group	Location
MSSQL1	AZRG1	East US
MSSQL2	AZRG2	West US

Storage Accounts:

Name	Resource Group	Location	Account Kind
st1	AZRG1	East US	StorageV2 (general purposev2)
st2	AZRG2	Central US	BlobStorage

You've deployed three Azure SQL databases with varying pricing tiers:

Name	Resource Group	Server	Pricing Tier
MSSQLdb1	AZRG1	MSSQLsvr1	Standard
MSSQLdb2	AZRG1	MSSQLsvr1	Standard
SQLdb3	RG2	SQLsvr2	Premium

For each statement, indicate whether it's true or false:

1. When enabling auditing for MSSQLdb1, you can store the audit information to st1.
2. When enabling auditing for MSSQLdb2, you can store the audit information to st2.
3. When enabling auditing for SQLdb3, you can store the audit information to st2.
4. When enabling auditing for SQLdb1, you can store the audit information to st1.

Options:

- A. Yes, No, No, No
- B. Yes, Yes, Yes, Yes
- C. Yes, No, Yes, Yes
- D. Yes, No, No, Yes

Answer: C

Feedback(if correct): explain the correct selection

Yes, no, yes, yes

Explanation:

Statement 1: Yes. MSSQLdb1 can store audit information to st1 as they are both located in the East US region.

Statement 2: No. MSSQLdb2's audit information cannot be stored in st2 because they are in different regions (East US for MSSQLdb2 and Central US for st2).



Statement 3: Yes. SQLdb3 and st2 are both located in the Central US region, allowing for audit information storage in st2.

Statement 4: Yes. SQLdb1 and st1 are in the same East US region, enabling audit information storage in st1.

Feedback(if wrong):

Option 1: Yes, yes, yes, yes

Statement 1: Incorrect. Enabling auditing for SQLdb1 allows storing audit information to st1, not st2.

Statement 2: Incorrect. MSSQLdb2's audit information cannot be stored in st2 because they are in different regions (East US for MSSQLdb2 and Central US for st2).

Statement 3: Incorrect. SQLdb3 and st2 are both located in the Central US region, allowing for audit information storage in st2.

Statement 4: Incorrect. SQLdb1 and st1 are in the same East US region, enabling audit information storage in st1.

Option 2: Yes, no, no, no

Statement 1: Correct.

Statement 2: Incorrect. MSSQLdb2's audit information cannot be stored in st2 because they are in different regions (East US for MSSQLdb2 and Central US for st2).

Statement 3: Incorrect. SQLdb3 and st2 are both located in the Central US region, allowing for audit information storage in st2.

Statement 4: Incorrect. SQLdb1 and st1 are in the same East US region, enabling audit information storage in st1.

Option 3: No, yes, yes, yes

Statement 1: Incorrect. Enabling auditing for SQLdb1 allows storing audit information to st1, not st2.

Statement 2: Correct.

Statement 3: Incorrect. SQLdb3 and st2 are both located in the Central US region, allowing for audit information storage in st2.

Statement 4: Incorrect. SQLdb1 and st1 are in the same East US region, enabling audit information storage in st1.

Option 4: Yes, no, Yes, no

Statement 1: Correct.

Statement 2: Incorrect. MSSQLdb2's audit information cannot be stored in st2 because they are in different regions (East US for MSSQLdb2 and Central US for st2).

Statement 3: Correct.

Statement 4: Incorrect. Enabling auditing for SQLdb1 allows storing audit information to st1, not st2.

skill map:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Compute and Network Infrastructure

Competency: Analytical Thinking and Problem Solving

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

38. You are tasked with architecting an Azure infrastructure for a company's new web application. The application will utilize the Azure SQL Database as its backend data store. However, since its deployment, users have reported latency issues when accessing data from the database. Upon investigation, it was discovered that the latency is due to network overhead when accessing the database from Azure virtual machines (VMs) within the same virtual network (VNet). You need to recommend a solution to minimize latency and improve performance when accessing the Azure SQL Database from the Azure VMs.

- A) Implement Azure SQL Database Managed Instance
- B) Migrate the Azure SQL Database to a higher pricing tier
- C) Utilize Azure Cosmos DB for data storage
- D) Establish a Virtual Network (VNET) service endpoint

Answer: D

Feedback(if correct): Option D) Establishing a Virtual Network (VNET) service endpoint is the correct choice in this scenario. By creating a VNET service endpoint, you can ensure that traffic between the Azure virtual machines and the Azure SQL database stays within the Azure network, minimizing latency

and enhancing performance. Additionally, this solution aligns with the requirement to minimize costs as it utilizes existing Azure networking capabilities without additional infrastructure overhead.

Feedback(if wrong):

A) Implement Azure SQL Database Managed Instance:

This option involves migrating the Azure SQL Database to a managed instance, which could potentially increase the overall performance and management capabilities of the database. However, it does not directly address the latency issues caused by network overhead when accessing the database from Azure VMs within the same VNet. Therefore, this option is incorrect.

B) Migrate the Azure SQL Database to a higher pricing tier:

While migrating the database to a higher pricing tier might offer additional performance capabilities, it does not directly address the latency issues caused by network overhead. Increasing the pricing tier may provide more resources for processing queries but won't necessarily optimize network communication between the Azure VMs and the SQL Database. Therefore, this option is incorrect.

C) Utilize Azure Cosmos DB for data storage:

Azure Cosmos DB is a globally distributed, multi-model database service designed for high availability, low latency, and scalability. However, migrating the database to Azure Cosmos DB would involve significant architectural changes and might not be the most suitable solution for addressing the specific latency issues related to network overhead within Azure VNet. Therefore, this option is also incorrect.

skill map:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Compute and Network Infrastructure

Competency: Analytical Thinking and Problem Solving

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

39. You are responsible for implementing an Azure Kubernetes Service (AKS) solution that will utilize Windows Server 2019 nodes. The solution must adhere to specific requirements, including minimizing the provisioning time for computing resources during scale-out operations and supporting the autoscaling of Windows Server containers.



Which scaling option should you recommend to meet the specified requirements for the AKS solution described in the scenario?

- A) Horizontal Pod Autoscaler
- B) Cluster Autoscaler
- C) Kubernetes kubectl
- D) Virtual Machines

Answer: B

Feedback(if correct):-

To meet the requirements of minimizing provisioning time for compute resources during scale-out operations and supporting the autoscaling of Windows Server containers in the AKS solution, the recommended scaling option is the Cluster Autoscaler. This option dynamically adjusts the number of nodes in a container service, effectively addressing the specified requirements. The other options listed do not align with the specific needs outlined in the scenario.

Feedback(if wrong):-

- A) Horizontal Pod Autoscaler would be incorrect as this option is focused on adjusting the number of pods in response to CPU usage. While it is a valid feature of Kubernetes, it does not directly address the specific requirements outlined in the scenario for Windows Server containers and provisioning time during scale-out operations.
- C) Kubernetes kubectl is incorrect because it is a command-line interface for running commands against Kubernetes clusters. It does not directly relate to the requirements for autoscaling Windows Server containers and minimizing provisioning time during scale-out operations.
- D) Virtual Machines are incorrect as it does not align with the specific requirements for autoscaling Windows Server containers within an Azure Kubernetes Service (AKS) solution.

Therefore, understanding the specific needs of the scenario is crucial in selecting the correct scaling option for the AKS solution.

Skill Map:



Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Sub Skills: Designing Compute and Network Infrastructure

Competency: Selecting appropriate scaling options for Azure Kubernetes Service (AKS) solutions based on workload requirements and cost considerations.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

40. You are designing an Azure infrastructure solution that requires high availability and scalability.

The solution needs to handle sudden spikes in traffic and ensure continuous availability. Which Azure service should you recommend?

- A) Azure Virtual Machines
- B) Azure Functions
- C) Azure App Service
- D) Azure Kubernetes Service (AKS)

Answer: C

Feedback (if correct):

You have selected Azure App Service, which is an excellent choice for high availability and scalability. Azure App Service allows easy scaling, either manually or automatically, depending on the traffic needs. Its built-in load balancer distributes traffic efficiently, ensuring continued availability even during sudden spikes. Additionally, Azure App Service boasts a 99.95% monthly SLA, contributing to its reputation as a reliable PaaS offering. Well done!

Feedback (if wrong):

Even though the other Azure services you chose have merits, they may not fully satisfy the requirements for high availability and scalability. For example, Azure Virtual Machines (Option A) usually require manual scaling and load balancing, while Azure Functions (Option B) is better suited for event-triggered scenarios rather than high-traffic situations. On the other hand, Azure Kubernetes Service (Option D) imposes management overhead and increased complexity compared to Azure App Service. Make sure to weigh all factors when designing future Azure infrastructure solutions. Keep practicing and honing your skills!

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ305)

Subskill: Designing Compute and Network Infrastructure

Competency: High Availability and Scalability

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

41. Your organization has an Azure subscription containing a storage account where an application occasionally writes duplicate files. Currently, a PowerShell script identifies and deletes these duplicate files manually after approval from the operations manager. You need to recommend a serverless solution that automates this process. The solution should run the script hourly to check for duplicate files, process an email response from the operations manager for deletion approval, and execute the script if approval is received. What should you recommend?

- A) Azure Automation and Azure Event Grid
- B) Azure Logic Apps and Azure Functions
- C) Azure Batch and Azure Logic Apps
- D) Azure Data Factory and Azure Event Hub

Answer: B

Feedback(if correct): Excellent choice! Azure Logic Apps and Azure Functions provide a robust serverless solution for automating the process, integrating with various services, and executing the script based on predefined triggers.

Feedback(if wrong):

Option A (Azure Automation and Azure Event Grid): While Azure Automation can automate tasks, it may not be the most suitable choice for this scenario, as it focuses more on managing your Azure resources

through runbooks. Azure Event Grid is used for event-based routing and processing but doesn't directly address the requirements of running the script and processing email responses.

Option C (Azure Batch and Azure Logic Apps): Azure Batch is designed for large-scale parallel and high-performance computing jobs, which may be overkill for this scenario. Azure Logic Apps is a suitable choice but requires Azure Functions to execute the PowerShell script.

Option D (Azure Data Factory and Azure Event Hub): Azure Data Factory is an ETL (Extract, Transform, Load) service, primarily used for data integration and orchestration. Azure Event Hub is a big data streaming platform, which doesn't directly align with the requirements of the scenario.

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Plan and implement disaster recovery strategies, Design and implement business continuity and high availability

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

42. You are tasked with designing an application that analyzes video files using Azure Linux virtual machines. The files will be uploaded from corporate offices connecting to Azure via ExpressRoute. Which Azure Storage account configuration should you recommend to meet the following requirements: supporting video files up to 7 TB, providing the highest availability, optimizing storage for large video files, and ensuring files from on-premises networks are uploaded via ExpressRoute?

- A) Premium file shares with Locally-redundant storage (LRS)
- B) Premium page blobs with Geo-redundant storage (GRS)
- C) Standard general-purpose v2 with Zone-redundant storage (ZRS)
- D) Standard general-purpose v2 with Geo-redundant storage (GRS)

Feedback(if correct): Option D) Standard general-purpose v2 with Geo-redundant storage (GRS) is correct. It meets all the requirements: supporting video files up to 7 TB, providing high availability, optimizing storage for large video files, and ensuring files from on-premises networks are uploaded via ExpressRoute.

Feedback(if wrong): Options A, B, and C do not fully meet all the specified requirements. Option A provides premium file shares, which may not be necessary for storing large video files, and LRS redundancy, which does not ensure high availability across Azure regions. Option B provides premium page blobs, which are not typically used for storing video files, and GRS redundancy, which is not optimized for large video files. Option C uses ZRS redundancy, which does not provide the required high availability across Azure regions. Therefore, they are not the best choices for this scenario.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Plan and implement disaster recovery strategies, Design and implement business continuity and high availability

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

43. Your organization plans to deploy an application that processes large video files in Azure. The files will be uploaded from corporate offices connecting to Azure via ExpressRoute. What Azure Storage redundancy option ensures that the storage is optimized for large video files and provides redundancy across Azure Availability Zones?

- A) Locally redundant storage (LRS)
- B) Geo-redundant storage (GRS)
- C) Zone-redundant storage (ZRS)
- D) Read-access geo-redundant storage (RA-GRS)

Feedback(if correct): Option C) Zone-redundant storage (ZRS) is correct. ZRS ensures that the storage is optimized for large video files by providing redundancy across Azure Availability Zones, ensuring high availability and durability.

Feedback(if wrong): Option C) Zone-redundant storage (ZRS) is the correct choice because it provides redundancy across Azure Availability Zones, which ensures high availability and durability for the storage. Options A, B, and D do not specifically address redundancy across Availability Zones, making them incorrect choices for this scenario.



Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Plan and implement disaster recovery strategies, Design and implement business continuity and high availability

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

44. You are designing a solution to store and process large video files in Azure. The files will be uploaded from on-premises networks connected to Azure via ExpressRoute. Which Azure Storage account type supports video files up to 7 TB and ensures the highest availability?

- A) Premium file shares
- B) Premium page blobs
- C) Standard general-purpose v2
- D) Azure Blob Storage

Feedback(if correct): Option D) Azure Blob Storage is correct. Azure Blob Storage supports video files up to 7 TB and ensures the highest availability among the options provided.

Feedback(if wrong): Option D) Azure Blob Storage is the correct choice because it supports large video files and ensures the highest availability. Options A, B, and C do not specifically address the storage of large video files or ensure the highest availability, making them incorrect choices for this scenario.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Plan and implement disaster recovery strategies, Design and implement business continuity and high availability

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

45. Your company is preparing to deploy multiple instances of an Azure web application across diverse Azure regions. The application is vital for business operations and necessitates high availability and fault tolerance. You're tasked with devising an access solution that accommodates rate limiting, distributes requests evenly across instances, and guarantees uninterrupted access to the application during regional outages. Which Azure service should you propose to fulfill these criteria?

- A) Azure Traffic Manager
- B) Azure Application Gateway
- C) Azure Front Door
- D) Azure Load Balancer

Answer: A

Feedback(if correct): Azure Traffic Manager is not suitable for this scenario as it primarily focuses on distributing traffic across different datacenters and endpoints based on routing methods such as priority, weighted, performance, or geographic routing. Azure Front Door is designed for global load balancing and acceleration, but it does not offer rate limiting capabilities or direct control over routing to specific instances. Azure Load Balancer is a Layer 4 (TCP, UDP) load balancer that distributes incoming network traffic across multiple servers in a backend pool to ensure high availability and reliability. However, it does not provide rate limiting or application-level routing features. Azure Application Gateway is the correct choice as it is a Layer 7 (HTTP, HTTPS) load balancer that offers features such as URL-based routing, SSL termination, and cookie-based session affinity, making it suitable for handling web traffic. Additionally, it supports rate limiting and provides control over routing to specific instances, fulfilling all the requirements of the scenario.

Feedback(if wrong): Azure Traffic Manager primarily focuses on distributing traffic across different datacenters and endpoints based on routing methods such as priority, weighted, performance, or geographic routing. Azure Front Door is designed for global load balancing and acceleration, but it does not offer rate limiting capabilities or direct control over routing to specific instances. Azure Load Balancer

is a Layer 4 (TCP, UDP) load balancer that distributes incoming network traffic across multiple servers in a backend pool to ensure high availability and reliability. However, it does not provide rate limiting or application-level routing features.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Solution Design, Azure Service Selection

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

46. Your organization is planning to deploy multiple instances of an Azure web application across various Azure regions. The application is critical for business operations and requires high availability and fault tolerance. You need to design an access solution that supports rate limiting, balances requests between instances and ensures continuous access to the application even in the event of a regional outage. Which Azure service should you recommend to meet these requirements?

- A) Azure Application Gateway
- B) Azure Traffic Manager
- C) Azure Front Door
- D) Azure Load Balancer

Feedback(if correct): Azure Application Gateway is the correct choice for this scenario. It is a Layer 7 (HTTP, HTTPS) load balancer that supports rate limiting, distributes requests evenly across instances, and provides continuous access to the application even during regional outages.

Feedback(if wrong):

B) Azure Traffic Manager primarily focuses on DNS-based traffic routing across multiple datacenters or endpoints based on routing methods such as priority, weighted, performance, or geographic routing. It does not provide application-level features like rate limiting or direct control over routing to specific instances.

C) Azure Front Door is a global service that offers scalable and secure routing of HTTP traffic to backend services and supports features like SSL termination, URL-based routing, and session affinity. However, it does not provide native support for rate limiting or direct control over routing to specific instances.

D) Azure Load Balancer is a Layer 4 (TCP, UDP) load balancer that distributes incoming network traffic across multiple servers in a backend pool to ensure high availability and reliability. While it balances requests between instances, it does not support rate limiting or application-level routing features.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Solution Design, Azure Service Selection

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

47. Your company is preparing to deploy multiple instances of an Azure web app across several Azure regions. You are tasked with designing an access solution that adheres to the following replication requirements:

Support rate limiting.

Balance requests between all instances.

Ensure users can access the app in the event of a regional outage.

3. You are responsible for designing an access solution for the Azure web app. The solution must fulfill the specified replication requirements. You propose using Azure Application Gateway to provide access to the app. Will this solution meet the goal?

A) Yes

B) No

Answer: A

Feedback(if correct): Yes, Azure Application Gateway is a Layer 7 load balancer that can provide features such as rate limiting, SSL termination, and session affinity. It can balance requests between instances and

ensures high availability by distributing traffic across multiple instances. Therefore, this solution meets the specified replication requirements.

Feedback(if wrong): The correct answer is A. Azure Application Gateway meets the goal as it supports rate limiting, balancing requests between instances, and ensuring continuous access to the application, even in the event of a regional outage.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Solution Design, Azure Service Selection

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

48. Your organization is preparing to deploy multiple instances of an Azure web app across various Azure regions. You are tasked with designing an access solution that meets the following replication requirements:

Support rate limiting.

Balance requests between all instances.

Ensure users can access the app in the event of a regional outage.

You are responsible for designing an access solution for the Azure web app. You suggest using Azure Front Door. to provide access to the app. Will this solution fulfill the requirements?

A) Yes

B) No

Answer: A

Feedback(if correct): Using Azure Front Door to provide access to the Azure web app will fulfill the specified replication requirements. It supports rate limiting, balances requests between instances using intelligent routing, and ensures high availability by automatically rerouting traffic in the event of a regional outage.

Feedback(if wrong): The correct answer is A) Yes. Azure Front Door is designed to meet the specified replication requirements, including supporting rate limiting, balancing requests between instances, and ensuring users can access the app in the event of a regional outage. It achieves this through its global load balancing and failover capabilities, making it the suitable solution for this scenario.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Solution Design, Azure Service Selection

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

49. You've been assigned to provision Azure resources for a company. The company intends to establish an Azure Virtual Network (VNet) and needs seamless integration with an on-premises network that employs custom DNS servers. Your proposal entails a local network gateway. Does this proposal align with the company's requirements?

- A) Yes
- B) No

Answer: B

Feedback(if correct): Deploying a local network gateway does not align with the company's requirement of seamless integration with custom DNS servers in an on-premises network. A local network gateway is used to establish a connection between an on-premises network and an Azure virtual network, but it does not provide seamless integration with custom DNS servers. To achieve seamless integration with custom DNS servers, other solutions such as Azure DNS private zones or deploying your own DNS server would be more appropriate.

Feedback(if wrong):

Option A is incorrect because deploying a local network gateway alone does not ensure seamless integration with custom DNS servers. While a local network gateway facilitates connectivity between Azure and on-premises networks, it does not inherently address the requirement for integrating with custom DNS servers. Additional configurations or solutions, such as Azure DNS private zones or deploying custom DNS servers, would be needed to achieve seamless integration with custom DNS servers. Therefore, Option B is the correct choice as it acknowledges the mismatch between the proposed solution and the company's requirements.

Skill: Designing Microsoft Azure Infrastructure Solutions Certification (AZ305)

Subskill: Designing Compute and Network Infrastructure

Competency: Recommending appropriate Azure networking solutions to meet specific requirements

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

50. You've been assigned to provision Azure resources for a company. The company intends to establish an Azure Virtual Network (VNet) and needs seamless integration with an on-premises network that employs custom DNS servers. Your proposal entails deploying a virtual network gateway and a local network gateway and Azure DNS. Does this proposal align with the company's requirements?

- A) Yes
- B) No

Answer: A

Feedback(if correct):

Deploying a virtual network gateway and a local network gateway facilitates integration between the Azure VNet and the on-premises network, fulfilling the company's need for network integration.

Feedback(if wrong):

the proposed solution of deploying a virtual network gateway and a local network gateway, along with Azure DNS, does align with the company's requirement for seamless integration with an on-premises network that uses custom DNS servers. This selection implies that the proposed solution may not adequately address the company's specific needs and could result in a lack of seamless integration between the Azure Virtual Network and the on-premises network.

Skill: Designing Microsoft Azure Infrastructure Solutions Certification (AZ305)

Subskill: Designing Compute and Network Infrastructure

Competency: Recommending appropriate Azure networking solutions to meet specific requirements

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

az305 final exam3

51. You are required to design a hybrid cloud solution for your organization. The company currently has an on-premises data center and an Azure subscription. They want to implement the following requirements:

Transfer large volumes of data from on-premises to Azure with minimal latency

Implement a disaster recovery solution for on-premises applications in Azure

Which Azure service should you recommend to meet these requirements in the context of designing hybrid cloud solutions?

- A) Azure Functions
- B) Azure Event Grid
- C) Azure ExpressRoute
- D) Azure Logic Apps

Answer: C

Feedback(if correct):-

Transfer large volumes of data: Azure ExpressRoute establishes a dedicated, private connection between your on-premises network and Azure. This connection bypasses the public internet, significantly reducing latency and improving transfer speeds for large data volumes compared to standard internet connections.

Disaster recovery for on-premises applications: ExpressRoute's dedicated and reliable connectivity facilitates efficient data replication and backup of your on-premises applications to Azure. This enables faster failover and recovery in case of outages or disasters at your data center, minimizing downtime and data loss.

By implementing Azure ExpressRoute, you can establish a robust and high-performance hybrid cloud environment, efficiently transferring large data volumes and ensuring seamless disaster recovery for your on-premises applications in Azure. Remember to evaluate specific requirements and choose the ExpressRoute configuration and complementary services that best align with your organization's goals.

Feedback(if wrong):-

A) Azure Functions: While useful for event-driven serverless computing, it doesn't directly address data transfer or disaster recovery needs.

B) Azure Event Grid: This event routing service enables communication between different event sources and handlers within Azure. While potentially helpful for specific automation tasks in your hybrid solution, it doesn't provide the dedicated connectivity and data transfer capabilities you require.

D) Azure Logic Apps: These offer workflow automation possibilities, but again, they don't provide the core functionalities of dedicated network connectivity and disaster recovery through private links.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Identity and Security Solutions

Competency: Implement Azure Role-Based Access Control (RBAC), Implement Azure Active Directory (Azure AD) authentication, Evaluate and mitigate organizational security risks

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

52. Your company has two divisions, North and South, each with its own Azure subscription. The North division's subscription is named Subscription1, and the South division's subscription is named Subscription2. Both subscriptions are linked to the Azure AD tenant, with Subscription1 associated with the contoso.com tenant and Subscription2 associated with the fabrikam.com tenant. In Subscription2, there is an Azure Virtual Machine (VM) named VM1, running a critical application. You need to ensure that only users from the fabrikam.com tenant can access VM1. What should you recommend?

- A) Use Azure AD B2B collaboration.
- B) Configure Azure AD conditional access policies.
- C) Implement Azure AD Privileged Identity Management.
- D) Enable Azure AD Managed Service Identity (MSI) for VM1.

Answer: B

Feedback (if correct):

The correct answer is configuring Azure AD conditional access policies to restrict access to VM1 to users from the fabrikam.com tenant. This approach centralizes user authentication and authorization management for seamless enforcement of organizational policies.

Feedback (if wrong):

Option A, using Azure AD B2B collaboration, is incorrect as it aims to collaborate with external organizations, while the question concerns distinct tenants within the same organization. Options C and D, referring to Azure AD Privileged Identity Management and enabling Azure AD Managed Service Identity (MSI) for VM1, do not address restricting VM1 access to users from the fabrikam.com tenant.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Architecting for Business Continuity and Disaster Recovery

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

53. Your task involves designing access control and security measures for a data platform within Azure. You oversee an Azure Active Directory (Azure AD) tenant synchronized with an on-premises Active Directory domain. Your objective is to enable SAML single sign-on (SSO) and enforce multi-factor authentication (MFA) for users accessing a line-of-business (LOB) application developed internally, particularly when users attempt to access from unknown locations. To meet the security requirements for the data platform, which two features should you incorporate into the solution? Select the appropriate options from the choices provided below:

- A) Azure AD enterprise applications
- B) Azure AD Identity Protection
- C) Azure Application Gateway
- D) Conditional Access policies

Answer: A, D

Feedback (if correct):

The correct selection involves utilizing Azure AD enterprise applications to configure SAML single sign-on (SSO) for the line-of-business (LOB) application, allowing users to authenticate seamlessly, and implementing Conditional Access policies to enforce multi-factor authentication (MFA) based on specific conditions such as accessing the application from unknown locations. This approach ensures enhanced security and access control measures for the data platform in alignment with the specified requirements.

Feedback (if wrong):

- B) Azure AD Identity Protection: It is a useful tool to detect vulnerabilities, risk detections, and suspicious activities but does not directly apply to the requirements of enabling SAML SSO and enforcing MFA for the LOB application.
- C) Azure Application Gateway: Primarily focused on HTTP load balancing, SSL offloading, and web application firewall features, it does not play a significant role in SAML SSO and MFA enforcement for the LOB application.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Securing access to applications and services

Difficulty Level: Expert

Bloom's Taxonomy Level: Application

54. You have been appointed to design a monitoring solution for a healthcare company that utilizes Azure Active Directory (Azure AD) for user authentication. The stakeholders expressed interest in receiving alerts whenever specific user sign-in attempts occur. Which Azure components and configurations should you propose to fulfill the client's requirements?

Component Selection:

- A) Send Azure AD logs to An Azure Event Hub
- B) Component Selection: An Azure Log Analytics workspace
- C) Alert Rule Settings: Activity log - Graphical user interface
- D) Alert Rule Settings: Metrics - Text

Answer: B, D

Feedback (if correct):

When designing a monitoring solution for the healthcare company using Azure Active Directory (Azure AD), you should send Azure AD logs to an Azure Log Analytics workspace, and then create an alert rule using Log as the signal type. This allows the stakeholders to receive alerts based on specific user sign-in events.

Feedback (if wrong):

- A) Sending Azure AD logs to an Azure Event Hub might not be the best option for this scenario because Event Hub is mainly designed for ingesting and processing massive amounts of real-time data streams. It does not provide extensive log querying and analysis capabilities compared to Azure Log Analytics.
- C) Activity log is used to monitor the events happening at the resource level, whereas Metrics (Option D) tracks numerical values measured over time. These options do not help us monitor user sign-in events coming from Azure AD.

Keep in mind that when designing monitoring solutions, it's essential to select components and configurations that closely match the client's requirements.

Skill mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ305)

Subskill: Designing Identity and Security Solutions

Competency: Monitoring and Alerting

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

55. You are tasked with designing the authentication mechanism for an ASP.NET application named App1, which runs on a server named Server1 in your on-premises network. The application needs to allow users to sign in using their Azure AD account and utilize Azure Multifactor Authentication (MFA) when accessing it from the internet. Which Azure service should you recommend deploying and configuring first?

- A) Azure AD managed identity
- B) Azure AD enterprise application
- C) Azure AD conditional access policy
- D) Azure AD Application Proxy

Answer: D

Feedback(if correct):

The correct answer is D) Azure AD Application Proxy.

Azure AD Application Proxy enables secure remote access to on-premises applications like App1 by integrating with Azure AD for authentication and authorization. It allows users to sign in using their Azure AD accounts and facilitates Azure Multifactor Authentication (MFA) for enhanced security.

Feedback(if wrong):

The incorrect options are:

- A) Azure AD managed identity: Azure AD managed identities are used to authenticate Azure services with other Azure resources but are not relevant for securing on-premises applications like App1.
- B) Azure AD enterprise application: While configuring an Azure AD enterprise application is part of the authentication setup, it comes after deploying the Azure AD Application Proxy.

C) Azure AD conditional access policy: Conditional access policies define access rules and security requirements but do not directly enable access to on-premises applications from the internet. Azure AD Application Proxy is required for that purpose.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Executing the deployment and configuration of Azure services to enable secure authentication mechanisms for the web application, ensuring compliance with organizational security policies and best practices.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

56. Your organization, named AdventureWorks, hosts several Azure logic apps with HTTP triggers that provide access to an on-premises web service. AdventureWorks collaborates with a partner company, Woodgrove, Inc. Woodgrove does not have an existing Azure Active Directory (Azure AD) tenant and relies on a third-party OAuth 2.0 identity provider for user authentication. Woodgrove developers plan to use a subset of the logic apps to build applications that integrate with the on-premises web service of AdventureWorks. You are tasked with designing a solution to grant Woodgrove developers access to the logic apps, ensuring that their requests are limited to lower rates than those from AdventureWorks users and that the developers can rely on their existing OAuth 2.0 provider for access. Additionally, the solution should not necessitate changes to the logic apps or the use of Azure AD guest accounts. What should be included in the solution?

- A) Azure Cognito
- B) Azure Front Door
- C) Azure Application Proxy
- D) Azure API Management

Answer: D

Feedback(if correct):

This solution aligns with the scenario's requirements by allowing Woodgrove developers to access the logic apps using their existing OAuth 2.0 provider while also enabling rate limiting to control request rates.

Azure API Management provides the necessary capabilities to publish APIs securely to external developers, including Woodgrove, and manage access using OAuth 2.0 authentication. It supports rate limiting to ensure that Woodgrove developers' requests are limited to lower rates than those from AdventureWorks users.

Feedback(if wrong):

Option A) Azure Cognito: Azure Cognito is not a Microsoft Azure service. It is a service provided by Amazon Web Services (AWS) for identity management, authentication, and authorization.

Option B) Azure Front Door: Azure Front Door is a global, scalable entry point for web applications, but it is not primarily designed for managing access to APIs or enforcing rate limits.

Option C) Azure Application Proxy: Azure Application Proxy enables remote access to on-premises applications, but it does not support rate limiting or integrate with Woodgrove's OAuth 2.0 provider.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Executing the deployment and configuration of Azure services to enable secure authentication mechanisms for the web application, ensuring compliance with organizational security policies and best practices.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

57. You are designing a solution for a global enterprise that plans to deploy a cloud-based application, App2, on Azure. App2 will utilize Azure Active Directory (Azure AD) for authenticating users. The application must be accessible over the internet to employees who use corporate laptops running Windows 10, which are registered with Azure AD. You need to ensure two key requirements:

1. Employees should be able to access App2 seamlessly without being prompted for their credentials if they are already signed in to their Windows 10 devices.

2. Access to App2 must be restricted to only those accessing it from company-managed laptops.

Based on the scenario above, which two actions should you recommend to meet the requirements?
(Choose two.)

- A. Implement an Azure AD app registration for App2 to enable Azure AD authentication.
- B. Utilize an Azure AD-managed identity for App2 to automatically handle the authentication process.
- C. Configure Azure AD Application Proxy to facilitate secure remote access to App2.
- D. Establish a conditional access policy in Azure AD to enforce access from company-managed devices only.

Answers:- A. D

Feedback(if correct):

To meet the requirements of seamless access for employees to App2, without being prompted for credentials if they are already signed in to their Windows 10 devices, and ensuring that access to App2 is restricted to only company-managed laptops, the following actions are recommended:

- A. Implement an Azure AD app registration for App2 to enable Azure AD authentication.** This step is crucial for integrating App2 with Azure AD, which allows the application to leverage Azure AD for user authentication. By registering App2 with Azure AD, you set the foundation for supporting single sign-on (SSO). SSO enables employees to access App2 seamlessly without being prompted for their credentials again if they are already signed in to their Windows 10 devices.
- D. Establish a conditional access policy in Azure AD to enforce access from company-managed devices only.** Conditional access policies in Azure AD allow you to define conditions under which users can access Azure AD-connected applications. By creating a policy that requires device compliance, you can ensure that only devices managed by the organization (in this case, company-managed laptops running Windows 10) can access App2. This approach directly addresses the requirement to restrict access to App2 to only company-managed laptops.

Feedback(if wrong):

- B. Utilize an Azure AD-managed identity for App2 to automatically handle the authentication process.** Azure AD-managed identities are used for authenticating Azure services to other Azure services securely without storing credentials in code. This option does not directly contribute to achieving seamless access for users or restricting access to company-managed devices.
- C. Configure Azure AD Application Proxy to facilitate secure remote access to App2.** While Azure AD Application Proxy does provide secure remote access to web applications, it is not specifically required to

meet the outlined requirements of seamless user access and device-based access restrictions. The scenario does not specify that App2 is an on-premises application needing remote access via a proxy, making this option less relevant to the stated goals.

This solution ensures that employees experience a frictionless access experience to App2 while maintaining strict access control aligned with organizational security policies.

Skill Mapping

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Designing Identity and Security Solutions
- Competencies: Utilizing Azure AD for application authentication and implementing conditional access policies to enhance security.
- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Application

58. You manage a Free edition of a hybrid Azure Active Directory (Azure AD) tenant utilizing password hash synchronization. There's a need to enhance security by preventing Active Directory domain user accounts from being locked out due to brute force attacks targeting Azure AD user accounts, while also aiming to minimize costs. To protect against brute force attacks, which feature should you recommend?

- A. Azure AD Password Protection
- B. Conditional Access Policies
- C. Pass-through Authentication
- D. Smart Lockout

Answer: D

Feedback(if correct):-

Smart Lockout is designed to differentiate between sign-in attempts by legitimate users and those by attackers. It locks out the attackers after several failed attempts while allowing legitimate users to continue accessing their accounts. This functionality is crucial for protecting user accounts from brute force attacks without incurring additional costs, making it the ideal choice for a Free edition Azure AD tenant.

The best feature to recommend in this scenario to protect against brute-force attacks while minimizing costs for a Free tier Azure AD tenant with password hash synchronization is:

Functionality: Smart Lockout is a security feature available in Azure AD that helps mitigate brute-force attacks by dynamically adjusting lockout thresholds based on user sign-in behavior. It monitors sign-in attempts and increases the lockout threshold for trusted locations or devices while enforcing stricter thresholds for suspicious activity or unknown locations.

Free Tier Availability: Smart Lockout is a built-in Azure AD feature available in all tiers, including the Free edition. This makes it a cost-effective solution for your scenario.

Addressing Brute-Force Attacks: By dynamically adjusting lockout thresholds, Smart Lockout can prevent attackers from repeatedly attempting to guess passwords and locking out legitimate users.

Additional Considerations:

While Smart Lockout helps mitigate brute-force attacks, it's still recommended to educate users about strong password practices as an additional security layer.

Consider enabling Azure AD Identity Protection for additional threat detection and reporting capabilities, which might be available in the Free tier with limited functionalities.

Feedback(if wrong):-

A. Azure AD Password Protection: While this feature is helpful, it's not available in the Free tier. It requires an Azure AD Premium license and offers functionalities like banned password lists and customizable password strength requirements.

B. Conditional Access Policies: Conditional access policies can be used to define additional security controls for user access, but they don't directly address brute-force attacks on passwords. You might use conditional access policies for other security measures like multi-factor authentication (MFA).

C. Pass-through Authentication: This feature is primarily used for single sign-on (SSO) scenarios and doesn't address brute-force attack prevention on Azure AD user accounts.

skill mapping :

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: configuring Azure AD Conditional Access Policies to enhance security, authentication methods and how to secure Azure AD integrated apps against vulnerabilities associated with legacy authentication.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

59. You manage a Free edition of a hybrid Azure Active Directory (Azure AD) tenant utilizing password hash synchronization. There's a need to enhance security by preventing Active Directory domain user accounts from being locked out due to brute force attacks targeting Azure AD user accounts, while also aiming to minimize costs. Alongside enhancing security against brute force attacks, there's also a requirement to block legacy authentication attempts to Azure AD integrated apps to further secure the tenant against potential vulnerabilities. To block legacy authentication attempts, which solution should you recommend?

- A. Azure AD Application Proxy
- B. Azure AD Password Protection
- C. Conditional Access Policies
- D. Enable Security Defaults

Answer: C

Feedback(if correct):- Implementing Conditional Access Policies is the recommended solution to block legacy authentication attempts to Azure AD-integrated apps. This approach provides the necessary granularity to specify access rules that effectively prevent insecure authentication methods. Conditional Access Policies allow for the creation of policies that can enforce authentication requirements, such as requiring multi-factor authentication (MFA) or blocking sign-ins from outdated authentication protocols. This capability is essential for enhancing the security of the Azure AD tenant by ensuring that only secure, modern authentication methods are used, thereby protecting against vulnerabilities associated with legacy authentication.

Feedback(if wrong):- A. Azure AD Application Proxy is designed to provide secure remote access to internal applications, not specifically to block legacy authentication attempts. While it enhances security, its main function does not align with the requirement to block legacy authentication protocols.

B. Azure AD Password Protection helps prevent weak passwords by enforcing strong password policies. However, it does not address the blocking of legacy authentication attempts, which is the focus of the requirement.

D. Enable Security Defaults provides a set of basic security enhancements, including requiring MFA for all users. While enabling Security Defaults can indirectly reduce the risk of legacy authentication by enforcing MFA, it is not as targeted or configurable as Conditional Access Policies for specifically blocking legacy authentication attempts. Security Defaults apply broadly and may not offer the fine-grained control needed for specific scenarios or organizational needs.

skill mapping :

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: configuring Azure AD Conditional Access Policies to enhance security, authentication methods and how to secure Azure AD integrated apps against vulnerabilities associated with legacy authentication.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

60. Your organization uses Azure services extensively, including Azure Key Vault for secure key management. The Security Department requires improved management and monitoring of administrative roles, while the Quality Assurance Department needs temporary administrator access for testing purposes.

To address the needs of the Security and Quality Assurance departments, which Azure service would you recommend?

- A. Azure AD Identity Protection
- B. Azure Managed Identity
- C Azure AD Privileged Identity Management.
- D. Azure Monitor

Answers: C.

Feedback(if correct):- **Azure AD Privileged Identity Management (option C) since it provides improved management and monitoring of administrative roles for the Security Department and temporary administrator access for Quality Assurance Department testing purposes.**

Feedback(if wrong):-

option A): Azure AD Identity Protection (option A) handles identifying vulnerabilities in your organization's identities and detecting potential identity threats. It does not improve the management and monitoring of administrative roles nor grant temporary administrator access for testing purposes.

option B): Azure Managed Identity (option B) assists in managing machine identities for applications running in Azure services without needing to manage credentials explicitly. It does not aid in improving the management and monitoring of administrative roles or grant temporary administrator access for testing purposes.

Azure Monitor (option D) monitors the performance and health of applications, networks, and Azure resources. Unlike Azure AD Privileged Identity Management, it does not deal with enhancing management and monitoring of administrative roles or supplying temporary administrator access for testing purposes.

Skill mapping:

Topic: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskill: Designing Identity and Security Solutions

Competency: Integrating identity and access management systems

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

61. Your organization uses Azure services extensively, including Azure Key Vault for secure key management. The Security Department requires improved management and monitoring of administrative roles, while the Quality Assurance Department needs temporary administrator access for testing purposes.

Continuing the focus on security, the Development Department needs a solution for securely accessing Azure Key Vault to retrieve keys directly in their code, without managing credentials explicitly.

Which Azure service should you recommend to provide secure, simplified access to Azure Key Vault for application development?

- A. Azure AD Privileged Identity Management
- B. Azure Managed Identity
- C. Azure Key Vault
- D. Azure AD Identity Protection

Answer: B.

Feedback(if correct):-

Azure Managed Identity is specifically designed to provide Azure services with an automatically managed identity in Azure Active Directory (Azure AD). This enables Azure services, like Azure App Service or Azure Virtual Machines, to securely access other Azure resources such as Azure Key Vault, without needing to manage credentials in the code. Managed Identity simplifies security management by handling the authentication to services that support Azure AD authentication, making it the ideal choice for the Development Department's requirement to access Azure Key Vault securely and efficiently. This approach eliminates the risks associated with storing and managing credentials directly in the application's code or configuration files.

Feedback(if wrong):-

- A. Azure AD Privileged Identity Management: While crucial for managing, monitoring, and auditing privileged access within Azure, Azure AD PIM does not directly facilitate secure access to Azure resources like Key Vault for application development purposes. It's more focused on governance and security of administrative roles rather than providing a service identity for application access to Azure resources.
- C. Azure Key Vault: This is the resource the development team needs to access securely. While Azure Key Vault is central to managing secrets, keys, and certificates, it does not, by itself, provide a mechanism for secure, credentialless access from applications. The question focuses on the method of access, not the resource being accessed.
- D. Azure AD Identity Protection: This service provides risk-based conditional access to protect Azure AD identities from potential vulnerabilities and attacks. However, it does not offer a solution for applications to securely access other Azure services like Key Vault without managing credentials. Azure AD Identity Protection is more about safeguarding user identities than facilitating service-to-service authentication and authorization.

Skill mapping:

Topic: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskill: Designing Identity and Security Solutions

Competency: Integrating identity and access management systems

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

62. Your company is in the process of migrating a critical business application, App2, to Azure. This application requires secure access to various Azure services and external APIs. To ensure the application's authentication and authorization processes meet your security standards, you need to decide on the appropriate Azure service for managing access tokens.

App2 must authenticate with Azure services and several external APIs. The solution must provide a secure and scalable way to manage authentication and authorization.

Which Azure service should App2 use to obtain access tokens for accessing Azure services and external APIs?

- A. Azure CosmosDB
- B. Microsoft Identity Platform
- C. Azure DMS
- D. Azure HDInsight

Answer: B.

Feedback(if correct):-

The correct answer is option B, Microsoft Identity Platform. It is the most suitable service for obtaining access tokens to authenticate and authorize App2 to interact with Azure services and external APIs. The Microsoft Identity Platform offers modern authentication protocols, such as OAuth 2.0 and OpenID Connect, supporting secure and scalable ways for App2 to access protected resources and safeguard sensitive data throughout the process.

Feedback(if wrong):-

Azure Cosmos DB is a globally distributed, multimodel database service, while Azure DMS (Database Migration Service) focuses on assisting migrations across heterogeneous platforms. Azure HDInsight, conversely, is an open-source framework optimized for processing big data. All these fall outside the scope of managing access tokens for App2.

Skill mapping:

Topic: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskill: Designing Identity and Security Solutions

Competency: Integrating identity and access management systems

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

63. In your Azure environment within resource group RG1, you have an Azure Logic App named App1 that needs to interact with Azure Key Vault instances KV1 (East US) and KV2 (West Europe). App1 already possesses the 'Get' permission for secrets in KV1. You are tasked with configuring



permissions to enable App1 to copy all the secrets from KV1. What additional permission should you assign to App1 to ensure it can retrieve (copy) the secrets from KV1 effectively?

- A. Add
- B. Backup
- C. List
- D. Unwrap Key

Answer: C.

Feedback(if correct):-

To enable App1, an Azure Logic App, to effectively retrieve (copy) secrets from KV1, the 'List' permission is essential in addition to the 'Get' permission it already has. The 'Get' permission allows App1 to fetch the value of a specific secret within KV1. However, to copy all secrets from KV1, App1 needs the ability to enumerate all secrets within the vault. The 'List' permission grants this capability, allowing App1 to identify and access all available secrets for copying. This is a crucial step before transferring these secrets to another key vault, ensuring App1 can retrieve and then replicate the secrets as required.

Feedback if Wrong:

- A. Add: This permission would be required on the target Key Vault (KV2) for creating or updating secrets, not for retrieving secrets from KV1.
- B. Backup: This permission allows taking a backup of the secret, which is different from listing or copying them.
- D. Unwrap Key: This is related to cryptographic operations on keys rather than managing secrets.

skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Knowledge of Azure Key Vault service, including how to manage secrets and the necessary permissions for interacting with these secrets across different instances. Ability to configure Azure Logic Apps with the appropriate permissions to securely access and manipulate resources across Azure services.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

64. In your Azure environment within resource group RG1, you have an Azure Logic App named App1 that needs to interact with Azure Key Vault instances KV1 (East US) and KV2 (West Europe). App1 already possesses the 'Get' permission for secrets in KV1. You are tasked with configuring permissions to enable App1 to copy all the secrets from KV1.

Following the retrieval of secrets from KV1, you now need to ensure App1 can store (copy) these secrets into KV2 located in West Europe.

Which permission must you assign to App1 to enable it to store the copied secrets in KV2?

- A. Create
- B. Import
- C. List
- D. Wrap Key

Answer: A.

Feedback(if correct):- The "Create" permission is essential for App1 to be able to add new secrets to Azure Key Vault (KV2). This permission allows App1 to create new secrets in KV2, effectively enabling the storage (copying) of secrets retrieved from KV1. The "Create" permission is specifically required for adding or updating secrets within a Key Vault, making it the necessary permission for this operation.

Feedback if Wrong:

- B. Import might seem like a relevant choice, but in the context of Azure Key Vault, the "Create" permission encompasses the ability to add new secrets, which is what the process of storing copied secrets involves.
- C. List permission allows viewing the secrets but does not grant the ability to add or update secrets in the Key Vault.
- D. Wrap Key is related to cryptographic operations on keys and does not apply to the operation of storing secrets.

skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Knowledge of Azure Key Vault service, including how to manage secrets and the necessary permissions for interacting with these secrets across different instances. Ability to configure Azure Logic Apps with the appropriate permissions to securely access and manipulate resources across Azure services.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

65. Your organization is migrating an on-premises application, named AppY, to Azure. The application relies on data from multiple Microsoft SQL Server databases hosted locally. These databases and their sizes are as follows:

DB1: 500 GB

DB2: 350 GB

DB3: 420 GB

DB4: 80 GB

AppY is utilized only on specific days of the quarter, and there are no projections for significant data growth. As part of the migration plan, the company aims to transfer the databases to Azure SQL Database. Your task is to recommend the appropriate service tier to minimize costs. Which service tier should you suggest?

- A) DTU-based Business Critical
- B) DTU-based General Purpose
- C) DTU-based Standard
- D) DTU-based Basic

Answer: C

Feedback(if correct): The correct selection is option C) DTU-based Standard. This service tier is suitable for databases of up to 1 TB in size, making it suitable for the sizes mentioned in the scenario. DTU-based Standard offers a balance between performance and cost, making it ideal for applications with intermittent usage patterns and minimal data growth.

Feedback(if wrong): DTU-based Business Critical is not the best choice for this scenario because it is typically used for applications that require high availability and performance, which may not be necessary for an application that is only used intermittently. DTU-based General Purpose might not be suitable either, as it is designed for applications with varying usage patterns and may not provide the cost efficiency needed for an application used only on specific days. DTU-based Basic is also not the optimal choice as it is designed for light workloads and may not handle the size and occasional usage of the application effectively.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ-305)

Subskill: Designing Data Platforms

Competency: Select appropriate Azure SQL Database service tiers based on workload requirements and cost considerations.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

66. You have been tasked with designing a data engineering solution for your company, which currently holds application data in an on-premises Microsoft SQL Server database. The company aims to transfer transactional data from the on-premises SQL server to a data warehouse in Azure, with a requirement for scheduled nightly data transfers. Additionally, the solution requires a managed Spark cluster for data analysis, allowing data engineers to develop notebooks in Scala, R, and Python. Furthermore, a data lake store is needed for ingesting data from multiple sources.

Which Azure service should be used for hosting the data warehouse to meet these requirements in the context of designing data platforms?

- A) Azure AD
- B) Azure Synapse Analytics
- C) Azure Data Lake Gen2
- D) Azure Databricks

Answer: B

Feedback(if correct):

Azure Synapse Analytics (Option B) is the correct selection. Azure Synapse Analytics aligns with the requirements for hosting the data warehouse, providing the necessary capabilities for data ingestion, preparation, management, and analytics. It also integrates with Spark for big data analysis and supports notebook development in Scala, R, and Python.

Feedback(if wrong):

- Option A (Azure AD): Azure Active Directory (Azure AD) is a cloud-based identity and access management service, which is not suitable for hosting a data warehouse or fulfilling the requirements stated in the scenario.
- Option C (Azure Data Lake Gen2): Azure Data Lake Gen2 is a scalable data lake solution for big data analytics and storage, but it does not provide the full capabilities required for hosting a data warehouse or supporting scheduled nightly data transfers.
- Option D (Azure Databricks): Azure Databricks is a managed Apache Spark-based analytics platform, but it is not specifically designed for hosting a data warehouse or handling scheduled data transfers. While it supports Spark for data analysis and notebook development, it does not offer the comprehensive data warehouse features needed in this scenario.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions (AZ305)

Subskill: Designing Data Platforms

Competency: Choosing the right Azure service to host a data warehouse based on specific business needs and requirements.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

67. Your organization aims to archive massive quantities of completed project documents, spanning across multiple disciplines, totaling less than 10 GB each. Due to legal obligations, these records must remain intact for seven years, with absolutely no modifications or deletions permitted within that time frame. Post-retention, they could potentially become obsolete and eligible for removal. Cost-efficient data storage is crucial, alongside negligible monitoring and minimal ongoing maintenance responsibilities.

Based on these requirements, which Azure storage account type and access tier should you recommend?

- A. General purpose v2 with Hot access tier for blobs
- B. General purpose v2 with Cool access tier for blobs
- C. General purpose v2 with Archive access tier for blobs
- D. Blob Storage with Hot access tier

Answer: C

Feedback(if correct):-

- General purpose v2 with Archive access tier for blobs is designed for data that needs to be stored long-term and accessed very infrequently. The Archive tier offers the lowest cost for storage, aligning with the need for cost-efficient data storage. It is ideal for scenarios where data must remain unaltered for a significant period, such as the seven-year retention period specified, with no modifications or deletions allowed. This tier's low cost and policy-driven immutability make it the optimal choice for archiving sensitive documents under the outlined legal obligations and operational considerations.

Feedback(if wrong):-

- A. General purpose v2 with a Hot access tier for blobs and D. Blob Storage with a Hot access tier are optimized for data that is accessed frequently, which incurs higher costs compared to the Cool and Archive tiers. These options do not align with the requirement for cost-efficient storage of data that will be accessed minimally.
- B. General purpose v2 with a Cool access tier for blobs offers a more cost-effective solution for infrequently accessed data compared to the Hot tier. However, it still does not provide the same level of cost efficiency as the Archive tier for data that does not require access over the retention period and fits the use case of long-term preservation with minimal access better.
- D. Blob Storage with Hot access tier: This option is not suitable because the Hot access tier is optimized for data that is accessed frequently, which incurs higher costs compared to the Cool and Archive tiers. Since the scenarios emphasize long-term storage with very infrequent access, the Hot tier would not be cost-efficient. Additionally, the Blob Storage account type does not inherently differentiate the necessity of the access tiers, as both General purpose v2 accounts and Blob Storage accounts can utilize Hot, Cool, and Archive tiers. The key is selecting the appropriate access tier based on the data access pattern and retention requirements.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms, Architecting for Business Continuity and Disaster Recovery

Competencies: Selecting appropriate Azure Storage tiers, applying data immutability policies

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

68. Your organization aims to archive massive quantities of completed project documents, spanning across multiple disciplines, totaling less than 10 GB each. Due to legal obligations, these records must remain intact for seven years, with absolutely no modifications or deletions permitted within that time frame. Post-retention, they could potentially become obsolete and eligible for removal. Cost-efficient data storage is crucial, alongside negligible monitoring and minimal ongoing maintenance responsibilities.

Continuing with the scenario for the Azure Storage solution, which configuration should be applied to ensure that once written, the data can only be read, and modifications and deletions are prevented for five years?

- A. Enable soft delete on the storage account
- B. Set the container access level to private
- C. Apply an Azure Blob storage immutability policy
- D. Implement a storage account resource lock

Answer: C

Feedback(if correct):-

C. Apply an Azure Blob storage immutability policy: This option directly addresses the requirement to prevent modifications and deletions of the data for a specified period (seven years in this scenario). Azure Blob Storage's immutability policy allows for the creation of time-based retention rules that enforce WORM (Write Once, Read Many) policies on the data, ensuring it remains unchanged for the duration of the retention period. This meets both the legal obligations for document preservation and the operational need for data immutability.

Applying an immutability policy within Azure Blob Storage is the most effective way to meet the stringent requirements for legal compliance, data preservation, and operational efficiency in this scenario.

Feedback(if wrong):-

- A. Enable soft delete on the storage account: While soft delete provides a way to recover data that has been accidentally deleted, it does not prevent modifications or ensure that data remains undeleted for a specific period.
- B. Set the container access level to private: Setting the access level to private restricts access to the data, which is essential for security, but it does not inherently enforce an immutability policy that prevents data from being modified or deleted.
- D. Implement a storage account resource lock: Resource locks can prevent accidental deletion or modification of the storage account itself but do not apply granular immutability policies to the data stored within Blob storage. Resource locks are more about managing deployment and management actions at the resource or resource group level.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms, Architecting for Business Continuity and Disaster Recovery

Competencies: Selecting appropriate Azure Storage tiers, applying data immutability policies

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

69. Your team is developing a cloud-native e-commerce platform on Azure, designed to integrate various services like product catalogs, customer profiles, order processing, and payment gateways. The architecture demands that these services communicate efficiently to exchange data regarding user activities, order status updates, and inventory levels. To ensure scalable and reliable inter-service communication, you need a mechanism that allows these components to exchange messages asynchronously, adhering to REST architectural principles. Which Azure service should you recommend to facilitate asynchronous communication between these cloud services using REST messages?

- A. Azure Service Bus
- B. Azure Blob Storage
- C. Azure Event Grid
- D. Azure AD

Answer: A

Feedback(if correct):-

Azure Service Bus is designed to support complex message brokering, including topics and subscriptions, queues, and reliable messaging patterns. It excels in scenarios requiring secure and transactional asynchronous communication between different cloud services, making it ideal for a distributed architecture like a cloud-native e-commerce platform. By utilizing Service Bus, you can ensure that messages related to user activities, order updates, and inventory changes are delivered reliably between services, even in the presence of transient faults or varying load conditions. Service Bus's support for REST-based communication further aligns with the need for a scalable and interoperable messaging solution within Azure's ecosystem.

Feedback(if wrong):-

- B. Azure Blob Storage is primarily used for storing large amounts of unstructured data and does not inherently support messaging or direct service-to-service communication patterns.
- C. Azure Event Grid focuses on event routing and is best for scenarios requiring reactive programming models to trigger actions in response to events. While it supports asynchronous communication, it does not offer the same level of messaging features as Service Bus for complex application flows.
- D. Azure AD is a cloud-based identity and access management service and does not facilitate inter-service messaging or data exchange within application architectures. It is unrelated to the requirement of enabling asynchronous communication between services in an e-commerce platform.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: - Understanding and applying Azure messaging services for inter-service communication, Knowledge of integrating various Azure services using asynchronous messaging patterns.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

70. Your organization is implementing a cloud solution to manage real-time sensor data from IoT devices deployed globally. The solution needs to efficiently route millions of events per day to downstream analytics services and must be capable of filtering, processing, and delivering these events in near real-time. To handle the high volume of events generated by IoT devices and ensure their efficient processing and delivery to analytics services, which Azure service is most appropriate?



- A. Azure Event Hubs
- B. Azure Queue Storage
- C. Azure Service Bus
- D. Azure IoT Hub

Answer: A

Feedback(if correct):-

Selecting Azure Service Bus for facilitating asynchronous communication between cloud services in a cloud-native e-commerce platform is correct because it provides a highly reliable and scalable messaging service that supports complex messaging patterns and protocols, including REST. Azure Service Bus is designed to ensure secure and orderly communication among distributed services, making it ideal for handling the exchange of data like user activities, order status updates, and inventory levels. Its support for queues, topics, and subscriptions allows for efficient decoupled communication across services, ensuring that the architecture remains scalable and resilient to changes and growth.

Feedback(if wrong):-

- B. Azure Blob Storage is primarily used for storing large amounts of unstructured data and does not inherently support messaging or direct service-to-service communication patterns.
- C. Azure Event Grid focuses on event routing and is best for scenarios requiring reactive programming models to trigger actions in response to events. While it supports asynchronous communication, it does not offer the same level of messaging features as Service Bus for complex application flows.
- D. Azure AD is a cloud-based identity and access management service and does not facilitate inter-service messaging or data exchange within application architectures. It is unrelated to the requirement of enabling asynchronous communication between services in an e-commerce platform.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: - Understanding and applying Azure messaging services for inter-service communication, Knowledge of integrating various Azure services using asynchronous messaging patterns.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

71. You are tasked with designing a database for a new application focused on aggregating content for users. The database must efficiently handle dynamic content updates and ensure that users experience minimal latency during read operations.

Requirements:

- Must support SQL commands for database operations.
- Capable of handling multi-master writes to facilitate concurrent updates from various sources.
- Guarantees low latency for read operations to ensure a seamless user experience.

Which database solution should you recommend that meets the above requirements?

- A. Azure Database for PostgreSQL
- B. Azure SQL Database that uses active geo-replication
- C. Azure SQL Database Hyperscale
- D. Azure Cosmos DB SQL API

Answer: D

Feedback(if correct):- Choosing Azure Cosmos DB SQL API is the correct decision because it uniquely meets all the specified requirements for the content aggregation application. It supports SQL for database operations, making it accessible to those familiar with SQL syntax. Its built-in capability for multi-master writes allows for concurrent updates from multiple sources, essential for dynamic content management. Moreover, Azure Cosmos DB's global distribution architecture guarantees low latency for read operations, providing a seamless user experience. This combination of features makes it exceptionally suited for applications requiring real-time data updates and fast content delivery.

Feedback(if wrong):- A. Azure Database for PostgreSQL and C. Azure SQL Database Hyperscale offer robust SQL support and scalability but lack native multi-master write capabilities required for real-time, concurrent content updates from various sources.

B. Azure SQL Database with active geo-replication provides high availability and disaster recovery features. However, it does not inherently support multi-master writes as seamlessly as Azure Cosmos DB, making it less effective for scenarios demanding immediate data consistency across global regions.

C. Azure SQL Database Hyperscale. Azure SQL Database Hyperscale offers significant scale and performance capabilities, supporting SQL commands and accommodating large volumes of data. However, it does not inherently provide multi-master write capabilities across globally distributed regions in the manner required by the application scenario.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Knowledge of Azure data storage options and their capabilities, particularly in designing solutions that require global distribution, low latency, and multi-master writes.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

72. You are tasked with configuring Azure Storage Accounts for two distinct applications, aiming to optimize them according to their specific performance and cost requirements, while ensuring data availability even in the event of a data center failure.

Requirements for Application1:

- Requires the highest possible transaction rates.
- Needs the lowest possible latency.
- Optimized for both uploads and downloads.
- Must remain available in the event of a data center failure.

For Application1, which Azure Storage Account configuration should you recommend?

- A. BlobStorage with Standard performance, Hot access tier, and Read-access geo-redundant storage (RA-GRS) replication
- B. BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication
- C. General purpose v1 with Premium performance and Locally-redundant storage (LRS) replication
- D. General purpose v2 with Standard performance, Hot access tier, and Locally-redundant storage (LRS) replication

Answer: B

Feedback (if Correct):

Selecting BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication is the correct decision for Application1. This choice caters to the application's need for the highest possible transaction rates and the lowest latency, essential for high-performance requirements. Premium performance ensures rapid access and processing speeds for both uploads and downloads, while ZRS replication maintains data availability across multiple data centers within the same Azure region, offering resilience in the event of a data center failure. This configuration strikes the optimal balance between performance and data durability for Application1.

Feedback (if Wrong):

- A. BlobStorage with Standard performance, Hot access tier, and Read-access geo-redundant storage (RA-GRS) replication provides geo-redundancy but does not meet the premium performance criteria required for high transaction rates and low latency.
- C. General purpose v1 with Premium performance and Locally-redundant storage (LRS) replication might offer premium performance but lacks the geographic redundancy of ZRS, making it less suitable for ensuring availability in the event of a data center failure.
- D. General purpose v2 with Standard performance, Hot access tier, and Locally-redundant storage (LRS) replication offers a balance of cost and performance but does not provide the premium performance level necessary for the lowest possible latency and highest transaction rates, nor does it ensure data center failure resilience as effectively as ZRS replication.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: - Understanding and applying Azure Storage options and access tiers based on application requirements. Configuring storage accounts for optimal performance, cost, and data availability.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

73. You are tasked with configuring Azure Storage Accounts for two distinct applications, aiming to optimize them according to their specific performance and cost requirements, while ensuring data availability even in the event of a data center failure. Application2 has different storage requirements focused on minimizing costs while still ensuring optimized uploads/downloads and availability during data center failures.

Requirements for Application2:

- Aim to minimize storage costs per GB.
- Optimized for both uploads and downloads.
- Must remain available in the event of a data center failure.

For Application2, which Azure Storage Account configuration should you recommend?

- A. BlobStorage with Standard performance, Cool access tier, and Geo-redundant storage (GRS) replication
- B. BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication
- C. General purpose v1 with Standard performance and Read-access geo-redundant storage (RA-GRS) replication
- D. General purpose v2 with Standard performance, Cool access tier, and Read-access geo-redundant storage (RA-GRS) replication

Answer: D.

Feedback if Correct:

Choosing General purpose v2 with Standard performance, Cool access tier, and Read-access geo-redundant storage (RA-GRS) replication is the most suitable option for Application2. This configuration is designed to minimize storage costs per GB, which aligns with the goal of cost reduction for Application2. The Cool access tier is specifically optimized for data that is infrequently accessed, offering lower storage costs while still facilitating optimized uploads and downloads. Additionally, the Read-access geo-redundant storage (RA-GRS) replication ensures that data remains available even in the event of a data center failure by replicating it across geographically dispersed regions for high availability and disaster recovery purposes.

Feedback if Wrong:

A. BlobStorage with Standard performance, Cool access tier, and Geo-redundant storage (GRS) replication offer cost savings and data redundancy, but RA-GRS provides better availability by allowing read access to the replicated data in the secondary location, which is crucial for maintaining availability during data center failures.

- B. BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication focuses on high-performance scenarios rather than minimizing costs and is therefore not the most cost-efficient option for Application2.
- C. General purpose v1 with Standard performance and Read-access geo-redundant storage (RA-GRS) replication could be a contender but general purpose v2 accounts offer a broader set of features and better cost efficiency for new deployments.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: - Understanding and applying Azure Storage options and access tiers based on application requirements. Configuring storage accounts for optimal performance, cost, and data availability.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

74. Your organization is developing a new version of a critical application, named App2, which heavily relies on data currently stored in on-premises Microsoft SQL Server databases. The details of these databases are as follows:

- DbA: 500 GB
- DbB: 200 GB
- DbC: 350 GB

The usage pattern of App2 and its data is unique, with the application being actively used only on the first Monday of each quarter. The data growth is projected to not exceed 2% annually. As part of the upgrade, App2 is being redeveloped as an Azure-based application, necessitating the migration of its databases to Azure SQL Database in a cost-efficient manner.

To migrate the databases of your organization's App2 to Azure SQL Database, while ensuring cost efficiency in line with the application's specific usage patterns and data growth expectations, which service tier is most appropriate?

- A. vCore-based Business Critical

- B. vCore-based General Purpose
- C. DTU-based Standard
- D. DTU-based Basic

Answer: C

Feedback(if correct):- For App2, the DTU-based Standard tier in Azure SQL Database stands out as the optimal choice, given its ability to accommodate databases of sizes up to 1 TB, which more than covers the sizes of DbA, DbB, and DbC, factoring in the modest 2% annual data growth. The DTU-based pricing model offers a balanced mix of compute, memory, and IO resources, tailored to App2's distinctive usage pattern that sees it being used intensely only once at the start of each quarter. This tier allows for efficient resource utilization and scaling according to the demand, ensuring that the service remains cost-effective without overspending on higher-tier resources that the application's workload doesn't justify. It provides the necessary performance and availability for App2's requirements while avoiding the higher costs associated with the vCore-based options, and it offers more resources and capabilities than the Basic tier, which is too restrictive in size and performance for this scenario.

Feedback if Wrong:

- A. vCore-based Business Critical: This tier is designed for workloads requiring the highest performance and lowest latency, which, given App2's infrequent usage, would likely result in unnecessary expense.
- B. vCore-based General Purpose: While offering a higher level of performance than the DTU-based options, this tier also comes at a higher cost, which may not be justifiable given the application's limited active usage.
- D. DTU-based Basic: The Basic tier is intended for small, lightweight workloads. Given the size of the databases and the potentially moderate to high workload on the first Monday of each quarter, the Basic tier might not provide sufficient resources, potentially leading to performance issues.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Knowledge of Azure SQL Database service tiers and their respective capabilities and costs, strategic planning for data migration with a focus on efficiency and cost-effectiveness.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application



75. You are tasked with designing a highly available Azure SQL Database solution that adheres to the following critical requirements:

- Failover between replicas of the database must occur without any data loss.
- Highest levels of performance, availability, and rapid failover capabilities without data loss

Considering these requirements, the focus is on ensuring high availability, data durability during failovers, and cost efficiency.

Given the need for zero data loss failover, zone redundancy for outage resilience, and cost efficiency, which Azure SQL Database deployment option best meets these criteria?

- A. Azure SQL Database General Purpose with Zone Redundant Configuration
- B. Azure SQL Database Managed Instance Business Critical
- C. Azure SQL Database Hyperscale
- D. Azure SQL Database Business Critical

Answer: D

Feedback(if Correct):

Selecting Azure SQL Database Business Critical is the most suitable choice under these conditions because it provides the highest performance due to its in-memory technologies, ensuring rapid processing and minimal latency. The Business Critical tier is designed for applications that require fast failover capabilities and guarantees zero data loss during failover events, which aligns with the need for immediate failover without compromising data integrity. Moreover, it supports zone redundancy, which is crucial for maintaining availability in the event of a zone outage, thus meeting the requirement for resilience against regional disruptions.

Feedback if Wrong:

- A. Azure SQL Database General Purpose with Zone Redundant Configuration offers zone redundancy and cost efficiency but does not match the Business Critical tier in terms of performance and rapid failover capabilities, which are essential for the stated requirements.
- B. Azure SQL Database Managed Instance Business Critical provides similar benefits in terms of performance and availability as the Business Critical service tier but in a managed instance model, which might not be the best fit depending on the specific architecture and operational preferences of the solution.
- C. Azure SQL Database Hyperscale is optimized for scalability and large databases, offering rapid scale-out and scale-up capabilities. While it provides excellent performance for large workloads, its primary

focus isn't on the same level of failover capabilities and in-memory performance optimization found in the Business Critical tier.

skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Select appropriate Azure SQL Database tiers for specific workload requirements focusing on availability, performance, and disaster recovery. Implementing high availability and disaster recovery strategies in Azure SQL databases, including understanding zone redundant configurations and failover capabilities.

Difficulty Level: Expert

Bloom's Taxonomy Level: Application

76. Your organization has been leveraging Azure Cosmos DB for storing operational data that are critical for day-to-day business functions. This data is updated continuously to reflect real-time business operations. To derive insights and enhance decision-making, there's a requirement to perform daily analysis on this operational data using Azure Synapse Analytics. The challenge is to accomplish this without impacting the performance of the operational data store in Azure Cosmos DB, ensuring that business operations remain unaffected by the analytics processes. Devise a solution that allows for daily analysis of operational data stored in Azure Cosmos DB using Azure Synapse Analytics, prioritizing the operational store's performance. To conduct daily analytics on the operational data from Azure Cosmos DB SQL API account using Azure Synapse Analytics, while ensuring the performance of the operational data store remains unaffected, which solution is most appropriate?

- A. Utilize Azure Cosmos DB change feed.
- B. Activate Azure Synapse Link for Azure Cosmos DB.
- C. Employ Azure Synapse Analytics with PolyBase for data loading.
- D. Implement Azure HDInsight for both Azure Cosmos DB and Azure Synapse Analytics.

Answer: B

Feedback(if correct):-

Azure Synapse Link for Azure Cosmos DB is the optimal solution for this scenario. It provides a seamless integration between Azure Cosmos DB and Azure Synapse Analytics, enabling near-real-time analytics over operational data without impacting the performance of the operational database. Synapse Link creates a tight coupling between these services, allowing for analytical store capabilities within Azure Cosmos DB. This means that operational workloads can continue unaffected while analytics processes run concurrently on the same data, ensuring that the analytics do not impact the transactional workload's performance.

Feedback if Wrong:

- A. Utilize Azure Cosmos DB change feed: While the change feed can be used to listen for changes in Azure Cosmos DB and process them, it's not specifically designed for analytics workloads and would require additional components or services to perform analytics, potentially affecting performance.
- C. Employ Azure Synapse Analytics with PolyBase for data loading: PolyBase is a technology that allows for SQL querying across relational and non-relational databases. While it's a powerful tool within Synapse Analytics for integrating data, it doesn't inherently solve the performance impact on the operational store that Synapse Link is designed to address.
- D. Implement Azure HDInsight for both Azure Cosmos DB and Azure Synapse Analytics: Azure HDInsight is a cloud service for processing big data in Hadoop, Spark, and other open-source frameworks. Although it's capable of processing large datasets, it's not as directly applicable to this scenario as Synapse Link, which specifically addresses the need for real-time analytics on operational data without performance degradation.

skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Select appropriate Azure SQL Database tiers for specific workload requirements focusing on availability, performance, and disaster recovery. Implementing high availability and disaster recovery strategies in Azure SQL databases, including understanding zone redundant configurations and failover capabilities.

Difficulty Level: Expert

Bloom's Taxonomy Level: Application

77. You are developing a sales application that will encompass several Azure cloud services to handle different components of a transaction such as processing customer orders, billing, payment inventory, and shipping. The sales application is composed of multiple

microservices that need to be developed, deployed and managed independently. To facilitate asynchronous communication of transaction information using XML messages among these cloud services, what should you include in the recommendation?

- A) Azure Data Lake
- B) Azure Blob Storage
- C) Azure Queue Storage
- D) Azure Service Fabric

Answer: C

Feedback(if correct):

Azure Queue Storage is ideal for asynchronous communication between different components of an application, making it suitable for transmitting transaction information in XML format.

Feedback(if wrong):

- A) Azure Data Lake: Azure Data Lake is optimized for big data analytics and is best suited for storing and analyzing large volumes of data. It's not primarily designed for messaging or communication between microservices.
- B) Azure Blob Storage: While Azure Blob Storage is excellent for storing large amounts of unstructured data, such as text or binary data, it is not specifically designed for messaging or ensuring message delivery and retrieval in the asynchronous communication patterns required by microservices.
- D) Azure Service Fabric: Azure Service Fabric is a distributed systems platform that makes it easy to package, deploy, and manage scalable and reliable microservices and containers. Although it supports microservices development and management, it doesn't inherently provide a messaging system for asynchronous communication between those microservices.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Designing Compute and Network Infrastructure

- Competencies: Decision-Making, Solution Design
- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Application

78. You have an Azure subscription that contains the Virtual Machines (VMs) shown in the following table.

Resource Group	Location	Name	Size
AZRG1	East US	VM1	Standard
AZRG2	West US	VM2	Standard
AZRG3	Central US	VM3	Standard

The subscription also includes the storage accounts listed in the following table.

Name	Resource Group	Location	Account kind
st1	AZRG1	East US	StorageV2 (general purposev2)
st2	AZRG2	Central US	BlobStorage
st3	AZRG3	West US	StorageV2 (general purposev2)

You enable auditing for the VMs, and each audit needs to be stored in the corresponding storage account. Which of the following statements is true?

Statements

1. When you enable auditing for VM1, you can store audit information to st1.
2. When you enable auditing for VM2, you can store audit information to st2.
3. When you enable auditing for VM3, you can store audit information in st3.

- A) Yes, No, No
- B) Yes, Yes, No
- C) No, Yes, No



D) Yes, No, Yes

Answer: A

Feedback(if correct):

Option A) Yes, No, No:

Statement 1: Yes, audit information for VM1 can be stored in st1, which aligns with the scenario.

Statement 2: No, audit information for VM2 cannot be stored in st2, as it contradicts the scenario.

Statement 3: No, audit information for VM3 cannot be stored in st3, as it contradicts the scenario.

Feedback(if wrong):

Option B) Yes, Yes, No:

Statement 1: Yes, audit information for VM1 can be stored in st1, which aligns with the scenario.

Statement 2: Yes, audit information for VM2 can be stored in st2, which contradicts the scenario.

Statement 3: No, audit information for VM3 cannot be stored in st3, as it contradicts the scenario.

Option C) No, Yes, No:

Statement 1: No, audit information for VM1 cannot be stored in st1, which contradicts the scenario.

Statement 2: Yes, audit information for VM2 can be stored in st2, which contradicts the scenario.

Statement 3: No, audit information for VM3 cannot be stored in st3, as it contradicts the scenario.

Option D) Yes, No, Yes:

Statement 1: Yes, audit information for VM1 can be stored in st1, which aligns with the scenario.

Statement 2: No, audit information for VM2 cannot be stored in st3, which aligns with the scenario.

Statement 3: Yes, audit information for VM3 can be stored in st3, which contradicts the scenario.

skill map:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Compute and Network Infrastructure

Competency: Analytical Thinking and Problem Solving

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

79. You're tasked with designing an Azure infrastructure for a company planning to deploy several Azure App Service instances alongside Azure SQL databases. The company has a regulatory obligation to confine the App Service instances to specific Azure regions, ensuring that all resources are located within the same region. Your suggestion involves creating location-specific resource groups and implementing resource locks on these groups. Does this approach adhere to the regulatory requirement?

A) Yes

B) No

Answer: B

Feedback(if correct): The correct selection is B) No. While creating location-specific resource groups and implementing resource locks can restrict changes to resources, it does not guarantee that the App Service instances will be deployed only to specific Azure regions. Therefore, this approach does not fully adhere to the regulatory requirement.

Feedback(if wrong): This option is incorrect because the approach described does not meet the regulatory requirement of confining the App Service instances to specific Azure regions. While resource locks prevent changes to resources, they do not enforce deployment restrictions based on region. Therefore, the correct answer is B) No.

Skill mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Compute and Network Infrastructure

Competency: Planning and Implementing Azure Virtual Networks

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Synthesis

80. You're tasked with designing an Azure infrastructure for a company planning to deploy several Azure App Service instances alongside Azure SQL databases. The company has a regulatory obligation to confine the App Service instances to specific Azure regions,

ensuring that all resources are located within the same region. Your suggestion involves creating and applying Azure Policies that enforce deployment restrictions based on specific Azure regions, you can ensure that the App Service instances are deployed only to the required regions.

A) Yes

B) No

Answer: A

Feedback(if correct): The correct selection is A) Yes. By applying Azure Policies that enforce deployment restrictions based on specific Azure regions, the regulatory requirement to confine the App Service instances to specific regions is met.

Feedback(if wrong): The wrong selection is B) No. This option is incorrect because implementing Azure Policies to enforce deployment restrictions based on specific Azure regions is an effective way to meet the regulatory requirement. Therefore, the correct answer is A) Yes.

skill mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Compute and Network Infrastructure

Competency: Planning and Implementing Azure Virtual Networks

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Synthesis

81. Your organization has developed a cloud-based application hosted on Azure Virtual Machines (VMs). This application includes both frontend and backend components, with the backend service designed to be accessible exclusively by certain VMs within the organization. External partners are also required to access the frontend service over the Internet. The VM deployment configuration is as follows:

- VM1: Hosts part of the backend service.
- Virtual Network: VNet1
- Subnet: BackendSubnet



- VM2: Hosts the frontend service.
- Virtual Network: VNet2
- Subnet: FrontendSubnet
- An Azure API Management (APIM) service is deployed to manage access to these services with the following setup:
 - Location: East US
 - Integrated into VNet2 on the FrontendSubnet

Given this setup, evaluate the following statements:

1. The backend service is effectively restricted to be accessible only by VM1 and an unspecified VM3.
2. The frontend service on VM2 is configured to allow external partners access over the Internet.
3. The Azure API Management service can directly access real-time data from VM1 for management and routing purposes.

Select the correct combination of True (Yes) or False (No) for these statements:

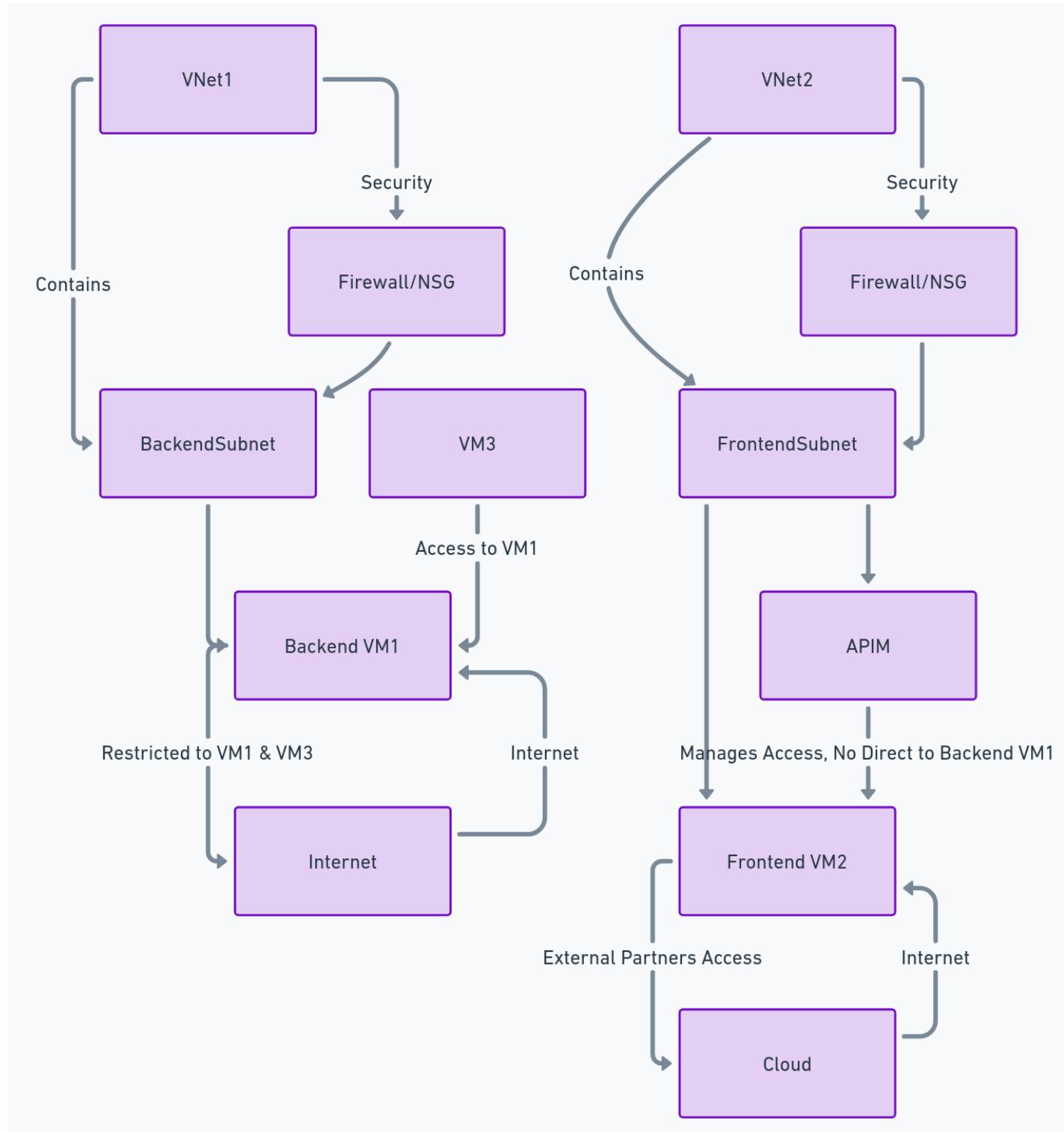
- A) Yes, Yes, No
- B) No, Yes, Yes
- C) Yes, No, No
- D) No, No, Yes

Answer: A

Feedback (if Correct):

- The backend service being accessible only from VM1 and VM3 implies proper network security controls and routing configurations are in place within VNet1 and potentially across VNet peering if VM3 is in a different VNet, ensuring restricted access as per the organization's policy.
- The frontend service on VM2 being accessible to external partners over the Internet indicates that public IP assignments, network security group (NSG) rules, and possibly Azure API Management configurations are correctly set up in VNet2 to allow inbound internet traffic to reach the frontend service.
- The Azure API Management instance's inability to access real-time data from VM1 directly relates to the network segmentation and security boundaries between VNet1 (BackendSubnet) and VNet2

(FrontendSubnet). Unless a specific networking and service endpoint configuration is enabling APIM to communicate with resources in VNet1, it would not have direct access to real-time data from VM1, especially if APIM is intended to manage frontend access primarily.



Feedback (if Wrong):

Option B (No, Yes, Yes)

Incorrect Assumption: This option assumes the backend service isn't restricted and can be accessed by any VM within the organization. While VM1 likely has access by default within VNet1, additional configuration is needed (like NSGs) to restrict access further as per the scenario requirement.

Correct Understanding: Access to the frontend service over the internet through APIM is accurate, aligning with its intended role as a public gateway.

Option C (Yes, No, No)

Incorrect Assumption: This option assumes the backend service is restricted only by being in VNet1, but doesn't consider additional control mechanisms. NSGs within VNet1 likely control access further, restricting it to authorized sources like VM1 and potentially VM3.

Incorrect Assumption: Similar to Option B, this choice denies APIM access to VM1 data, which might be a requirement depending on APIM's specific role. However, without VNet peering or other configurations, direct access wouldn't be possible due to VNet separation.

Option D (No, No, Yes)

Incorrect Assumption: Both options B and D underestimate the security implications of separate VNets. Without additional configuration, resources in VNet1 (backend service) and VNet2 (frontend service and APIM) wouldn't be able to communicate directly.

Incorrect Conclusion: While APIM might be configured to manage access to the frontend service, direct access to VM1 data wouldn't be possible due to network segmentation, unless specifically configured for such communication.

Common Misunderstandings:

These incorrect options might reflect misunderstandings about:

Network Security Groups (NSGs): Their role in controlling traffic flow within and between VNets.

VNet Peering: How it facilitates secure communication across VNets if required.

Azure API Management (APIM): Its intended role as a gateway and potential need for access to backend service data depending on its configuration.

By understanding these concepts, a clearer picture emerges of how network segmentation, security controls, and service placement combine to achieve secure and controlled access within the Azure environment.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskill: Designing Compute and Network Infrastructure

Competency: Expertise in implementing Azure networking solutions like Azure Traffic Manager for DNS-level traffic distribution to enhance global connectivity and application performance.

Difficulty Level: Expert

Bloom's Taxonomy Level: Analysis

82. Your organization has a hybrid environment with workloads running on Azure and on-premises servers. You've noticed significant latency in the application's response times, affecting user experience. Your current setup includes Azure Virtual Network and VPN Gateway for connectivity.

Solution: Deploy Azure Application Gateway with Web Application Firewall (WAF) enabled, and use its performance monitoring and diagnostic capabilities to identify and mitigate the latency issues.

Does this solution meet the goal of reducing latency and improving application response times?

A. Yes

B. No

Answer: B

Feedback(if correct):-

Here's why deploying Azure Application Gateway with WAF enabled wouldn't directly address the latency issue in this scenario:

Application Gateway Functionality: While Application Gateway offers various benefits like load balancing, traffic management, and security through WAF, its primary focus is not latency reduction. It might even introduce some additional processing overhead depending on the configuration.

Root Cause of Latency: The scenario describes significant latency between Azure and on-premises resources. The current setup using Azure Virtual Network and VPN Gateway is a potential culprit for the latency. VPN connections typically have higher latency compared to direct connections within Azure.

Some alternative Solutions for Latency Reduction:

Azure ExpressRoute: Consider establishing a dedicated private connection between your on-premises network and Azure using ExpressRoute. This can significantly reduce latency compared to VPN connections.

Optimize Azure Virtual Network Peering: If feasible, configure virtual network peering between your Azure virtual networks where your application components reside. This can further minimize latency within Azure.

Application Performance Analysis: Utilize Azure Application Insights or similar tools to analyze application performance and identify specific bottlenecks. This can help pinpoint areas within your application that could be optimized to improve response times.

While Application Gateway can be a valuable addition to your architecture for future enhancements, it wouldn't directly address the current latency issue related to the VPN connection between Azure and your on-premises environment.

Feedback(if wrong):-

Selecting "Yes" suggests a misconception that Azure Application Gateway with Web Application Firewall (WAF) directly mitigates network latency issues in a hybrid environment. While Azure Application Gateway can improve security and manage HTTP-based traffic more efficiently, its primary function is not to enhance network connectivity or reduce latency between Azure and on-premises servers. Its performance monitoring and diagnostic capabilities are valuable for identifying and addressing web application-level issues rather than optimizing network paths or reducing network latency. For latency concerns, especially in hybrid environments, focusing on network architecture and connectivity solutions, like optimizing VPN configurations or considering Azure ExpressRoute, would be more effective.

Skill Mapping:

Skills: Designing Azure Infrastructure Solutions (AZ-305)

Subskills: Designing Compute and Network Infrastructure

Competencies: Proficient use of Azure Network Watcher for network traffic analysis.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

83. Your organization utilizes a hybrid cloud setup, with numerous virtual machines (VMs) deployed both on-premises and in Azure. You have Azure ExpressRoute in place to facilitate connectivity between your on-premises infrastructure and Azure services. Recently, some VMs have started facing intermittent network connectivity issues.

Scenario: To diagnose these network issues, you need a method to inspect the network traffic flowing to and from these VMs, specifically to identify if the network traffic is being blocked or allowed.

Solution: Implement Azure Network Watcher's IP flow verify feature to examine the network traffic to the VMs.

Does this solution meet the goal of identifying whether the network packets to the VMs are being allowed or denied?

- A. Yes
- B. No

Answer: A

Feedback(if correct):-

Azure Network Watcher's IP flow verify feature is precisely designed to analyze and diagnose network traffic issues to and from Azure VMs. It allows administrators to verify inbound and outbound network traffic rules, identifying whether packets are being allowed or denied by network security groups (NSGs) or other network filters. This tool is essential for troubleshooting connectivity problems in Azure and hybrid environments, making it an appropriate solution for diagnosing the intermittent network connectivity issues faced by VMs in this scenario. By using IP flow verification, you can determine if specific network traffic is being blocked or allowed, which is critical for resolving the network connectivity issues experienced by the VMs.

Feedback(if wrong):-

Selecting "No" might indicate a misunderstanding of Azure Network Watcher's capabilities or how network traffic analysis tools can be applied to troubleshoot connectivity problems. Azure Network Watcher's IP flow verify feature is specifically designed to provide insights into network traffic rules affecting Azure VMs, allowing users to check if specific network traffic is being allowed or denied based on the existing network security configurations. This makes it an effective tool for identifying and diagnosing the root causes of network connectivity issues within Azure and hybrid cloud environments. Utilizing IP flow verification enables administrators to efficiently determine the status of network packets—whether they are being permitted or blocked by network security groups (NSGs) or firewall rules—thereby directly addressing the need to analyze network traffic and resolve the VMs' intermittent connectivity issues.



Skill Mapping:

Skills: Designing Azure Infrastructure Solutions (AZ-305)

Subskills: Designing Compute and Network Infrastructure

Competencies: Proficient use of Azure Network Watcher for network traffic analysis.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

84. Your company operates an Azure Web App hosted by the Premium App Service Plan. A development team will use the Azure Web App, and you need to arrange the following actions for the setup:

1. Switch the web app from the current version to a newer version
2. Test newer versions of the application before transitioning
3. Roll back the application version if needed
4. Reduce downtime

Please choose the corresponding action from the given options:

- A. Creating a separate App Service Plan
- B. Use Azure App manager
- C. Leveraging deployment slots
- D. Backup restoration

Answer: C

Feedback(if correct):-

Deployment slots are the correct choice for managing web application versions on Azure App Service. They allow for testing new versions in a production-like environment, seamless transitioning between versions with minimal downtime, and easy rollback to previous versions if necessary. Deployment slots offer a robust solution for continuous deployment and version management without the need for additional resources or complex backup and restore processes.

Feedback(if wrong):-

Creating a separate App Service Plan is not the most efficient method for version management as it introduces additional costs and complexity without directly supporting version testing or easy rollbacks.

Use Azure App Manager does not refer to a specific Azure service designed for version testing and management, indicating a possible confusion with other Azure services or features.

Backup restoration is primarily useful for disaster recovery rather than as a method for regular version testing and updates. It does not facilitate the testing of new versions in a production-like environment or allow for quick rollbacks with minimal downtime.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Implementing and managing web applications on Azure App Service, Utilizing deployment slots in Azure Web Apps for staging and production environments.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

85. You are tasked with configuring the storage for a high-performance application hosted on Azure.

The deployment includes SQL Server 2016 running on two virtual machines. These machines are deployed in different data centers within the same Azure region and are part of an Always On availability group. Given the storage priority for speed and availability, which of the following storage types should you recommend for the operating system and databases?

- A. Geo-redundant storage (GRS) account
- B. Locally-redundant storage (LRS) account
- C. Premium managed disk
- D. Standard managed disk

Answer: C.

Feedback if Correct:

Choosing Premium managed disks is the correct decision for configuring storage for a high-performance application's operating system and databases on Azure. Premium managed disks are specifically designed to provide high IOPS (Input/Output Operations Per Second) and low-latency disk performance, which are critical for the demanding nature of SQL Server workloads and ensuring the operating system's efficiency. This selection aligns with the need for speed and availability, as premium disks offer persistent, high-performance storage necessary to support the robust operation of database applications within an Always On availability group.

Feedback if Wrong:

- A. Geo-redundant storage (GRS) account offers data replication across multiple regions for high availability, but it does not address the direct need for high IOPS and low latency for the operating system and databases.
- B. Locally redundant storage (LRS) account provides data redundancy within a single region but still falls short in delivering the performance level required by high-transaction SQL Server applications.
- D. Standard managed disk offers a cost-effective storage solution with lower performance compared to premium disks, making it unsuitable for scenarios demanding high-speed and highly available database operations.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Knowledge in selecting the appropriate Azure storage options based on performance, availability, and application requirements. Understanding how to optimize SQL Server deployments on Azure VMs for high performance.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

86. You are tasked with configuring the storage for a high-performance application hosted on Azure. The deployment includes SQL Server 2016 running on two virtual machines. These machines are deployed in different data centers within the same Azure region and are part of an Always On availability group. Continuing with the setup of a high-performance application on Azure, you need to ensure the SQL Server data is backed up using the Automated Backup feature of the SQL Server IaaS Agent Extension (SQLIaaSExtension). Considering the priority for the lowest cost in storage for backups, which of the following options should you choose?

- A. Geo-redundant storage (GRS) account
- B. Locally-redundant storage (LRS) account
- C. Premium Managed Disk
- D. Standard Managed Disk

Answer: D

Feedback (if Correct):

Selecting Standard Managed Disks for backup storage is the correct approach when the main objective is to minimize costs. Standard managed disks are specifically designed to offer a more cost-effective solution for data storage needs that do not require the high throughput or low latency provided by premium managed disks. For backups, especially SQL Server data backups utilizing the Automated Backup feature of the SQL Server IaaS Agent Extension, high-speed access is typically not a requirement. Therefore, standard managed disks strike the perfect balance between cost efficiency and the necessary reliability for storing backups, ensuring that data is protected without incurring unnecessary expenses.

Feedback (if Wrong):

- A. Geo-redundant storage (GRS) account offers high availability and data durability by replicating data to another region. While it provides enhanced data protection, it is more expensive than standard managed disks, making it less optimal for scenarios where cost minimization is crucial.
- B. Locally redundant storage (LRS) account replicates data within a single data center. It's cost-effective but still typically more expensive than standard managed disks for backup purposes.
- C. Premium managed disk delivers high performance with low latency, suited for I/O-intensive applications rather than cost-effective backup storage.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Knowledge in selecting the appropriate Azure storage options based on performance, availability, and application requirements. Understanding how to optimize SQL Server deployments on Azure VMs for high performance.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

87. Your organization operates a hybrid cloud environment with multiple virtual machines (VMs) both on-premises and in Azure, utilizing Azure ExpressRoute for seamless connectivity between these environments. Recently, some VMs have started experiencing network connectivity issues, necessitating a thorough investigation to ensure optimal performance and reliability.

To address these connectivity issues, you are considering a strategy to effectively monitor and analyze network traffic to and from these VMs. This will help in identifying whether the network packets are being successfully transmitted or if any are being blocked, thus pinpointing the root cause of the connectivity problems.

You are planning the deployment of the Microsoft Monitoring Agent and the Dependency Agent across all affected VMs. The intention is to leverage the Wire Data solution within Azure Monitor as a means to scrutinize the network traffic patterns and identify any anomalies that could be contributing to the connectivity issues.

Given the need to accurately determine the status of network packets to these VMs and identify potential blockages, will installing and configuring the Microsoft Monitoring Agent and the Dependency Agent on all VMs, followed by utilizing the Wire Data solution in Azure Monitor for traffic analysis, effectively meet this objective?

A. Yes

B. No

Answer: B

Feedback(if correct):- While installing the Microsoft Monitoring Agent and the Dependency Agent, followed by utilizing the Wire Data solution in Azure Monitor, provides valuable insights into network traffic and dependencies among various resources, it may not directly address the specific need to analyze network traffic to determine whether packets are being allowed or denied to the VMs in question. This approach is more suited for understanding general network behavior and dependencies rather than providing a detailed analysis of packet-level network security rules and their enforcement. For the precise task of analyzing network traffic to determine packet allowance or denial, tools and features specifically designed for network security analysis, such as Azure Network Watcher's IP flow verify feature, would be more appropriate and effective in meeting the stated goal.

Feedback if Wrong:

Selecting "Yes" suggests that installing and configuring the Microsoft Monitoring Agent and the Dependency Agent on all VMs, combined with using the Wire Data solution in Azure Monitor, would effectively analyze network traffic to determine packet flow to the VMs. However, this approach does not directly address the specific requirement of analyzing network traffic to determine whether packets

are being allowed or denied to the VMs in the context of connectivity issues related to Azure ExpressRoute.

The Microsoft Monitoring Agent and Dependency Agent provide valuable insights into application dependencies and performance metrics, but they are not primarily focused on the network security posture or the allow/deny the status of network traffic at the level of network security groups or Azure Firewall rules, which are more directly involved in the decision process for allowing or denying packets.

The Wire Data solution in Azure Monitor offers detailed network protocol activity across your Azure and on-premises environments, but it is more geared towards performance monitoring and troubleshooting rather than security analysis of allowed or denied packets specifically related to Azure ExpressRoute connectivity issues.

For analyzing whether packets are being allowed or denied specifically, tools and services like Azure Network Watcher, especially its IP flow verify feature, are more directly suited to this task. These tools can provide detailed information on network security groups and firewall rules, showing exactly how and why packets are allowed or denied, which is essential for troubleshooting the stated connectivity issues.

The focus should be on utilizing Azure services that directly analyze network security configurations and their impact on traffic flow, such as Azure Network Watcher's IP flow verification, to address the scenario's needs.

skill mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Compute and Network Infrastructure

Competency: Planning and Implementing Azure Virtual Networks

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Synthesis

88. Your company utilizes several virtual machines (VMs) deployed both on-premises and within Azure. To facilitate on-premises to Azure connectivity, Azure ExpressRoute has been established. However, you've noticed network connectivity issues affecting several VMs.

You are tasked with analyzing the network traffic to identify whether packets to the VMs are being allowed or denied, aiming to pinpoint the root cause of the connectivity issues observed.

Install and configure Azure Network Watcher in your Azure subscription. Utilize the IP flow verify feature within Azure Network Watcher to examine the network traffic rules affecting packet flow to and from the VMs.

Does utilizing Azure Network Watcher, specifically its IP flow verify feature, meet the goal of determining whether packets are being allowed or denied to the VMs to the Azure ExpressRoute connectivity issues?

A. Yes

B. No

Answer: A

Feedback (if Correct):

Choosing Azure Network Watcher with the IP flow verify feature is the correct solution for this scenario. Azure Network Watcher provides advanced monitoring, diagnostic, and visualization tools to better understand network performance and health. The IP flow verify feature specifically allows you to test a packet's journey from a source to a destination, showing you whether it's allowed or denied based on the current network security group and firewall configurations. This capability is essential for troubleshooting the network connectivity issues observed with the VMs connected via Azure ExpressRoute, as it directly addresses the need to analyze network traffic rules and their impact on connectivity.

This adjustment ensures the solution directly aligns with the troubleshooting requirements presented by the scenario, providing a clear and accurate method to achieve the goal of analyzing network traffic concerning Azure ExpressRoute connectivity issues.

Feedback (if Wrong):

Choosing any solution other than Azure Network Watcher, particularly its IP flow verify feature, for analyzing whether packets are being allowed or denied to the VMs would be incorrect under the given scenario for the following reasons:

- B. No: Selecting this option implies that utilizing Azure Network Watcher and its IP flow verify feature does not meet the requirement of determining the allow/deny status of network traffic to VMs, which is inaccurate. Azure Network Watcher is specifically designed for monitoring, diagnosing, and gaining insights into network traffic and security rules affecting Azure resources. The IP flow verify feature is a critical tool for troubleshooting connectivity issues, as it provides a detailed analysis of how network security rules are applied to traffic, effectively identifying blocked or allowed connections.
- If the proposed solution involved tools or features other than Azure Network Watcher's IP flow verification, such as general-purpose monitoring solutions without specific capabilities to analyze network security rules, it would not effectively address the precise requirement of identifying allowed or denied packet flows due to network security configurations.
- Utilizing general monitoring agents, dependency agents, or data collection methods that do not specifically analyze network security rules and their impact on traffic flow may offer valuable insights into network performance and dependencies but fall short in diagnosing security rule enforcement's direct effect on packet flow, which is essential for resolving the described connectivity issues.

- The correct approach involves leveraging Azure's dedicated network diagnostic tools that provide targeted insights into network security and connectivity, ensuring that the analysis directly informs on the security posture and its operational impact, as required in the scenario.

skill mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Compute and Network Infrastructure

Competency: Planning and Implementing Azure Virtual Networks

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Synthesis

89. Your organization is optimizing network traffic management for a critical application, App1. As part of this effort, you're considering Azure Traffic Manager to enhance global connectivity and performance. Determining the minimal deployment necessary is key to ensuring the service effectively supports App1's traffic management requirements without excess resource allocation. What is the least number of Azure Traffic Manager configurations required to support effective traffic management for App1?

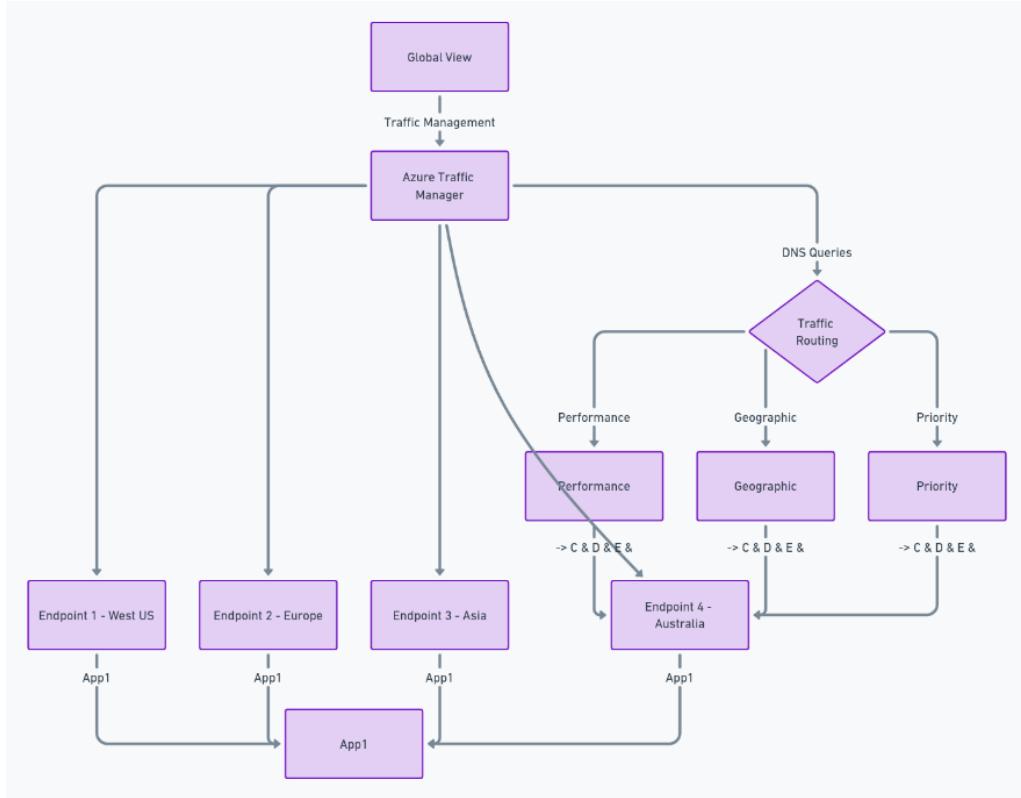
- A. 0
- B. 1
- C. 2
- D. 3

Answer: B

Feedback (if Correct):

The correct answer, option B, signifies that only one Azure Traffic Manager configuration is required to effectively manage network traffic for App1. This is because Azure Traffic Manager is a global DNS-based load-balancing service that enables you to distribute traffic optimally across various service endpoints. A single Traffic Manager profile can define multiple endpoints along with the traffic-routing method to use, such as performance, geographic, or priority-based routing. This setup ensures App1 remains highly available and performs optimally for users worldwide, without the need for multiple Traffic Manager

configurations. Thus, establishing one Traffic Manager profile suffices to meet the application's global connectivity and performance enhancement goals.



Feedback (if Wrong):

A. 0: Suggests that no Azure Traffic Manager configuration is needed, which is incorrect because, without Traffic Manager, you miss the benefits of DNS-level traffic distribution and the enhancement of global connectivity and performance for App1.

C. 2 & D. 3: Indicate that more than one Traffic Manager configuration is necessary. This is unnecessary and misaligned with how Traffic Manager is designed to function. Azure Traffic Manager's single profile can manage multiple endpoints and does not require multiple configurations to be effective.

Implementing more than one profile for a single application scenario could complicate traffic management without offering additional benefits, contrary to the goal of minimizing resource allocation while ensuring effective support for App1's traffic management requirements.

skill mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Compute and Network Infrastructure

Competency: Azure Application Gateway

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Synthesis

90. Your organization is optimizing network traffic management for a critical application, App1. As part of this effort, you're considering Azure Traffic Manager to enhance global connectivity and performance. Determining the minimal deployment necessary is key to ensuring the service effectively supports App1's traffic management requirements without excess resource allocation.

Continuing your effort to enhance App1's connectivity and reliability, you're now focusing on Azure Application Gateway for secure application delivery. The goal is to determine the minimal number of Application Gateway instances necessary to ensure high availability and fault tolerance for App1's users.

To guarantee high availability for App1 through Azure Application Gateway, what is the minimum number of instances that must be deployed?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: B

Feedback (if correct)

The minimum number of Azure Application Gateway instances required to ensure high availability for App1 is 2. This is because Azure Application Gateway utilizes an internal mechanism for automatic failover and load distribution among instances. Deploying two instances ensures that if one instance faces downtime due to maintenance or unexpected issues, the other instance can seamlessly take over, maintaining uninterrupted access to App1 for users. This setup provides the necessary fault tolerance and redundancy to meet high availability demands.

Feedback (if Wrong):

A. 1: Deploying a single instance of Azure Application Gateway would not suffice for high availability. If this lone instance goes down, it would result in App1 becoming inaccessible, thus failing to meet the high availability requirement.

C. 3 and D. 4: While deploying three or four instances could potentially increase fault tolerance and the ability to handle more traffic, it exceeds the minimum requirement necessary to achieve high availability. The question specifically asks for the minimum number of instances required, making options C and D incorrect for this scenario. Deploying more than two instances without a corresponding need could lead

to unnecessary complexity and increased costs without proportionate benefits in terms of availability or performance for App1.

skill mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Compute and Network Infrastructure

Competency: Azure Application Gateway

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Synthesis

91. You are leading the design of a microservices architecture for a web application. The solution must meet the following requirements:

Allow independent upgrades to each microservice

Deploy the solution both on-premises and to Azure

Set policies for performing automatic repairs to the microservices

Support low-latency and hyper-scale operations

Which technology should you recommend?

- A) Azure Service Fabric
- B) Azure Kubernetes Service (AKS)
- C) Azure Functions
- D) Azure App Service

Answer: A

Feedback(if correct):

Azure Service Fabric is a distributed systems platform that allows developers to easily build and deploy microservices-based applications. It supports independent upgrades to each microservice, deployment

both on-premises and to Azure, policy-based automatic repairs and provides low latency and hyperscale operations.

Feedback(if wrong):

- B) Azure Kubernetes Service (AKS) While AKS is a managed Kubernetes service that supports containerized applications, it may not provide native support for independent upgrades to microservices or policy-based automatic repairs.
- C) Azure Functions Azure Functions is a serverless compute service that allows you to run event-triggered code without managing infrastructure. However, it may not be the best choice for a microservices architecture with specific deployment and scalability requirements.
- D) Azure App Service Azure App Service is a fully managed platform for building, deploying, and scaling web apps and APIs. While it supports deployment to Azure, it may not provide the necessary features for independent upgrades to microservices or policy-based automatic repairs.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskills: Designing Compute and Network Infrastructure

Competencies: Microservices Architecture Design

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

92. You have an on-premises data center that does not have a VPN connection to your Azure subscription named Sub1, which is linked to a hybrid Azure Active Directory (Azure AD) tenant. Within the data center, there is a computer named SRV1 running Microsoft SQL Server 2016. However, SRV1 is restricted from accessing the internet.

You need to recommend a solution to provide LogicApp1 with write access to a database located on SRV1. What should you recommend deploying on-premises?

- A) Web Application Proxy for Windows Server
- B) Azure AD Application Proxy connector
- C) On-premises data gateway

D) Hybrid Connection Manager

Answer: C

Feedback(if correct):-

The on-premises data gateway allows LogicApp1 to securely access on-premises data sources, such as the database located on SRV1, without requiring direct internet access for SRV1. The on-premises data gateway acts as a bridge between the on-premises network and Azure services, enabling secure communication and data transfer. By deploying the on-premises data gateway, LogicApp1 can establish a connection to the database on SRV1 and perform write operations.

Feedback(if wrong): Option A) Web Application Proxy for Windows Server is incorrect. This proxy is typically used for publishing internal web applications securely to external users. It does not provide the required connectivity between LogicApp1 in Azure and the on-premises SQL Server.

Option B) Azure AD Application Proxy connector is also incorrect. This connector is used to enable remote access to on-premises applications securely through Azure AD. However, it does not facilitate direct database access for LogicApp1 to SRV1.

Option D) Hybrid Connection Manager is not the correct choice. It is used to establish bi-directional connectivity between Azure and on-premises resources, but it primarily focuses on connecting web apps and services, not directly to SQL Server databases.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Analyzing and Evaluating

Difficulty Level: Intermediate or Expert

Bloom's Taxonomy Level: Analysis and Evaluation

93. You have an on-premises data center that does not have a VPN connection to your Azure subscription named Sub1, which is linked to a hybrid Azure Active Directory (Azure AD) tenant. Within the data center, there is a computer named SRV1 running Microsoft SQL Server 2016. However, SRV1 is restricted from accessing the internet. You need to recommend a solution to enable LogicApp1 to securely access the database on Server1 from Azure. What should you recommend deploying in Azure?

- A) Connection gateway resource
- B) Azure Application Gateway
- C) Azure Event Grid domain
- D) Enterprise application

Answer: A

Feedback(if correct): This solution enables LogicApp1 in Azure to securely connect to the on-premises SQL Server database (SRV1) via the hybrid connection established by the on-premises data gateway. It ensures secure communication without requiring SRV1 to have internet access.

Feedback(if wrong): Option B) Azure Application Gateway is incorrect. This service is primarily used for load balancing, SSL termination, and web application firewall capabilities for web applications. It is not suitable for enabling direct access to an on-premises SQL Server database like SRV1.

Option C) The Azure Event Grid domain is also incorrect. Azure Event Grid is a service for managing and routing events from various Azure services and custom sources. It is not designed to provide connectivity between Azure services and on-premises resources like SRV1.

Option D) Enterprise application is not the correct choice. This term typically refers to the registration of an application in Azure AD for identity and access management purposes. It does not facilitate direct access to on-premises resources from Azure services like LogicApp1.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Analyzing and Evaluating

Difficulty Level: Expert

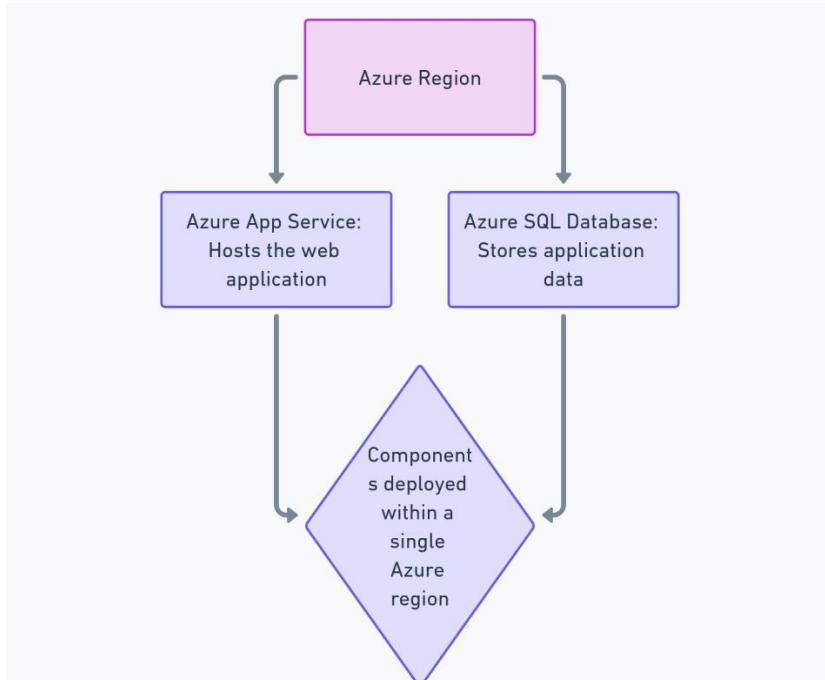
Bloom's Taxonomy Level: Analysis and Evaluation

94. Your organization plans to deploy a global e-commerce web application on Azure. The application needs to offer high availability, low latency access to customers worldwide, and resilience to region-specific outages. Additionally, the solution must be capable of dynamically scaling to handle varying loads and support automated disaster recovery processes. Choose the architecture diagram that best meets the application's requirements for global reach, high availability, scalability, and disaster recovery.

A) Single-Region Architecture

- Description: Deploys the application and its data storage in a single Azure region, using Azure App Service for hosting and Azure SQL Database for data persistence. This setup lacks specific configurations for global distribution or high availability beyond Azure's built-in features.

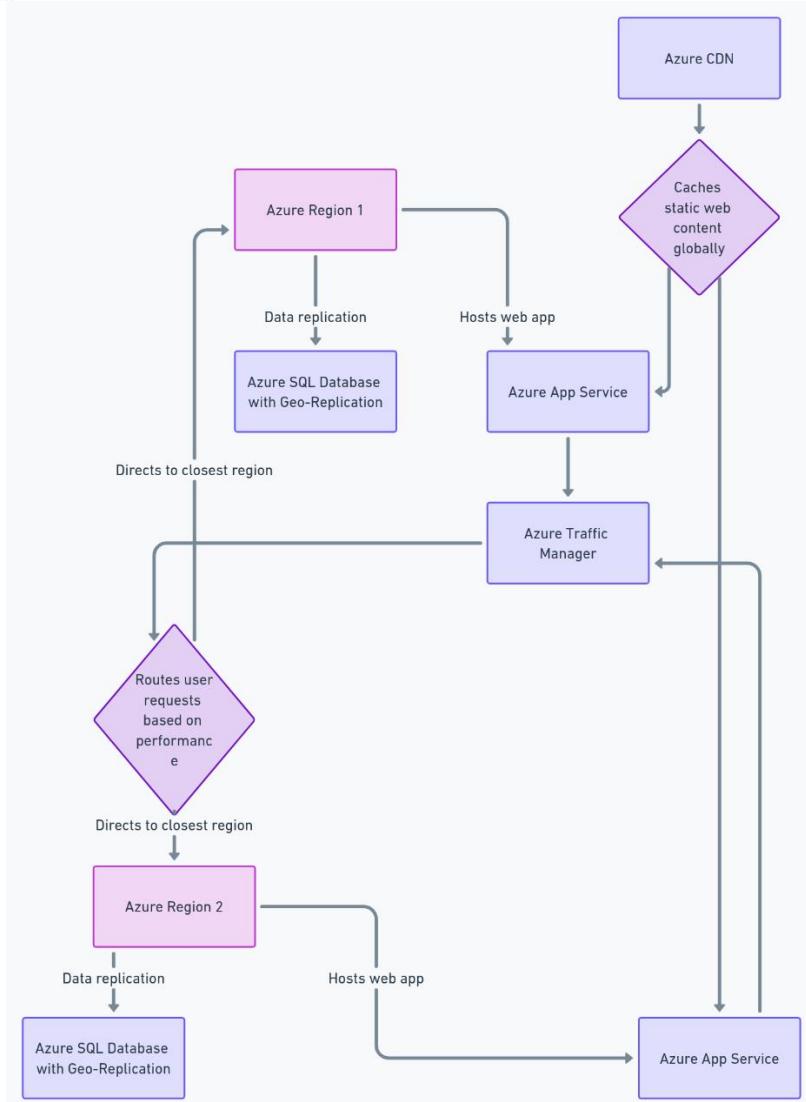
- Diagram



B) Multi-Region with Active-Active Services

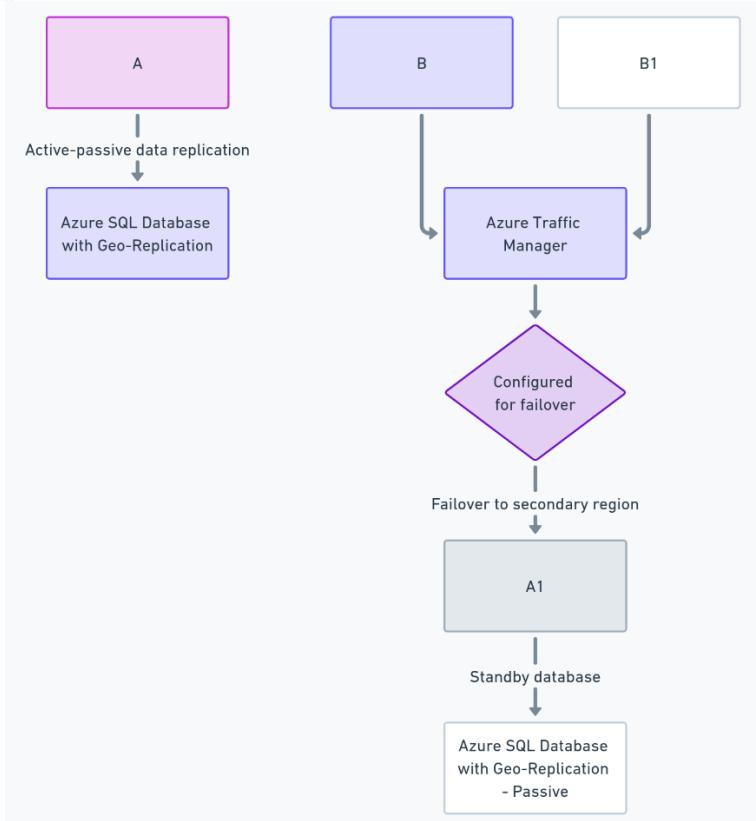
- Description: Utilizes an active-active configuration across multiple Azure regions for the web hosting layer (Azure App Service) and data layer (Azure SQL Database with Geo-Replication), complemented by Azure Traffic Manager for global DNS-based traffic routing and Azure CDN for caching static content closer to users.

- Diagram:



C) Multi-Region with Active-Passive Services

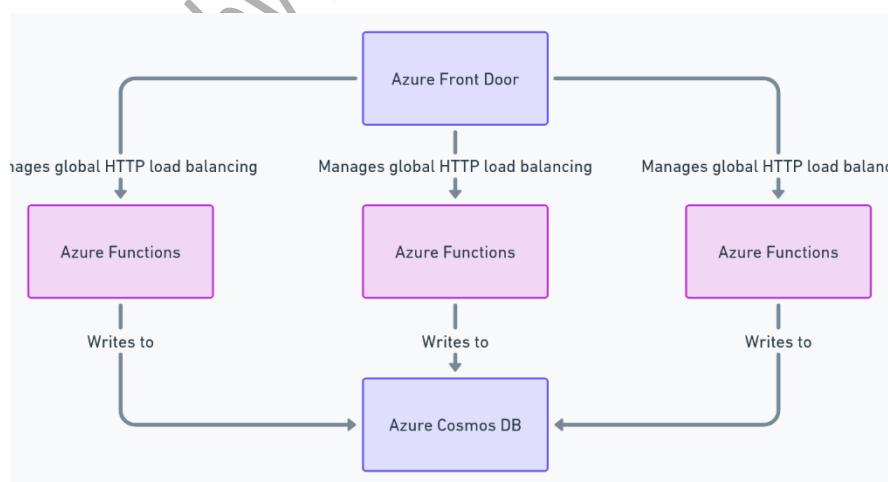
- Description: Features a primary region with actively serving components and a secondary region set up as a passive disaster recovery site. The architecture uses Azure App Service for hosting, Azure SQL Database with Geo-Replication for data synchronization, and Azure Traffic Manager for managing failover.
- Diagram:



D) Global Distribution with Azure Functions and Cosmos DB

- Description: Employs Azure Functions for serverless compute and Azure Cosmos DB for a globally distributed database with multi-region writes, ensuring low latency and high availability. Azure Front Door is used for global HTTP load balancing and SSL offloading.

- Diagram:



Answer: B

Feedback(if correct):- The correct architecture ensures the global e-commerce application is highly available, scalable, resilient to regional outages, and capable of providing low latency access worldwide. It achieves this by distributing the application across multiple Azure regions in an active-active setup, utilizing Azure Traffic Manager for intelligent user request routing and Azure CDN for caching content close to users globally. This setup not only guarantees the application remains operational during regional disruptions but also dynamically scales to meet varying demands, ensuring an optimal user experience regardless of geographic location.

Feedback(if wrong):- Single-Region Architecture is unsuitable for a global application as it limits the application's availability and resilience to a single region, potentially increasing latency for international users and risking downtime during regional outages.

- Multi-Region with Active-Passive Services offers improved resilience and disaster recovery through failover capabilities but may not provide the best user experience in terms of latency, as passive regions do not serve traffic until an active region fails.
- Global Distribution with Azure Functions and Cosmos DB presents a highly scalable and globally distributed approach but might necessitate significant architectural adjustments for traditional web applications. It's an excellent choice for specific use cases but may not align with all the operational requirements of a conventional e-commerce platform, especially if the application relies heavily on relational database structures and complex transactional processes.

skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Azure App Service, Azure SQL Database with Geo-Replication, Azure Traffic Manager, and Azure CDN

Difficulty Level: Expert

Bloom's Taxonomy Level: Analysis

95. Your organization is migrating an on-premises OLTP database to Azure and needs a solution that meets specific requirements, including the ability to scale, support for geo-redundant backups, and optimization for online transaction processing (OLTP) workloads. Additionally, the solution must accommodate a database size of up to 75 TB.

Based on these requirements, which Azure database service would best suit your needs?

- A. SQL Server on Azure Virtual Machines
- B. Azure SQL Managed Instance
- C. Azure Synapse Analytics
- D. Azure SQL Database

Answer: D

Feedback(if correct):- D. Azure SQL Database is ideally suited for this scenario, particularly when leveraging the Hyperscale service tier. Azure SQL Database's Hyperscale tier is specifically designed for large databases, offering auto-scaling capabilities up to 100 TB. This makes it perfect for handling large OLTP databases that require both high performance and the ability to scale dynamically. Moreover, it provides built-in support for geo-redundant backups, ensuring that data remains secure and recoverable in the event of a disaster. This combination of features addresses all the migration criteria effectively, making Azure SQL Database the optimal choice for organizations looking to migrate large OLTP databases to Azure.

Feedback(if wrong):-

- A. SQL Server on Azure Virtual Machines: While offering full control and feature compatibility with on-premises SQL Server, this option requires more manual management for scaling and backup configurations. It's more suited for specific scenarios demanding full SQL Server feature compatibility but may not offer the same level of ease and scalability as Azure SQL Database's Hyperscale service tier.
- B. Azure SQL Managed Instance: Provides broad feature compatibility with SQL Server and managed environment benefits. However, its scalability, while generally sufficient, doesn't match the Hyperscale service tier's capabilities within Azure SQL Database for very large databases or provide the same level of flexibility in dynamic scaling up to 75 TB.
- C. Azure Synapse Analytics: Focused on analytics and large-scale data processing rather than OLTP workloads. While powerful for its intended use cases, Azure Synapse Analytics doesn't align with the

requirements for hosting a scalable, high-performance OLTP database that requires up to 75 TB of storage and geo-redundant backups.

skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Understanding the capabilities and use cases of different Azure SQL Database service tiers, specifically regarding scalability, data backup, and OLTP workload optimization.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

96. Your organization is migrating an on-premises OLTP database to Azure and needs a solution that meets specific requirements, including the ability to scale, support for geo-redundant backups, and optimization for online transaction processing (OLTP) workloads. Additionally, the solution must accommodate a database size of up to 75 TB.

Continuing from the selection of Azure SQL Database for migrating your OLTP workload to Azure, which service tier within Azure SQL Database should you choose to ensure support for a database size up to 75 TB, along with the ability to scale and include geo-redundant backups?

- A. Basic
- B. Business Critical
- C. General Purpose
- D. Hyperscale

Answer: D

Feedback(if correct):-

D. Hyperscale is specifically designed to meet and exceed the requirements for large databases in Azure SQL Database, providing auto-scaling capabilities up to 100 TB. This makes it ideally suited for very large OLTP databases that need both high performance and the ability to scale dynamically. Hyperscale tier offers rapid scaling, innovative storage technology, and instant backup and restore capabilities that do not impact database performance. Additionally, it supports geo-redundant backups, ensuring data is secure and recoverable in case of a disaster. This combination of features addresses all specified criteria for the migration, making Hyperscale the optimal choice.



Feedback(if wrong):-

- A. Basic: Intended for small databases, offering limited resources and capabilities. The Basic tier is suitable for development and testing environments or small applications but cannot support the scalability, performance, and backup requirements for large OLTP workloads.
- B. Business Critical: Provides high resilience, I/O performance, and in-memory capabilities, suitable for high-performance applications that require fast transaction processing and have high availability needs. Despite its advantages, it does not inherently support the extensive scaling up to 75 TB required for the scenario.
- C. General Purpose: Offers a balanced amount of computing, storage, and resources. It's a cost-effective option for many business workloads but doesn't provide the massive scalability or the same level of backup and restore capabilities as the Hyperscale service tier.

skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Understanding the capabilities and use cases of different Azure SQL Database service tiers, specifically regarding scalability, data backup, and OLTP workload optimization.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

97. You're tasked with deploying a two-tier application on Azure, with each tier packaged as a separate Docker Linux-based image. The application must satisfy specific networking and reliability requirements while also being cost-effective.

Requirements:

1. The front-end tier should be publicly accessible on port 80.
2. The back-end tier should only be accessible from the front-end tier, using port 8080.
3. Both containers need to share access to the same Azure file share.
4. Automatic restart of the application if a container fails.
5. Minimization of costs.

Based on the requirements, which Azure service is most appropriate for hosting the application?

- A. Azure Kubernetes Service (AKS)
- B. Azure Service Fabric
- C. Azure Container Instances
- D. Azure Container Registries

Answer: C

Feedback(if correct):- Azure Container Instances (ACI) is the best choice for hosting this two-tier application due to its ability to quickly start containers and bill by the second, making it a cost-effective option for scenarios with variable workloads. ACI provides the simplicity and flexibility needed for this scenario, including:

- Easy configuration for public access on specific ports, satisfying the front-end tier's accessibility requirement.
- Network isolation capabilities that allow the back-end tier to only be accessible from the front-end tier, fulfilling the specified networking constraint.
- Support for shared Azure file shares between containers, ensuring both tiers can access the necessary data.
- Automatic container restart in case of failure, providing the required reliability without additional configuration or overhead.
- A cost-efficient model, as ACI does not require managing the underlying VMs or orchestrators, reducing operational costs.

Feedback if Wrong:

- A. Azure Kubernetes Service (AKS) provides comprehensive orchestration features for complex applications involving multiple containers and microservices but might introduce unnecessary complexity and cost for simpler, two-tier applications.
- B. Azure Service Fabric is an excellent choice for microservices and complex, stateful applications but is overkill for scenarios that do not require its advanced orchestration and state management capabilities.
- D. Azure Container Registries is a service for storing and managing container images but does not host containerized applications, making it an incorrect choice for the application hosting requirement.

Skill mapping:



Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Designing and implementing high-availability systems in Azure. Utilizing Azure services to ensure application resilience and data durability. Implementing disaster recovery strategies for cloud-native applications.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

98. Your enterprise is leveraging Azure Firewall for safeguarding network traffic in various geographical locations, managed through specific firewall policies per region as detailed below.

Firewall Policies Configuration:

EU-North-Firewall-Policy: Azure Firewall Policy in North Europe

US-West-Firewall-Policy: Azure Firewall Policy in West US

Asia-South-Firewall-Policy: Azure Firewall Policy in South East Asia

The goal is to enhance security protocols by introducing universal security rules that will apply to all Azure Firewall instances within the enterprise. To achieve this, a master policy will be established to encompass these global rules.

Requirement:

Devise a strategy to incorporate a set of global security rules across every Azure Firewall instance by setting up a master policy that existing regional policies will derive.

To ensure a standardized set of security rules is applied across every Azure Firewall instance through a master policy model, what is the least number of new Azure Firewall policies required to create?

A. 1

B. 2

C. 4

D . 5

Answer: A

Feedback(if correct):-

Introducing a singular new Azure Firewall policy as the master policy is the most efficient way to centralize and standardize essential security rules across the organization. This master policy will encapsulate the global security rules needed by the enterprise. Existing firewall policies for North Europe, West US, and South East Asia will inherit from this master policy, thereby uniformly applying the defined security rules across all firewall instances. This hierarchical policy structure enables effective governance, allowing for updates or modifications to be made centrally in the master policy, which then cascades automatically to the child policies, maintaining consistency and simplification in managing security rules across regions.

Feedback (if Wrong):

B. 2, C. 4, and D. 5 indicate the creation of multiple new policies beyond the necessary, which would complicate the governance and enforcement of universal security rules without offering additional advantages.

Overprovisioning policies increases complexity, raises maintenance efforts, and possibly leads to confusion or inconsistent settings among the distributed firewall instances. Thus, selecting B. 2, C. 4, and D. 5 would not be the optimal or most efficient solution.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Developing strategies to maintain network security and integrity across distributed environments. Ensuring continuous protection and quick recovery of network infrastructure in the face of regional disruptions. Implementing hierarchical firewall policies to support disaster recovery plans and maintain operational continuity.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

99. In an organization with a widespread on-premises network and an active Azure subscription, there's a particular branch in Toronto hosting a vital virtual machine, VM1, serving as a file server. This VM is critical for the daily operations of users across various offices, who rely on accessing shared files stored on VM1. Given the potential risk of the Toronto branch becoming inaccessible due to unforeseen circumstances, there's an urgent need to devise a fail-safe plan to maintain uninterrupted access to these shared files.

Requirement:

The primary objective is to recommend a resilient solution that ensures continuous availability of shared files to all users, irrespective of the operational status of the Toronto branch, thereby minimizing downtime and preserving productivity across the organization.

To guarantee that users retain swift access to shared files, even in the event of the Toronto branch office being temporarily or permanently inaccessible, which Azure-based solution should you recommend?

- A. Utilize a Recovery Services vault coupled with Azure Backup for real-time file replication and backup.
- B. Implement an Azure file share integrated with Azure File Sync for centralized file storage and seamless synchronization.
- C. Deploy Azure blob containers in conjunction with Azure File Sync to facilitate file storage and synchronization.
- D. Configure a Recovery Services vault alongside Windows Server Backup to ensure comprehensive backup and recovery.

Answer: B.

Feedback(if correct):-

The integration of an Azure file share with Azure File Sync stands out as the most effective solution for this scenario. It enables the centralization of file shares in Azure Files, thus ensuring that files are accessible from anywhere, not just within the confines of the Toronto office. Azure File Sync transforms the on-premises Windows Server into a quick cache for the Azure file share, facilitating efficient access to files with minimal latency. This setup not only ensures that users can access files even if the Toronto office is offline but also maintains the familiar performance and compatibility of on-premises file servers, thereby aligning perfectly with the need for a resilient and user-friendly file access solution across the organization.

Feedback if Wrong:

Feedback(if wrong):

Utilizing a Recovery Services vault combined with Azure Backup (option A) and configuring a Recovery Services vault alongside Windows Server Backup (option D) primarily focus on backup and restore, not maintaining constant availability for shared files in case of Toronto branch issues.

Azure Blob containers paired with Azure File Sync (option C) are close but incorrect since Azure Files, rather than Blob containers, are more suited for file-sharing scenarios.

Skill Mapping:



Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Developing strategies to maintain network security and integrity across distributed environments. Ensuring continuous protection and quick recovery of network infrastructure in the face of regional disruptions. Implementing hierarchical firewall policies to support disaster recovery plans and maintain operational continuity.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

100. A healthcare organization utilizes Azure to store sensitive patient records. To comply with regulatory standards, they require a robust data protection strategy for their Azure Blob Storage. The strategy must ensure that:

1. Deleted blob data can be restored within 30 days to mitigate against accidental or malicious deletions.
2. The restoration process must be straightforward to enable quick recovery in emergencies.

Given these specific requirements, the organization seeks advice on which Azure Blob Storage feature to implement.

Which Azure Blob Storage feature should the healthcare organization enable to meet its data protection and compliance requirements?

- A. Access tiers
- B. Blob versioning
- C. Geo-replication
- D. Soft delete for blobs

Answer: D

Feedback(if correct):-

The Soft Delete for Blobs feature in Azure Blob Storage is designed specifically to protect against accidental or malicious deletion of data. When enabled, it retains deleted blob data for a specified retention period, allowing for its recovery. For the healthcare organization's scenario, setting a retention

period of 30 days meets their need to restore deleted blob data within this timeframe. This feature ensures that even if blob data is deleted, it remains recoverable, thus aligning with the organization's regulatory compliance and data protection strategy. Options A, B, and C, while useful in various contexts, do not directly address the requirement to recover deleted data within a specified period.

Feedback(if wrong):-

- A. Access tiers: Incorrect because access tiers (hot, cool, and archive) are used to manage storage costs based on data access patterns and do not offer data protection against deletion.
- B. Blob versioning: Incorrect as it maintains multiple versions of a blob but is primarily aimed at protecting against unintended overwrites rather than deletions.
- C. Geo-replication: Incorrect because it replicates data across regions for availability, not specifically for deletion recovery within a retention period.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Azure Blob Storage.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

az305 final exam 4

101. You have an Azure Active Directory (Azure AD) tenant named contoso.com that has a security group named G1. G1 is configured for assigned membership. G1 has 200 members, including 50 guest users.

You need to recommend a solution for evaluating the membership of G1. The solution must meet the following requirements:

The evaluation must be repeated automatically every three months.

Every member must be able to report whether they need to be in G1.

Users who report that they do not need to be in G1 must be removed from Group1 automatically.

Users who do not report whether they need to be in G1 must be removed from G1 automatically.

What should you include in the recommendation?

- A) Implement Azure AD Identity Protection.
- B) Change the Membership type of Group1 to Dynamic User.
- C) Implement Azure AD Privileged Identity Management.
- D) Create an access review.

Answer: D

Feedback(if correct):

To meet the requirements of automatically evaluating the membership of G1 every three months, allowing members to report whether they need to be in the group, and automatically removing users who do not report or do not need to be in the group, you should create an access review. An access review allows you to periodically review and manage access to resources, such as security groups, in Azure AD. It enables members to report whether they need to be in the group and automatically removes users who do not report or do not need to be in the group.

Feedback(if wrong):

Option A) Implement Azure AD Identity Protection: This option is incorrect because Azure AD Identity Protection is not designed for evaluating group membership or conducting access reviews.

Option B) Change the Membership type of Group1 to Dynamic User: This option is incorrect because changing the membership type to Dynamic User would not facilitate the required recurring evaluations and selfreviews by members.

Option C) Implement Azure AD Privileged Identity Management: This option is incorrect because Azure AD Privileged Identity Management is not intended for evaluating regular group membership and conducting access reviews.

Skill Mapping:



Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskills: Designing Identity and Security Solutions

Competencies: Designing Identity and Security Solutions, Designing Compute and Network Infrastructure, Identity and Access Management, Security, Authentication, Authorization

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

102. You have the divisions East and West within your company, each with its own Azure subscription. The East division's subscription is named Subscription1, while the West division's subscription is named Subscription2. Both subscriptions are linked to the Azure AD tenant, with Subscription1 associated with the contoso.com tenant and Subscription2 associated with the fabrikam.com tenant. In Subscription1, there is an Azure App Service web app named App1, which utilizes Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to Application1. You are tasked with recommending a solution to enable users in the fabrikam.com tenant to authenticate to Application1. What should you recommend?

- A) Utilize Azure AD for external users.
- B) Configure the Azure AD roles.
- C) Implement Single Sign-On (SSO) for Application1 authentication.
- D) Enable Azure AD pass-through authentication and update the sign-in endpoint.

Answer: D

Feedback(if correct):-

The correct selection is option D) Enable Azure AD pass-through authentication and update the sign-in endpoint. This solution allows users from the fabrikam.com tenant to authenticate to Application1 by passing their credentials through Azure AD.

Feedback(if wrong):-

- Option A) Utilize Azure AD for external users: This option is incorrect because it does not address the need for authentication from users within the fabrikam.com tenant specifically. Azure AD for external users typically refers to guest users or users from external organizations.

- Option B) Configure the Azure AD roles: This option is incorrect because it focuses on configuring roles within Azure AD, which is not directly related to enabling authentication for users from the fabrikam.com tenant to Application1.
- Option C) Implement Single Sign-On (SSO) for Application1 authentication: This option is incorrect because while SSO can be a part of the solution, it alone does not address the need to enable authentication for users from the fabrikam.com tenant to Application1. Additionally, the scenario does not specify the use of SSO as a requirement.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Identity and Security Solutions

Competency: Implementing authentication and access management solutions in Azure Active Directory (Azure AD)

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

103. Your organization possesses an Azure subscription equipped with a blob container housing assorted blobs. During May, twenty individuals dispersed across five teams demanded access to the contained blobs. You are tasked with proposing a remedy to restrict access exclusively to May. Recommend an appropriate security solution enabling constrained access to the blob container assets in May.

- A) Shared Access Signatures (SAS)
- B) Private Endpoints
- C) Azure Content Delivery Network (CDN) Rules Engine
- D) Point-to-Site Virtual Private Network (VPN)

Answer: A

Feedback (if correct):

Selection A, "shared access signatures (SAS)", is the correct answer. By creating SAS tokens, you can provide limited-time access to Azure Blob Storage resources without sharing the entire storage account.

With SAS tokens, you can precisely set expiration dates and times, enabling access to the blobs in April only.

Feeback (if wrong):

- B) Access keys: These are permanent secrets granting unrestricted access to Azure Storage Account resources. Restricting access to April is impossible using Access keys.
- C) Conditional access policies: Primarily employed for identity-driven access control in Azure AD, Conditional Access Policies do not regulate temporal access to blob containers.
- D) Certificates: Like access keys, SSL/TLS certificates are permanent identifiers not suited for governing transient access to blob containers.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Identity and Security Solutions

Competency: Implement Azure Role-Based Access Control (RBAC), Implement Azure Active Directory (Azure AD) authentication, Evaluate and mitigate organizational security risks

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

104. Contoso is collaborating with Fabrikam on a project that involves access to an Azure-hosted application, App1. To ensure secure and appropriate access control, Contoso needs a solution that allows for the regular review and management of Fabrikam users' access permissions to App1. Specifically, they require a process whereby an account manager at Fabrikam can monthly review which users have access to App1 and remove those who no longer require access. Contoso aims to implement a solution with minimal development effort. Considering Contoso's requirements for managing Fabrikam's access to App1, which Azure service and feature should you recommend to efficiently manage and review Fabrikam users' access permissions?

- A. Azure AD Identity Governance with Access packages
- B. Azure AD Identity Protection with Approvals
- C. Azure AD Privileged Identity Management (PIM) with Access reviews
- D. Azure Automation with Runbooks

Answer: C.

Feedback(if correct):-

C. Azure AD Privileged Identity Management (PIM) with Access reviews is the correct answer because Azure AD PIM provides the capability to manage, control, and monitor access within Azure AD, Azure, and other Microsoft Online Services. The Access reviews feature of Azure AD PIM allows organizations to review and audit access permissions and memberships regularly. This fits perfectly with Contoso's requirement to enable an account manager at Fabrikam to periodically review Fabrikam users' access to App1 and ensure that only those who need access retain it. This solution also minimizes development effort, as it leverages existing Azure services without the need for custom development.

Feedback(if wrong):-

A. Azure AD Identity Governance with Access packages is incorrect because, while Azure AD Identity Governance offers comprehensive identity management capabilities, Access packages are more suited for granting and managing access for users to groups, applications, and SharePoint sites, rather than for the periodic review of access permissions.

B. Azure AD Identity Protection with Approvals is incorrect as Azure AD Identity Protection focuses on identifying potential vulnerabilities affecting the organization's identities and configuring automated responses. It does not directly address the requirement for regular access reviews.

D. Azure Automation with Runbooks is incorrect because Azure Automation and Runbooks are designed for automating repetitive tasks and managing resources at scale, not specifically for reviewing and managing user access permissions in a governance context.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing and managing Azure AD Privileged Identity Management (PIM) and Azure AD access reviews.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

105. Your organization's web application, App1, requires secure authentication to access credentials and connection strings stored for third-party services. Ensuring the integrity and confidentiality of these secrets is paramount.

Requirement:

Choose the best authentication method for App1 to securely access these secrets stored in Azure Key Vault.

- A. Use a certificate for authenticating App1.
- B. Implement a service principal for App1 authentication.
- C. Employ a system-assigned managed identity for App1.
- D. Utilize a user-assigned managed identity for App1.

Answer: B.

Feedback(if correct):-

Implementing a service principal provides a dedicated identity for App1 within Azure AD, facilitating secure access to Azure resources. This method is ideal for applications that need to access other Azure services securely.

Feedback(if wrong):-

A. Use a certificate for authenticating App1:

Certificates expire eventually, which translates to additional management overhead and potential security risks if neglected. Also, this method requires manual rotation and revocation, adding to the administration burden.

C. Employ a system-assigned managed identity for App1:

System-assigned managed identities are tied to the lifecycle of the Azure resource they belong to (such as virtual machines or app services). Because of this constraint, the identity ceases to exist when the resource is decommissioned or deleted. This limitation prevents the use of system-assigned managed identities when persistent identification is required, like in cases where access rights need to persist after resource deletion.

D. Utilize a user-assigned managed identity for App1:

User-assigned managed identities suffer from a similar drawback as system-assigned managed identities. When the resource is destroyed, the identity becomes unusable as well. Additionally, user-assigned managed identities require explicit assignment to multiple resources, which increases the likelihood of errors and adds to the management overhead.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing authentication and authorization strategies in Azure, focusing on service principal for authentication and RBAC for authorization.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

106. Your organization's web application, App1, requires secure authentication to access credentials and connection strings stored for third-party services. Ensuring the integrity and confidentiality of these secrets is paramount. Following secure authentication, App1 must have authorized access to retrieve secrets from Azure Key Vault without compromising the security or integrity of the stored secrets. Select the most appropriate authorization mechanism for App1 to access the necessary secrets within Azure Key Vault.

- A. Configure an access policy in Azure Key Vault.
- B. Integrate a connected service with Azure Key Vault.
- C. Establish a private link to Azure Key Vault.
- D. Assign a role to App1 for retrieving Key Vault secrets.

Answer: D

Feedback(if correct):-

Assigning a role to App1 for retrieving Key Vault secrets leverages Azure's role-based access control (RBAC) to precisely define and limit the permissions granted to the application. This method ensures that App1 has only the necessary permissions to access the secrets it needs, adhering to the principle of least privilege and enhancing the overall security posture without compromising the integrity or confidentiality of the stored secrets.

Feedback(if wrong):-

- A. Configure an access policy in Azure Key Vault: While access policies can specify permissions within Key Vault, they do not offer the same granular control or simplicity in management as RBAC, especially as your Azure environment scales.
- B. Integrate a connected service with Azure Key Vault: This option doesn't directly relate to the authorization of applications to access Key Vault secrets and is more about integrating Azure services.

C. Establish a private link to Azure Key Vault: While Azure Private Link provides a secure connection to Azure Key Vault, it's a network-level security feature and does not replace the need for proper authorization mechanisms such as RBAC.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing authentication and authorization strategies in Azure, focusing on service principal for authentication and RBAC for authorization.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

107. Your task is to ensure all Azure SQL databases within your organization's production environment have Transparent Data Encryption (TDE) enabled to meet stringent security and compliance requirements. To initiate the process of enforcing TDE on Azure SQL databases, which of the following actions should you perform first?

- A. Create a user-assigned managed identity.
- B. Invoke a remediation task.
- C. Create an Azure policy definition that uses the deployIfNotExists effect.
- D. Create an Azure policy assignment.

Answer: C

Feedback(if correct): Initiating the process with the creation of an Azure policy definition that uses the deployIfNotExists effect is the foundational step. This action defines the criteria and actions for identifying and automatically enforcing TDE on all Azure SQL databases that currently do not have it enabled. It sets the stage for the subsequent steps of assigning this policy and remediating any non-compliant resources, thereby meeting the security and compliance requirements.

Feedback(if wrong):

A (Create a user-assigned managed identity): This step is necessary for assigning permissions but does not directly enforce TDE on Azure SQL databases. It is a subsequent step after defining and assigning the policy.

B (Invoke a remediation task): Remediation tasks are invoked to correct non-compliance, which presupposes that a policy definition and assignment are already in place. Hence, it cannot be the first step.

D (Create an Azure policy assignment): Policy assignment is an essential step to apply the policy across resources. However, it must be preceded by creating a policy definition that specifies what the policy is and how it should be enforced.

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing and managing security solutions in Azure, specifically Azure Policy and Azure SQL Database security features.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

108. Your task is to ensure all Azure SQL databases within your organization's production environment have Transparent Data Encryption (TDE) enabled to meet stringent security and compliance requirements. Following the initial setup of an Azure policy to enforce TDE on Azure SQL databases, you need to apply this policy and address any non-compliance to ensure all databases comply with your organization's security and compliance requirements. After creating an Azure policy definition that enforces TDE on Azure SQL databases, what is the next step to ensure compliance across all databases?

- A. Create a user-assigned managed identity.
- B. Invoke a remediation task.
- C. Create an Azure policy definition that uses the Modify effect.
- D. Create an Azure policy assignment.

Answer: D

Feedback(if correct): After creating a policy definition, the next critical step is to create an Azure policy assignment. This action applies the policy to the specified scope, such as a subscription, resource group,

or individual resources. By doing so, you ensure that the policy for enforcing Transparent Data Encryption (TDE) on Azure SQL databases is actively evaluated against existing databases, paving the way for identifying and remediating any instances of non-compliance.

Feedback(if wrong):

A (Create a user-assigned managed identity): While managed identities might be utilized in various scenarios for accessing Azure services securely, creating one isn't the direct next step after the policy definition for enforcing TDE.

B (Invoke a remediation task): Remediation tasks are crucial for correcting non-compliance issues but should be considered after the policy has been assigned and non-compliant resources have been identified.

C (Create an Azure policy definition that uses the Modify effect): This action would be relevant if you were modifying existing resources directly based on policy evaluation outcomes, but it does not apply directly after creating a policy definition for TDE enforcement. The priority is to assign the created policy to target resources.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing and managing security solutions in Azure, specifically Azure Policy and Azure SQL Database security features.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

109. Your client, Fabrikam, is expanding its digital footprint and plans to deploy several cloud-based applications using Azure services. Fabrikam has stringent security and compliance requirements, especially regarding user authentication and access management. They want to ensure that their cloud infrastructure supports centralized identity management and can enforce conditional access based on specific criteria such as user role, location, and device state. Fabrikam has partnered with multiple vendors and wants to provide them with limited access to certain applications. Additionally, Fabrikam is considering a multi-geographical deployment strategy to cater to its diverse user base spread across different regions.

Requirement:

You are tasked with designing an Azure Active Directory (Azure AD) strategy that supports Fabrikam's authentication and access management requirements. Your solution must enable centralized

management of identities, support custom domain names for application access, and allow the creation of conditional access policies to secure application access.

Options:

Minimum number of Azure AD tenants: How many Azure AD tenants are required to efficiently manage Fabrikam's global user base and vendor partnerships?

Minimum number of custom domains to add: Given Fabrikam's need for branded application access, how many custom domains should be added to the Azure AD tenants?

Minimum number of conditional access policies to create: To enforce Fabrikam's security and compliance requirements across its applications, how many conditional access policies should be created?

To meet Fabrikam's authentication requirements with an Azure AD-based solution, which configuration should you recommend?

A.

- Azure AD tenants: 1
- Custom domains: 2
- Conditional access policies: 3

B.

- Azure AD tenants: 2
- Custom domains: 1
- Conditional access policies: 4

C.

- Azure AD tenants: 1
- Custom domains: 1
- Conditional access policies: 2

D.

- Azure AD tenants: 2
- Custom domains: 3

- Conditional access policies: 1

Answer: A

Feedback (if correct):

The correct setup involves configuring one Azure AD tenant to centralize authentication across all applications, ensuring streamlined management and security. Adding one custom domain enhances user experience by incorporating familiar branding into authentication processes. Implementing two conditional access policies allows for granular security controls based on specific conditions like user location or device compliance, enhancing overall security without unnecessary complexity. This setup optimally balances functionality with simplicity, meeting the specified requirements effectively.

Feedback (if wrong):

Multiple Azure AD tenants complicate management and do not enhance security or functionality for the given scenario, making options suggesting more than one tenant less ideal.

More than one custom domain is unnecessary unless there are distinct branding needs for different applications or services, which is not indicated in the scenario.

Less than two conditional access policies may not adequately address the nuanced security requirements, such as differentiating access controls based on user location or device compliance.

More than two conditional access policies could imply an overly complex configuration that might not be required to meet the specified requirements, potentially introducing unnecessary administrative overhead.

Choosing the configuration that simplifies management while ensuring security and functionality is crucial. The scenario provided does not warrant the complexity of multiple tenants or custom domains beyond what is necessary to meet the user experience and security requirements.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing and managing Azure AD for application access, Conditional Access policies, and custom domain configurations.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

110. Your organization's IT support team requires an efficient way to receive notifications regarding the health, performance, and availability of Azure services and any identity synchronization issues. The solution should enable proactive management and rapid response to potential disruptions or performance degradations in Azure-based applications and services. Design a notification solution that ensures the IT support distribution group is promptly informed about critical events impacting Azure services and identity synchronization processes, enabling the team to maintain optimal service levels and user satisfaction. To ensure the IT Support team receives timely notifications about Azure service health and identity synchronization status, which Azure solution should you recommend implementing?

- A. Azure Network Watcher
- B. Action Groups
- C. SendGrid account with advanced reporting
- D. Azure AD Connect Health

Answer: D

Feedback(if correct):- Azure AD Connect Health offers monitoring and notifications for Azure Active Directory (Azure AD) Connect, providing insights into synchronization services' health and performance. It alerts IT support teams about synchronization failures or performance issues, making it an ideal choice for ensuring the IT support distribution group receives critical notifications.

Feedback(if wrong):

- A. Azure Network Watcher is primarily used for monitoring and diagnosing network performance issues within Azure networks, not for identity synchronization or general Azure service health notifications.
- B. Action Groups provide a way to trigger automated responses based on Azure Monitor alerts, but on their own, they don't monitor health and performance.
- C. SendGrid account with advanced reporting is an email delivery service that offers detailed email analytics, not a direct solution for monitoring Azure services or Azure AD synchronization health.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing and managing Azure AD Connect Health for monitoring and notification.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

111. Contoso Ltd. is in the process of enhancing the security of its Azure-managed production environment. The company wants to ensure that all administrators who manage the Azure resources are subjected to stringent authentication protocols to prevent unauthorized access. The administrators access Azure resources through the Azure portal and are required to use Multi-Factor Authentication (MFA) for an additional layer of security.

Requirements:

- All administrators must be registered for Azure MFA.
- Administrators must authenticate using Azure MFA every time they sign in to the Azure portal.
- The solution must minimize administrative effort and ensure compliance with corporate security policies.

Given the scenario, how should you configure Azure to meet Contoso Ltd.'s requirements for securing access to the production environment?

- A) Enroll users for Azure MFA by enabling security defaults in Azure AD. Implement a Conditional Access policy that requires MFA for all sign-ins to the Azure portal.
- B) Require all users to manually register for per-user MFA in the MFA management UI. Configure a Conditional Access policy named capolicy1 with session controls to enforce MFA authentication.
- C) Utilize Azure AD Identity Protection to automate the registration for Azure MFA. Define a sign-in risk policy in Azure AD Identity Protection, applying it to users managing the Azure subscription for the production environment.
- D) Activate Azure AD Privileged Identity Management (PIM) for just-in-time access and require users to register for Azure MFA. Use Azure AD Identity Protection to enforce MFA authentication based on the user risk policy.

Answer: C

Feedback(if correct):- Azure AD Identity Protection offers a streamlined approach to enforce MFA registration across the organization. By leveraging Conditional Access policies within Azure AD Identity Protection, Contoso Ltd. can automatically require MFA registration for administrators accessing the Azure portal. This method reduces administrative effort and ensures all administrators are compliant

with the security policy. The sign-in risk policy further enhances security by evaluating the risk level of sign-ins and enforcing MFA authentication accordingly, meeting the requirement for administrators to authenticate via MFA every time they access the Azure portal.

Feedback(if wrong):

Option A: While enabling security defaults is a straightforward method to enforce MFA, it lacks the granularity and the automated user registration capabilities provided by Azure AD Identity Protection.

Option B: Manual registration for MFA and the use of session controls do not specifically address the automated enrollment and conditional MFA enforcement requirements.

Option D: Azure AD PIM is focused on managing, controlling, and monitoring access within Azure AD, but for the scenario provided, Azure AD Identity Protection directly addresses the need for automated MFA registration and enforcement based on sign-in risk, making it a more suitable choice.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing and managing Azure AD Connect Health for monitoring and notification.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

112. WebApp1 requires an efficient and scalable data storage solution. Evaluate the following options and select the best one.

- A. Pooled Azure SQL Database
- B. Fixed-sized DTU AzureSQL Database
- C. Azure VM with 2014 SQL Server
- D. vCore-based Azure SQL Database

Answer: D.

Feedback(if correct):

A vCore-based Azure SQL Database is the best option for WebApp1, as it offers scalability, performance, and flexible resource allocation. This choice allows you to manage multiple databases effortlessly, improve database restore operations, and utilize burst capacity during peak usage—all leading to an enhanced user experience.

Feeback(if wrong):

- A. Pooled Azure SQL Database: Although an appealing choice for consolidating and administering multiple databases, this option might not always guarantee optimal performance due to shared resources within the pool.
- B. Fixed-sized DTU AzureSQL Database: Limited by preset boundaries, expanding this kind of database to match increasing demands can prove challenging. It does not inherently pose the most efficient or scalable solution.
- C. Azure VM with SQL Server 2014: Running an SQL Server instance on an Azure VM introduces additional maintenance tasks, licensing concerns, and potential performance limitations. Generally speaking, native Azure SQL databases tend to perform better in terms of scalability and efficiency.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing and managing Azure AD Connect Health for monitoring and alerting on directory synchronization status and health.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

113. Fabrikam Ltd. desires to protect its Azure-based production environment further and wishes to leverage Azure Multi-Factor Authentication (MFA) for all users connecting to the environment. They anticipate that users will sign in through a Conditional Access policy named cppolicy2, which will demand Azure MFA when users manage the Azure subscription for a production environment via the Azure portal. What actions should you undertake to fulfill Fabrikam Ltd.'s expectations?

- A. Register users for Azure MFA via Per-user MFA in the MFA management UI
- B. Enforce Azure MFA authentication using the Sign-in risk policy in Azure AD Identity Protection
- C. Configure Conditional Access policy in Azure AD Identity Protection
- D. Enable User Risk policy in Azure AD Identity Protection

Answer: C

Feedback(if correct):

Option C: Configuring a Conditional Access policy in Azure AD Identity Protection to demand Azure MFA during sign-ins effectively meets Fabrikam Ltd.'s requirement. Conditional Access policies allow for the customization of security demands based on the company's specific needs, including the enforcement of MFA for accessing certain resources, such as the Azure portal when managing production environments. This approach ensures that all users are subjected to MFA, aligning with Fabrikam Ltd.'s security expectations.

Feedback(if wrong):

Option A: Registering users for Azure MFA via Per-user MFA in the MFA management UI requires manual intervention and does not automatically enforce MFA through Conditional Access policies.

Option B: Enforcing Azure MFA authentication using a Sign-in risk policy in Azure AD Identity Protection primarily focuses on the risk associated with the sign-in attempt rather than universally applying MFA to all users accessing the production environment.

Option D: Enabling a User Risk policy in Azure AD Identity Protection is designed to evaluate the risk level of a user's profile and actions over time, which does not directly enforce MFA upon every sign-in attempt to the Azure portal for production environment management.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing and managing Azure AD Connect Health for monitoring and notification.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

114. Your organization is developing WebApp1, an application expected to handle a significant volume of data transactions and queries. The application's data usage is anticipated to fluctuate considerably, with periods of high demand interspersed with times of relatively low activity. Your task is to recommend a data storage solution that optimizes for performance, scalability, and cost. Given the requirements for WebApp1's data storage, which Azure data service configuration should you recommend to ensure scalability, performance, and cost-effectiveness?

- A. Deploy an Azure SQL Database elastic pool to manage and scale multiple databases with varying performance demands efficiently.
- B. Use a vCore-based Azure SQL Database to provide precise control over compute and storage resources, allowing for scalable performance and cost optimization.
- C. Provision an Azure virtual machine running SQL Server for full control over the database environment and configuration, suited for specific legacy requirements.
- D. Opt for a fixed-size DTU Azure SQL Database for a simplified, pre-configured set of resources that can easily scale within set tiers.

Answer: B

Feedback(if correct):-

Opting for a vCore-based Azure SQL Database aligns perfectly with WebApp1's needs, offering a balance between scalability, performance, and cost-effectiveness. The vCore model allows for independent scaling of compute and storage, enabling the database to adapt to varying loads efficiently. This model also offers the benefits of reserved capacity savings and the Azure Hybrid Benefit for SQL Server, further optimizing costs while meeting the application's performance requirements.

Feedback(if wrong):-

- A. Azure SQL Database elastic pool might seem like a viable option for managing fluctuating demands, but it is best suited for scenarios with multiple databases that experience variable and unpredictable usage, which might not precisely match WebApp1's scenario.
- C. Azure virtual machine running SQL Server offers maximum control and customization but requires more management and typically incurs higher costs, making it less ideal for WebApp1's focus on cost-effectiveness.
- D. Fixed-size DTU Azure SQL Database provides simplicity in scaling and management but lacks the fine-grained control over performance and cost optimization provided by the vCore model, potentially leading to over-provisioning or under-provisioning of resources.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Selecting appropriate Azure SQL Database configurations for scalability, performance, and cost optimization.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

115. After your application, App1, has been transitioned to Azure, ensuring compliance with security mandates becomes a top priority. Specifically, you are tasked with safeguarding the data storage against unauthorized alterations or deletions, in line with stringent regulatory demands. What action should you undertake to align the data storage of App1 with the necessary security and regulatory standards?

- A. Implement an access policy specific to the blob, regulating data interactions.
- B. Adjust the blob service's access level to enhance security measures.
- C. Deploy Azure resource locks to protect against unintended modifications or deletions.
- D. Establish Azure Role-Based Access Control (RBAC) assignments to manage access rights and permissions.

Answer: A

Feedback(if correct):- Creating an access policy for the blob is the correct solution because it allows for the specific configuration of permissions on the blob storage, ensuring that data can be written while preventing the modification of new and existing data. This approach directly aligns with the requirement to allow new data to be written to the app while ensuring that the modification of this data is restricted, effectively meeting the security and compliance requirements specified.

Feedback(if wrong):

- B) Modifying the access level of the blob service might change how the blobs are accessed but does not enforce the specific compliance requirement of preventing the modification of data.
- C) Implementing Azure resource locks can prevent accidental deletion or modification of resources but does not provide the granular control needed for compliance with data modification restrictions.
- D) Creating Azure RBAC assignments offers a way to manage access to Azure resources but does not address the specific need to prevent data modification while allowing data writing, which is essential for meeting the compliance requirement.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Data Protection and Compliance in Azure Storage

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

116. Your organization has recently moved its online retail application to Azure. Now, you need to determine the most suitable Azure-based data storage solution for two relational databases, DB1 and DB2. These databases must meet specific requirements, such as maintaining high availability in case two adjacent availability zones fail and having low latency for improved user experience. What would be the best Azure data storage solution for DB1 and DB2 in this context?

- A. Individual Azure SQL databases
- B. Azure SQL Database Elastic Pool
- C. Azure SQL Managed Instance with auto-failover groups
- D. Azure SQL Managed Instance in General Purpose service tier

Answer: C

Feedback(if correct): Azure SQL Managed Instance with auto-failover groups meets the requirements by providing high availability and disaster recovery across multiple regions. The auto-failover groups' feature allows for the replication and automatic failover of a group of databases or all databases in a managed instance to another region, ensuring business continuity in case of regional failures. This option also supports minimizing I/O latency, which is crucial for maintaining a good user experience for an online retail application.

Feedback(if wrong):

- A. Individual Azure SQL databases might not offer the same level of integrated management and native capabilities as a managed instance, particularly for complex availability and disaster recovery requirements.
- B. Azure SQL Database Elastic Pool is useful for managing multiple databases that have varying and unpredictable usage demands but does not specifically address high availability across availability zones or low latency requirements.

D. Azure SQL Managed Instance in General Purpose service tier might not meet the low latency requirement as effectively as the Business-Critical service tier, which is specifically designed for applications with low I/O latency requirements and provides in-memory performance.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Managing and implementing SQL in Azure, understanding service tiers and performance features for Azure SQL

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

117. Contoso is working on a project that requires elevated performance for its proprietary software's accompanying databases. The software handles massive amounts of data, requiring minimal I/O latency and near-zero influence from underlying maintenance activities. DB1 and DB2, the two databases involved, must operate smoothly, even during maintenance periods. What Azure service and service tier should you propose for DB1 and DB2 to fulfill these performance needs?

- A. Azure SQL Managed Instance in General Purpose service tier
- B. Azure SQL Database Elastic Pool
- C. Azure SQL Database in Hyperscale service tier
- D. Azure SQL Managed Instance in Business Critical service tier

Answer: D

Feedback(if correct):- Choosing an Azure SQL Managed Instance in the Business Critical service tier is the optimal solution for DB1 and DB2 to meet the high performance and availability requirements. The Business Critical service tier is specifically designed to offer low I/O latency and minimal impact from maintenance operations, ensuring smooth database performance even during maintenance. Additionally, it supports auto-failover groups for high availability across multiple availability zones, addressing the need for maintaining service even if two availability zones fail.

Feedback(if wrong):-

- A: The General Purpose service tier might not provide the low I/O latency required for high-performance applications.
- B: An Azure SQL Database Elastic Pool is cost-effective for managing multiple databases with variable and unpredictable usage patterns but might not meet specific performance and latency requirements.
- C: While the Hyperscale service tier offers high scalability for large databases, it's not specifically optimized for low latency and minimal maintenance impact like the Business Critical tier.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Managing and implementing SQL in Azure, understanding service tiers and performance features for Azure SQL

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

118. You are tasked with designing an Azure Storage solution to store sensitive data that is less than 10 GB in size. This data will be accessed daily but must be stored securely under specific conditions to meet compliance and operational requirements.

Requirements:

- The data must be retained for five years.
- Once written, the data should be read-only, with no modifications or deletions allowed.
- After five years, the data can be deleted but must not be modified at any point.
- The solution must minimize data access charges.

For an Azure Storage solution that stores less than 10 GB of sensitive data accessed daily, which configuration meets the specified requirements for data retention, immutability, and cost-efficiency?

- A) General purpose v2 storage account with hot access tier and blob-level WORM (Write Once, Read Many) policy.
- B) General purpose v2 storage account with cool access tier and account-level immutability policy.
- C) General purpose v2 storage account with archive access tier and blob-level immutability policy.
- D) Blob storage account with cool access tier and no immutability policy.

Answer: C

Feedback(if correct): A General-purpose v2 storage account with an archive access tier and a blob-level immutability policy meets all the specified requirements by providing a cost-effective solution for storing infrequently accessed data, enforcing a read-only state to ensure compliance with immutability requirements, and allowing for data deletion after five years without the possibility of modification. This setup optimizes both compliance with the retention and immutability requirements and minimizes data access charges by leveraging the archive access tier for infrequently accessed data.

Feedback(if wrong):

- A) The hot access tier, while suitable for frequently accessed data, would not minimize data access charges as efficiently as the archive access tier.
- B) The cool access tier offers a balance between access frequency and cost but does not optimize cost as well as the archive access tier for data that is accessed less frequently and can tolerate retrieval latency.
- D) Lacking an immutability policy fails to meet the compliance requirement that data must be read-only after writing and protected against deletion or modification for five years.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Designing solutions for cost management, and implementing data storage solutions that comply with security and compliance requirements.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

119. In the process of architecting a solution for SQL databases to support your business operations, you're tasked with creating a structure for 15 databases, each approximately 20 GB in size, characterized by their differing access demands. The deployment must adhere to the following criteria to ensure optimal performance and cost efficiency:

- Dynamically scale computing power in response to fluctuating database demands.
- Guarantee a minimum of 99.99% availability to meet service level agreements.
- Ensure reserved computational resources are available for peak performance.
- Prioritize cost reduction in computational expenses.

Given these prerequisites, which database hosting option would best align with your objectives?

- A) Host 15 databases on a Microsoft SQL Server on an Azure Virtual Machine.
- B) Deploy 15 serverless instances of Azure SQL Database.
- C) Position 15 databases on a Microsoft SQL Server on an Azure Virtual Machine within an availability set.
- D) Configure an Azure SQL Database elastic pool to encompass all 15 databases.

Answer: D

Feedback(if correct):

For the scenario where you're designing a SQL database solution involving 15 databases, each 20 GB in size, with varying usage patterns, the optimal solution to host these databases, considering dynamic scaling of compute resources, a service level agreement (SLA) of 99.99% uptime, reserved capacity, and minimized compute charges, is indeed to utilize an elastic pool containing 15 Azure SQL databases (Option D).

An Azure SQL Database elastic pool is the recommended choice because it efficiently manages and scales multiple databases with varying usage patterns within a set budget. This approach offers dynamic scaling of compute resources, meets the high availability requirements with a 99.99% SLA, provides reserved capacity for consistent performance, and helps minimize compute costs by sharing resources across databases.

Feedback(if wrong):

Option A: Hosting 15 databases on a Microsoft SQL server running on an Azure virtual machine could meet some requirements but does not offer the same level of resource flexibility or cost efficiency as an elastic pool.

Option B: While Azure SQL Database serverless can dynamically allocate compute resources, it might not guarantee the reserved capacity required for this scenario and could result in higher costs for 15 databases.

Option C: Hosting 15 databases on a Microsoft SQL server on an Azure virtual machine within an availability set improves availability but lacks the dynamic scaling and cost efficiency of an elastic pool.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Implementing Azure SQL Database solutions with high availability, dynamic scaling, and cost efficiency.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

120. Your organization is in the process of transitioning its on-premises SQL Server environment, which hosts several critical databases, to Azure for enhanced scalability and flexibility. The environment includes 10 databases, with the largest database not exceeding 2 TB in size. You aim to ensure the transition aligns with the following criteria:

- Minimize the adjustments needed on the databases to enable the migration.
- Ensure that database management is as streamlined as possible post-migration.
- Allow for seamless Active Directory authentication for user access.

Given these requirements, which Azure service would you recommend for hosting the databases?

- A) Azure SQL Database single instances for each database.
- B) Azure SQL Database Managed Instance for a blend of managed service benefits and compatibility.
- C) Azure SQL Database elastic pools to efficiently manage resources across multiple databases.
- D) Hosting SQL Server on Azure Virtual Machines for full control over the database environment.

Answer: B

Feedback(if correct): Azure SQL Database Managed Instance is the optimal choice because it provides a high degree of compatibility with on-premises SQL Server, including support for larger databases and features such as CLR. It also simplifies database management by offering a managed service that reduces administrative overhead while supporting Active Directory authentication, aligning with the requirements for a streamlined migration process and minimal adjustments to the databases.

Feedback(if wrong):

- A (Azure SQL Database single instances): While Azure SQL Database offers a PaaS solution with managed capabilities, single instances might require more adjustments for each database and do not inherently provide the same level of on-premises SQL Server feature compatibility as Managed Instances.

- C (Azure SQL Database elastic pools): Elastic pools provide a cost-effective solution for managing multiple databases with variable usage patterns. However, they might not offer the seamless migration path and feature set required for databases that need minimal adjustments.
- D (Hosting SQL Server on Azure Virtual Machines): This option gives full control over the database environment, mirroring the on-premises setup. While it supports all SQL Server features, including CLR, it does not minimize administrative overhead since it requires manual management of the VM, making it less aligned with the streamlined management goal.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Designing Data Platforms
- Competencies: Migrating on-premises SQL Server databases to Azure, managing databases in the cloud, integrating Azure services with Active Directory.
- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Application

121. To design a solution that empowers developers to provision Azure virtual machines with specific regional and size constraints, it is essential to ensure that the deployment adheres to organizational guidelines and cost management objectives. Your organization aims to streamline the development process by providing developers with the autonomy to provision Azure virtual machines for various projects. However, to maintain compliance with regulatory requirements and optimize cloud expenditures, you need to enforce restrictions on where these virtual machines can be located and their sizes.

Requirements:

- Restrict virtual machine deployment to approved Azure regions only, to comply with data residency regulations.
- Limit the sizes of the virtual machines to a predefined list to avoid unnecessary costs associated with over-provisioning.
- Implement a solution that minimizes manual oversight while ensuring compliance with these policies.

Given these considerations, which Azure service should you recommend to automatically enforce these requirements when developers provision new virtual machines?

- A) Implement Conditional Access policies to restrict login regions.
- B) Utilize role-based access control (RBAC) to limit provisioning capabilities.
- C) Leverage Azure Resource Manager (ARM) templates to standardize deployment configurations.
- D) Apply Azure Policy to enforce location and size restrictions on virtual machines.

Answer: D

Feedback(if correct):- The correct answer is D) Apply Azure Policy to enforce location and size restrictions on virtual machines. Azure Policy allows organizations to create, assign, and manage policies that enforce rules over their resources, ensuring compliance with corporate and regulatory standards. By using Azure Policy, you can automate the enforcement of rules that restrict the regions in which virtual machines can be deployed and the sizes available for provisioning, directly aligning with the requirements to control data residency and manage costs without manual intervention.

Feedback(if wrong):-

- A) Implementing Conditional Access policies would primarily restrict user access based on conditions like user location or device state, but it does not directly control the provisioning of resources like virtual machine sizes or locations.
- B) Utilizing role-based access control (RBAC) can limit what actions a user can perform within Azure, such as provisioning capabilities. However, RBAC alone does not provide the granular control needed to enforce specific location and size restrictions for virtual machine deployment.
- C) Leveraging Azure Resource Manager (ARM) templates allows for the standardization of deployment configurations and can define allowed sizes and locations. Still, it relies on users selecting from predefined templates and does not enforce these restrictions across all provisioning actions outside of those templates.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Implementing Azure SQL Database Managed Instances for scalable, high-availability database solutions with Active Directory integration.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

122. Your organization is deploying a globally distributed application, App2, with instances placed in multiple availability zones. To ensure data consistency and durability, you need to recommend a data storage solution that meets App2's unique requirements.

Recommend a solution that meets the following requirements:

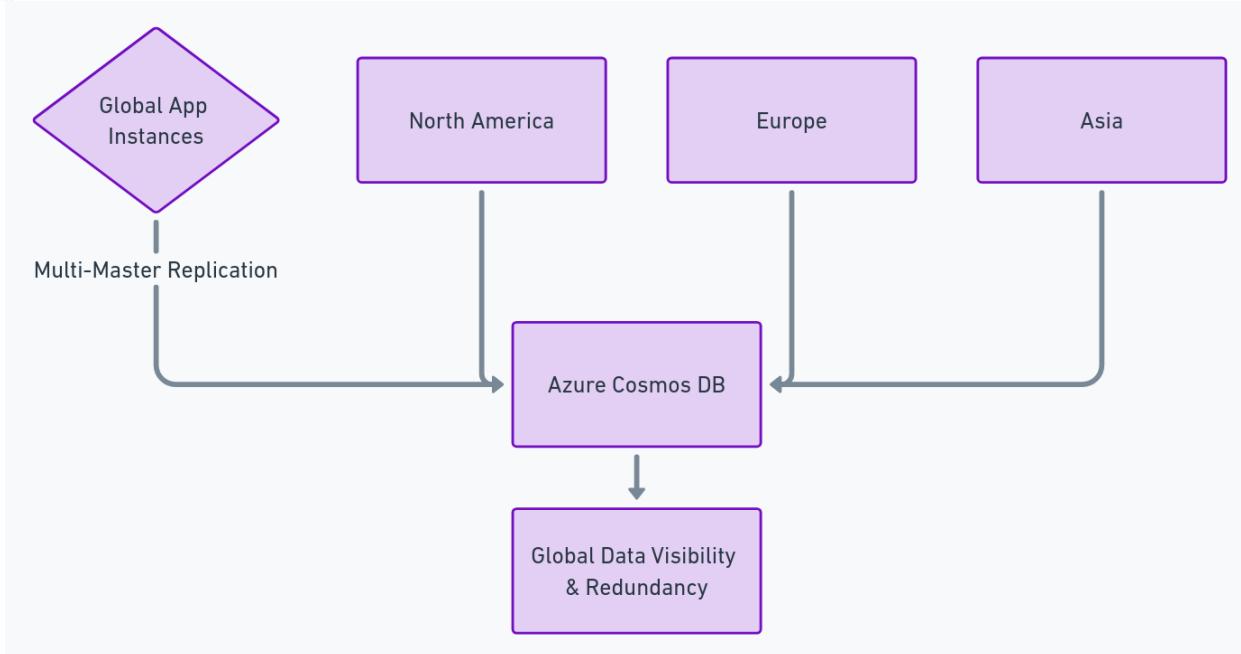
- Data written by any App2 instance should be immediately visible to all other instances.
- Each instance must write data to a data store in the same availability zone.
- Data redundancy is ensured across different zones within the same region.

- A) Azure Storage account with ZRS
- B) Azure SQL Database with active geo-replication
- C) Azure Data Lake Store with GZRS
- D) Azure Cosmos DB with multi-master replication

Answer: D

D) Azure Cosmos DB with multi-master replication

Feedback(if correct): Azure Cosmos DB with multi-master replication is the optimal choice for App2's requirements. It allows each App2 instance to write data locally within its availability zone, ensuring low-latency operations. The multi-master replication feature ensures that data is immediately visible to all other instances globally, providing data consistency. Additionally, Azure Cosmos DB inherently supports data redundancy across zones within the same region, satisfying the need for data durability and availability.



Feedback(if wrong):

- A) Azure Storage account with Zone-Redundant Storage (ZRS) provides data redundancy across multiple availability zones within the same region but does not ensure that data written by one instance is immediately visible to all other instances.
- B) Azure SQL Database with active geo-replication supports data replication across regions but may not offer the lowest latency for writes in local availability zones and does not inherently support immediate visibility of written data across all instances.
- C) Azure Data Lake Store with Geo-Zone-Redundant Storage (GZRS) ensures data durability and redundancy but does not specialize in providing low-latency writes within availability zones or immediate data visibility across global instances.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Designing Data Platforms
- Competencies: Implementing Azure Cosmos DB solutions with multi-master replication for global distribution and immediate data visibility.
- Difficulty Level: Expert
- Bloom's Taxonomy Level: Application

123. To ensure compliance with data retention policies for a critical application's database hosted on Azure SQL Database, your organization mandates the storage of database backups for an extended period. Your organization's application utilizes Azure SQL Database for its operational data needs. Given the critical nature of the data and regulatory requirements, there's a necessity to store backups for a substantial duration to facilitate potential future access and audits.

Requirements:

- The solution must automate the backup process without manual intervention.
- Backups must be retained for a specified period exceeding the default backup retention periods provided by Azure.
- Ensure that the backup storage solution is cost-effective and secure.

Given these requirements, which of the following options would best suit the organization's needs for extended database backup retention?

- A) Implement Azure Site Recovery for continuous backup and replication.
- B) Activate geo-replication for the Azure SQL Database to another region.
- C) Establish automatic Azure SQL Database backups with default retention settings.
- D) Configure a Long-Term Backup Retention (LTR) policy for the Azure SQL Database.

Answer: D

Feedback(if correct):- Automated Backups: Enables the scheduling of backups to occur automatically, ensuring data is consistently backed up without manual intervention.

Extended Retention: LTR policies allow for the configuration of backup retention for periods much longer than the default, catering to compliance and regulatory needs.

Cost-Effectiveness: Utilizing LTR policies for long-term backup storage can be more cost-effective compared to other methods, as backups can be stored in cost-efficient storage tiers.

Security: Azure ensures that backups are encrypted, maintaining the security of the data even over long retention periods.

Feedback(if wrong):

- A) Azure Site Recovery: Focuses on real-time data replication for disaster recovery rather than backup retention.

- B) Geo-Replication: Primarily provides data redundancy and high availability across regions, not extended backup retention.
- C) Default Azure SQL Database backups: While offering backup capabilities, may not meet the extended retention requirements specified without additional configuration.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Configuring backup and data retention policies in Azure SQL Database to meet organizational compliance and data protection requirements.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

124. Your organization plans to migrate a critical business application, App1, from an on-premises data center to Azure. App1 has a three-tier architecture with a web front end, an application layer, and a SQL Server database. The SQL Server database is currently hosted on a physical server. To ensure a smooth transition with minimal downtime, you need to formulate a migration strategy that aligns with Azure's best practices. Given these prerequisites, which Azure migration strategy should you recommend for the SQL Server database component of App1?

- A) Implement Azure Database Migration Service to move the SQL Server database to Azure SQL Database.
- B) Utilize Azure Site Recovery to replicate the SQL Server databases directly to Azure VMs.
- C) Migrate the SQL Server database to a BACPAC file and upload it to Azure Blob Storage, then import it to Azure SQL Database.
- D) Convert the physical server to a virtual hard disk (VHD) and upload it to Azure Blob Storage, then attach it to an Azure VM.

Answer: A

Feedback(if correct):-

Azure Database Migration Service (DMS) provides a streamlined, fully managed migration experience for moving your SQL Server databases to Azure SQL Database with minimal downtime. It supports a wide range of migration scenarios and is specifically designed for this purpose.

Azure SQL Database offers scalability, high availability, and security, aligning with the organization's requirements for critical business applications.

Feedback(if wrong):

- B) Utilizing Azure Site Recovery primarily targets disaster recovery scenarios rather than database migration and might not provide the smooth transition needed for a critical database migration.
- C) Migrating the SQL Server database to a BACPAC file involves additional steps and complexity, potentially leading to longer downtime during migration.
- D) Converting the physical server to a VHD for migration is a viable option for lifting and shifting the entire server but does not leverage the managed services and capabilities of Azure SQL Database, which can optimize performance and management post-migration.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Migrating on-premises SQL Server databases to Azure SQL Database using Azure Database Migration Service.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

125. A company plans to move its marketing analytics platform, MarketingApp1, to Azure. The application comprises a web tier that employs Apache Tomcat and a database tier that uses MySQL Server 2017. Both tiers are installed on virtual machines operated by VMware. Considering this scenario, what strategy should you suggest for transferring MarketingApp1's database content to Azure?

- A) Use Azure Site Recovery to copy the VMware virtual machines to Azure.
- B) Implement MySQL Server transactional replication.
- C) Export the MySQL database schema and data to a dump file, then import it into Azure Database for MySQL.
- D) Convert the MySQL Server virtual machine to an Azure virtual hard disk (VHD) and save it to Azure Blob storage.



Answer: C

Feedback(if correct): This approach is correct because it leverages the native capabilities of MySQL for exporting and importing databases. Azure Database for MySQL provides a fully managed MySQL database service, making it an ideal target for hosting MarketingApp1's database. This method ensures that the data and schema are properly formatted for Azure, offering a seamless transition with minimal adjustments required.

Feedback(if wrong):

- A) Using Azure Site Recovery focuses more on disaster recovery and may not be the optimal choice for database migrations, especially when the goal is to leverage managed database services in Azure.
- B) Implementing MySQL Server transactional replication is primarily used for high availability within the same environment, not for migrating databases between different platforms.
- D) Converting the MySQL Server VM to a VHD involves migrating the entire VM, not just the database. This does not take advantage of the managed database services available in Azure, potentially leading to higher management overhead.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Migrating on-premises database systems to Azure-managed database services, specifically focusing on strategies for transitioning from MySQL Server to Azure Database for MySQL.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

126. Your task is to develop a logging pipeline that accurately captures and logs every instance of user creation and role assignment within your Azure Active Directory (AAD) environment. This recorded data needs to be efficiently stored in Azure Cosmos DB for further analysis and compliance auditing. Considering Azure's suite of services and tools, you must identify the most effective combination to implement this pipeline. Which sequence of Azure services would best facilitate the construction of this logging pipeline, ensuring data from AAD is captured accurately and stored in Azure Cosmos DB?

- A) AAD Audit logs > Stream to Event Hub > Process with Azure Functions > Save to Azure Cosmos DB

- B) Azure Activity Logs > Send to Azure Monitor > Filter and export to Azure Storage > Import to Azure Cosmos DB
- C) AAD Audit logs > Send to Azure Event Grid > Fan-out to multiple subscribers > Save to Azure Cosmos DB
- D) Azure Diagnostics > Collect from AAD > Transfer to Azure Event Hub > Process with Azure Stream Analytics > Persist to Azure Cosmos DB

Answer: A

Feedback(if correct): Option A correctly outlines the end-to-end process of capturing, processing, and storing AAD audit logs for user creations and role assignments in Azure Cosmos DB. It utilizes AAD Audit logs for the initial data source, Azure Event Hub for real-time data streaming, Azure Functions for processing and transformation, and Azure Cosmos DB for scalable and secure data storage, making it the optimal choice for this scenario.

Feedback(if wrong):

Option B relies on Azure Activity Logs, which are not directly related to capturing AAD audit logs for user creations and role assignments, and involves unnecessary steps of filtering and exporting data to Azure Storage before importing to Azure Cosmos DB.

Option C involves Azure Event Grid, which, while useful for event routing, does not align with the requirement for a continuous data processing pipeline from AAD to Cosmos DB.

Option D mentions Azure Diagnostics and Azure Stream Analytics, which adds complexity and is not directly aligned with the straightforward process of capturing AAD audit logs and storing them in Cosmos DB as outlined in option A.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Implementing solutions for logging and monitoring within Azure Active Directory and integrating with Azure services for data processing and storage.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

127. You are designing an order processing system in Azure that will contain the following Azure resources:

Name	Type	Performance
storage1	StorageV2	Standard
storage2	StorageV2	Premium
storage3	BlobStorage	Standard
storage4	FileStorage	Premium

The order processing system will have the following transaction flow:

1. A customer will place an order using App1.
2. When the order is received, App1 will generate a message to check for product availability at vendor 1 and vendor 2.
3. An integration component will process the message, and then trigger either Function1 or Function2 depending on the type of order.
4. Once a vendor confirms the product availability, a status message for App1 will be generated by Function1 or Function2.
5. All the steps of the transaction will be logged to storage1.

Which type of resource should you recommend for the integration component?

- A. An Azure Data Factory pipeline
- B. An Azure Service Bus queue
- C. An Azure Event Grid domain
- D. An Azure Event Hubs capture

Answer: A

Feedback(if correct):

A data factory can have one or more pipelines, which are logical groupings of activities that perform tasks. Azure Data Factory supports various activities, including data movement, data transformation, and control activities. Additionally, Azure Functions can be integrated with Azure Data Factory, allowing the execution of Azure Functions as steps in data factory pipelines.

Feedback(if wrong):

- B) An Azure Service Bus queue While Azure Service Bus is a messaging service that enables communication between applications and services, it may not provide the necessary capabilities for processing and triggering functions based on message content.
- C) An Azure Event Grid domain Azure Event Grid is a fully managed event routing service that allows you to easily build event-driven applications. However, it may not be the best choice for orchestrating the transaction flow described in the scenario.
- D) An Azure Event Hubs capture Azure Event Hubs is a scalable event processing service, but it focuses on ingesting and processing large volumes of events rather than orchestrating transactional workflows.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskills: Designing Compute and Network Infrastructure

Competencies: Architecting for Business Continuity and Disaster Recovery

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application, Analysis

128. You plan to deploy multiple instances of an Azure web app across several Azure regions.

You need to design an access solution for the app. The solution must meet the following replication requirements:

- Support rate limiting
- Balance requests between all instances

Does using Azure Application Gateway meet these goals?

A. Yes

B. No

Answer: B

Feedback (if correct):

Azure Application Gateway partially meets these goals. While it can balance requests between all instances, it does not support rate limiting natively. To achieve rate limiting, you can pair Azure Application Gateway with Azure API Management, Azure Front Door, or another service. Keep in mind that this additional service will add complexity to the overall solution.

Why Azure Application Gateway Alone Isn't Enough:

While Azure Application Gateway provides important features like SSL termination, custom routing, and Web Application Firewall capabilities, it operates within a single Azure region and doesn't inherently support rate limiting. For scenarios requiring global distribution and rate limiting, the combination of Azure Front Door or Traffic Manager with Azure API Management is a more comprehensive solution.

Feedback (if wrong):

Azure Application Gateway can balance requests between all instances, ensuring high availability and load distribution. However, it does not support rate limiting natively, and therefore, another solution must be added to meet that requirement. Using Azure Application Gateway alone will not suffice.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskills: Designing Compute and Network Infrastructure

Competencies: Scaling Applications & Services

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

129. You plan to deploy multiple instances of an Azure web app across several Azure regions.

You need to design an access solution for the app. The solution must meet the following replication requirements:

- Support rate limiting
- Balance requests between all instances

Does using Azure Front Door (AFD), Azure Application Gateway for internal load balancing, Web Application Firewall (WAF), and SSL termination. meet these goals?

- A. Yes
B. No

Answer: A

Feedback(if correct):-

Azure Front Door (AFD): AFD is designed for global traffic management and can distribute traffic across multiple Azure regions. It provides advanced routing capabilities to ensure that requests are balanced across all instances of your web app.

Rate Limiting: While Azure Front Door itself does not provide explicit rate limiting, it offers integration with Azure Web Application Firewall (WAF), which can be configured with custom rules to manage and limit the rate of requests, thereby indirectly achieving rate limiting.

Azure Application Gateway: For internal load balancing within a region, Azure Application Gateway can distribute traffic to web app instances. It also supports WAF for added security and SSL termination for secure communications.

Web Application Firewall (WAF) and SSL Termination: WAF protects against common web vulnerabilities and can be configured with custom rules for rate limiting. SSL termination ensures that encrypted traffic is efficiently managed, enhancing security while reducing the encryption/decryption load on the web app instances.

This combination of Azure services allows for global distribution of requests to multiple instances of a web app across various Azure regions while supporting rate limiting through WAF, internal load balancing via Azure Application Gateway, and ensuring secure communications with SSL termination.

130. You are tasked with deploying resources to host a stateless web app in an Azure subscription. The solution must provide access to the full .NET framework, offer redundancy in case of an Azure region failure, and allow administrators access to the operating system for installing custom application dependencies. You plan to deploy an Azure virtual machine scale set that uses autoscaling. Does this solution meet the goal?

A. Yes

B. No

Answer: B

Feedback(if correct): The correct answer is B. No. Deploying an Azure virtual machine scale set with autoscaling does not inherently provide redundancy across Azure regions, which is required in this scenario. Additionally, it does not directly grant administrators access to the operating system for installing custom application dependencies.

Feedback(if wrong): Option A is incorrect because deploying an Azure virtual machine scale set with autoscaling does not meet the requirement for redundancy across Azure regions or provide direct access for administrators to install custom application dependencies.

Feedback(if wrong):-

Selecting "No" is incorrect because the combination of Azure Front Door (AFD), Azure Application Gateway, Web Application Firewall (WAF), and SSL termination indeed meets the requirements for rate limiting and balancing requests between all instances. Azure Front Door provides global load balancing

and rate limiting to ensure efficient traffic distribution and security across multiple regions. The use of Azure Application Gateway for internal load balancing, along with WAF for security and SSL termination for secure communications, supports the solution's goals effectively.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskills: Designing Compute and Network Infrastructure

Competencies: Analyzing requirements and recommending appropriate Azure services

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

131. Your organization plans to utilize Azure reservations for an Azure SQL database. Which resource type will the reservation discount be applied to?

- A) vCore compute
- B) DTU compute
- C) Storage
- D) License

Answer: A

Feedback(if correct): The correct selection is A) vCore compute. Azure reservations are applied to compute resources such as vCores in the Azure SQL Database, allowing for discounted pricing based on the reserved capacity.

Feedback(if wrong): The reservation discount is not applied to DTU computing, storage, or licensing. It specifically applies to compute resources like vCores in Azure SQL Database.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskill: Designing Compute and Network Infrastructure

Competency: Understanding Azure pricing and cost management, Designing cost-effective, Solutions using Azure reservations, Understanding Azure resource types and their billing models, Designing Azure infrastructure for optimized cost management

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

132. Your organization is planning to optimize costs by utilizing Azure reservations. Which Azure services can Azure reservations be applied to? Choose all that apply.

- A. Virtual Machines
- B. Azure SQL Databases
- C. Azure Cosmos DB
- D. Azure DevOps

Answer: A, B

Feedback(if correct):- Azure reservations can indeed be applied to Virtual Machines and Azure SQL Databases. Both options A) and B) are correct.

Feedback(if wrong):- Option C) Azure Cosmos DB and option D) Azure DevOps are incorrect. Azure reservations cannot be applied to these services.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskill: Designing Compute and Network Infrastructure

Competency: Understanding Azure pricing and cost management, Designing cost-effective, Solutions using Azure reservations, Understanding Azure resource types and their billing models, Designing Azure infrastructure for optimized cost management

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

133. Match the Azure services to their corresponding functionalities. Instructions: For each functionality listed below, match it with the correct Azure service that provides that capability.

1. Functionality: Host web applications that can scale automatically based on demand.

- A. Azure Functions
- B. Azure Kubernetes Service (AKS)
- C. Azure App Service
- D. Azure Virtual Machines

2. Functionality: Deploy and manage containerized applications with a serverless Kubernetes service.

- A. Azure Functions
- B. Azure Kubernetes Service (AKS)
- C. Azure App Service
- D. Azure Virtual Machines

3. Functionality: Execute code in response to events without the need to manage server infrastructure.

- A. Azure Functions
- B. Azure Kubernetes Service (AKS)
- C. Azure App Service
- D. Azure Virtual Machines

4. Functionality: Run virtual machines for Windows and Linux in the cloud.

- A. Azure Functions
- B. Azure Kubernetes Service (AKS)
- C. Azure App Service
- D. Azure Virtual Machines

Correct Matches:

1. C. Azure App Service
2. B. Azure Kubernetes Service (AKS)
3. A. Azure Functions
4. D. Azure Virtual Machines

Feedback(if correct):

Azure App Service provides a platform for hosting web applications, allowing them to scale automatically with demand. Azure Kubernetes Service (AKS) is designed for deploying and managing containerized applications without managing the underlying server infrastructure, offering a serverless Kubernetes environment. Azure Functions enables running code in response to events without the need to provision or manage servers, perfect for executing small pieces of code or "functions" in the cloud. Azure Virtual Machines offer scalable computing infrastructure, allowing you to run virtualized servers in the cloud for both Windows and Linux.

Feedback(if wrong):

- Azure Functions is specifically designed for serverless computing, allowing execution of code triggered by events, making it incorrect for hosting web applications or managing containerized services.

Azure App Service scalability.



- Azure Kubernetes Service (AKS) is for managing containerized applications, not for serverless function execution or traditional web hosting.
- Azure App Service is optimized for hosting web applications with auto-scaling capabilities, making it unsuitable for low-level infrastructure management or container orchestration.
- Azure Virtual Machines provide infrastructure as a service (IaaS) for running virtual machines, not for serverless computing, container management, or auto-scaling web hosting.

skill mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ305

Subskill: Designing Compute and Network Infrastructure

Competency: Planning and Implementing Azure Virtual Networks

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Synthesis

134. A multinational enterprise utilizes Azure Kubernetes Service (AKS) for hosting its container-based applications, ensuring global reach and availability. Given the critical nature of these applications, the enterprise seeks to implement a robust disaster recovery strategy that guards against regional outages, maintaining uninterrupted service access for its global user base. Advise on integrating two Azure services to enhance the resilience of multi-region AKS deployments, ensuring the applications remain accessible even during regional disruptions. Which two services should you recommend to protect the multi-region AKS deployments from regional outages, thus ensuring continuous global application availability?

- A. Azure Traffic Manager
- B. Azure Backup
- C. Azure Load Balancer
- D. Azure App Service

Answers: A, C

Feedback(if correct):-

To ensure high availability and disaster recovery for multi-region AKS deployments, integrating Azure Traffic Manager (A) and Azure Load Balancer (C) is essential.

Azure Traffic Manager acts as a DNS-based traffic load balancer, distributing client requests across all global AKS instances based on traffic-routing methods like geographic routing. This ensures users are directed to the nearest operational region, enhancing performance and availability.

Azure Load Balancer, on the other hand, ensures that traffic within each region is efficiently distributed among the AKS nodes, offering high availability and network performance. In the event of a regional outage, the Load Balancer facilitates the seamless redirection of traffic to the surviving regions without service interruption.

Feedback(if wrong):-

B. Azure Backup is crucial for data protection and recovery strategies but does not directly contribute to real-time traffic management or disaster recovery in the context of regional outages.

D. Azure App Service provides a platform for hosting web applications and does not directly support container-based workloads in AKS or offer a solution for regional resilience as required in this scenario.

Skill Mapping:

Skill: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskill: Designing Compute and Network Infrastructure

Competency: Understanding Azure pricing and cost management, Designing cost-effective, Solutions using Azure reservations, Understanding Azure resource types and their billing models, Designing Azure infrastructure for optimized cost management

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

135. Your company maintains an Azure subscription that includes a Basic Azure virtual WAN named Virtual/WAN1, which encompasses multiple virtual hubs located across different Azure regions. You have an ExpressRoute circuit configured in one of these regions. What initial step is required to establish an ExpressRoute association with VirtualWAN1?

- A) Configure a hub virtual network in the region where the ExpressRoute circuit is deployed.
- B) Create a gateway on one of the virtual hubs within Virtual/WAN1.
- C) Upgrade Virtual/WAN1 from Basic to Standard tier.
- D) Enable the ExpressRoute premium add-on for Virtual/WAN1.

Answer: C

Feedback(if correct): Upgrading Virtual/WAN1 from the Basic to the Standard tier is the correct initial step because ExpressRoute associations require the Standard tier for connectivity. By upgrading, Virtual/WAN1 will have the necessary capabilities to establish the ExpressRoute association.

Feedback(if wrong): A) Configure a hub virtual network in the region where the ExpressRoute circuit is deployed: While configuring a hub virtual network is a necessary step in setting up network connectivity within Azure Virtual WAN, it is not the initial step required specifically for establishing an ExpressRoute

association with VirtualWAN1. Moreover, the ability to associate an ExpressRoute circuit depends on the Virtual WAN being in the Standard tier.

B) Create a gateway on one of the virtual hubs within Virtual/WAN1: Creating a gateway is a part of setting up connectivity in Azure Virtual WAN. However, the ability to link an ExpressRoute circuit specifically requires the Virtual WAN to be in the Standard tier, making this option not the correct initial step for the scenario described.

D) Enable the ExpressRoute premium add-on for Virtual/WAN1: While the ExpressRoute Premium add-on provides additional features and increased limits for ExpressRoute circuits, the primary requirement for associating an ExpressRoute circuit with an Azure Virtual WAN is for the WAN to be in the Standard tier. This option does not directly address the tier requirement for Virtual WAN.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Analytical thinking, Problem-solving

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

136. Your team is in the process of designing a highly available web application, App1, to be deployed on Azure. App1 is expected to experience varying levels of traffic, with peaks during specific times of the year. The primary goal is to ensure the high availability and resilience of App1 across different geographic locations while also keeping the operational costs as low as possible.

Requirement:

The architecture must ensure that App1 remains highly available and resilient against failures in any single location, with the ability to scale resources according to traffic demands. Cost efficiency is a critical factor in the selection of the architecture, emphasizing the need for a solution that balances performance, availability, and cost.

To meet the high availability, resilience, and cost-efficiency requirements for App1, which Azure App Service architecture should you recommend?

- A. Deploy one App Service Environment (ASE) across multiple availability zones.
- B. Utilize one App Service plan per availability zone.
- C. Implement one App Service plan across multiple regions.

D. Configure one App Service Environment (ASE) in each targeted region.

Answer: B

Feedback(if correct):-

Choosing one App Service plan per availability zone ensures App1's high availability and resilience by leveraging the intrinsic benefits of availability zones. This setup offers a scalable and cost-efficient solution by allowing the application to utilize resources across multiple zones within the same region, ensuring operational continuity even if one zone fails. This method optimally balances performance, availability, and cost considerations, making it an ideal choice for App1.

Feedback(if wrong):-

A. Deploy one App Service Environment (ASE) across multiple availability zones. ASEs provide a dedicated environment but at a significantly higher cost, making it less ideal for cost minimization efforts.

C. Implement one App Service plan across multiple regions. This option doesn't align with Azure's geographic distribution capabilities and could introduce latency and complexity without providing regional resilience benefits.

D. Configure one App Service Environment (ASE) in each targeted region. While offering high isolation and geographic distribution, the costs associated with maintaining ASEs in each region make this option the least cost-effective for the scenario described.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Architecting scalable and cost-effective solutions on Azure App Service

Difficulty Level: Intermediate

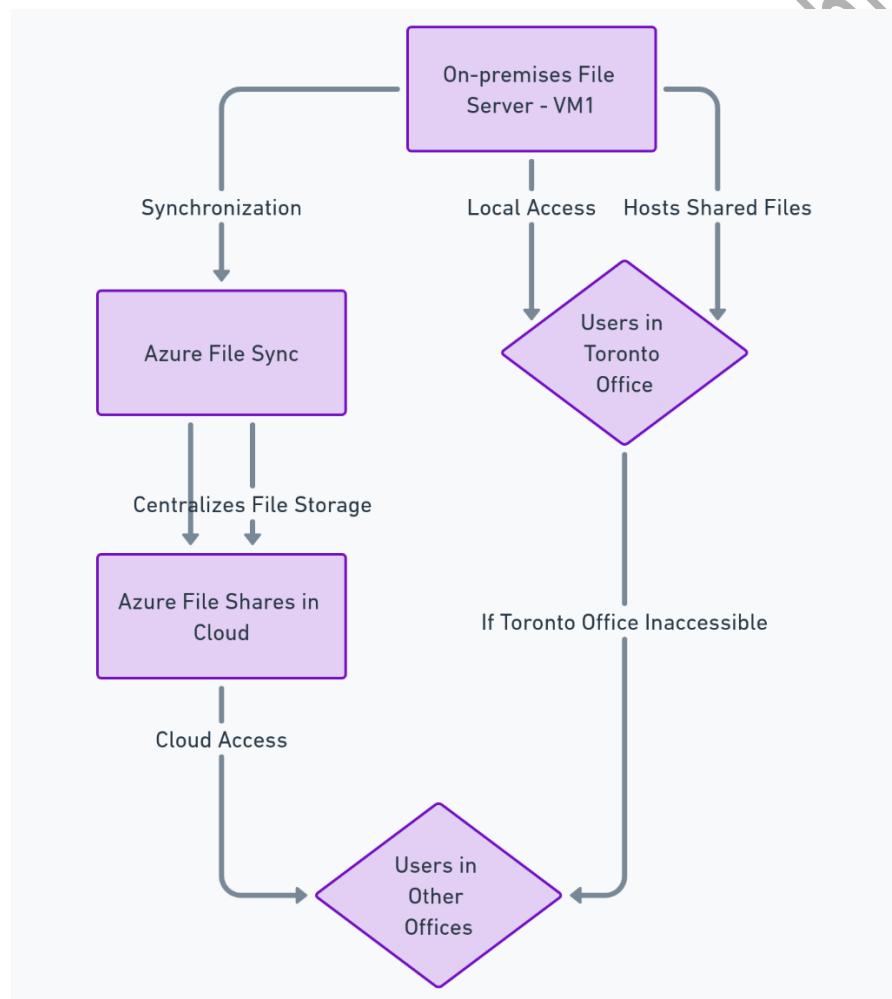
Bloom's Taxonomy Level: Application

137. Your organization operates with a network distributed across multiple locations, including an essential branch in Toronto that hosts a file server, VM2, crucial for daily operations. Users from all branches require continuous access to the files stored on VM2. However, there's a need to maintain file accessibility even if the Toronto branch experiences downtime. What strategy should you employ to ensure uninterrupted file access across the organization, considering the potential inaccessibility of the Toronto branch?

- A. Implement Azure Blob Containers with Azure File Sync for distributed file sharing.
- B. Establish an Azure File Share coupled with Azure File Sync to replicate file accessibility.
- C. Set up a Recovery Services vault with Azure Backup for the Toronto VM2 file server.
- D. Deploy Azure Blob Containers and utilize Windows Server Backup on VM2.

Answer: B

Feedback(if correct):- The optimal solution for ensuring users can access shared files quickly if the Toronto branch office is inaccessible is to utilize Azure File Sync alongside an Azure file share. This setup centralizes file storage in Azure Files, maintaining on-premises file server flexibility, performance, and compatibility. Azure File Sync ensures that even if the local server is down, users can still access files stored in Azure, effectively acting as a backup and access point.



Feedback(if wrong):-

A. a Recovery Services Vault and Azure Backup: This option is designed for data protection and recovery rather than optimizing file access across locations.

C. Azure blob containers and Azure File Sync: While Azure Blob Storage is great for unstructured data storage, it's not the best fit for a scenario that requires file server capabilities and seamless integration with Windows Server.

D. a Recovery Services vault and Windows Server Backup: Similar to option A, this is more about data protection rather than ensuring continuous access to file shares across multiple locations.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Implementing Azure storage solutions and Azure File Sync for hybrid scenarios.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

138. Your organization runs a mission-critical LoB web application that collects sensitive user data. The application is currently hosted on-premises, but you plan to migrate it to Azure. The solution must meet the following requirements:

- Meet strict compliance standards for data handling.
- Store data in a physically isolated manner.
- Guarantee minimal latency for end-users.

Would deploying the web application using Azure Service Fabric Mesh meet these goals?

A. Yes

B. No

Answer: B

Feedback(if correct):-

No, deploying the web application using Azure Service Fabric Mesh alone might not fully meet these goals. While Service Fabric Mesh is a fully managed service that enables you to deploy microservices applications without managing virtual machines or storage, it doesn't inherently guarantee physical data

isolation or compliance with specific data handling standards. For compliance and data isolation, additional Azure services and configurations such as Azure SQL Database with Advanced Data Security, Azure Dedicated Host, or Azure Virtual Network could be necessary to ensure data is stored in compliance with strict standards and a physically isolated manner.

Feedback(if wrong):-

Service Fabric Mesh simplifies microservices application deployment and management but does not specifically address physical data isolation or compliance requirements directly. Additional measures and Azure services are required to meet strict compliance and data isolation needs.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Understanding of Azure Service Fabric Mesh, Azure compliance features, and data isolation strategies

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

139. Your organization requires a highly available and scalable solution to deploy a line-of-business (LoB) application in Azure. The LoB application consists of a mission-critical front-end web app and a back-end database that experiences frequent fluctuations in user traffic. Additionally, there are strict regulatory compliance requirements mandating strong network isolation between the front-end and back-end environments for security reasons.

Requirements:

High Availability: The front-end web app must be highly available with minimal downtime even during infrastructure failures.

Horizontal Scaling: The solution needs to support automatic scaling of the web app based on real-time traffic demands.

Network Isolation: The front-end and back-end environments must be completely isolated from each other on a network level for enhanced security and compliance.

Ease of Management: The chosen solution should be relatively easy to manage and maintain.

Would deploying the LoB application using an Azure App Service Environment (ASE) be the most suitable solution to meet all the specified requirements?

A. Yes

B. No

Answer: A.

Feedback(if correct):-

An Azure App Service Environment (ASE) is the ideal choice for hosting the line-of-business application due to its ability to fulfill all the specified requirements effectively:

High Availability: ASEs are built on top of Azure App Service, offering high availability configurations and the ability to run on multiple instances, ensuring minimal downtime even in the face of infrastructure failures.

Horizontal Scaling: ASE supports automatic scaling based on demand, allowing the front-end web app to handle fluctuating user traffic efficiently.

Network Isolation: ASE provides a fully isolated and dedicated environment for running Azure App Services, which ensures strong network isolation between the front-end web app and back-end database environments, meeting strict regulatory compliance requirements.

Ease of Management: Despite offering advanced features like network isolation and scalability, ASE integrates with Azure management tools, making it relatively straightforward to manage and maintain compared to managing similar configurations on virtual machines or containers.

Feedback(if wrong):-

B (No) would imply that there's an alternative Azure service that better meets the combined requirements of high availability, horizontal scaling, network isolation, and ease of management for both the front-end and back-end components of the LoB application. However, ASE is specifically designed to provide these capabilities within a single, managed service, making it the most suitable choice for scenarios with these specific requirements.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Understanding of Azure Service Fabric Mesh, Azure compliance features, and data isolation strategies

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

140. To ensure the integration of an ExpressRoute circuit with a Basic Azure Virtual WAN (VirtualWAN1) for enhanced connectivity and broader network architecture within your Azure subscription, what initial step is required to establish this connection successfully?

- A. Upgrade VirtualWAN1 to Standard.
- B. Create a gateway on Hub1.
- C. Create a hub virtual network in the US East.
- D. Enable the ExpressRoute premium add-on.

Answer: A

Feedback(if correct): Upgrading VirtualWAN1 from Basic to Standard is the essential first step to establishing an ExpressRoute association. The Basic tier of Azure Virtual WAN supports site-to-site VPN connections but does not support ExpressRoute connections. Upgrading to the Standard tier enables integration with ExpressRoute, providing a broader network architecture and enhanced connectivity options within Azure.

Feedback(if wrong):

- B. Create a gateway on Hub1: Creating a gateway on Hub1 is necessary for connecting virtual networks but is not the first step needed for integrating an ExpressRoute circuit with VirtualWAN1.
- C. Create a hub virtual network in the US East: While having a virtual network in the same region as the ExpressRoute circuit can be beneficial, it's not the prerequisite step for ExpressRoute integration with VirtualWAN1.
- D. Enable the ExpressRoute premium add-on: Enabling the ExpressRoute premium add-on offers extended features like increased route limits and global connectivity. However, it's not required for the initial step of establishing an ExpressRoute association with a Basic Azure Virtual WAN, which first needs to be upgraded to Standard.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Implementing and managing networking solutions, Designing for high-availability

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

141. To accommodate the growing demand for an application hosted on Azure Container Instances, your team has decided to transition from single-instance deployments to a managed Kubernetes service. The solution must provide fast provisioning, autoscale Linux containers, and minimize administrative tasks. Based on these criteria, which scaling option should you recommend?

- A) Vertical Pod Scaling
- B) Cluster Autoscaler
- C) Virtual Nodes
- D) Desired State Configuration

Answer: C

Feedback(if correct): Virtual Nodes is the right choice because it enables Azure Kubernetes Service (AKS) to provision pods inside Azure Container Instances (ACI) that start in seconds. This solution meets the need for quick provisioning and autoscaling of Linux containers without requiring additional management of VMs, thus minimizing administrative effort.

Feedback(if wrong):

- A) Vertical Pod Scaling adjusts the CPU and memory resources of existing pods, which doesn't address the need for fast provisioning or minimizing administrative tasks.
- B) Cluster Autoscaler adjusts the number of nodes in a cluster, which could help with scaling but doesn't provide the same speed in provisioning resources as ACI or minimize administrative tasks as efficiently.
- D) Desired State Configuration is more about maintaining configuration states of nodes rather than scaling or rapid provisioning of resources.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Implementing autoscaling in Azure Kubernetes Service (AKS), Utilizing Azure Container Instances for rapid provisioning

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

142. Your organization is planning to launch a new customer service portal that will include an HTTP-based API to handle inquiries about service requests. This API will be built using Azure Functions and should allow users to submit inquiries and receive information about their service requests. However, to protect against unauthorized modifications, the API should only permit public read operations; all write operations must be restricted.

Given these requirements:

1. Implement Azure Functions to support HTTP-based requests.
2. Public read operations are allowed but must ensure data integrity by preventing write operations.
3. Maintain high security to protect against unauthorized access or modifications.

What configuration should you choose for the Azure Functions to meet the above specifications?

- A) Set the trigger type to HTTP, allow only POST methods, and set the authorization level to Function.
- B) Set the trigger type to HTTP, allow only GET methods, and set the authorization level to Anonymous.
- C) Set the trigger type to Timer, allow GET and POST methods, and set the authorization level to Admin.
- D) Set the trigger type to HTTP, allow GET, POST, and DELETE methods, and set the authorization level to User.

Answer: B

Feedback(if correct): Option B is correct because it meets all specified requirements by utilizing Azure Functions to implement an HTTP-based API that supports public read-only operations through GET methods and ensures open access by setting the authorization level to Anonymous, thereby preventing any write operations and ensuring data security and integrity.

Feedback(if wrong): Option A incorrectly permits only POST methods, which are used for write operations. Option C uses a Timer trigger, which is irrelevant for HTTP-based APIs, and allows both GET and POST methods, contradicting the read-only restriction. Option D permits GET, POST, and DELETE methods, enabling both read and write operations, which violates the specified requirement to prevent write operations.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Designing Compute and Network Infrastructure
- Competencies: Implementing Azure Functions with appropriate security and access control configurations for HTTP-based APIs.
- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Application

143. After migrating a financial application called FinApp to Azure, you need to ensure that the data storage complies with strict regulatory requirements. The regulations necessitate seven-year data retention and write protection for newly saved data. To address this, you decide to utilize Azure Blob Storage. What measures should you take to ensure the storage complies with the regulations?

- A. Apply an Azure Policy
- B. Alter the access level of the blob container
- C. Create a retention label for the blob
- D. Implement Azure resource locks

Answer: C

Feedback(if correct):

Implementing retention labels on Azure Blob Storage allows for the enforcement of data retention policies directly at the data level. By creating a retention label, you can specify a retention period (in this case, seven years) during which the data cannot be modified or deleted, ensuring compliance with regulatory requirements for data retention and write protection.

Feedback(if wrong):

- A. Applying an Azure Policy is used for enforcing resource management rules across your Azure resources, not for setting retention policies at the data level.

- B. Altering the access level of the blob container affects data accessibility, not retention or write-protection policies.
- D. Implementing Azure resource locks prevent accidental deletion or modification of Azure resources, but it does not enforce regulatory compliance for data retention and write protection within blob storage.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting Data Protection and Compliance

Competencies: Implementing data storage security solutions, Configuring data retention policies

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

144. Contoso intends to migrate a healthcare application named MedApp to Azure, and it is essential to follow tight security guidelines related to patient data. Among these restrictions is the prohibition of deleting medical records for five years. To tackle this, you choose Azure Blob Storage for data storage. How can you ensure the storage abides by the guidelines?

- A. Enable soft delete on the blob
- B. Generate a private endpoint for the blob
- C. Impart a custom role to the storage
- D. Set up a legal hold on the blob

Answer: D

Feedback(if correct): Setting up a legal hold on the blob is the most direct approach to comply with regulations that require retaining medical records for a specified period, like five years in this case. A legal hold prevents the deletion of data, ensuring that medical records are preserved intact for the duration of the hold, regardless of any attempts to delete or modify them. This feature is specifically designed to meet compliance and regulatory requirements, making it ideal for scenarios involving sensitive data such as patient records in healthcare applications.

Feedback(if wrong):

- A. Enable soft delete on the blob: While soft delete helps in recovering accidentally deleted data, it does not prevent data from being deleted in the first place, which does not fully comply with the requirement to prohibit deletions.
- B. Generate a private endpoint for the blob: Creating a private endpoint increases the security of accessing the blob storage but does not address the requirement to prevent the deletion of data.
- C. Impart a custom role to the storage: Custom roles can control access but cannot enforce restrictions on deleting data for a specified period like a legal hold can.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting Data Protection and Compliance

Competencies: Implementing data storage security solutions, Configuring data retention policies

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

145. To estimate and minimize the compute costs for migrating App1 to Azure, which tools and techniques should be used?

- A) Use The Azure Total Cost of Ownership (TCO) Calculator and implement Azure Reservations.
- B) Use the Azure Cost Management Power BI app and apply Azure Hybrid Benefit.
- C) Use Azure Advisor and enable Azure Spot Virtual Machine pricing.
- D) Use The Azure Total Cost of Ownership (TCO) Calculator and leverage Azure Hybrid Benefit.

Answer: D

Feedback(if correct): The Azure Total Cost of Ownership (TCO) Calculator is a comprehensive tool designed to estimate the cost savings that can be achieved by migrating to Azure, offering a detailed comparison between on-premises and Azure costs. Pairing this with Azure Hybrid Benefit optimizes cost efficiency by allowing the use of existing on-premises licenses for Windows Server and SQL Server on Azure. This combination provides an accurate cost estimate while ensuring maximum savings, making option D the correct choice.

Feedback(if wrong):

- A) Azure Reservations provide cost savings for predictable usage but don't leverage on-premises licenses like Azure Hybrid Benefit does.
- B) The Azure Cost Management Power BI app is great for ongoing cost management and analysis but doesn't offer the initial cost-benefit analysis provided by the TCO Calculator or the specific license savings of Azure Hybrid Benefit.
- C) Azure Advisor offers personalized recommendations to optimize resources, and Azure Spot VM pricing can reduce costs for interruptible workloads. However, this doesn't match the comprehensive cost estimation and license optimization offered by the TCO Calculator and Azure Hybrid Benefit respectively.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Cost estimation and optimization strategies in Azure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

146. To meet Litware's identified security and compliance requirements for App1 in Azure, what should be implemented?

- A) Allow modification of new and existing data, deny on-premises access to Azure Storage, enable public endpoint access, and disable TDE for Azure SQL databases.
- C) Prevent modification of new and existing data for
- B) Prevent modification of new and existing data for three years, grant on-premises access to Azure Storage, disable public endpoint access, and enable TDE for Azure SQL databases.
- three years, deny on-premises access to Azure Storage, enable public endpoint access, and enable TDE for Azure SQL databases.
- D) Allow modification of new and existing data, grant on-premises access to Azure Storage, disable public endpoint access, and disable TDE for Azure SQL databases.

Answer: B

Feedback(if correct):- The correct approach ensures that security and compliance requirements are met by preventing unauthorized access and modifications to the data stored in Azure. It allows for the secure and compliant migration of App1 to Azure by ensuring data integrity through the enforcement of Transparent Data Encryption (TDE) for Azure SQL databases, which secures the data at rest. Additionally, it ensures that only authorized on-premises users and services can access the Azure Storage account, enhancing security by disabling public endpoint access, which mitigates the risk of unauthorized external access.

Feedback(if wrong):-

- Option A is incorrect because it allows unrestricted data modification and denies necessary on-premises access, compromising both security and compliance with regulatory requirements.
- Option C is incorrect as it unnecessarily restricts on-premises access and permits public endpoint access, which could lead to security vulnerabilities.
- Option D is incorrect because it does not align with the security requirement to prevent data modification and fails to enforce TDE for Azure SQL databases, which is essential for data encryption and protection.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Cost estimation and optimization strategies in Azure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

147. To facilitate the migration of App1 to Azure and meet the security and compliance requirements effectively, you need to both accurately estimate the compute costs associated with running App1 in Azure and implement strategies to minimize these costs. Given the requirements and the need for cost optimization:

For the migration of App1 to Azure, which tool should you use to estimate the costs, and which feature should you implement to minimize the costs?

A. Use the Azure Total Cost of Ownership (TCO) Calculator to estimate costs and implement Azure Reservations to minimize costs.

B. Use Azure Advisor for cost estimation and Azure Spot Virtual Machine pricing for cost minimization.

C. Estimate costs with the Azure Cost Management Power BI app and minimize costs through the Azure Hybrid Benefit.

D. Utilize the Azure Total Cost of Ownership (TCO) Calculator for cost estimation and apply Azure Spot Virtual Machine pricing to reduce costs.

Answer: A

Feedback(if correct):- The Azure Total Cost of Ownership (TCO) Calculator is designed to estimate the potential savings when migrating to Azure, making it a valuable tool for initial cost assessment. Azure Reservations, on the other hand, offer a way to significantly minimize costs by allowing pre-payment for one or three years of service, which can lead to considerable savings compared to pay-as-you-go prices.

Feedback(if wrong):-

Azure Advisor, while useful for optimizing resource utilization and improving performance, security, and reliability, is not specifically designed for cost estimation in the context of migration.

The Azure Cost Management Power BI app is geared towards visualizing and analyzing existing Azure spend, rather than estimating costs for potential migrations.

Azure Spot Virtual Machine pricing offers discounted rates for spare capacity but with the possibility of VMs being evicted, which may not meet the reliability requirements for all applications.

Azure Hybrid Benefit allows the use of existing on-premises Windows Server and SQL Server licenses with Software Assurance to save on Azure services, which is a cost minimization strategy but doesn't specifically estimate migration costs.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Cost estimation and optimization strategies in Azure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

148. Your company is developing a new e-commerce platform hosted on Azure. The platform involves handling sensitive customer order data and serving product information. The solution must adhere to strict security and compliance standards.



Requirements:

- Only specifically authorized roles should access and modify customer order data.
- Customer order data, once recorded, must be immutable for compliance.
- Minimize storage costs for frequently accessed product information.

Which combination of Azure services and configurations best meets these requirements?

- A) Azure SQL Database with Row-Level Security for data access control and Azure Blob Storage with Hot access tier for product information.
- B) Azure Cosmos DB with role-based access control (RBAC) for order data and Azure Blob Storage with a Cool access tier for product information.
- C) Azure SQL Database with Transparent Data Encryption (TDE) and Time-Based Retention Policy for order data immutability and Azure Blob Storage with Cool access tier for product information.
- D) Azure Table Storage with SAS tokens for order data access control and Azure Blob Storage with Archive access tier for product information.

Answer: C

Feedback(if correct):

C) is the correct answer. Azure SQL Database equipped with Transparent Data Encryption (TDE) provides the necessary security for sensitive customer data, and implementing a Time-Based Retention Policy on Azure SQL Database ensures order data immutability. Azure Blob Storage with a Cool access tier balances the need for cost-effective storage while still providing timely access to frequently accessed product information.

Feedback(if wrong):

- A) While Azure SQL Database with Row-Level Security and Azure Blob Storage with a Hot access tier address parts of the requirements, they do not fully meet the immutability requirement for order data.
- B) Azure Cosmos DB with RBAC and Azure Blob Storage with a Cool access tier offer a robust solution but might not provide the strict immutability required for order data without additional configurations.
- D) Azure Table Storage with SAS tokens and Azure Blob Storage with an Archive access tier do not offer the comprehensive security, immutability, and cost-efficiency required for this scenario.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Implementing scalable and highly available web applications on Azure, utilizing Azure App Service Environment for enhanced security and isolation, understanding of Azure services for autoscaling and high availability

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

149. Your question and selections seem clear, especially when targeting the specific needs of a critical cloud-based application requiring horizontal scaling, high availability, and cost-effectiveness. However, to enhance clarity and ensure the question directly addresses the primary concerns of scalability, availability, and cost, you might consider a slight rephrasing. Here's a refined version:

Your organization's cloud-based application on Azure is facing unpredictable traffic spikes, affecting performance. You are tasked with finding a solution that ensures the application scales efficiently, remains highly available, and is cost-effective.

Which Azure service is BEST suited to meet these requirements?

- A. Azure App Service with auto-scaling enabled for dynamic resource allocation.
- B. Azure Cloud Services for legacy support with manual scaling options.
- C. Azure App Service Environment (ASE) for an isolated, high-availability environment with auto-scaling capabilities.
- D. Azure Kubernetes Service (AKS) for advanced container orchestration and scaling.

Answer: C

Feedback (if correct): Your choice of Azure App Service Environment (ASE) is correct because it uniquely meets the needs for automatic horizontal scaling based on user traffic, ensures high availability through isolation and Traffic Manager integration, and provides a cost-effective managed environment, reducing operational overhead.

Feedback (if wrong):

Option A (Azure App Service on a dedicated VM): This option does not fully leverage Azure's managed services for autoscaling and high availability. While Azure App Service supports scaling, using it on a

dedicated VM adds complexity and cost because you must manage the VM's scaling and availability manually.

Option B (Azure Cloud Services): Although Azure Cloud Services can provide some level of horizontal scaling and high availability, it's considered a legacy service with more limited and less user-friendly autoscaling capabilities compared to ASE. Moreover, it may not offer the same level of network isolation and ease of management as ASE.

Option D (Azure Kubernetes Service - AKS): AKS is a powerful service for container orchestration that supports autoscaling and high availability. However, it's generally more suited for containerized applications and can introduce additional complexity and management overhead for applications not originally designed to run in containers. While AKS offers great flexibility and control, it may not be the most cost-effective or straightforward solution for a traditional web application requiring simple scaling and high availability.

Each incorrect option either introduces unnecessary complexity, falls short of meeting all the specified requirements, or could lead to higher operational costs compared to the more streamlined and managed environment provided by Azure App Service Environment (ASE).

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Implementing scalable and highly available web applications on Azure, utilizing Azure App Service Environment for enhanced security and isolation, understanding of Azure services for autoscaling and high availability

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

150. You are tasked with ensuring that the data storage for Application 1 (App1) on Azure meets stringent security and compliance requirements. Which action should you take?

- A) Create an access policy for the blob
- B) Modify the access level of the blob service.
- C) Implement Azure resource locks.
- D) Create Azure RBAC assignments.

Answer: A

Feedback(if correct):-

To meet the specified security and compliance requirements, you should create an access policy for the blob storage associated with App1. This policy allows you to control who can access the data stored in the blob, ensuring that only authorized users or applications can read or modify the data. This aligns with the need to prevent unauthorized access or modifications to the data for a specified period.

Feedback(if wrong):-

- B) Modifying the access level of the blob service may not provide granular control over access to specific blobs within the storage account, which is necessary to meet the security and compliance requirements effectively.
- C) Implementing Azure resource locks is a broader measure that prevents accidental deletion or modification of Azure resources. While resource locks can be useful for protecting critical resources, they do not directly address the need to control access to specific data within a blob storage account.
- D) Creating Azure RBAC assignments allows you to grant permissions to users or groups for accessing Azure resources. While RBAC is important for managing access to Azure services, it may not provide the level of granularity needed to control access to individual blobs within a storage account.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Architecting for Business Continuity and Disaster Recovery

Competencies: Implementing scalable and highly available web applications on Azure, utilizing Azure App Service Environment for enhanced security and isolation, understanding of Azure services for autoscaling and high availability

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

151. You are the Azure administrator for your company, which utilizes Azure virtual machines running both Windows Server 2016 and Linux for its critical applications. Due to increasing security concerns, you've been tasked with enhancing the monitoring and alerting mechanisms for security-related events within your Azure environment.

To achieve this, you plan to leverage Azure Log Analytics to analyze and set up alerts based on specific security-related events from both the Windows and Linux virtual machines.

Given your requirement to design an alerting strategy for security-related events using Azure Log Analytics, which of the following tables should you primarily query to monitor security-related events from both Windows Server 2016 and Linux virtual machines effectively?

- A. SecurityEvent for Windows Server 2016 events and Syslog for Linux events.
- B. WindowsEvent for Windows Server 2016 events and LinuxSyslog for Linux events.
- C. Event for both Windows Server 2016 and Linux events.
- D. SecurityLog for Windows Server 2016 events and LinuxEvent for Linux events.

Answer: A.

Feedback(if correct): The SecurityEvent table in Azure Log Analytics is specifically designed to collect and store security-related events from Windows virtual machines, making it the optimal choice for monitoring security activities on Windows Server 2016 VMs. Similarly, the Syslog table is tailored for gathering system log information from Linux operating systems, including security-related events. This approach ensures comprehensive monitoring across both operating system environments by using the most relevant data sources available in Azure Log Analytics.

Feedback(if wrong):

- B. WindowsEvent and LinuxSyslog are incorrect because while WindowsEvent does collect Windows logs, it is not specifically focused on security events. LinuxSyslog is not a valid table in Azure Log Analytics, making this option incorrect.
- C. Event is too generic and does not specifically exist as a table dedicated to security logs for either Windows or Linux in Azure Log Analytics.
- D. SecurityLog and LinuxEvent do not exist as specific tables within Azure Log Analytics. The correct tables for security-related logs are SecurityEvent for Windows and Syslog for Linux.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing and managing monitoring solutions using Azure Log Analytics for security-related events across different operating systems.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

152. You're tasked with enhancing the security of a web application hosted on Azure App Service. The application's sensitive configuration data, currently hardcoded, needs a more secure management solution. You aim to leverage Azure Key Vault for storing these secrets, minimizing code changes, and adhering to the principle of least privilege.

The application already utilizes a system-assigned managed identity, allowing Azure services authentication without storing credentials in the code. Your solution must seamlessly integrate Azure Key Vault with the web application, enabling it to retrieve its configuration data securely and efficiently.

What strategy should you adopt to store the web application's settings in Azure Key Vault while meeting the outlined requirements?

- A) Configure the web app to use Azure Managed Identity and grant it the necessary permissions to access the Key Vault secrets.
- B) Embed Azure Key Vault client libraries in the app code and store the Key Vault access credentials within the web app settings.
- C) Create a new user-assigned managed identity specifically for Key Vault access and update the application code to use this identity for retrieving secrets.
- D) Directly reference Key Vault secrets in the application code without using managed identities, ensuring each secret's URI is properly hardcoded.

Answer: A

Feedback(if correct): Integrating Azure App Service with Azure Key Vault using a system-assigned managed identity is the correct approach. This setup minimizes changes to the app code by automating the authentication process between the service and the Key Vault. It leverages Azure's managed identity feature, eliminating the need to store or manage credentials manually, which aligns with the principle of least privilege by granting only necessary permissions to the app.

Feedback(if wrong):

Directly embedding secrets into the app code fails to minimize code changes and exposes the application to potential security risks.

Using a user-assigned managed identity without specific necessity complicates the configuration unnecessarily when a system-assigned managed identity provides a simpler and more integrated solution.

Storing settings outside of Azure Key Vault disregards the security and management benefits Key Vault offers, such as centralized management of secrets, keys, and certificates.

Over-complicating the access policy by not adhering to the principle of least privilege could introduce unnecessary risk, as it might grant broader access than needed.

For the scenario involving integrating Azure App Service with Azure Key Vault using a system-assigned managed identity:

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing secure and scalable apps using Azure services, managing secrets in Azure Key Vault, and configuring system-assigned managed identities for Azure resources.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

153. A multinational corporation seeks guidance on an Azure identity management strategy to support its increasingly remote workforce. The organization faces challenges such as disparate networking infrastructure, inconsistent bandwidth, and varied device types.

To address the identity management needs of the remote workforce, what Azure identity management strategy should you propose?

- A) Implement Azure AD Device Registration and Join for corporate devices, complemented by Conditional Access policies.
- B) Launch Azure AD Password Hash Synchronization (PHS) or Pass-through Authentication (PTA) for synced on-premises AD identities, backed by Azure AD Connect.
- C) Roll out self-service password reset (SSPR) for end-users, paired with Azure AD Premium P1/P2 licenses for advanced security features.
- D) Implement Multi-factor Authentication (MFA) for all remote access points, integrated with Azure AD Identity Protection and Conditional Access policies.

Answer: D

Feedback(if correct): D) Implement Multi-factor Authentication (MFA) for all remote access points, integrated with Azure AD Identity Protection and Conditional Access policies, is the correct choice because it ensures a robust security posture for remote workers. It leverages additional verification steps to secure access, mitigates risks associated with compromised credentials, and applies adaptive security measures based on user behavior and access patterns. This strategy addresses the diverse conditions remote workers face, including inconsistent network infrastructure and device types.

Feedback(if wrong):

- A) Implement Azure AD Device Registration and Join for corporate devices, complemented by Conditional Access policies: While this enhances security for corporate devices, it does not fully address the challenges of a remote workforce, especially when using personal or unmanaged devices.
- B) Launch Azure AD Password Hash Synchronization (PHS) or Pass-through Authentication (PTA) for synced on-premises AD identities, backed by Azure AD Connect: These methods improve the user experience by synchronizing identities, but they don't provide the same level of security against remote access threats as MFA.
- C) Roll out self-service password reset (SSPR) for end-users, paired with Azure AD Premium P1/P2 licenses for advanced security features: SSPR is beneficial for user autonomy and reducing IT support tickets but doesn't directly enhance security for remote access.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing Multi-factor Authentication (MFA) for secure remote access, integrating Azure AD Identity Protection for adaptive risk-based policies, and configuring Conditional Access policies to safeguard remote workforce access.

Difficulty Level: Expert

Bloom's Taxonomy Level: Application

154. Your development organization is expanding with the introduction of two specialized application development teams: Team Alpha, focusing on Line of Business (LoB) applications, and Team Bravo, dedicated to Customer Relationship Management (CRM) solutions. This growth necessitates a robust identity management strategy that supports seamless collaboration among internal teams, external consultants, and partner companies while ensuring secure access to

resources. Given the need for a scalable and secure identity management system that facilitates easy access for both internal and external users across a variety of collaboration scenarios, what is the best approach to meet these requirements?

- A) Utilize Azure AD Connect with default settings for syncing on-premises Active Directory (AD) identities with Azure AD, ensuring basic Single Sign-On (SSO) capabilities.
- B) Implement a hybrid identity solution with Password Hash Synchronization (PHS) or Pass-through Authentication (PTA) for on-premises AD identities, enhanced with Conditional Access policies for fine-grained access control based on user, location, and device state.
- C) Create separate Azure AD tenants for each application team to isolate their resources, applying Azure AD Premium P1/P2 licenses for advanced security features like Identity Protection and Privileged Identity Management.
- D) Deploy Azure AD Connect for each team in a hybrid identity configuration, with each team using a separate Azure AD tenant to maintain independence while enabling centralized identity management.

Answer: B

Feedback(if correct): B) is the most effective strategy, as it leverages a hybrid identity model with PHS or PTA, enhancing security and flexibility through Conditional Access policies. This approach supports the organization's need for scalable and secure identity management, enabling seamless collaboration across diverse teams and partners without the complexity of managing multiple Azure AD tenants.

Feedback(if wrong):

- A) Only provides basic SSO functionality without the enhanced security and flexibility needed for the organization's collaborative and dynamic environment.
- C) While offering advanced security features, managing separate Azure AD tenants for each team could lead to increased complexity and hinder seamless collaboration.
- D) Although it provides a hybrid identity model, managing separate Azure AD tenants for each team could complicate identity and access management across the organization's expanding ecosystem, outweighing the benefits of centralized management.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Designing Identity and Security Solutions

- Competencies: Implementing hybrid identity solutions, including Azure AD Connect with Password Hash Synchronization (PHS) or Pass-through Authentication (PTA), supplemented by Conditional Access policies for enhanced security.
- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Application

155. Your organization is undergoing a digital transformation, which involves migrating several on-premises applications and services to Azure. The transformation plan includes a modern approach to identity management to enhance security and simplify access for a global workforce.

Requirements:

- Maintain synchronization between on-premises Active Directory and Azure Active Directory to ensure a seamless user experience across cloud and on-premises environments.
- Ensure uninterrupted access to resources, even if the internet connectivity to Azure is temporarily unavailable.
- Prepare for the integration of future projects and possibly new subsidiary companies into the organization's Azure environment without disrupting the existing setup.

Given the scenario and requirements, which action is most appropriate for adapting the organization's identity management strategy to the planned digital transformation?

- A) Transition all on-premises Active Directory domain controllers to Azure.
- B) Implement additional Azure Active Directory domain controllers within Azure virtual networks.
- C) Extend the existing on-premises Active Directory infrastructure into Azure by deploying domain controllers for the primary domain within Azure virtual networks.
- D) Establish a separate Azure Active Directory tenant specifically for managing new projects and future acquisitions.

Answer: C

Feedback(if correct): Extending the on-premises Active Directory into Azure by deploying domain controllers within Azure virtual networks ensures continuous synchronization with Azure Active Directory. This approach maintains a unified identity management system across on-premises and cloud environments, meeting the requirement for seamless user access even during internet outages. It also provides the flexibility to integrate future projects and subsidiaries without disrupting existing configurations.

Feedback(if wrong):

- A) Transitioning all on-premises Active Directory domain controllers to Azure could disrupt the existing setup and does not guarantee access if internet connectivity is lost.
- B) Implementing additional Azure AD domain controllers within Azure virtual networks does not address the requirement for uninterrupted access if Azure connectivity is down, as it relies solely on cloud resources.
- D) Establishing a separate Azure AD tenant for new projects might complicate identity management and does not ensure uninterrupted access during internet outages.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing hybrid identity solutions to ensure seamless access across on-premises and cloud environments, including the deployment of domain controllers in Azure virtual networks.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

156. In a new Azure deployment, you are configuring an application to access Azure resources with the appropriate authentication. What type of endpoint should the application use to acquire an access token securely?

- A) Azure Active Directory (Azure AD)
- B) Azure Key Vault
- C) Azure Monitor
- D) Microsoft identity platform

Answer: D

Feedback (if correct):

The correct answer is D) Microsoft identity platform. The Microsoft identity platform enables applications to securely authenticate and access Azure resources using OpenID Connect protocols, OAuth 2.0 authorization, and refresh tokens.

Feedback (if wrong):

- A) Azure Active Directory (Azure AD) is an identity and access management service, not an endpoint for applications to acquire access tokens.
- B) Azure Key Vault is a service that manages cryptographic keys and secrets, not an endpoint for applications to acquire access tokens.
- C) Azure Monitor is a monitoring and alerting service for Azure resources, not an endpoint for applications to acquire access tokens.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Authenticating and authorizing access to Azure resources

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

157. In your Azure environment, there's a requirement to secure user access to the production environment. This involves ensuring that users are registered for and utilize Azure Multi-Factor Authentication (MFA) during their Azure portal sign-in process. To achieve this while aligning with the authentication and authorization specifications laid out for your environment, a structured approach must be adopted. Given the need for enhanced security measures:

1. Which Azure service should be configured to manage the enrollment and enforcement of Azure MFA for users accessing the production environment via the Azure portal?
2. What policy should be applied to strengthen the sign-in process, ensuring that access is granted only under safe conditions?

Select the correct configuration options to meet the specified requirements.

- A) Configure Azure AD Conditional Access policies and enforce MFA registration.
- B) Implement Azure AD Identity Protection to automatically enroll users in MFA and assess sign-in risks.
- C) Utilize Azure AD Privileged Identity Management (PIM) to require MFA at sign-in for privileged roles.
- D) Set up a sign-in risk policy in Azure AD Identity Protection to evaluate the risk level of sign-in attempts and enforce MFA for high-risk sign-ins.

Answer: B, D

Feedback(if correct):

For securing user access to the production environment with Azure Multi-Factor Authentication (MFA), the correct answers are B (Implement Azure AD Identity Protection to automatically enroll users in MFA and assess sign-in risks) and D (Set up a sign-in risk policy in Azure AD Identity Protection to evaluate the risk level of sign-in attempts and enforce MFA for high-risk sign-ins).

Implementing Azure AD Identity Protection for automatic MFA enrollment leverages the built-in capabilities of Azure AD to not only enforce MFA but also to evaluate sign-in risks dynamically. A sign-in risk policy further enhances security by assessing each sign-in attempt and applying MFA when necessary, ensuring that users can only access the production environment under safe conditions. This approach minimizes changes to the app code, adheres to the principle of least privilege, and effectively secures access to the production environment.

Feedback(if wrong):

A) Configure Azure AD Conditional Access policies and enforce MFA registration: While Conditional Access policies are powerful tools for defining access scenarios, they alone do not automatically enroll users in MFA nor assess sign-in risks without additional configuration.

C) Utilize Azure AD Privileged Identity Management (PIM) to require MFA at sign-in for privileged roles: Azure AD PIM is primarily focused on managing, controlling, and monitoring access within Azure AD, Azure, and other Microsoft Online Services for privileged accounts. It's not specifically designed for automatic MFA enrollment or sign-in risk assessments.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing solutions for managing identities and securing access within Azure environments.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

158. You're designing an access solution for a web application named 'WebApp1' hosted in your on-premises environment, which uses Integrated Windows authentication. Some users, working remotely without VPN access, require single sign-on (SSO) to 'WebApp1'. What components should be included to facilitate remote SSO access to 'WebApp1'?

- A) Azure AD Application Proxy and Conditional Access policies
- B) Azure AD Privileged Identity Management (PIM) and Azure AD enterprise applications
- C) Conditional Access policies and Azure Application Gateway
- D) Azure AD Application Proxy and Azure Arc

Answer: A

Feedback(if correct):-

For securely granting remote access to the on-premises web application 'WebApp1', the correct answer is
A) Azure AD Application Proxy and Conditional Access policies.

Azure AD Application Proxy extends Azure AD's secure access and single sign-on capabilities to your on-premises applications. This means users can access 'WebApp1' remotely without needing a VPN, while still being authenticated through Azure AD.

Conditional Access policies add an extra layer of security by defining conditions under which access is granted. For instance, you might allow access to 'WebApp1' only from devices that are compliant with your organization's security policies.

Feedback(if wrong):

B) Azure AD Privileged Identity Management (PIM) and Azure AD enterprise applications: PIM is used to manage, control, and monitor access within Azure AD, Azure, and other Microsoft Online Services. While it provides governance over privileged roles, it doesn't facilitate SSO for on-premises applications to remote users.

C) Conditional Access policies and Azure Application Gateway: While Conditional Access policies are relevant, Azure Application Gateway is a web traffic load balancer and doesn't provide a mechanism for enabling SSO to on-premises applications for remote users.

D) Azure AD Application Proxy and Azure Arc: Azure Arc is designed to extend Azure services and management to any infrastructure, but it doesn't directly provide SSO capabilities for on-premises web applications like 'WebApp1'.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing Azure AD Application Proxy to provide secure remote access to on-premises applications, and utilizing Conditional Access policies to enforce security policies and conditions.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

159. To support the deployment and scalable operation of a new application, 'App2', across multiple Azure virtual machines (VMs), with plans for future VM additions, a solution is needed to manage access to Azure resources securely and efficiently, including Azure Key Vault, Azure Logic Apps, and Azure SQL Database. The solution must minimize manual security management for new VM deployments and eliminate the need for storing sensitive information directly on the VMs. Considering the requirements for a scalable, secure authentication method for VMs accessing Azure resources without storing secrets on the VMs or frequently modifying roles and permissions:

- A) Use a service principal with certificate-based authentication.
- B) Implement a system-assigned managed identity for each VM.
- C) Utilize a service principal with client secret-based authentication.
- D) Apply a user-assigned managed identity shared across VMs.

Answer: D

Feedback (if correct):

D) A user-assigned managed identity is the optimal choice. This option enables Azure resources to authenticate and access other Azure services securely without the need to manage credentials. Unlike system-assigned managed identities, which are tied to a single resource, user-assigned managed identities can be shared across multiple resources. This makes it easier to manage identities for applications like App1 that span multiple virtual machines, as you won't need to assign new roles or permissions each time you deploy additional virtual machines. This approach also eliminates the need to store secrets or certificates directly on the virtual machines, enhancing security.

Feedback (if wrong):

A) A service principal configured with a certificate, and C) a service principal configured with a client secret, both require managing credentials and secrets, which contradicts the requirement to avoid storing secrets on the virtual machines.

B) A system-assigned managed identity is tied to a specific Azure resource and cannot be easily shared among multiple resources, making it less suitable for scenarios where additional virtual machines will be deployed to run the same application.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing Azure Active Directory for resource access management, utilizing managed identities for Azure resources.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

160. Your task is to ensure an existing web application, hosted on Azure VMs, is safeguarded against SQL injection attacks and benefits from Layer-7 load balancing. The solution must keep modifications to the current application code to a minimum. What Azure services should be implemented to meet these requirements without significantly altering the existing web app's codebase?

A) Integrate Azure Front Door for global Layer-7 load balancing and automatic protection against common web vulnerabilities.

B) Utilize Azure Application Gateway with Web Application Firewall (WAF) enabled for Layer-7 load balancing and to block SQL injection attacks.

C) Deploy Azure Firewall with DDoS Protection Standard for network-level protection and manual configuration of SQL injection prevention rules.

D) Implement Azure Traffic Manager for DNS-level traffic routing and leverage Azure Security Center for SQL injection attack detection and response.

Answer: B

Feedback(if correct):-

The correct answer is B) Utilize Azure Application Gateway with Web Application Firewall (WAF) enabled for Layer-7 load balancing and to block SQL injection attacks.

Feedback(if correct): Azure Application Gateway with Web Application Firewall (WAF) is designed to provide Layer-7 load balancing and protect against common web vulnerabilities, including SQL injection attacks, without requiring significant changes to your application code. WAF comes with pre-configured protection rules for SQL injection and other threats, making it an effective choice for safeguarding your web applications while also offering load-balancing capabilities.

Feedback(if wrong):

- A) Azure Front Door: While Azure Front Door offers global Layer-7 load balancing and some protection against web vulnerabilities, it doesn't provide the specific, granular control over SQL injection attack prevention as directly as WAF does with Azure Application Gateway.
- C) Azure Firewall with DDoS Protection Standard: This option focuses more on network-level security and DDoS protection rather than specifically addressing SQL injection attacks at the application layer.
- D) Azure Traffic Manager and Azure Security Center: Azure Traffic Manager is primarily a DNS-level traffic routing solution and doesn't offer application layer protection against SQL injection attacks. Azure Security Center can detect and respond to SQL injection attacks but does not provide direct prevention capabilities integrated with load balancing as Azure Application Gateway with WAF does.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing and configuring Azure Application Gateway and Web Application Firewall (WAF) to secure Azure web applications against common web vulnerabilities like SQL injection.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

161. Your company has a critical web application currently deployed on Azure virtual machines (VMs). You've identified a need to enhance its security by protecting it from SQL injection attacks and implementing a layer-7 load balancer. Minimizing changes to the existing application code is a priority. What Azure service can fulfill both requirements while minimizing code modifications for the existing web application?

- A. Azure Security Center with Web Application Vulnerability Assessment
- B. Azure Web App Service with built-in WAF
- C. Azure Firewall with Application Rules

D. Azure Application Gateway

Answer: D.

Feedback(if correct):, Azure Application Gateway with Web Application Firewall (WAF) is an optimal choice to ensure Layer-7 load balancing and safeguard the web application against SQL injection attacks without significant modification to the existing application code.

Feedback(if wrong):

Azure Security Center with Web Application Vulnerability Assessment (A) is a scanning and assessment tool rather than a runtime protection mechanism, hence it wouldn't suffice. Azure Web App Service with built-in WAF (B) isn't the right choice as the web application isn't deployed as an Azure App Service. Azure Firewall with Application Rules (C) doesn't quite fit the requirement, as it functions at a different level (network firewall) and wouldn't provide layer-7 load balancing capabilities.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing Azure Application Gateway with Web Application Firewall (WAF) for protecting web applications against common web vulnerabilities such as SQL injections, while also providing Layer-7 load balancing.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

162. To enhance security and ensure compliance within your Azure environment, you are evaluating options for monitoring and managing access permissions for a custom application named AppService1, developed by a third-party company, Fabrikam, Inc. You aim to implement a solution that accomplishes the following objectives:

- Automates the process of verifying whether Fabrikam developers still require access to AppService1.
- Sends a monthly email to the manager of the Fabrikam developers, summarizing their team's current access rights to AppService1.
- Automatically revokes access permissions if the manager fails to confirm the necessity of these permissions.
- Requires minimal additional development work.



Given these specific requirements, which Azure service or feature should you recommend for managing access reviews and permissions for AppService1?

- A) Configure Azure Active Directory (Azure AD) Privileged Identity Management with custom role assignments for AppService1.
- B) Implement an Azure Logic Apps workflow that utilizes the Get-AzureADUserAppRoleAssignment cmdlet to generate and send the access report.
- C) Deploy an Azure Automation runbook that executes the Get-AzureRmRoleAssignment cmdlet to monitor and report on role assignments.
- D) Utilize Azure Active Directory (Azure AD) Access Reviews to automate the review and management of access permissions to AppService1.

Answer: D

Feedback(if correct):-

Azure Active Directory (Azure AD) Access Reviews offers a comprehensive solution for managing and reviewing access permissions within Azure environments. This feature allows organizations to automate the process of access reviews, including the scheduling of periodic reviews, notifying reviewers, and taking action based on review outcomes. It meets all specified requirements by enabling automatic email notifications to managers, facilitating the review of access permissions, and supporting the automatic revocation of permissions if not verified. Additionally, it minimizes the need for custom development efforts.

Feedback(if wrong):-

- A) Implementing a custom role assignment in Azure AD Privileged Identity Management (PIM) would allow for the management of elevated privileges but does not directly address the requirements of verifying ongoing access needs or automating the review process for permissions to specific applications.
- B) Creating an Azure Automation runbook that runs the Get-AzureADUserAppRoleAssignment cmdlet would enable you to list the role assignments for users in Azure AD. However, this method requires additional development effort to send monthly emails and does not support automatic revocation of access based on the manager's verification.
- C) Creating an Azure Automation runbook that runs the Get-AzureRmRoleAssignment cmdlet would list role assignments within Azure resources. Like option B, this requires custom scripting for email notifications and does not automate the process of revoking unverified permissions.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing and managing access reviews for Azure resources and applications to ensure compliance with organizational security policies.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

163. Your task is to ensure continuous monitoring and timely alerts regarding the synchronization status between on-premises directories and Azure Active Directory (Azure AD) for the IT support team. The chosen solution must offer comprehensive insights into health and synchronization issues, enabling proactive maintenance and support. Which of the following options should you recommend to fulfill these needs effectively?

- A) Implement Azure Network Watcher to monitor network performance and diagnostics.
- B) Configure an action group to automate responses to system alerts and improve incident response times.
- C) Establish a SendGrid account for advanced email analytics and deliverability features.
- D) Utilize Azure AD Connect Health to actively monitor and receive alerts on the synchronization of health between on-premises directories and Azure AD.

Answer: D

Feedback(if correct):-

For ensuring the IT Support team is consistently updated on the synchronization status between on-premises directories and Azure Active Directory (Azure AD), the best solution is:

Azure AD Connect Health offers monitoring and insights into the health of on-premises AD components, synchronization services, and Azure AD Connect specifically. It provides alerts and detailed reports on synchronization performance, configuration issues, and overall health status, directly addressing the needs of the IT Support team for detailed health reports and alert notifications regarding synchronization issues.

Feedback(if wrong):-

- A) Azure Network Watcher: Primarily focused on monitoring, diagnosing, and gaining insights into network performance rather than directory synchronization or health status.
- B) An action group: While action groups in Azure can be used to trigger actions based on alerts, they don't specifically monitor or report directory synchronization issues unless configured with a specific monitoring tool like Azure AD Connect Health.
- C) A SendGrid account with advanced reporting: SendGrid is an email delivery service, offering solutions for email marketing and transactional emails with reporting capabilities. However, it does not provide monitoring or insights into Azure AD synchronization or health status.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing and managing Azure AD Connect Health for monitoring and alerting on directory synchronization status and health.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

164. Adatum Inc. is concerned about securing its production environment, and it wants to ensure that its employees log in using strong authentication methods. They expect users logging into the Azure portal to go through Azure MFA verification whenever they attempt to access the environment remotely. What steps should you take to meet Adatum Inc.'s authentication requirements?

- A. Register users for Azure MFA via Azure AD Identity Protection
- B. Enforce Azure MFA authentication using Session Control in capolicy1
- C. Configure Conditional Access policy in Azure AD Identity Protection
- D. Enable User Risk policy in Azure AD Identity Protection

Answer: C

Feedback(if correct): Configuring a Conditional Access policy in Azure AD Identity Protection is the most effective way to meet Adatum Inc.'s authentication requirements. This policy can be designed to require Azure Multi-Factor Authentication (MFA) for any sign-in attempt to the Azure portal, specifically when accessed remotely. This solution not only secures the authentication process but also allows for flexibility in applying the policy based on various conditions such as user role, location, and device state, ensuring that MFA is prompted when necessary.

Feedback(if wrong):

Option A: While registering users for Azure MFA via Azure AD Identity Protection is a critical step, registration alone does not enforce MFA at sign-in. The enforcement is achieved through Conditional Access policies.

Option B: Using Session Control in capolicy1 can help manage user sessions after they have authenticated but does not directly enforce MFA during the sign-in process.

Option D: The User Risk policy is a part of Azure AD Identity Protection that focuses on evaluating the risk level of a user's sign-in behavior. While it's important for overall security, it specifically targets risky sign-ins and not the blanket enforcement of MFA for all remote access attempts to the Azure portal.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing and managing Azure AD Connect Health for monitoring and notification.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

165. You are preparing to deploy a new application named App2 on Azure, which will utilize several Azure services. Your goal is to ensure that the application's components can securely authenticate to Azure services without the need to manage credentials or store secrets and certificates within the application's infrastructure. Additionally, you aim to avoid the hassle of assigning new roles and permissions for Azure services when scaling the application. What type of identity solution should you recommend to achieve these objectives?

- A) An Azure Active Directory (Azure AD) application registration with client secrets
- B) A system-assigned managed identity
- C) A service principal with certificate-based authentication
- D) A user-assigned managed identity

Answer: D

Feedback(if correct): Congratulations, your answer is correct! A user-assigned managed identity is indeed the best solution to securely authenticate to Azure services without managing credentials or storing secrets within the application's infrastructure. User-assigned managed identities can be shared among multiple resources, simplifying permission management and saving time when scaling the application.



Feeback(if wrong):

- A) An Azure Active Directory (Azure AD) application registration with client secrets- Registering an application with Azure AD and using client secrets is useful for authenticating APIs or daemon apps but not suitable for securing application components communicating with Azure services. Client secrets require rotation and careful management, increasing the likelihood of misconfiguration or compromise.
- B) A system-assigned managed identity- System-assigned managed identities are bound to a single Azure resource, making them unsuitable for cases where multiple resources need to share the same identity. Additionally, system-assigned managed identities cannot be reassigned with another resource after the original resource is deleted.
- C) A service principal with certificate-based authentication- While service principals can represent applications, they generally require managing credentials, such as certificates, which increases the chances of mismanagement or exposure. This option does not simplify permission management or reduce the need to assign new roles and permissions when scaling the application.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Identity and Access Management

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application and Evaluation

166. You're planning to migrate an application, App1, to Azure and need to ensure it meets specific authentication and authorization requirements. To secure access tokens for authentication purposes, you must decide which Azure service App1 should utilize. For App1's migration to Azure, which service should be utilized to obtain access tokens, aligning with the authentication and authorization requirements?

- A) Microsoft Identity Platform
- B) Azure Active Directory (Azure AD)
- C) Azure Instance Metadata Service (IMDS)
- D) Azure Service Management

Answer: A

Feedback(if correct):-

The Microsoft Identity Platform is a comprehensive framework for adding identity and access management capabilities to your applications. It's built on Azure Active Directory (Azure AD) and provides a secure, scalable, and reliable way for applications to obtain access tokens, enabling them to authenticate against Azure services securely. This platform supports advanced authentication scenarios, including single sign-on (SSO), multi-factor authentication (MFA), and conditional access policies, making it the most suitable option for App1's migration to Azure.

Feedback(if wrong):-

B) Azure Active Directory (Azure AD): Although Azure AD is a fundamental component for managing identities and access in Azure, it is not involved in acquiring access tokens directly. Instead, Microsoft Identity Platform uses Azure AD to issue tokens.

C) Azure Instance Metadata Service (IMDS): IMDS is a service that allows retrieving metadata related to the current Azure VM instance. It is not related to token acquisition for authentication purposes.

D) Azure Service Management: Azure Service Management deals with managing Azure resources via the classic deployment model. It is not relevant to acquiring access tokens for authentication and authorization purposes.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Implementing identity and access management solutions, managing authentication and authorization in Azure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

167. Your organization has developed Azure App Service Web and API applications that utilize Azure Key Vault. The Security Department needs to enhance administrative role oversight, including reviewing role memberships with justifications, receiving alerts on assignment changes, and viewing the history of administrator activations and changes to Azure resources. Which Azure service should be implemented to meet the Security Department's requirements for administrative role management and oversight?

A) Azure AD Privileged Identity Management (PIM)

B) Azure AD Managed Service Identity

- C) Azure AD Connect
- D) Azure AD Identity Protection

Answer: A

Feedback(if correct):-

A) Azure AD Privileged Identity Management (PIM) is the correct answer for meeting the Security Department's requirements for administrative role management and oversight. PIM provides just-in-time access to elevated roles, approvals, and time bounds for security officers to review role memberships and audit trail history. With PIM, you can receive alerts on assignment changes, view the history of administrator activations, and see changes to Azure resources.

Feedback(if wrong):-

B) Azure AD Managed Service Identity: This service is aimed at managing service identities for applications running in Azure services, not for administrative role management and oversight.

C) Azure AD Connect: This service is used for connecting and syncing on-premises active directories with Azure AD. It does not cater to the administrative role management and oversight requirements of the Security Department.

D) Azure AD Identity Protection: This service focuses on identifying, investigating, and remediating user risks related to identity theft and compromised accounts. It does not provide administrative role management and oversight features.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Designing Azure Infrastructure Solutions

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

168. As part of the deployment of Azure App Service Web and API applications using Azure Key Vault for storing keys, the Development Department requires a solution that enables the applications to access and retrieve keys directly from Azure Key Vault without managing credentials or secrets in the code. Which Azure service should be recommended to allow secure and seamless access to Azure Key Vault for the Development Department's applications?

- A) Azure AD Privileged Identity Management (PIM)
- B) Azure AD Managed Service Identity
- C) Azure AD Connect
- D) Azure AD Identity Protection

Answer: B

Feedback(if correct):-

Azure AD Managed Service Identity (MSI) enables secure access to Azure Key Vault without the need to store credentials or secrets in the code. It provides an automatically managed identity in Azure Active Directory (Azure AD) that the Azure services can use to authenticate with services that support Azure AD authentication, such as Azure Key Vault. By enabling MSI for the Azure App Service Web and API applications, the Development Department can securely retrieve keys directly from Azure Key Vault without managing credentials or secrets in the code.

Feedback(if wrong):-

- A) Azure AD Privileged Identity Management (PIM)

Rationale: Azure AD Privileged Identity Management (PIM) is a service that helps you manage, control, and monitor access within your organization. However, it is not directly related to enabling applications to access Azure Key Vault securely without managing credentials or secrets in the code. PIM focuses on managing access to privileged roles and resources in Azure AD, rather than providing seamless access to Key Vault for applications.

- C) Azure AD Connect

Rationale: Azure AD Connect is a tool used to integrate your on-premises directories with Azure Active Directory (Azure AD). It synchronizes identities from your on-premises directory to Azure AD, but it does not provide a solution for enabling applications to access Azure Key Vault securely without managing credentials or secrets in the code. Azure AD Connect is primarily used for user authentication and identity synchronization, rather than managing access to Key Vault for applications.

- D) Azure AD Identity Protection

Rationale: Azure AD Identity Protection is a security service that helps detect, investigate, and mitigate identity-based risks in Azure AD. While it enhances security for Azure AD users, it does not directly address the requirement of enabling applications to access Azure Key Vault securely without managing credentials or secrets in the code. Azure AD Identity Protection focuses on identity protection and risk management, rather than providing access to Key Vault for applications.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Designing Azure Infrastructure Solutions

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

169. In the context of developing Azure App Service Web and API applications, the Quality Assurance Department seeks temporary administrator access to create and configure additional Web and API applications in the test environment, ensuring controlled and temporary elevation of access. To provide temporary administrator access as requested by the Quality Assurance Department, which Azure service is most suitable?

- A) Azure AD Privileged Identity Management (PIM)
- B) Azure AD Managed Service Identity
- C) Azure AD Connect
- D) Azure AD Identity Protection

Answer: A

Feedback(if correct):-

Azure AD Privileged Identity Management (PIM) enables temporary administrator access for creating and configuring additional Web and API applications in the test environment, ensuring controlled and temporary elevation of access. PIM allows organizations to manage, control, and monitor access within Azure AD by providing just-in-time privileged access to users. With PIM, users can request and receive temporary elevated access to specific roles or resources, such as Azure App Service, for a limited duration, helping to maintain security and compliance.

Feedback(if wrong):

Answer: B) Azure AD Managed Service Identity

AD Managed Service Identity (MSI) is not directly related to providing temporary administrator access for creating and configuring additional Web and API applications in the test environment. MSI is primarily used to securely access Azure resources without the need to manage credentials explicitly, typically for services running in Azure, such as Azure Virtual Machines or Azure Functions. It does not address the requirement for temporary elevated access for administrative tasks.

C) Azure AD Connect

Azure AD Connect is used to synchronize identities from on-premises directories to Azure Active Directory (Azure AD). It is not designed to provide temporary administrator access in the test environment for creating and configuring additional Web and API applications. Azure AD Connect focuses on identity synchronization and authentication, rather than access management for temporary elevated privileges.

D) Azure AD Identity Protection

Azure AD Identity Protection is a security service focused on detecting and mitigating identity-based risks in Azure AD. It does not provide functionality for granting temporary administrator access to users for creating and configuring additional Web and API applications in the test environment. Azure AD Identity Protection is geared towards security monitoring and risk management, not access provisioning for temporary administrative tasks.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Identity and Security Solutions

Competencies: Designing Azure Infrastructure Solutions

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

170. You have the Free edition of a hybrid Azure Active Directory (Azure AD) tenant. The tenant uses password hash synchronization. You need to recommend a solution to meet the following requirements:

- Prevent Active Directory domain user accounts from being locked out as the result of brute force attacks targeting Azure AD user accounts.
- Block legacy authentication attempts to Azure AD integrated apps.
- Minimize costs.

What should you recommend to protect against brute force attacks:

- A) Azure AD Password Protection
- B) Conditional access policies
- C) Pass-through authentication
- D) Smart lockout

Answer: D

Feedback(if correct):-

To protect against brute force attacks, you should recommend D) Smart lockout. Smart lockout helps identify and defend against bad actors trying to guess your users' passwords or applying brute-force tactics to break into their accounts. Smart lockout achieves this by distinguishing genuine user sign-ins from illegitimate ones coming from suspect sources or attackers. Legitimate users can carry on accessing their accounts, whilst bad actors get locked out, ensuring productivity and safety.

Feedback(if wrong):-

A) Azure AD Password Protection: This feature aims to enforce strong password policies and obstruct the use of weak or commonly occurring passwords. It doesn't actively protect against brute force attacks.

B) Conditional access policies: They focus on controlling access depending on specific conditions such as location, device, and user risk level. Conditional access policies don't specifically guard against brute force attacks.

C) Pass-through authentication: This technique transparently relays authentication requests straight to on-premises Active Directory servers, bypassing password hash storage in Azure AD. Unfortunately, it does not counteract brute force assaults.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Designing Identity and Security Solutions
- Competencies: Implementing security measures to protect Azure AD environments against brute force attacks and legacy authentication methods.
- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Application

171. You have the Free edition of a hybrid Azure Active Directory (Azure AD) tenant. The tenant uses password hash synchronization. You need to recommend a solution to meet the following requirements:

- Prevent Active Directory domain user accounts from being locked out as the result of brute force attacks targeting Azure AD user accounts.
- Block legacy authentication attempts to Azure AD integrated apps.
- Minimize costs.

What should you recommend to block legacy authentication attempts:

- A) Azure AD Application Proxy
- B) Azure AD Password Protection
- C) Conditional access policies
- D) Enable Security defaults

Answer: D

Feedback(if correct): Enabling Security Defaults in Azure AD is the correct recommendation to block legacy authentication attempts. It's a set of default security settings recommended by Microsoft that includes blocking legacy authentication protocols, enforcing multi-factor authentication for all users, and protecting privileged activities.

Feedback(if wrong): The other options, while valuable for different aspects of security and access management, do not specifically address the blocking of legacy authentication attempts across an entire Azure AD tenant as directly and comprehensively as enabling Security Defaults does. Azure AD Application Proxy is used for secure remote access, Azure AD Password Protection enhances password security, and Conditional Access policies provide granular control but require more complex configuration and are not available in the Azure AD Free edition.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Designing Identity and Security Solutions
- Competencies: Implementing security measures to protect Azure AD environments against brute force attacks and legacy authentication methods.
- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Application

172. To enhance performance and resiliency for on-premises applications accessing Azure file shares in a transaction-intensive environment, your plan involves creating an Azure Storage account. You aim to minimize latency and ensure high resiliency. Given the requirements for high performance, low latency, and the highest level of resiliency for the storage tier, what configurations should you recommend for the Azure Storage account?

- A) Select the Standard storage tier with geo-redundant storage (GRS) replication.
- B) Opt for the Premium storage tier with locally-redundant storage (LRS) replication.
- C) Choose the Premium storage tier with zone-redundant storage (ZRS) replication.
- D) Utilize the Standard storage tier with zone-redundant storage (ZRS) replication.

Answer: C

Feedback(if correct):- Premium Storage Tier: Premium file shares are powered by SSDs, ensuring high performance and low latency, crucial for IO-intensive workloads. This makes it suitable for transaction-intensive on-premises applications accessing Azure file shares.

Zone-Redundant Storage (ZRS) Replication: ZRS maintains three copies of data in separate availability zones, offering high availability and resilience against zone-level failures. This option provides the highest level of resiliency available for Premium file shares.

Feedback(if wrong):-

- A: The standard tier with GRS doesn't offer the low latency required for transaction-intensive applications.
- B: Premium with LRS offers low latency but doesn't provide the highest level of resiliency because it's confined to a single location.
- D: Standard tier with ZRS, while resilient, doesn't offer the SSD-backed performance required for transaction-intensive applications.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Implementing storage solutions that optimize performance, cost, and resilience using Azure Storage accounts, specifically focusing on file shares for transaction-intensive on-premises applications.

Difficulty Level: Expert

Bloom's Taxonomy Level: Application

173. To ensure optimal performance and cost efficiency for two new applications being introduced in your Azure environment, it's essential to match their specific storage requirements with the appropriate type of Azure Storage accounts. Given the distinct characteristics and needs of each app, such as performance sensitivity, redundancy requirements, and access methods, the selection of the right storage account type will directly impact the app's efficiency and reliability. For an app that necessitates high-performance storage with transaction-heavy operations and another that requires long-term, cost-effective storage for large datasets, the correct types of Azure Storage accounts must be identified from the options provided.

Given the requirements:

- App1 requires high throughput and low latency for frequent transaction processing.
- App2 needs affordable storage solutions for archiving large amounts of data with less frequent access patterns.

Considering Azure Storage account options that vary in performance levels, access tiers, and pricing models, which storage accounts align best with the needs of App1 and App2? Your task is to recommend the most suitable storage accounts based on the specific requirements of each application.

- A) Recommend high-performance Premium Storage for App1 and Cool Access Tier storage for App2 for cost-effective archiving.
- B) Suggest using Blob Storage for App1 for unstructured data and File Storage for App2 for shared access.
- C) Propose Standard Storage with Hot Access Tier for App1 for balanced performance and cost, and Archive Access Tier for App2 for the lowest storage cost.
- D) Advise on using only General Purpose v2 (GPv2) storage accounts for both applications, leveraging different access tiers to balance performance and cost.

Answer: A

Feedback(if correct):-

For the scenario involving the selection of Azure Storage accounts for two new applications with distinct requirements, the correct choice is:

- A) Recommend high-performance Premium Storage for App1 and Cool Access Tier storage for App2 for cost-effective archiving.

Premium Storage: This option is ideal for App1, which demands high throughput and low latency to handle frequent transactions effectively. Premium Storage uses SSDs for storage, which provides the fastest read/write capabilities, crucial for performance-sensitive applications.

Cool Access Tier Storage: For App2, which involves storing large amounts of data that are infrequently accessed, Cool Access Tier storage offers a cost-efficient solution. It's optimized for storing data that is accessed less frequently, providing a balance between accessibility and lower storage costs.

Feedback (if wrong):

Option B: Blob Storage is suitable for unstructured data, but it doesn't specifically cater to the high-performance needs of App1 as Premium Storage does. File Storage could serve shared access needs but may not provide the most cost-efficient solution for App2's archival requirements.

Option C: Standard Storage with Hot Access Tier could support App1 but may not offer the best performance for transaction-heavy operations compared to Premium Storage. Archive Access Tier for App2 ensures the lowest cost but may impede access to data when needed, making Cool Access Tier a more balanced choice.

Option D: While General Purpose v2 storage accounts are versatile and support different access tiers, they may not deliver the specialized performance and cost benefits provided by Premium Storage for App1 and Cool Access Tier for App2.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Data Platforms

Competencies: Recommending appropriate Azure storage solutions and access tiers based on application requirements for performance and cost-efficiency.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

174. You are tasked with addressing a database retention requirement in your Azure environment. Which solution should you recommend?

- A. Deploy Azure Site Recovery for disaster recovery.
- B. Implement a long-term retention policy for the database.
- C. Enable geo-replication for the database.
- D. Utilize automatic backups for Azure SQL Database.

Answer: B

Feedback(if correct):-

Long-term retention (LTR) policies in Azure SQL Database allow you to automatically retain database backups in separate Azure Blob Storage containers for extended periods, up to 10 years. This solution fulfills the database retention requirement by ensuring backups are preserved for compliance and archival purposes.

Feedback(if wrong):-

- A. Deploying Azure Site Recovery for disaster recovery does not address the database retention requirement. Instead, it focuses on failing databases and applications to a secondary location in case of a disaster.
- C. Enabling geo-replication for the database replicates the database to a secondary region for improved availability and disaster recovery. Still, it does not fulfill the database retention requirement.
- D. Utilizing automatic backups for Azure SQL Database is a default feature that backs up databases regularly. However, it does not provide long-term retention options to comply with the database retention requirement.

Skill mapping:

- Skill: Designing Microsoft Azure Infrastructure Solutions (AZ-305)
- Subskill: Designing Data Platforms
- Competency: Designing solutions for data storage, management, and protection in Azure.
- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Application

175. You have an Azure Synapse Analytics instance (ASA29) and an Azure Cosmos DB SQL API account (DB) hosting a container storing continuously updated operational data. Your task is to design a solution using ASA29 to analyze the operational data daily without impacting the performance of the operational data store. What should you recommend?

- A) Azure Data Factory with Azure Synapse Analytics connectors
- B) Azure Synapse Link for Azure Cosmos DB
- C) Azure Synapse Analytics
- D) Azure Cosmos DB migration tool

Answer: B

Feedback(if correct): Option B) Azure Synapse Link for Azure Cosmos DB is the correct choice. It enables real-time analytics on operational data stored in Azure Cosmos DB without impacting its performance.

Feedback(if wrong):

- Option A (Azure Data Factory with Azure Synapse Analytics connectors) involves data movement and orchestration but doesn't specifically address real-time analytics without impacting the performance of the operational data store.
- Option C (Azure Synapse Analytics) focuses on analytics but doesn't address the requirement of avoiding performance impact on the operational data store.
- Option D (Azure Cosmos DB migration tool) is unrelated to the scenario described and doesn't fulfill the requirement of analyzing operational data without impacting performance.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskill: Designing Data Platforms
- Competencies: Designing solutions for real-time analytics on operational data
- Difficulty Level: Intermediate to Advanced
- Bloom's Taxonomy Level: Analysis or Synthesis

176. Design an Azure Storage Account configuration for two distinct applications, Application1 and Application2, abiding by the following requirements:

Application1:

- Highest possible transaction rates and lowest possible latency
- Upload and download optimized
- High availability during datacenter failure

Application2:

- Lowest possible storage costs per GB

- Upload and download optimized
- High availability during datacenter failure

What should you recommend for Application1

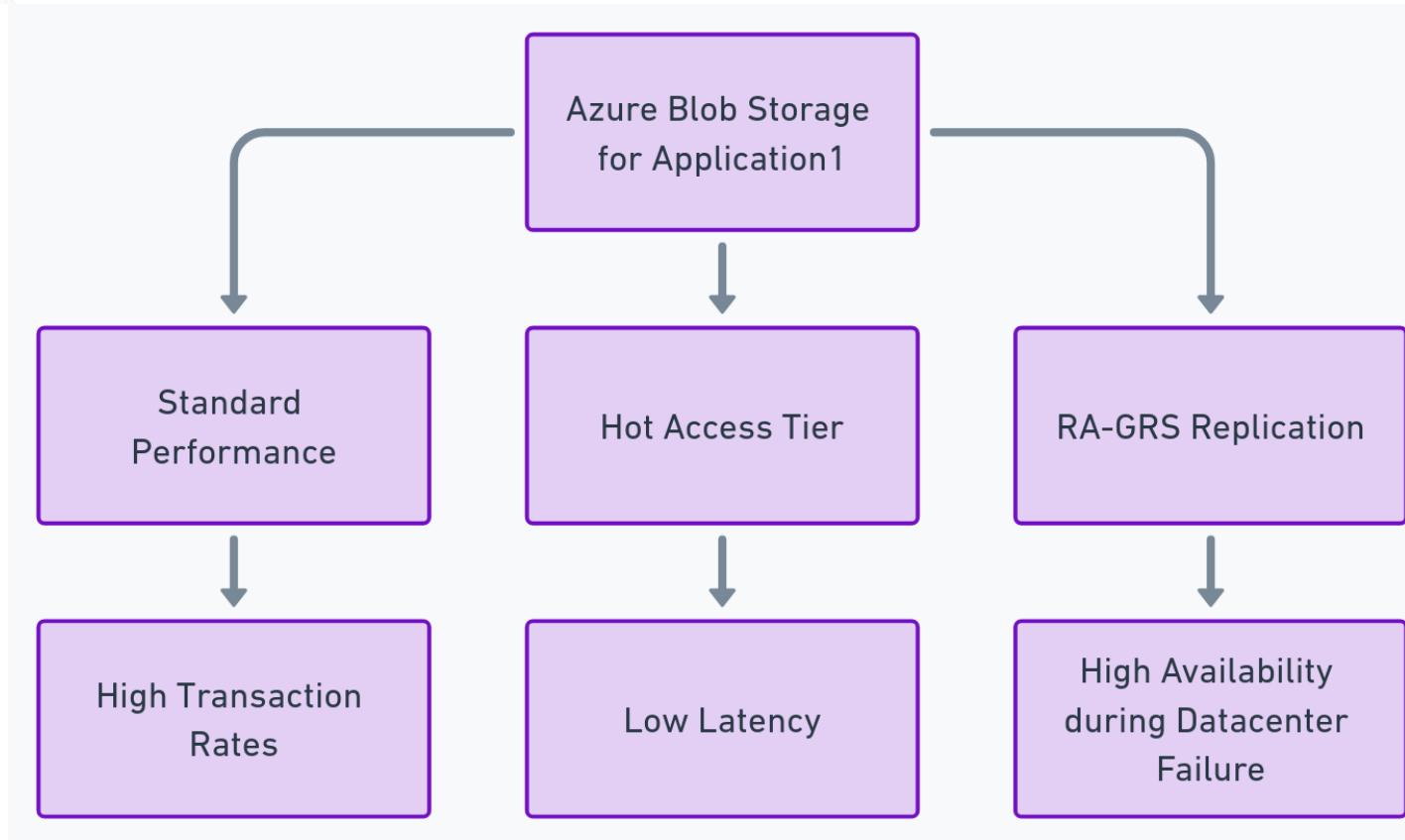
- A) BlobStorage with Standard performance, Hot access tier, and Read-access geo-redundant storage (RA-GRS) replication
- B) BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication
- C) General purpose v1 with Premium performance and Locally-redundant storage (LRS) replication
- D) General purpose v2 with Standard performance, Hot access tier, and Locally-redundant storage (LRS) replication

Answer: B

Feedback(if correct):- For Application1, the best choice would be:

- B) BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication

BlockBlobStorage accounts are optimized for high transaction rates and single-digit consistent storage latency, which makes them ideal for Application1's requirement of the highest possible transaction rates and lowest possible latency. Additionally, the Premium performance tier ensures optimum performance for uploads and downloads, and Zone-redundant storage (ZRS) replication offers high availability during datacenter failure.



Feedback(if wrong):-

- A) BlobStorage with Standard performance, Hot access tier, and Read-access geo-redundant storage (RA-GRS) replication- Standard performance may not provide the desired high transaction rates and low latency. RA-GRS replication provides geographical redundancy but not the performance and low latency offered by BlockBlobStorage with Premium performance.
- C) General purpose v1 with Premium performance and Locally-redundant storage (LRS) replication- Though the Premium performance is met, locally-redundant storage (LRS) does not offer high availability during datacenter failure.

- D) General purpose v2 with Standard performance, Hot access tier, and Locally-redundant storage (LRS) replication- Again, the Standard performance does not meet the high transaction rates and low latency requirements, and locally-redundant storage (LRS) does not offer high availability during datacenter failure.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Designing Data Platforms
- Competencies: Analyze and recommend appropriate Azure services and configurations for data analytics solutions.

- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Evaluation

177. Design an Azure Storage Account configuration for two distinct applications, Application1 and Application2, abiding by the following requirements:

Application1:

- Highest possible transaction rates and lowest possible latency
- Upload and download optimized
- High availability during datacenter failure

Application2:

- Lowest possible storage costs per GB
- Upload and download optimized
- High availability during datacenter failure

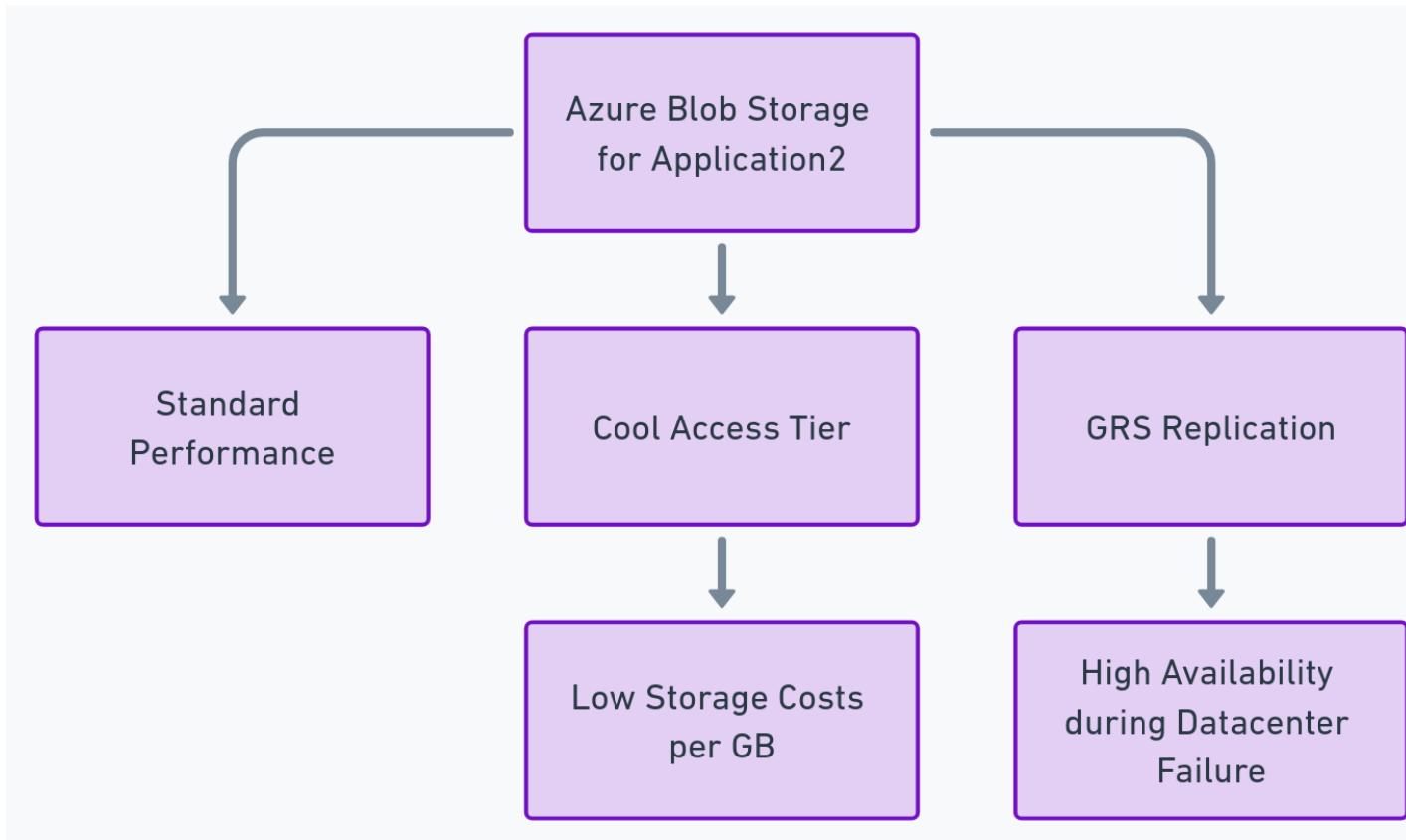
What should you recommend for Application2?

- A) BlobStorage with Standard performance, Cool access tier, and Geo-redundant storage (GRS) replication
- B) BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication
- C) General purpose v1 with Standard performance and Read-access geo-redundant storage (RA-GRS) replication
- D) General purpose v2 with Standard performance, Cool access tier, and Read-access geo-redundant storage (RA-GRS) replication

Answer: D

Feedback(if correct):- For Application2, the best choice would be: D) General purpose v2 with Standard performance, Cool access tier, and Read-access geo-redundant storage (RA-GRS) replication

General purpose v2 storage accounts provide the lowest storage costs per GB among the available options. The Cool access tier is suitable for infrequently accessed data and further reduces costs. Read-access geo-redundant storage (RA-GRS) replication ensures high availability during datacenter failure while adding minimal cost.



Feedback(if wrong):-

- A) BlobStorage with Standard performance, Cool access tier, and Geo-redundant storage (GRS) replication - While the Cool access tier and GRS replication meet the low-cost and high availability requirements, BlobStorage performance levels aren't ideally suited for the lowest possible storage costs per GB.
- B) BlockBlobStorage with Premium performance and Zone-redundant storage (ZRS) replication- This option is not cost-effective for low-cost storage and is optimized for high transaction rates and low latency, which conflicts with Application2's requirements.
- C) General purpose v1 with Standard performance and Read-access geo-redundant storage (RA-GRS) replication- General purpose v1 storage accounts have higher costs per GB compared to General purpose v2, making them less suitable for the lowest possible storage costs per GB.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Designing Data Platforms
- Competencies: Analyze and recommend appropriate Azure services and configurations for data analytics solutions.
- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Evaluation

178. Your organization is developing `AppServiceHighAvail`, a high-availability web application designed to serve users globally. The application is comprised of a front-end web tier and a back-end database tier. The back-end must be Azure-managed, supporting dynamic scaling and automatic backups, ensuring minimal downtime and data loss in case of regional Azure service disruptions. For the deployment of `AppServiceHighAvail`, you need to design a highly available architecture for the web tier that meets the organization's global availability requirements. What is the best option for deploying the web tier?

- A) Deploy using Azure App Service with multi-region deployment and Azure Traffic Manager for DNS-based traffic routing.
- B) Deploy on Azure Virtual Machines within an Availability Set in a single region.
- C) Use Azure Functions with a Consumption Plan across multiple regions.
- D) Implement Azure Kubernetes Service (AKS) with cluster autoscaler enabled in a single region.

Answer: A

Feedback(if correct):-

For the question regarding the deployment of a high-availability web application (`AppServiceHighAvail`), the correct choice is A) Deploy using Azure App Service with multi-region deployment and Azure Traffic Manager for DNS-based traffic routing. This setup ensures the application remains available globally, even in the event of a regional Azure service disruption. By utilizing Azure App Service in multiple regions, the application can serve users with high availability and resilience. Azure Traffic Manager enhances this by directing users to the closest or most optimal instance of the application, based on their geographic location and the health of the application instances. This combination offers an effective solution for achieving the required global availability and resilience for `AppServiceHighAvail`.

Feedback(if wrong):

B) Deploy on Azure Virtual Machines within an Availability Set in a single region: This option does not provide the required global availability as it restricts the deployment to a single region, making it susceptible to regional outages.

C) Use Azure Functions with a Consumption Plan across multiple regions: While Azure Functions can provide scalability and cost-efficiency, without explicit mention of multi-region deployment and traffic management, this option alone does not guarantee global availability and optimal traffic routing.

D) Implement Azure Kubernetes Service (AKS) with cluster autoscaling enabled in a single region: Similar to option B, deploying AKS in a single region does not address the global availability requirement, as it would be vulnerable to regional disruptions.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Implementing high-availability solutions using Azure App Service and Traffic Manager for global traffic distribution

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

179. Your organization is developing 'AppServiceHighAvail', a high-availability web application designed to serve users globally. The application is comprised of a front-end web tier and a back-end database tier. The back-end must be Azure-managed, supporting dynamic scaling and automatic backups, ensuring minimal downtime and data loss in case of regional Azure service disruptions. Continuing with the development of 'AppServiceHighAvail', a high-availability web application designed for a global audience, your focus shifts to the back-end database tier. This tier must be Azure-managed and capable of dynamic scaling, automatic backups, and ensuring minimal downtime and data loss in case of regional Azure service disruptions. To support 'AppServiceHighAvail', what is the most appropriate Azure-managed database solution to meet the application's requirements for high availability and global data distribution?

- A. Azure SQL Database with Geo-Replication for automatic failover between regions.
- B. Single Azure Cosmos DB instance with multi-region writes enabled.
- C. Azure MySQL Database with read replicas in the same region.
- D. Azure Blob Storage with geo-redundant storage (GRS) enabled for the database files.

Answer: B

Feedback(if correct):-

Global Data Distribution: Azure Cosmos DB with multi-region writes enabled allows data to be distributed globally, ensuring that users can access data from the nearest data center, thereby reducing latency and improving the user experience.

High Availability: By enabling multi-region writes, Azure Cosmos DB provides automatic failover capabilities, ensuring that the application remains available even if one region experiences a service disruption.

Dynamic Scaling: Cosmos DB supports automatic and manual scaling of throughput and storage, meeting the dynamic scaling requirements of 'AppServiceHighAvail'.

Automatic Backups: Azure Cosmos DB offers automatic and configurable backup options, safeguarding against data loss without manual intervention.

Feedback(if wrong):-

A) Azure SQL Database with Geo-Replication: While Azure SQL Database supports geo-replication and provides high availability, it doesn't inherently offer the same level of global distribution and ease of enabling multi-region writes as Cosmos DB.

C) Azure MySQL Database with read replicas: Read replicas in the same region do not provide the global distribution or the inter-regional automatic failover capabilities required for 'AppServiceHighAvail'.

D) Azure Blob Storage with GRS: While GRS provides data redundancy across regions, Blob Storage is not a database service and does not support dynamic scaling, automatic backups, or database-specific features like indexes, queries, and transactions needed for the application's back-end database tier.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Implementing high-availability solutions using Azure App Service and Traffic Manager for global traffic distribution

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

180. In your cloud architecture, there's a requirement to precisely manage user permissions for network administration across various Azure subscriptions. The goal is to provide a group of users (contributors) with the ability to manage only specific subnets within a larger virtual

network that crosses these subscription boundaries. Considering Azure's Role-Based Access Control (RBAC) capabilities, what is the least number of role assignments needed to ensure these contributors have the necessary permissions exclusively for the designated subnets, aligning with Azure's access control best practices?

- A) 1
- B) 2
- C) 5
- D) 10

Answer: B

Feedback (if correct):

The correct answer is B) 2. You need to create a custom role with permissions to manage specific subnets and assign that role at the subnet level. Then, assign the Network Contributor role at the virtual network level to the same group of users. Following Azure's best practices, this dual assignment grants the required permissions while minimizing privileges.

Feedback (if wrong):

- A) 1: This option would not grant users the ability to manage only specific subnets. Assigning a role at the subscription level would grant permissions to all resources within that subscription.
- C) 5: This is far too many assignments and excessively permissive. Over-permissions pose security and compliance risks.
- D) 10: Again, this is excessive and introduces potential security and compliance risks. Too many role assignments can hinder auditability and traceability, making incident investigation difficult.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskill: Designing Compute and Network Infrastructure

Competency: Architecting for Business Continuity and Disaster Recovery

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Analysis

181. Within your Azure-hosted SaaS application, you are tasked with securing the communication channels between microservices. Which technologies should be used in this scenario to encrypt communications and ensure secure data transmissions? Choose three.

- A) Azure ExpressRoute
- B) Azure Virtual Network
- C) Azure Service Bus
- D) Azure Private Link

Answer: C, D

Feedback(if correct):-

C) Azure Service Bus is appropriate for secure communications between microservices because it supports encrypted data transfers and secure messaging patterns.
D) Azure Private Link provides secure and private connectivity to Azure services, ensuring that data transmitted between services does not traverse the public internet, which aligns with the requirement for secure communications.

These options directly contribute to securing the communication channels by providing encrypted and protected pathways for data transmission.

The emphasis on using Azure Service Bus and Azure Private Link is because they offer mechanisms to encrypt and secure data in transit, directly addressing the requirement to secure communication channels between microservices within Azure.

Feedback(if wrong):-

A) Azure ExpressRoute mainly provides a dedicated, private connection from on-premises networks to Azure datacenters. While it enhances connectivity security, it's not specifically designed for encrypting communications between microservices within Azure.
B) Azure Virtual Network establishes an isolated network for Azure resources, which is vital for creating secure communication environments. However, it doesn't inherently encrypt application-level communications between microservices. It's more about network segmentation and isolation rather than encryption of communications.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Implementing secure communication strategies between Azure-hosted microservices using Azure Service Bus and Azure Private Link.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application-

182. Your organization has developed a .NET-based web service, named 'WebServiceApp', that needs to interact with the local file system and write entries to the Windows Application event log as part of its operational requirements. You are tasked with deploying 'WebServiceApp' on Azure, ensuring the solution aligns with the following objectives:

- Keep maintenance efforts to a minimum to allow the development team to focus on new features and improvements.
- Reduce hosting and operational costs without compromising on functionality and performance.

Given these criteria, what deployment option should you recommend for hosting 'WebServiceApp' on Azure?

- A) Deploy as an Azure App Service Web App to leverage PaaS benefits, including integrated management, scaling capabilities, and lower maintenance requirements.
- B) Utilize an Azure Virtual Machine Scale Set for granular control over the environment, allowing direct access to the file system and event log, albeit with higher management overhead.
- C) Implement in an App Service Environment (ASE) to gain the isolation and scalability of dedicated resources, suitable for highly sensitive applications but at a higher cost.
- D) Host as an Azure Functions app to take advantage of serverless computing, although this might limit direct access to the local file system and Windows event log required by 'WebServiceApp'.

Answer: A

Feedback(if correct): The correct answer is A) an Azure App Service web app. Azure App Service is ideal for hosting .NET web services like Service1. It inherently supports writing to the file system designated for the app and integrates easily with Azure Monitor for logging purposes, which can substitute for writing to

the Windows Application event log. This solution minimizes maintenance overhead by managing the infrastructure for you and is cost-effective due to Azure App Service's pricing model, which includes a variety of options suitable for different scenarios, including free and shared tiers for development and testing, as well as more robust tiers for production.

Feedback(if wrong):

B) An Azure virtual machine scale set: While it offers extensive control over the environment, allowing for the execution of tasks like writing to the local file system and the Windows Application event log, it significantly increases maintenance overhead and cost.

C) An App Service Environment (ASE): Offers an isolated environment for running Azure App Services in a VNet, which provides high scalability and customizability but at a much higher cost and complexity compared to basic App Service plans.

D) An Azure Functions app: Although it provides a serverless execution environment ideal for running small pieces of code, or "functions," in the cloud, it does not natively support tasks like writing to the local file system or the Windows Application event log without additional configuration and does not fit the traditional web service model as directly as Azure App Service.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Implementing solutions for hosting web applications on Azure, focusing on Azure App Service Web Apps for .NET applications. Understanding of how to leverage Azure services for logging and file storage to meet application requirements.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

183. To integrate an ExpressRoute circuit into a Basic Azure Virtual WAN (VirtualWAN1) and facilitate a direct, private connection that bypasses the internet, a critical initial step is required. This connection aims to enhance connectivity between your corporate network and your Azure services, providing a more reliable and secure communication path. Given the objective to associate an ExpressRoute circuit located in the US East region with VirtualWAN1, ensuring that the solution adheres to Azure's networking and connectivity standards while maximizing the capabilities of Virtual WAN, which action should you undertake first to achieve this integration?

- A) Develop a new virtual network hub in the US East region to directly associate with the ExpressRoute circuit.
- B) Establish a dedicated gateway in Hub1 to facilitate the ExpressRoute circuit integration.
- C) Upgrade VirtualWAN1 from Basic to Standard to enable support for ExpressRoute connections
- D) Activate the ExpressRoute Premium add-on to extend the ExpressRoute circuit's features and geographic reach.

Answer: C

Feedback(if correct): The correct answer is C) Upgrade VirtualWAN1 from Basic to Standard to enable support for ExpressRoute connections. Before connecting an ExpressRoute circuit to a Basic Azure Virtual WAN, you must upgrade it to Standard as Basic virtual WANs can only connect to site-to-site VPNs. Upon upgrading VirtualWAN1, you can proceed with associating the ExpressRoute circuit with the virtual WAN, ensuring a secure and reliable private connection between your corporate network and Azure services.

upgrading VirtualWAN1 to Standard to unlock support for ExpressRoute connections. This critical step precedes any attempt to associate the ExpressRoute circuit with the virtual WAN, thereby reinforcing a stable and secure communication pathway between your local infrastructure and Azure services.

Feedback(if wrong):

- A) Develop a new virtual network hub in the US East region to directly associate with the ExpressRoute circuit: This option is incorrect because creating a new virtual network hub does not resolve the limitation imposed by the Basic Azure Virtual WAN, which hinders ExpressRoute circuit integration.
- B) Establish a dedicated gateway in Hub1 to facilitate the ExpressRoute circuit integration: This option is incorrect since a dedicated gateway in Hub1, created specifically for ExpressRoute, is not compatible with a Basic Azure Virtual WAN.
- D) Activate the ExpressRoute Premium add-on to extend the ExpressRoute circuit's features and geographic reach: This option is incorrect because activating the ExpressRoute Premium add-on does not solve the constraint tied to the Basic Azure Virtual WAN's incapability to connect with ExpressRoute circuits.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Implementing Azure Virtual WAN for enhanced network connectivity and integration with Azure ExpressRoute.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

184. To accommodate the rapid scaling needs of your Linux-based containerized applications within Azure Kubernetes Service (AKS), ensuring minimal provisioning time for computing resources and reducing administrative tasks is crucial.

Requirements:

- Swiftly scale out compute resources to meet surges in demand.
- Enable autoscaling for Linux containers to optimize resource utilization.
- Streamline management efforts to focus on development rather than infrastructure.

Given these prerequisites, which AKS feature should be recommended to streamline operations while adhering to the scalability and management efficiency requirements?

- A) Virtual Nodes
- B) Cluster Autoscaler
- C) Manual node scaling
- D) Horizontal Pod Autoscaler

Answer: A

Feedback(if correct): Congratulations on selecting the correct option! Virtual Nodes truly stand out as the optimal solution for your Linux-based containerized applications in Azure Kubernetes Service (AKS). With their lightning-quick scaling, built-in autoscaling capabilities, and diminished administrative tasks, Virtual Nodes check all the boxes for your requirements.

Feeback(if wrong): Although the option you chose wasn't precisely what we were searching for, don't worry! It's essential to explore various options and learn from each experience. In this case, Virtual Nodes

proved to be the ideal choice for your Linux-based containerized applications within Azure Kubernetes Service (AKS). Offering swift scaling, embedded autoscaling, and decreased administrative efforts, Virtual Nodes certainly tick all the boxes for your scalability and management efficiency needs. Feel free to try again and fine-tune your knowledge!

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Implementing Azure Kubernetes Service (AKS) solutions for scalable and efficient application deployment, with a focus on minimizing provisioning time for compute resources, enabling autoscaling of Linux containers, and reducing administrative efforts.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

185. To optimize the architecture of an Azure App Service for an application while keeping costs low, which deployment strategy would be most effective?

- A) Deploy a singular App Service Environment (ASE) across multiple availability zones for resilience.
- B) Establish a dedicated App Service plan within each availability zone for scalability.
- C) Configure a single App Service plan to serve the entire region, minimizing resource duplication.
- D) Allocate an App Service Environment (ASE) to every region to enhance global accessibility.

Answer: A

Feedback(if correct):-

For the scenario where you're designing an App Service architecture for App1 with a focus on minimizing costs, the most effective solution is:

- A) One App Service Environment (ASE) per availability zone.

This choice is appropriate because:

Optimal Cost Management: Utilizing an App Service Environment in each availability zone allows for dedicated resources within a secured and isolated environment, which can be scaled according to the specific needs of App1, thus managing costs effectively.

High Availability: Deploying across multiple availability zones ensures high availability and fault tolerance, minimizing the risk of downtime without unnecessary redundancy that might increase costs.

Location Proximity: Placing ASEs in each availability zone also reduces latency by hosting the application closer to the end-users, improving performance while controlling costs.

Feedback(if wrong):-

B) One App Service plan per availability zone: While this could provide geographical distribution, it lacks the isolation and potential cost benefits offered by ASE. Moreover, App Service plans are more about resource allocation rather than environmental isolation.

C) One App Service plan per region: This approach might not provide the high availability required by App1 across different availability zones within the region, potentially compromising application resilience.

D) One App Service Environment (ASE) per region: While providing an isolated environment, this option doesn't leverage the high availability and fault tolerance benefits of distributing the architecture across multiple availability zones, which could be more cost-effective in the long run.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Evaluating and recommending appropriate Azure service configurations to meet specific application requirements while optimizing cost and performance.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

186. You are evaluating whether to use Azure Traffic Manager and Azure Application Gateway to meet the connection requirements for App1. What is the minimum number of instances required for each service? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

- A) One instance for Azure Traffic Manager and one instance for Azure Application Gateway
- B) Two instances for Azure Traffic Manager and one instance for Azure Application Gateway
- C) One instance for Azure Traffic Manager and two instances for Azure Application Gateway
- D) Two instances for Azure Traffic Manager and two instances for Azure Application Gateway

Answer: A

Feedback(if correct): The correct answer is A) One instance for Azure Traffic Manager and one instance for Azure Application Gateway.

- Azure Traffic Manager operates at the DNS level to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints. It does not require multiple instances as a single instance can manage traffic for multiple Azure services or external services.
- Azure Application Gateway is a web traffic load balancer that can be deployed across multiple zones for high availability. However, a single instance of Application Gateway can suffice for load balancing and routing traffic, depending on the scale and redundancy requirements of the application.

Feedback(if wrong):-

B) Two instances for Azure Traffic Manager and one instance for Azure Application Gateway- This option proposes multiple Traffic Manager instances, but as explained earlier, a single instance is enough for managing traffic to multiple Azure services or external services, making this choice unnecessary.

C) One instance for Azure Traffic Manager and two instances for Azure Application Gateway- This option recommends multiple Application Gateway instances, which can be viable for high availability, but a single instance can suffice if scaled and configured appropriately for the application's requirements. Introducing additional instances may complicate management and raise costs without tangible benefits.

D) Two instances for Azure Traffic Manager and two instances for Azure Application Gateway- Similar to option B, this choice advocates for multiple Traffic Manager instances, which is unwarranted. Further, it encourages deploying two Application Gateway instances, which might not be justified unless high availability is a strict requirement, as discussed in option C. Overall, this option escalates costs and complexity without evident advantages.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Selecting and configuring appropriate Azure services to meet connectivity and load-balancing requirements for applications.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

187. You are tasked with advising on a notification solution for the IT Support distribution group. What recommendation should you provide?

A. Implement Azure Network Watcher

- B. Set up an action group
- C. Create a SendGrid account with advanced reporting
- D. Configure Azure AD Connect Health

Answer: B.

Feedback(if correct):

When recommending a notification solution for the IT Support distribution group, setting up an action group is indeed the best choice. This allows you to notify members of the group whenever specific triggers or events take place within your Azure environment.

Feeback(if wrong):

- A) Implement Azure Network Watcher- This solution is mostly used for diagnostics, troubleshooting, and monitoring Azure virtual networks and applications, making it unsuitable for notifying the IT Support distribution group.
- C) Create a SendGrid account with advanced reporting- Although SendGrid is commonly used for sending emails, newsletters, or promotional content, it doesn't exactly fit the scenario presented. Advanced reporting is nice to have, but it won't send notifications to the IT Support distribution group.
- D) Configure Azure AD Connect Health- While Azure AD Connect Health helps monitor and sync on-premises and Azure Active Directory identities, it doesn't relate to the scenario of providing a notification solution for the IT Support distribution group.

Skill mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Advising on appropriate Azure services for specific requirements

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

188. You are responsible for migrating Application A to Azure. To ensure high availability, you must devise a resilient solution to meet specific prerequisites. What measures should be included in your proposal? Choose the proper options from the answer section. Each valid choice contributes one point.

- A) Create a host group in each availability zone; distribute the Azure virtual machines across the designated zones.
- B) Employ a single host group in an availability zone supported by Azure.
- C) Utilize Azure virtual machine scale sets for automatic scaling of the application.
- D) Do not employ automatic scaling for Azure virtual machines.

Answer: A, C

Feedback(if correct):-

To ensure high availability during the migration of Application A to Azure, the recommended measures include:

- A) Create a host group in each availability zone; distribute the Azure virtual machines across the designated zones.
 - This option leverages Azure Availability Zones to distribute resources across multiple physical locations within a region, ensuring fault isolation and resilience against zone failures.
- C) Utilize Azure virtual machine scale sets for automatic scaling of the application.
 - Azure virtual machine scale sets enable automatic scaling of application instances based on demand, ensuring optimal performance and availability during fluctuations in workload.

Feedback(if wrong):-

Option B is not optimal because relying on a single availability zone may introduce a single point of failure. Option D, not employing automatic scaling, does not directly contribute to high availability, as it may result in under-provisioning or over-provisioning of resources during varying workloads.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Designing resilient and highly available solutions in Azure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

189. You're tasked with granting a user access to manage a specific virtual network within your Azure environment. To minimize complexity and adhere to least privilege principles, what is the minimum number of Azure RBAC role assignments required using the Network Contributor role?

- A) 1
- B) 2
- C) 5
- D) 10

Answer: A

Feedback(if correct):-

When assigning the Network Contributor role, you only need to create one role assignment to grant the necessary permissions for managing the specified virtual network. This role assignment provides the user with the required access while minimizing complexity and adhering to the principle of least privilege.

Feedback(if wrong):-

Assigning multiple role assignments for the same role to the same user can lead to unnecessary complexity and potential security risks. In this scenario, only one role assignment is needed to grant access to manage the specific virtual network, ensuring simplicity and adherence to least privilege principles.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Designing resilient and highly available solutions in Azure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

190. You're designing a high-availability solution for a critical application, App1, which needs to be migrated to Azure. The solution must ensure continued operation even if a localized outage

occurs within the Azure region. What combination of Azure Virtual Machine Scale Sets (VMs) and Availability Zones best achieves this high-availability requirement?

- A. 1 VM Scale Set deployed across 3 Availability Zones
- B. 3 VM Scale Sets, each deployed in a separate Availability Zone
- C. 1 VM Scale Set with automatic scaling enabled
- D. 3 VMs deployed individually across 3 Availability Zones

Answer: B

Feedback(if correct):-

The correct answer is B. 3 VM Scale Sets, each deployed in a separate Availability Zone.

Availability Zones are isolated locations within an Azure region with independent infrastructure. By distributing VM Scale Sets across different Availability Zones, you ensure App1 remains operational even if an outage affects one zone.

Feedback(if wrong):-

A. While a single VM Scale Set can be deployed across zones, it wouldn't guarantee high availability if the entire Scale Set is impacted by a zone outage.

C. Automatic scaling within a single Availability Zone wouldn't offer protection against a zone-wide outage.

D. Individual VMs are not managed as a group and lack scaling capabilities. This option wouldn't provide the high availability or scalability needed for App1.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Designing resilient and highly available solutions in Azure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

191. You are tasked with recommending a solution for creating an Azure Storage account to host file shares. These shares will be accessed from on-premises applications that are transaction-intensive. Your goal is to minimize latency when accessing the file shares while ensuring the highest level of resiliency for the selected storage tier. What should you recommend?

- A) Storage tier: Hot; Resiliency: Geo-redundant storage (GRS)
- B) Storage tier: Premium; Resiliency: Zone-redundant storage (ZRS)
- C) Storage tier: Transaction optimized; Resiliency: Locally redundant storage (LRS)
- D) Storage tier: Premium; Resiliency: Geo-redundant storage (GRS)

Answer: B

Feedback(if correct):-

The correct answer is B) Storage tier: Premium; Resiliency: Zone-redundant storage (ZRS). Premium file shares backed by solid-state drives (SSDs) provide consistent high performance and low latency, making them suitable for transaction-intensive workloads. Zone-redundant storage (ZRS) ensures resiliency by storing three copies of each file across different Azure availability zones.

Feedback(if wrong):

- A) Storage tier: Hot; Resiliency: Geo-redundant storage (GRS) – The Hot tier is suitable for frequently accessed data, but it does not necessarily mean lower latency. Also, GRS replicates data across regions, which can introduce additional latency.
- C) Storage tier: Transaction optimized; Resiliency: Locally-redundant storage (LRS) – There is no such thing as a "Transaction optimized" storage tier in Azure Storage accounts. Additionally, LRS only replicates data within a single data center, making it less resilient than ZRS.
- D) Storage tier: Premium; Resiliency: Geo-redundant storage (GRS) – GRS is designed for resiliency across regions, but it may not minimize latency as much as ZRS.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Designing resilient and highly available solutions in Azure

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

192. You are tasked with deploying multiple applications to Azure, with each application being deployed to two Azure Kubernetes Service (AKS) clusters, each located in a separate Azure region. The deployment must meet the following requirements:

- Ensure the applications remain available if a single AKS cluster fails.
- Encrypt connection traffic over the internet using SSL without configuring SSL on each container.

Which Azure service should you recommend to meet these requirements?

- A) AKS ingress controller
- B) Azure Traffic Manager
- C) Azure Front Door
- D) Azure Load Balancer

Answer: C

Feedback(if correct):

The correct answer is C) Azure Front Door. Azure Front Door provides global load-balancing and SSL termination, ensuring that the applications remain available if a single AKS cluster fails and encrypting connection traffic over the internet with SSL without the need to configure SSL on each container.

Feedback(if wrong):

- Option A) AKS ingress controller: This option is incorrect because the AKS ingress controller primarily manages inbound traffic to the AKS cluster and does not provide global load-balancing or SSL termination.
- Option B) Azure Traffic Manager: This option is incorrect because Azure Traffic Manager provides DNS-based traffic routing but does not offer SSL termination or global load-balancing capabilities.
- Option D) Azure Load Balancer: This option is incorrect because Azure Load Balancer provides basic layer 4 load-balancing and does not offer SSL termination or global load-balancing for internet traffic to AKS clusters.

Skill Mapping:

- Skill: Designing Microsoft Azure Infrastructure Solutions Certification (AZ-305)
- Subskills: Designing Compute and Network Infrastructure
- Competencies: Designing Azure infrastructure solutions, Leading successful implementation projects

- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Application, Analysis

193. Your organization is developing a web application with a microservices architecture that will be containerized. This application is divided into a front-end service that must be publicly accessible and a back-end service that should only communicate with the front-end service. The entire application must automatically recover from any single container failures and efficiently share data between services while minimizing operational costs. Which Azure service should you utilize to host these services under the specified conditions?

- A) Deploy on Azure Kubernetes Service (AKS) with appropriate network policies.
- B) Use Azure Service Fabric clusters with custom container orchestration.
- C) Opt for Azure Container Instances with shared Azure file storage.
- D) Configure Azure Container Registry to manage and deploy containers.

Answer: C

Feedback(if correct): The correct answer is indeed C) Azure Container Instances (ACI). ACI provides a streamlined and cost-effective solution for running containerized applications without the need for complex orchestration. It supports rapid scaling, billing by the second, and fast startup times, making it suitable for applications with varying workload patterns. Additionally, ACI allows you to meet all specified requirements, including public accessibility for the front-end service, restricted communication between front-end and back-end services, shared storage using Azure File Share, and automatic restart in case of container failures.

Feedback(if wrong): The other options provided do not fully meet all the specified requirements. While Azure Kubernetes Service (AKS) provides robust orchestration capabilities, it may introduce additional complexity for applications that don't require it. Azure Service Fabric clusters offer custom container orchestration but might be overkill for this scenario and not as cost-effective. Azure Container Registry is used for managing and deploying container images but does not provide the runtime environment needed for hosting containerized applications. Therefore, option C remains the most suitable choice.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Designing Compute and Network Infrastructure
- Competencies: Designing Azure infrastructure solutions, Implementing Azure networking solutions
- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Application, Analysis

194. You are tasked with deploying a two-tier application using Docker images in a Linux environment on Azure. The front-end tier should be publicly accessible via port 80, while the back-end tier should only be accessible via port 8080 from the front-end tier. Both containers should share the same Azure file share, and the application should automatically restart if a container fails. Costs should be kept to a minimum. Which Azure service should you use to deploy this two-tier application?

- A) Azure Kubernetes Service (AKS)
- B) Azure Service Fabric
- C) Azure Container Instances
- D) Azure Container Registry

Answer: C

Feedback(if correct): The correct answer is C) Azure Container Instances, which provides a straightforward and cost-effective solution for deploying containerized applications on Azure while meeting all specified requirements.

Azure Container Instances (ACI) provides a simple and cost-effective solution for deploying containerized applications without the need for managing infrastructure. With ACI, you can run both the front-end and back-end tiers of your application as separate containers. You can expose the front-end tier publicly via port 80 and restrict access to the back-end tier to port 8080 from the front-end tier only. ACI supports mounting Azure File Shares, allowing both containers to share the same storage. Additionally, ACI offers automatic restart capabilities, ensuring the high availability of the application. Overall, Azure Container Instances aligns with the specified requirements and helps minimize operational costs.

Feedback(if wrong): Azure Kubernetes Service (AKS) is a robust container orchestration platform but may introduce unnecessary complexity and overhead for this scenario. Azure Service Fabric is designed for building and managing microservices-based applications but may not be the most cost-effective solution.

Azure Container Registry is used for managing container images but does not provide the runtime environment needed for hosting containerized applications. Therefore, option C remains the most suitable choice for this scenario.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Designing Compute and Network Infrastructure
- Competencies: Designing Azure infrastructure solutions, Implementing Azure networking solutions
- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Application, Analysis

195. You're overseeing the deployment process for a critical web application hosted on Azure. The development team needs a streamlined way to manage version updates, allowing for thorough testing before making a new version live. Additionally, it's vital to have the option to revert to the previous version with minimal service disruption. To manage application versions effectively, ensuring both testing and rollback capabilities with minimal downtime, which Azure feature should you leverage?

- A) Initiate a new App Service plan.
- B) Utilize deployment slots.
- C) Assign a custom domain.
- D) Conduct backups of the Azure Web App.

Answer: B

Feedback(if correct):-

Deployment slots allow you to stage new versions of your web application, enabling thorough testing before swapping the slot to make the new version live. This swap operation can be done with zero downtime. Should any issues arise, you can quickly roll back to the previous version by reverting the swap operation.

Deployment slots are a feature of Azure App Service that allow for the staging of web app versions in isolated environments before they're pushed live. This setup facilitates A/B testing, previews of new

features, and a straightforward rollback process if necessary. Using deployment slots significantly reduces downtime during deployments by allowing seamless swapping between the current and new versions of the web app.

Feedback(if wrong):-

Initiating a new App Service Plan (A) does not address the challenge of managing application versions, updating, testing, and rolling back. Custom domains (C) deal with URL presentation and have nothing to do with versioning and rollbacks. Performing backups (D) is essential but does not assist in managing application versions, testing, or rollbacks.

skill mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Designing Compute and Network Infrastructure
- Competencies: Deploying and managing containerized applications using Azure services
- Difficulty Level: Intermediate
- Bloom's Taxonomy Level: Application

196. To establish a High-Performance Computing (HPC) cluster in Azure that integrates with a third-party scheduler, which solution would you recommend for the efficient provisioning and administration of the HPC cluster nodes?

- A) Azure Lighthouse
- B) Azure CycleCloud
- C) Azure Purview
- D) Azure Automation

Answer: B

Feedback(if correct):-

The correct answer is B) Azure CycleCloud.

Azure CycleCloud is a fully managed service designed specifically for provisioning, managing, and scaling HPC clusters in Azure, including integration with third-party schedulers. It offers automation, governance, and cost management features, making it an ideal choice for efficiently handling HPC environments.

Azure CycleCloud is a pivotal tool for orchestrating and managing High Performance Computing (HPC) environments within Azure. It enables users to dynamically provision and manage HPC clusters, integrating seamlessly with various HPC schedulers. Additionally, Azure CycleCloud facilitates the efficient scaling of infrastructure to accommodate jobs of any size, enhancing the management of HPC workloads.

Feedback(if wrong):-

- A) Azure Lighthouse is a delegated resource management solution that allows service providers to manage customer tenants centrally, but it does not directly contribute to provisioning or administering HPC cluster nodes.
- C) Azure Purview is a data governance service focused on discovering, classifying, and cataloging metadata across hybrid data estates, with no relation to HPC cluster management.
- D) Azure Automation is a service that enables automating repetitive tasks and processes across Azure and on-premises environments, though it is not specialized for HPC cluster management.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Implementing and managing High Performance Computing (HPC) solutions in Azure.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

197. Your task is to devise a strategy that enables developers to provision Azure Virtual Machines (VMs) within specified parameters. This strategy must ensure that VMs can only be created in certain regions and restrict the VM sizes that can be provisioned. To manage the provisioning of Azure virtual machines by developers, allowing only specific regions and VM sizes, which Azure feature should you recommend?

- A) Conditional Access policies
- B) Role-based Access Control (RBAC)
- C) Azure Resource Manager (ARM) templates

D) Azure Policy

Answer: D

Feedback(if correct):-

The correct answer is D) Azure Policy.

Azure Policy is a service that enables you to create, assign, and manage policies for enforcing rules across your Azure resources. By defining policies, you can control the conditions under which resources can be created, modified, or deleted. This ensures that developers adhere to predetermined standards and guidelines, such as creating VMs only in specified regions and using approved VM sizes.

Explanation: Azure Policy is designed to enforce organizational standards and to assess compliance at scale. By using Azure Policy, you can ensure that only specific regions are available for VM deployment and restrict the VM sizes that can be provisioned. This approach enables compliance with organizational requirements while minimizing manual oversight and intervention. Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules, which are described in policies. By defining policies that restrict VM sizes and regions, you can provide developers with the ability to provision VMs within predefined constraints, thereby meeting the specified requirements.

Feedback(if wrong):-

Conditional Access policies (A) are primarily used to control access to Azure services and applications based on conditions such as user location, application, and device. Thus, they do not directly influence VM provisioning settings.

Role-based Access Control (RBAC) (B) is utilized to manage who has access to Azure resources and what actions they can perform on those resources, but it does not dictate the specific regions or VM sizes for provisioning.

Azure Resource Manager (ARM) templates (C) are JSON files describing the infrastructure and configuration of Azure resources. ARM templates can be used to standardize deployments and enforce consistency, but they do not impose constraints on regions or VM sizes.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Implementing governance and compliance features in Azure, including Azure Policy to enforce organizational standards and SLAs.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

198. Your company utilizes several virtual machines (VMs) both on-premises and within Azure. To ensure connectivity between these environments, Azure ExpressRoute has been deployed. However, you're encountering network connectivity issues with several VMs. You are tasked with analyzing the network traffic to determine whether packets are being allowed or denied to these virtual machines. Which Azure service should you use to accurately perform this analysis?

- A) Azure Traffic Analytics in Azure Network Watcher
- B) Azure Network Watcher IP Flow Verify
- C) Azure Monitor
- D) Azure Log Analytics

Answer: B

Feedback(if correct):-

The correct answer is B) Azure Network Watcher IP Flow Verify.

This service allows you to analyze and diagnose the flow of network traffic to and from Azure Virtual Machines, effectively identifying whether packets are being allowed or denied, which is essential for resolving the network connectivity issues described in the scenario.

Azure Network Watcher IP Flow Verify is the recommended service for this scenario. It enables administrators to verify whether packets are allowed or denied to or from a VM, providing detailed information such as the direction, protocol, and port. This service can quickly diagnose connectivity issues, distinguishing it as the most appropriate tool for analyzing network traffic and identifying filtering issues at a VM level. Azure Traffic Analytics, while useful for analyzing network traffic patterns, does not provide the granular, real-time analysis of packet flow required in this scenario.

Feedback(if wrong):-

A) Azure Traffic Analytics in Azure Network Watcher: While Azure Traffic Analytics provides valuable insights into network traffic patterns and security threats, it focuses on broader network diagnostics rather than the specific task of determining if individual packets are allowed or denied to VMs.

C) Azure Monitor: Azure Monitor collects, analyzes, and acts on telemetry data from various cloud and on-premises environments. Although it can monitor the health and performance of applications and services, it does not provide the granular packet-level analysis required to diagnose the connectivity issues described.

D) Azure Log Analytics: Part of Azure Monitor, Azure Log Analytics aggregates and queries log data across different resources. While it can help identify trends and issues across your networks, it cannot specifically verify packet flows to and from virtual machines as needed for this scenario.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Implementing network traffic analysis solutions, diagnosing network connectivity issues using Azure Network Watcher

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application

199. Within your organization, a file server named VM1 is housed in a Toronto branch office, serving as a central point for accessing shared files across various branch offices linked by an on-premises network and an Azure subscription. To ensure seamless access to these shared files—even in scenarios where the Toronto office might be unreachable—what solution would you recommend implementing?

- A) Implement a Recovery Services vault paired with Azure Backup for data redundancy.
- B) Leverage an Azure File Share combined with Azure File Sync to replicate file access in the cloud.
- C) Use Azure Blob Containers in conjunction with Azure File Sync for cloud-based file sharing.
- D) Deploy a Recovery Services vault alongside Windows Server Backup for enhanced file protection.

Answer: B

Feedback(if correct):- The recommended solution effectively addresses the need for continuous access to shared files, even if the primary file server location becomes inaccessible. Leveraging Azure File Share in conjunction with Azure File Sync offers a resilient, cloud-based file storage solution that ensures users can access files from anywhere, aligning perfectly with the continuity and accessibility objectives.

By integrating Azure File Share with Azure File Sync, your organization's file-sharing capabilities are centralized within Azure Files. This setup not only retains the on-premises file server's flexibility and performance but also transforms it into an efficient cache for your Azure file share, ensuring

uninterrupted access to shared files even if the primary site is offline. This solution is specifically designed to be deployed in the same Azure region as the Azure File Sync to optimize performance and reliability.

Feedback (if wrong):

- A) Implement a Recovery Services vault paired with Azure Backup: This option focuses on data protection and backup, rather than ensuring quick and continuous access to shared files across branch offices. It's more about data recovery than maintaining active file access in case an office is inaccessible.
- C) Use Azure Blob Containers in conjunction with Azure File Sync: While Azure Blob Containers offer scalable and secure storage solutions, they are not directly compatible with Azure File Sync, which is specifically designed to work with Azure File Shares for seamless file synchronization and access.
- D) Deploy a Recovery Services vault alongside Windows Server Backup: Similar to option A, this focuses on backup solutions rather than providing uninterrupted access to shared files. It does not address the need for immediate and continuous file access if a specific branch office goes offline.

Skill Mapping:

Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305

Subskills: Designing Compute and Network Infrastructure

Competencies: Implementing hybrid storage solutions, including data replication and synchronization across multiple locations using Azure File Share and Azure File Sync.

Difficulty Level: Intermediate

Bloom's Taxonomy Level: Application- This involves applying the knowledge of Azure storage solutions to design a system that ensures data availability and accessibility across geographic locations.

200. An organization operates an on-premises file server named "cbflserver" running Windows Server 2019, managed by the Windows Admin Center. The company possesses an Azure subscription. To protect against data loss in the event of a failure of the file server, you propose an Azure solution. The plan involves creating an Azure Storage Account and configuring scheduled backups using Azure Table Storage. Does this solution fulfill the requirement?

- A) Yes
- B) No



Answer: B

Feedback(if correct):-

B) No, this solution does not fulfill the requirement. Azure Table Storage is not designed for backup and restore operations, unlike Azure Blob Storage. Azure Table Storage is a NoSQL key-value store suitable for storing semi-structured data and big tables. It does not natively support scheduled backups or point-in-time restore capabilities. Therefore, using Azure Table Storage for backups would not provide the necessary protections against data loss in the event of a server failure.

Feedback(if wrong):-

Utilizing Azure Table Storage for scheduled backups does not meet the requirement since Azure Table Storage is not optimized for backup and restore operations. Its core strength lies in handling massive amounts of structured NoSQL data, whereas Azure Blob Storage is particularly designed to store unstructured data like backups.

Feedback (if wrong):

Creating an Azure Storage Account and configuring scheduled backups using Azure Table Storage may not be the best solution to protect against data loss in the event of an observer failure. While Azure Table Storage is a NoSQL key-value store suitable for storing large quantities of semi-structured data, it is not the most optimal choice for backups.

Instead, you may consider the following solutions to fulfill the requirement:

1. Azure Backup: Create an Azure Recovery Services vault and install the Azure Backup agent on the on-premises file server. Schedule regular backups to protect data and enable quick recovery in case of a failure.
2. Azure Files: Replace the on-premises file server with Azure Files, which offers a fully managed file share service in Azure. Azure Files provides durable, highly available, and globally accessible file shares using the industry-standard Server Message Block (SMB) protocol.
3. Azure File Sync: Combine Azure Files with Azure File Sync, allowing you to centralize your file shares in Azure while keeping the flexibility, performance, and compatibility of a local file server. Azure File Sync transforms your Windows Servers into caches of your Azure file share, allowing you to use the server as a high-performance front-end to your data.

By considering these alternate approaches, you can ensure data protection, high availability, and performance while maintaining compatibility with existing systems and processes.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Architecting for Business Continuity and Disaster Recovery

- Competencies: Designing infrastructure solutions, Designing business continuity solutions
- Difficulty Level: Intermediate to Expert
- Bloom's Taxonomy Level: Analysis, Evaluation

201. An organization operates an on-premises file server named "cbflserver" running Windows Server 2019, managed by the Windows Admin Center. The company possesses an Azure subscription. To safeguard against data loss in the event of a failure of the file server, you propose an Azure solution. The plan involves creating an Azure Recovery Services vault, installing the Azure Backup agent, and scheduling backups. Does this solution fulfill the requirement?

- A) Yes
- B) No

Answer: A

Feedback(if correct):

The proposed solution of creating an Azure Recovery Services vault, installing the Azure Backup agent, and scheduling backups aligns with best practices for safeguarding against data loss in case of a file server failure. This approach ensures that backups are regularly taken and stored securely in Azure, providing a reliable mechanism for data recovery.

Feedback(if wrong):

This option would be incorrect because creating an Azure Recovery Services vault, installing the Azure Backup agent, and scheduling backups is a recommended approach for safeguarding against data loss in case of a file server failure.

Skill Mapping:

- Skills: Designing Microsoft Azure Infrastructure Solutions Certification AZ-305
- Subskills: Architecting for Business Continuity and Disaster Recovery
- Competencies: Designing infrastructure solutions, Designing business continuity solutions
- Difficulty Level: Intermediate to Expert
- Bloom's Taxonomy Level: Analysis, Evaluation

Done by Ahmed Fiuad . Nokhba Academy