**Question 1 of 50**

You manage an Azure App Service web app named **app1**. App1 is registered as an application in Microsoft Entra ID.

You need to ensure that Microsoft Entra ID signed-in user information can be retrieved by app1 by using Microsoft Graph.

What should you configure?

Select only one answer.

1. appRoles
2. application permissions
3. groupMembershipClaims
4. delegated permissions **This answer is correct.**

**Question 2 of 50**

You plan to use a shared access signature to protect access to services within a general-purpose v2 storage account.

You need to identify the type of service that you can protect by using the user delegation shared access signature.

Which service should you identify?

Select only one answer.

1. Blob T**his answer is correct.**
2. File
3. Queue
4. Table

**Notes:** This item tests the candidate’s knowledge of identifying the supported authorization method, which is the first step of implementing it.

The blob service is the only one that supports user delegation shared access signatures. The file service supports account and service shared access signatures. The queue service supports account and service shared access signatures. The table service supports account and service shared access signatures.

[Discover shared access signatures - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/implement-shared-access-signatures/2-shared-access-signatures-overview)

[Grant limited access to data with shared access signatures (SAS) - Azure Storage | Microsoft Learn](https://learn.microsoft.com/azure/storage/common/storage-sas-overview)

**Question 3 of 50**

You plan to use Microsoft Graph to retrieve a list of users in a Microsoft Entra ID tenant.

You need to optimize query results.

Which two query options should you use? Each correct answer presents part of the solution.

Select all answers that apply.

1. $filter **This answer is correct.**
2. $count
3. $orderby **This answer is incorrect.**
4. $select **This answer is incorrect.**
5. $expand

**Notes:** This item tests the candidate's knowledge of Microsoft Graph query options.

The $filter query option must be used to limit the results returned. The $select query option limits the attributes projected from the result set, making the query more efficient. The $count query option retrieves the total number of matching resources. The $expand query option retrieves related resources.

[Query Microsoft Graph by using REST - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/microsoft-graph/3-microsoft-graph-api)

[Paging Microsoft Graph data in your app - Microsoft Graph | Microsoft Learn](https://learn.microsoft.com/graph/paging)

**Question 4 of 50**

You manage a Microsoft Entra ID registered application named **app1**. App1 calls a web API, which then calls Microsoft Graph.

You need to ensure the signed-in user identity is delegated through the request chain.

Which authentication flow should you use?

Select only one answer.

1. Authorization code
2. On-Behalf-Of **This answer is correct.**
3. Client credentials
4. Implicit

**Notes:** This item tests the candidate’s knowledge of accessing user data from Microsoft Graph, which is part of implementing user authentication and authorization.

OAuth 2.0 On-Behalf-Of flow (OBO) is used when an application invokes a service or web API, which in turn needs to call another service or web API. The idea is to propagate the delegated user identity and permissions through the request chain. The OAuth 2.0 authorization code grant can be used in apps that are installed on a device to gain access to protected resources, such as web APIs. The OAuth 2.0 client credentials grant flow permits a web service (confidential client) to use its own credentials, instead of impersonating a user, to authenticate when calling another web service. Implicit is a redirection-based flow. The client must be capable of interacting with the resource owner's user-agent (typically a web browser). Authorization code, On-Behalf-Of, and implicit cannot be used to delegate user permission and identity.

[Implement authentication by using the Microsoft Authentication Library - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/implement-authentication-by-using-microsoft-authentication-library/)

[Microsoft identity platform and OAuth2.0 On-Behalf-Of flow - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/azure/active-directory/develop/v2-oauth2-on-behalf-of-flow)

[OAuth 2.0 client credentials flow on the Microsoft identity platform - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/azure/active-directory/develop/v2-oauth2-client-creds-grant-flow)

**Question 5 of 50**

You develop a multitenant web application named **App1**. You plan to register App1 with multiple Microsoft Entra ID tenants.

You need to identify the relationship between the application objects and security principals associated with App1.

Which relationship should you identify?

Select only one answer.

1. App1 will have multiple application objects and multiple service principals.
2. App1 will have multiple application objects and a single service principal.
3. App1 will have a single application object and multiple service principals.**This answer is correct.**
4. App1 will have a single application object and a single service principal.

**Notes:** This item tests the candidate’s knowledge of configuring authentication of multitenant applications, which is a common scenario when implementing authentication.

App1 will have a single application object and multiple service principals. App1 will not have multiple application objects. multiple application objects and a single service principal., or a single service principal.

[Explore service principals - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/explore-microsoft-identity-platform/3-app-service-principals)

[Apps & service principals in Azure AD - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/azure/active-directory/develop/app-objects-and-service-principals)

**Question 6 of 50**

You manage an Azure App Service Functions app named **app1** and a storage account named **account1**.

You have the following requirements:

* App1 should access account1 without managing credentials.
* The service principal associated with app1 cannot be explicitly deleted.

You need to configure a security principal for app1.

Which security principal should you use?

Select only one answer.

1. application
2. system-assigned managed identity T**his answer is correct.**
3. user-assigned managed identity
4. legacy

**Notes:** This item tests the candidate’s knowledge of implementing managed identities, which is part of implementing secure cloud solutions.

Managed identities for Azure resources eliminate the need to manage credentials in code. A system-assigned managed identity is restricted to one per resource and is tied to the lifecycle of the resource. Once enabled for app1, it will automatically create a service principal without the need to manage credentials and cannot be explicitly deleted.

A Microsoft Entra ID application is defined by its one and only application object, which resides in the Microsoft Entra ID tenant where the application was registered (known as the application's home tenant). It cannot be used by app1 to access a storage account without managing credentials. A user-assigned managed identity can be created and assigned to one or more instances of an Azure service. Once enabled for app1, a user-assigned managed identity will automatically create a service principal without the need to manage but will need to be explicitly deleted. The legacy service principal represents a legacy app, which is an app created before app registrations were introduced or an app created through legacy experiences. The legacy service principal cannot be used to access a storage account without managing credentials.

[Implement managed identities - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/implement-managed-identities/)

[Apps & service principals in Azure AD - Microsoft Entra | Microsoft Learn](https://learn.microsoft.com/azure/active-directory/develop/app-objects-and-service-principals)

**Question 7 of 50**

You have 10 applications running in Azure App Service.

You need to ensure the applications have access to items stored in Azure App Configuration by using a common configuration. Passwords or keys must not be used.

Which solution should you use?

Select only one answer.

1. system-assigned managed identities
2. user-assigned managed identity **This answer is correct.**
3. service principal with permissions to Azure App Configuration
4. developer's credentials in code

**Notes:** This item tests the candidate's knowledge of managed identities.

User-assigned managed identities are a way to reuse the permissions across applications. User-assigned managed identities associate the managed identity to the new applications, with no keys or passwords. System-assigned managed identities use a new identity for each application, which does not meet the common configuration requirement. A service principal has keys that need to be rotated. The developer does not run the application, so the developer’s identity cannot be assumed.

[Implement Azure App Configuration - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/implement-azure-app-configuration/)

[Managed identities - Azure App Service | Microsoft Learn](https://learn.microsoft.com/azure/app-service/overview-managed-identity?tabs=portal%2Chttp)

**Question 8 of 50**

You need to group keys in Azure App Configuration.

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

Select all answers that apply.

1. Use Azure role-based access control. Grant the Read permission to read keys that belong to the application.
2. Organize keys by using key prefixes. **This answer is correct.**
3. Use managed identity. Grant the Read permission to read keys that belong to the application.
4. Organize keys by using labels. **This answer is correct.**

**Notes:** This item tests the candidate’s knowledge of best practices when working with keys in Azure App Configuration.

Key prefixes are the beginning parts of keys. A set of keys can be grouped by using the same prefix in names. Labels are an attribute on keys. Labels are used to create variants of a key. For example, labels can be assigned to multiple versions of a key. Authorizing role-based access control to read Azure App Configuration is not a valid way to group keys. Authorizing a managed identity to read Azure App Configuration is not a valid way to group keys.

[Implement Azure App Configuration - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/implement-azure-app-configuration/)

[Azure App Configuration best practices | Microsoft Learn](https://learn.microsoft.com/azure/azure-app-configuration/howto-best-practices)

**Question 9 of 50**

You manage an Azure App Service web app named **app1** and an Azure Key Vault named **vault1**.

You need to ensure app1 can authenticate and conduct operations with vault1 without managing the rotation of a secret.

Which authentication method should you use for app1?

Select only one answer.

1. user-assigned managed identity
2. service principal and secret
3. service principal and certificate
4. system-assigned managed identity **This answer is correct.**

**Notes:** This item tests the candidate’s knowledge of implementing Azure Key Vault, which is part of implementing Secure Cloud solutions.

A system-assigned managed identity can be used to ensure app1 can authenticate and perform operations with vault1 without managing rotation of a secret. A user-assigned managed identity can be used to ensure app1 can authenticate and perform operations with vault1, but the secret rotation needs to be managed. A service principal and a secret can be used to authenticate to the key vault, but it is difficult to automatically rotate the secret that is used to authenticate to the key vault. A service principal and an associated certificate with access to the key vault can be used for authentication but would require managing the rotation of a secret.

[Implement Azure Key Vault - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/implement-azure-key-vault/)

[Azure Key Vault soft-delete | Microsoft Learn](https://learn.microsoft.com/azure/key-vault/general/soft-delete-overview)

[Assign an Azure Key Vault access policy (CLI) | Microsoft Learn](https://learn.microsoft.com/azure/key-vault/general/assign-access-policy?tabs=azure-portal)

**Question 10 of 50**

A company plans to use Azure App Configuration for feature flags in an application.

The company has the following encryption requirements:

* customer-managed keys
* hardware security module (HSM)-protected keys

You need to recommend service tiers.

Which two tiers should you recommend? Each correct answer presents part of the solution.

Select all answers that apply.

1. Azure App Configuration Free tier
2. Azure App Configuration Standard tier **This answer is correct.**
3. Azure Key Vault Standard tier
4. Azure Key Vault Premium tier **This answer is correct.**

**Notes:** This item tests the candidate’s knowledge of the service tiers for Azure App Configuration and Azure Key Vault.

App Configuration Standard tier must be used for customer-managed keys to be used in App Configuration. Key Vault Premium tier is required to support HSM-protected keys. App Configuration Free tier does not allow the use of customer-managed keys. Key Vault Standard tier does not support HSM-protected keys.

[Secure app configuration data - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/implement-azure-app-configuration/5-secure-app-configuration-data)

[Azure Managed HSM Overview - Azure Managed HSM | Microsoft Learn](https://learn.microsoft.com/azure/key-vault/managed-hsm/overview)

**Question 11 of 50**

You have an Azure Storage account container named **container1**.

You need to configure access to the container to meet the following requirements:

* The shared access signature (SAS) token should be secured with Microsoft Entra ID credentials.
* Role-based access control (RBAC) should be used.
* The SAS token should support granting access to containers.

Which type of SAS should you use?

Select only one answer.

1. account
2. user delegation**This answer is correct.**
3. service
4. stored access policy

This item tests the candidate’s knowledge of securing an Azure Storage account, which is part of developing solutions that use blob storage.

User delegation SAS fulfills all the requirements, including securing the SAS token with Microsoft Entra ID credentials, RBAC support, and granting access to containers. Azure Storage supports creating a new type of SAS at the level of the storage account. A service SAS delegates access to a resource in just one of the storage services (i.e., Blob, Queue, Table, or File). A stored access policy serves to group shared access signatures and to provide additional restrictions for signatures that are bound by the policy. The account, service, and stored access policy SAS types do not fulfill the requirement of securing the SAS token with Microsoft Entra ID credentials and RBAC support to manage permissions.

[Store application data with Azure Blob storage - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/store-app-data-with-azure-blob-storage/)

[Secure your Azure Storage account - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/secure-azure-storage-account/)

[Create a user delegation SAS - Azure Storage | Microsoft Learn](https://learn.microsoft.com/rest/api/storageservices/create-user-delegation-sas)

[Create an account SAS - Azure Storage | Microsoft Learn](https://learn.microsoft.com/rest/api/storageservices/create-account-sas)

[Create a service SAS - Azure Storage | Microsoft Learn](https://learn.microsoft.com/rest/api/storageservices/create-service-sas)

**Question 12 of 50**

You manage APIs in production by using Azure API Management.

You need to remove X-Powered-By and X-AspNet-Version headers from a response.

Which code segment should you use?

Select only one answer.

1. <policies> <inbound> <base /> </inbound> <backend> <base /> </backend> <outbound> <set-header name="X-Powered-By" exists-action="append" /> <set-header name="X-AspNet-Version" exists-action="append" /> <base /> </outbound> <on-error> <base /> </on-error> </policies>
2. <policies> <inbound> <base /> </inbound> <backend> <set-header name="X-Powered-By" exists-action="delete" /> <set-header name="X-AspNet-Version" exists-action="delete" /> <base /> </backend> <outbound> <base /> </outbound> <on-error> <base /> </on-error> </policies>
3. <policies> <inbound> <base /> </inbound> <backend> <base /> </backend> <outbound> <set-header name="X-Powered-By" exists-action="delete" /> <set-header name="X-AspNet-Version" exists-action="delete" /> <base /> </outbound> <on-error> <base /> </on-error> </policies> **This answer is correct.**
4. <policies> <inbound> <base /> </inbound> <backend> <set-header name="X-Powered-By" exists-action="append" /> <set-header name="X-AspNet-Version" exists-action="append" /> <base /> </backend> <outbound> <base /> </outbound> <on-error> <base /> </on-error> </policies>

**Note:** This item tests the candidate’s knowledge of defining policies for APIs using Azure API Management.

The code segment that includes the set-header policy element in the outbound section and exists-action="delete" will remove a header from the HTTP response. The code segment that includes the exists-action with append value will not remove the specified headers. The code segments that do not include the set-header policy element in the outbound section will not remove a header from the HTTP response.

[Introduction to Azure API Management - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/introduction-to-azure-api-management/)

[Azure API Management transformation policies | Microsoft Learn](https://learn.microsoft.com/azure/api-management/api-management-transformation-policies#example---removing-header)

**Question 13 of 50**

You manage an Azure event hub.

You need to ensure that multiple load-balanced instances of a .NET application (version 5.0) can be used to scale event processing.

Which event processor client should you use?

Select only one answer.

1. EventHubConsumerClient
2. EventProcessorHost
3. EventHubProducerClient
4. EventProcessorClient **This answer is correct.**

This item tests the candidate’s knowledge of scaling event processing applications, which is part of developing event-based solutions.

**Note:** EventProcessorClient balances the load between multiple instances of a program in newer .NET versions (version 5.0). EventHubConsumerClient balances the load between multiple instances of a program in Python and JavaScript. EventProcessorHost balances the load between multiple instances of a program in earlier .NET versions. The EventHubProducerClient class is used to send events to an event hub.

[Explore Azure Event Hubs - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/azure-event-hubs/)

[Scale your processing application - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/azure-event-hubs/4-event-processing)

[EventHubProducerClient class | Microsoft Learn](https://learn.microsoft.com/javascript/api/@azure/event-hubs/eventhubproducerclient?view=azure-node-latest)

**Question 14 of 50**

You plan to implement event routing in your Azure subscription by using Azure Event Grid. An event is generated each time an Azure resource is deleted. A message corresponding to the event is automatically displayed in an Azure App Service web app you deployed into the same Azure subscription.

You create a custom topic.

You need to subscribe to the custom topic.

What should you do first?

Select only one answer.

1. Create an endpoint.**This answer is correct.**
2. Create an event handler.
3. Enable the Azure Event Grid resource provider.
4. Configure filtering.

**Note:** This item tests the candidate’s knowledge of setting up Azure Event Grid subscriptions, which is an integral part of implementing solutions that use Azure Event Grid.

Before subscribing to the custom topic, you need to create an endpoint for event messages. The Azure App Service web app acts as the event handler in this case, so this task is already completed. The Azure Event Grid resource provider is already enabled at this point because this is a prerequisite for creating a custom topic. Event filtering is part of configuring an event subscription, so it takes place either during or after provisioning of the subscription.

[Exercise: Route custom events to web endpoint by using Azure CLI - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/azure-event-grid/8-event-grid-custom-events)

[Quickstart: Send custom events with Event Grid and Azure CLI - Azure Event Grid | Microsoft Learn](https://learn.microsoft.com/azure/event-grid/custom-event-quickstart)

**Question 15 of 50**

You develop the following code to read all published events for the first partition in Azure Event Hubs. (Line numbers are included for reference only.)

You need to complete the code.

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

Select all answers that apply.

1. Insert the following code segment at line 6: EventPosition startingPosition = EventPosition.Earliest; **This answer is correct.**
2. Insert the following code segment at line 6: EventPosition startingPosition = EventPosition.Latest;
3. Insert the following code segment at line 7: string partitionId = (await consumer.GetPartitionIdsAsync()).First(); **This answer is correct.**
4. Insert the following code segment at line 7: int partitionId = (await consumer.GetPartitionIdsAsync()).First();

**Note:** This item tests the candidate’s knowledge of reading events from Azure Event Hubs.

Inserting the code segment that includes startingPosition = EventPosition.Earliest at line 6 uses the earliest starting position, which is required to read all published events. Inserting the code segment that includes string partitionId = (await consumer.GetPartitionIdsAsync()).First(); at line 7 is required. The GetPartitionIdsAsync() method returns a string[]. The First() method will, therefore, return a string. The code segment at line 6 that uses startingPosition = EventPosition.Latest does not use the earliest starting position. The code segment at line 7 that includes int partitionId is incorrect because the GetPartitionIdsAsync() method returns a string[]. The First() method will, therefore, return a string, and not an int, as the return variable expects.

[Perform common operations with the Event Hubs client library - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/azure-event-hubs/6-event-hubs-programming-guide)

[EventHubProducerClient.GetPartitionIdsAsync(CancellationToken) Method (Azure.Messaging.EventHubs.Producer) - Azure for .NET Developers | Microsoft Learn](https://learn.microsoft.com/dotnet/api/azure.messaging.eventhubs.producer.eventhubproducerclient.getpartitionidsasync?view=azure-dotnet)

[EventPosition.Earliest Property (Azure.Messaging.EventHubs.Consumer) - Azure for .NET Developers | Microsoft Learn](https://learn.microsoft.com/dotnet/api/azure.messaging.eventhubs.consumer.eventposition.earliest?view=azure-dotnet)

**Question 16 of 50**

You have an Azure Service Bus instance.

You need to provide first-in, first-out (FIFO) guarantee for message processing.

What should you configure?

Select only one answer.

1. dead-letter queue
2. message deferral
3. message sessions **This answer is correct.**
4. scheduled delivery

**Notes:** This item tests the candidate’s knowledge of setting up FIFO guarantees in Azure Service Bus, which is a common task when implementing solutions by using Azure Service Bus.

To provide FIFO guarantees in Service Bus, sessions must be configured. Message sessions enable exclusive, ordered handling of unbounded sequences of related messages. A dead-letter queue holds messages that cannot be delivered to any receiver. Message deferral makes it possible to defer retrieval of a message until a later time. Scheduled delivery allows submitting messages to a queue or topic for delayed processing. A dead-letter queue, message deferral, and scheduled delivery do not provide FIFO guarantees.

[Explore Azure Service Bus - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/discover-azure-message-queue/3-azure-service-bus-overview)

[Azure Service Bus message sessions - Azure Service Bus | Microsoft Learn](https://learn.microsoft.com/azure/service-bus-messaging/message-sessions)

**Question 17 of 50**

You need to write a filter condition for an Azure Service Bus topic.

Which three filters can you use? Each correct answer presents a complete solution.

Select all answers that apply.

1. SQL **This answer is correct.**
2. Boolean **This answer is correct.**
3. Size
4. Correlation **This answer is correct.**
5. Content

This item tests the candidate’s knowledge of implementing solutions that use Azure Service Bus.

A SqlFilter holds a SQL-like conditional expression that is evaluated in the broker against the arriving message’s user-defined properties and system properties. The TrueFilter and FalseFilter either cause all arriving messages (true) or none of the arriving messages (false) to be selected for the subscription. A CorrelationFilter holds a set of conditions that are matched against one or more of an arriving message's user and system properties. Size Filter and Content are not valid options for Service Bus topic filtering.

[Implement message-based communication workflows with Azure Service Bus - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/implement-message-workflows-with-service-bus/)

[Azure Service Bus topic filters - Azure Service Bus | Microsoft Learn](https://learn.microsoft.com/azure/service-bus-messaging/topic-filters)

**Question 18 of 50**

You have an Azure Service Bus queue.

You need to ensure a publisher can send messages into a topic and multiple subscribers can become eligible to consume the messages.

Which message routing pattern should you use?

Select only one answer.

1. simple request/reply
2. multicast request/reply**This answer is correct.**
3. multiplexing
4. multiplexed request/reply

**Notes:** This item tests the candidate’s knowledge of message routing in Azure Service Bus, which is part of developing message-based solutions.

A publisher can send a message into a topic and multiple subscribers can become eligible to consume the message. A publisher can send a message into a queue and expect a reply from the message consumer, but multiple subscribers cannot consume the message. This session feature enables multiplexing of streams of related messages through a single queue but cannot be consumed by multiple subscribers. This session feature enables multiplexed replies, allowing several publishers to share a reply queue, but a message cannot be consumed by multiple subscribers.

[Explore Service Bus message payloads and serialization - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/discover-azure-message-queue/5-messages-payloads-serialization)

[Azure Service Bus messages, payloads, and serialization - Azure Service Bus | Microsoft Learn](https://learn.microsoft.com/azure/service-bus-messaging/service-bus-messages-payloads)

**Question 19 of 50**

You have an application that requires message queuing.

You need to recommend a solution that meets the following requirements:

* automatic duplicate message detection.
* ability to send 2 MB messages.

Which message queuing solution should you recommend?

Select only one answer.

1. Azure Service Bus Premium tier **This answer is correct.**
2. Azure Service Bus Standard tier
3. Azure Storage queues with locally redundant storage (LRS)
4. Azure Storage queues with zone-redundant storage (ZRS)

**Notes:** This item tests the candidate's knowledge of Azure Service Bus.

Service Bus detects duplicate messages. The Premium tier is required to send messages larger than 256 KB. Although Service Bus detects duplicate messages, the Standard tier only supports messages that are up to 256 KB in size. Azure Storage queues do not support duplicate message detection. Azure Storage queues do not support duplicate message detection.

[Explore Azure Service Bus - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/discover-azure-message-queue/3-azure-service-bus-overview)

[Compare Azure Storage queues and Service Bus queues - Azure Service Bus | Microsoft Learn](https://learn.microsoft.com/azure/service-bus-messaging/service-bus-azure-and-service-bus-queues-compared-contrasted)

**Question 20 of 50**

You manage a multiregion deployment of an Azure Cosmos DB account named **account1**.

You need to configure the default consistency level for account1. The consistency level must maximize throughput and minimize latency for write operations.

Which consistency level should you use?

Select only one answer.

1. bounded staleness
2. consistent prefix
3. eventual **This answer is correct.**
4. session

**Notes:** This item tests the candidate’s knowledge of selecting the consistency level, which is part of developing Azure Cosmos DB solutions.

The eventual consistency level maximizes throughput and minimizes latency. The bounded staleness consistency level provides lower throughput and higher latency comparing with the remaining answer choices. The consistent prefix consistency level provides higher throughput and lower latency for write operations than the session consistency level but lower throughput and higher latency than the eventual consistency levels. The session consistency level provides higher throughput and lower latency for write operations than the bounded staleness consistency level but lower throughput and higher latency than the eventual and consistent prefix consistency levels.

[Choose the right consistency level - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/explore-azure-cosmos-db/5-choose-cosmos-db-consistency-level)

[Consistency levels in Azure Cosmos DB | Microsoft Learn](https://learn.microsoft.com/azure/cosmos-db/consistency-levels)

**Question 21 of 50**

You have an application that writes data to Azure Cosmos DB.

The application must offer consistent prefix and monotonic reads.

You need to configure the consistency level.

Which consistency level should you use?

1. Select only one answer.
2. strong
3. bounded staleness
4. session **This answer is correct.**
5. eventual

**Notes:** This item tests the candidate's knowledge of Azure Cosmos DB consistency levels.

Session consistency offers all the guarantees listed. It provides write latencies, availability, and read throughput comparable to that of eventual consistency. It also provides the consistency guarantees that suit the needs of applications written to operate in the context of a user. Strong consistency has reads guaranteed to return the most recent committed version of an item. A client never sees an uncommitted or partial write. Users are guaranteed to read the latest committed write. It has the highest write latency and lowest read throughput of all consistency levels. In bounded staleness consistency, the reads are guaranteed to honor the consistent-prefix guarantee. It should be used when there is a need for low write latencies but require a total global order guarantee. In eventual consistency, there is no ordering guarantee for reads. In the absence of any further writes, the replicas eventually converge. It is the weakest form of consistency because a client may read values that are older than the ones it had read before. Eventual consistency is ideal when the application does not require any ordering guarantees.

[AZ-204: Develop solutions that use Azure Cosmos DB - Training | Microsoft Learn](https://learn.microsoft.com/training/paths/az-204-develop-solutions-that-use-azure-cosmos-db/)

[Consistency levels in Azure Cosmos DB | Microsoft Learn](https://learn.microsoft.com/azure/cosmos-db/consistency-levels)

**Question 22 of 50**

You have blobs in Azure Blob storage. The blobs store pictures.

You need to record the location and weather condition information from when the pictures were taken. You must ensure you can use up to 2,000 characters when recording the information.

What should you do?

Select only one answer.

1. Append a suffix to the blob name by using the location and weather. Add a delimiter between them.
2. Use metadata headers defined with a POST request.
3. Use metadata headers defined with a PUT request. **This answer is correct.**
4. Create one container for each location. Inside each container, define the blob name as the weather type and a random suffix.

**Notes:** This item tests the candidate's knowledge about structuring data for blob storage.

Metadata is the proper way to define this kind of data, allowing independent modification and supporting up to 8 KB in total size. The HTTP verb to define metadata is a PUT, and this is the correct format to define metadata values. The maximum size of a blob name is 1,024 characters. Also, this is not an optimal approach because metadata can be obtained and set independently, maintaining the same file name. Metadata is the proper way to define this kind of data, allowing independent modification and supporting up to 8 KB in total size. But the HTTP verb to define metadata is a PUT, not POST. The combination of locations and weather types can be potentially unlimited, and container names are limited to 63 characters.

[AZ-204: Develop solutions that use Blob storage - Training | Microsoft Learn](https://learn.microsoft.com/training/paths/develop-solutions-that-use-blob-storage/)

[Setting and retrieving properties and metadata for Blob service resources (REST API) - Azure Storage | Microsoft Learn](https://learn.microsoft.com/rest/api/storageservices/setting-and-retrieving-properties-and-metadata-for-blob-resources)

[Naming and Referencing Containers, Blobs, and Metadata - Azure Storage | Microsoft Learn](https://learn.microsoft.com/rest/api/storageservices/Naming-and-Referencing-Containers--Blobs--and-Metadata)

**Question 23 of 50**

You need to download blob content to a byte array after a transient fault happens.

Which code statement should you use?

Select only one answer.

1. byte[] data; BlobClient client = new BlobClient(new Uri("https://mystorageaccount.blob.core.windows.net/containers/blob.txt"), null); Response<BlobDownloadResult> response = client.DownloadContent(data);
2. BlobRequestOptions optionsWithRetryPolicy = new BlobRequestOptions(); byte[]destinationArray = blob.DownloadContent( index: 0, accessCondition: null, options: optionsWithRetryPolicy);
3. byte[] data; BlobClient client = new BlobClient(new Uri(“https://mystorageaccount.blob.core.windows.net/containers/blob.txt”), null); Response<BlobDownloadResult> response = client.DownloadContent(); data = response.Value.Content.ToArray();
4. byte[] data; BlobClientOptions options = new BlobClientOptions(); options.Retry.MaxRetries = 10; options.Retry.Delay = TimeSpan.FromSeconds(20); BlobClient client = new BlobClient(new Uri("https://mystorageaccount.blob.core.windows.net/containers/blob.txt"), options); Response<BlobDownloadResult> response = client.DownloadContent(); data = response.Value.Content.ToArray(); **This answer is correct.**

**Notes:** This item tests the candidate’s knowledge of implementing storage policies.

The code segment that includes options.Retry.MaxRetries = 10; and options.Retry.Delay = TimeSpan.FromSeconds(20); defines the retry strategy and downloads the content to the variable data. The code segments that do not include these parameters do not define the retry strategy.

[Microsoft Azure Fundamentals: Describe Azure architecture and services - Training | Microsoft Learn](https://learn.microsoft.com/training/paths/azure-fundamentals-describe-azure-architecture-services/)

[BlobBaseClient.DownloadContent Method (Azure.Storage.Blobs.Specialized) - Azure for .NET Developers | Microsoft Learn](https://learn.microsoft.com/dotnet/api/azure.storage.blobs.specialized.blobbaseclient.downloadcontent?view=azure-dotnet)

**Question 24 of 50**

You need to implement an Azure Storage lifecycle policy for append blobs.

Which rule action should you use?

Select only one answer.

1. Delete **This answer is correct.**
2. enableAutoTierToHotFromCool
3. tierToArchive
4. tierToCool

**Notes:** This item tests the candidate’s knowledge of configuring Azure Storage lifecycle policy for blobs, which is an essential part of developing solutions for blob storage.

The delete rule action supports both block blobs and append blobs. The enableAutoTierToHotFromCool, tierToArchive, and tierToCool rule actions only supports block blobs.  
[Discover Blob storage lifecycle policies - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/manage-azure-blob-storage-lifecycle/3-blob-storage-lifecycle-policies)

[Optimize costs by automatically managing the data lifecycle - Azure Storage | Microsoft Learn](https://learn.microsoft.com/azure/storage/blobs/lifecycle-management-overview)

**Question 25 of 50**

You need to rehydrate a blob stored in the Archive tier.

Which destination blob should you use?

Select only one answer.

1. A blob in the Archive tier in the same region.
2. A blob in the Archive tier in a different region.
3. A blob in the Cool tier in a different region.
4. A blob in the Cool tier in the same region. **This answer is correct.**

**Notes:** This item tests the candidate’s knowledge of rehydrating blobs.

Blobs in the Archive tier can be rehydrated only to online tiers (that is, Cool or Hot). The destination can be any storage account in the same region.

[Rehydrate blob data from the archive tier - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/manage-azure-blob-storage-lifecycle/5-rehydrate-blob-data)

[Blob rehydration from the Archive tier | Microsoft Learn](https://learn.microsoft.com/azure/storage/blobs/archive-rehydrate-overview)

**Question 26 of 50**

A company plans to host a static website that uses a custom domain and Azure Storage in multiple regions.

You need to serve website content and minimize latency.

What are two possible ways to achieve this goal? Each correct answer presents part of the solution.

Select all answers that apply.

1. Upload static content to a storage container named \*\*$web.\*\* **This answer is correct.**
2. Use Azure Traffic Manager to route users to the closest region.
3. Upload static content to a storage container named \*\*web.\*\*
4. Use Azure Content Delivery Network for regional caching. **This answer is correct.**

**Notes:** This item tests the candidate’s knowledge of developing solutions that use blob storage.

Static content needs to be uploaded to a storage container named $web. Using Azure Content Delivery Network is required for multiregional website hosting. Azure Traffic Manager is not recommended when using a custom domain because of how Azure Storage verifies custom domain names. The storage container needs to be named $web.

[Create a Content Delivery Network for your Website with Azure CDN and Blob Services - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/create-cdn-static-resources-blob-storage/)

[Static website hosting in Azure Storage | Microsoft Learn](https://learn.microsoft.com/azure/storage/blobs/storage-blob-static-website)

**Question 27 of 50**

A company implements a multi-region Azure Cosmos DB account.

You need to configure the default consistency level for the account. The consistency level must ensure that update operations made as a batch within a transaction are always visible together.

Which consistency level should you use?

Select only one answer.

1. Bounded Staleness
2. Session
3. Consistent Prefix **This answer is correct.**
4. Eventual

**Notes:** This item tests the candidate’s knowledge of selecting the appropriate consistency level for operations in Azure Cosmos DB. The Consistent Prefix consistency level ensures that updates made as a batch within a transaction are returned consistently with the transaction in which they were committed. Write operations within a transaction of multiple documents are always visible together. The Bounded Staleness consistency level is used to manage the lag of data between any two regions based on an updated version of an item or the time intervals between read and write. The Session consistency level is used to ensure that within a single client session, reads are guaranteed to honor the read-your-writes and write-follows-reads guarantees. The Eventual consistency level is used when no ordering guarantee is required.

[Explore consistency levels](https://learn.microsoft.com/training/modules/explore-azure-cosmos-db/4-cosmos-db-consistency-levels-overview)

[Consistency levels in Azure Cosmos DB](https://learn.microsoft.com/azure/cosmos-db/consistency-levels)

**Question 28 of 50**

You manage the deployment of an Azure Cosmos DB account.

You must define custom logic by using the .NET SDK change feed processor to process changes that the change feed reads.

You need to select the appropriate change feed processor component.

Which component should you use?

Select only one answer.

1. monitored container
2. delegate **This answer is correct.**
3. compute instance
4. lease container

**Notes:** This item tests the candidate’s knowledge of implementing change feed notifications in Azure Cosmos DB. The change feed processor in Azure Cosmos DB simplifies the process of reading the change feed and can be used to distribute the event processing across multiple consumers effectively. There are four main components in the change feed processor: the monitored container, the lease container, the compute instance, and the delegate. The monitored container has the data from which the change feed is generated. The delegate component can be used to define custom logic to process the changes that the change feed reads. The compute instance hosts the change feed processor to listen for changes. It can be represented by a VM, a Kubernetes pod, an Azure App Service instance, or an actual physical machine. The lease container acts as a state storage and coordinates the processing of the change feed across multiple workers.

[Understand change feed features in the SDK](https://learn.microsoft.com/training/modules/consume-azure-cosmos-db-sql-api-change-feed-use-sdk/2-understand-features-sdk)

[Change feed processor in Azure Cosmos DB](https://learn.microsoft.com/azure/cosmos-db/nosql/change-feed-processor?tabs=dotnet)

**Question 29 of 50**

You are planning to host a static website in an Azure Storage account.

The website must be accessible only through HTTPS by using a custom domain name.

You enable the static website hosting feature. You set the default page to index.html and the error page to error.html.

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

Select all answers that apply.

1. Set the access level of the web hosting container to public.
2. Add the custom domain under networking in the Azure Storage account.
3. Integrate the static website with Azure Content Delivery Network (CDN). **This answer is correct.**
4. Create a container named $web.
5. Upload the index.html and error.html files to the web hosting container. **This answer is correct.**

**Notes:** This item tests the candidate’s knowledge of implementing static website hosting. To host a static website in a storage account, the feature must be enabled. When enabling it, the names of the default and error documents must be informed. This creates a $web container, with private access, where the site files must be uploaded to. A custom domain can be added to the site. For HTTP only access, it can be registered to the networking tab of the storage account. For HTTPS access, Azure Content Delivery Network (CDN) must be used.

[Static website hosting in Azure Storage | Microsoft Learn](https://learn.microsoft.com/azure/storage/blobs/storage-blob-static-website)

[Host a static website in Azure Storage | Microsoft Learn](https://learn.microsoft.com/azure/storage/blobs/storage-blob-static-website-how-to?tabs=azure-cli)

**Question 30 of 50**

A company plans to use Azure Cache for Redis. The company plans to use Redis modules.

You need to recommend an Azure Cache for Redis service tier.

Which service tier should you recommend?

Select only one answer.

1. Basic
2. Standard
3. Premium
4. Enterprise **This answer is correct.**

**Notes:** This item tests the candidate's knowledge of Azure Cache for Redis service tiers.

Redis modules are only supported in the Enterprise service tier. The Basic, Standard, and Premium service tiers do not support Redis modules.

[Develop for Azure Cache for Redis - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/develop-for-azure-cache-for-redis/)

[Explore Azure Cache for Redis - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/develop-for-azure-cache-for-redis/2-azure-cache-redis-overview)

[What is Azure Cache for Redis? | Microsoft Learn](https://learn.microsoft.com/azure/azure-cache-for-redis/cache-overview)

**Question 31 of 50**

You need to set a duration of 10 seconds for a key stored in Azure Cache for Redis.

Which code segment should you use?

Select only one answer.

1. using (var cache = ConnectionMultiplexer.Connect("")) { IDatabase db = cache.GetDatabase(); bool setValue = await db.StringSetAsync("test:key", "10"); }
2. using (var cache = ConnectionMultiplexer.Connect("")) { IDatabase db = cache.GetDatabase(); bool setValue = await db.StringSetAsync("test:key", "10", TimeSpan.FromSeconds(10)); } **This answer is correct.**
3. using (var cache = ConnectionMultiplexer.Connect("")) { IDatabase db = cache.GetDatabase(); bool setValue = await db.StringSetAsync("test:key", "10", DateTime.UtcNow.AddSeconds(10)); }
4. using (var cache = ConnectionMultiplexer.Connect("")) { IDatabase db = cache.GetDatabase(); bool setValue = await db.StringSetAsync("test:key", "10", DateTime.Now.AddSeconds(10)); }

**Notes:** This item tests the candidate’s knowledge of implementing caching.

The code segment that includes TimeSpan.FromSeconds(10)); sets time to live of 10 seconds for a key. To set time to live for a key, the parameter ‘expiry’ (third parameter) of StringSet methods needs to be specified. The time to live parameter needs to be set as a TimeSpan, not a DateTime.

[Develop for Azure Cache for Redis - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/develop-for-azure-cache-for-redis/)

[Azure Redis Cache SDK for .NET - Azure for .NET Developers | Microsoft Learn](https://learn.microsoft.com/dotnet/api/overview/azure/redis-cache?view=azure-dotnet)

**Question 32 of 50**

You plan to use Azure Cache for Redis as the caching layer for several applications.

You have the following requirements:

* Prevent data loss if nodes are down.
* Minimize storage costs.
* Optimize performance.

Which solution should you use?

Select only one answer.

1. Redis database (RDB) persistence with the soft-delete feature enabled on the associated storage account.
2. Redis database (RDB) persistence with the soft-delete feature disabled on the associated storage account. **This answer is correct.**
3. Append only File (AOF) persistence with the soft-delete feature disabled on the associated storage account.
4. Append only File (AOF) persistence with the soft-delete feature enabled on the associated storage account.

This item tests the candidate's knowledge of data persistence in Azure Cache for Redis.

RDB persistence saves backups based on the configured backup interval with minimal effect on performance. Disabling the soft-delete feature on a storage account means Azure Cache for Redis can minimize storage costs by deleting the old backup data. Enabling the soft-delete feature on a storage account means Azure Cache for Redis cannot minimize storage costs by deleting the old backup data. AOF persistence saves every write to a log, which has a significant effect on throughput. Disabling and enabling the soft-delete feature on a storage account means Azure Cache for Redis cannot minimize storage costs by deleting the old backup data.

[Configure Azure Cache for Redis - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/develop-for-azure-cache-for-redis/3-configure-azure-cache-redis)

[Configure data persistence - Premium Azure Cache for Redis | Microsoft Learn](https://learn.microsoft.com/azure/azure-cache-for-redis/cache-how-to-premium-persistence)

**Question 33 of 50**

You have an Azure Cache for Redis instance.

You have the following requirements:

* Replica nodes must be hosted in different availability zones.
* Nonvolatile memory must be used.

You need to select a pricing tier.

Which pricing tier should you use?

Select only one answer.

1. Standard
2. Premium
3. Enterprise
4. Enterprise Flash **This answer is correct.**

**Notes:** This item tests the candidate’s knowledge of Azure Cache for Redis pricing, which is part of implementing caching for solutions.

The Enterprise Flash tier is capable of hosting replica nodes in different availability zones and uses nonvolatile memory to reduce cost. The Standard tier is not capable of hosting replica nodes in different availability zones. The Premium and Enterprise tiers are capable of hosting replica nodes in different availability zones but do not use nonvolatile memory to reduce cost.

[What is Azure Cache for Redis? - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/intro-to-azure-cache-for-redis/2-what-is-azure-cache-for-redis)

[Pricing - Azure Cache for Redis | Microsoft Azure](https://azure.microsoft.com/pricing/details/cache/)

**Question 34 of 50**

You deploy a .NET web application to an on-premises web server. You plan to use Application Insights to monitor the web application’s performance.

You need to allow the web application to upload its telemetry to Application Insights.

Which authorization method should you use?

Select only one answer.

1. access key
2. instrumentation key **This answer is correct.**
3. system-assigned managed identity
4. user-assigned managed identity

**Notes:** This item tests the candidate’s knowledge of configuring Application Insights authorization, which is an essential part of configuring an app or service to use Application Insights.

An instrumentation key uniquely designates an Application Insights resource and is the only piece of information required to provide authorized access for the purpose of uploading telemetry from monitored applications to Application Insights. Access keys are used by a variety of Azure resources, such as Azure Storage, but not Application Insights. Microsoft Entra ID system-assigned managed identities and Microsoft Entra ID user-assigned managed identities are not supported as an authorization mechanism by Application Insights.

[Explore Application Insights - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/monitor-app-performance/3-application-insights-overview)

[Create a new Azure Application Insights resource - Azure Monitor | Microsoft Learn](https://learn.microsoft.com/azure/azure-monitor/app/create-new-resource?tabs=net)

**Question 35 of 50**

You develop an Azure function that connects to a SQL database. The function is instrumented by using Application Insights.

You need to view the full SQL query text when inspecting the Dependency tab in Application Insights.

Which two settings in the host.json file should you use? Each correct answer presents part of the solution.

Select all answers that apply.

1. "enableDependencyTracking": true **This answer is correct.**
2. "dependencyTrackingOptions": { "enableSqlCommandTextInstrumentation": true }, **This answer is correct.**
3. "enablePerformanceCountersCollection": true
4. "logLevel": { "default": "Verbose" }

**Notes:** This item tests the candidate’s knowledge of tracking dependencies in Azure Functions instrumented with Application Insights.

Azure Functions requires setting "EnableDependencyTracking" to true in the host.json file. Azure Functions requires setting "enableSqlCommandTextInstrumentation" to true int he host.json file. The enablePerformanceCountersCollection setting is not related to enabling the full SQL query text in the Dependency tab in Application Insights. Changing the logLevel is not related to enabling the full SQL query text in the Dependency tab in Application Insights.

[Monitor app performance - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/monitor-app-performance/)

[Dependency tracking in Application Insights - Azure Monitor | Microsoft Learn](https://learn.microsoft.com/azure/azure-monitor/app/asp-net-dependencies#advanced-sql-tracking-to-get-full-sql-query)

**Question 36 of 50**

You need to track the availability of an Azure App Service web app by using an Application Insights multi-step availability test.

Which tool should you use?

Select only one answer.

1. Azure portal
2. Azure CLI
3. Visual Studio **This answer is correct.**
4. Visual Studio Code

**Notes:** This item tests the candidate’s knowledge of configuring multi-step tests, which is an essential part of implementing Application Insights web tests and alerts.

To create multi-step tests, Visual Studio is required, not Azure portal, Azure CLI, or Visual Studio Code.

[Select an availability test - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/monitor-app-performance/6-availability-tests)

[Monitor with multistep web tests - Application Insights - Azure Monitor | Microsoft Learn](https://learn.microsoft.com/azure/azure-monitor/app/availability-multistep)

**Question 37 of 50**

You plan to develop a web job that performs calculations on top of data that is collected from users.

You need to send pre-aggregated summary metrics to Azure Monitor.

Which Application Insights method should you use?

Select only one answer.

1. GetMetric **This answer is correct.**
2. TrackMetric
3. SetMetric
4. LogMetric

**Notes:** This item tests the candidate’s knowledge of using metrics and log data.

The GetMetric method handles local pre-aggregation and then only submits an aggregated summary metric at a fixed interval of one minute. TrackMetric sends raw telemetry, missing pre-aggregation. SetMetric and LogMetric are not valid methods to send pre-aggregated summary metrics to Azure Monitor.

[AZ-204: Instrument solutions to support monitoring and logging - Training | Microsoft Learn](https://learn.microsoft.com/training/paths/az-204-instrument-solutions-support-monitoring-logging/)

[Get-Metric in Azure Monitor Application Insights - Azure Monitor | Microsoft Learn](https://learn.microsoft.com/azure/azure-monitor/app/get-metric)

**Question 38 of 50**

You need to create a container in a container group and mount an Azure file share as volume.

Which code segment should you use?

Select only one answer.

1. az container create -g MyResourceGroup --name myapp --image myimage:latest --command-line "cat /mnt/azfile/myfile" --azure-file-volume-share-name myshare --azure-file-volume-account-name mystorageaccount --azure-file-volume-account-key mystoragekey --azure-file-volume-mount-path /mnt/azfile **This answer is correct.**
2. az container create -g MyResourceGroup --name myapp --image myimage:latest --command-line "cat /mnt/azfile/myfile" --azure-file-volume-share-name myshare --azure-file-volume-account-name mystorageaccount --azure-file-volume-account-key mystoragekey --secrets-mount-path /mnt/azfile
3. az container create -g MyResourceGroup –name myapp –image myimage:latest --command-line “cat /mnt/azfile/myfile” --azure-file-volume-account-name mystorageaccount --azure-file-volume-account-key mystoragekey --azure-file-volume-mount-path /mnt/azfile
4. az container create -g MyResourceGroup --name myapp --image myimage:latest --command-line "cat /mnt/azfile/myfile" --azure-file-volume-account-name mystorageaccount --azure-file-volume-account-key mystoragekey --secrets-mount-path /mnt/azfile

This item tests the candidate’s knowledge of running containers by using Azure Container Instances.

The code segment that includes the –azure-file-volume-mount-path parameter and the --azure-file-volume-share-name parameter creates a container in a container group and mounts an Azure file share as volume.

**Notes:** The code segments that include the --secrets-mount-path parameter will not mount an Azure file share as volume. The code segment that does not include the --azure-file-volume-share-name is invalid.

[Exercise - Use data volumes - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/run-docker-with-azure-container-instances/5-use-data-volumes)

[az container | Microsoft Learn](https://learn.microsoft.com/cli/azure/container?view=azure-cli-latest#az-container-create)

**Question 39 of 50**

You plan to develop an Azure App Service web app named **app1** by using a Windows custom container.

You need to load a TLS/SSL certificate in application code.

Which app setting should you configure?

Select only one answer.

1. WEBSITE\_LOAD\_CERTIFICATES **This answer is correct.**
2. WEBSITE\_ROOT\_CERTS\_PATH
3. WEBSITE\_CORS\_ALLOWED\_ORIGINS
4. WEBSITE\_AUTH\_TOKEN\_CONTAINER\_SASURL

**Notes**: This item tests the candidate’s knowledge of configuring app settings, which is part of creating Azure App Service Web Apps.

The WEBSITE\_LOAD\_CERTIFICATES app setting makes the specified certificates accessible to Windows or Linux custom containers as files. The WEBSITE\_ROOT\_CERTS\_PATH app setting is read-only and does not allow comma-separated thumbprint values to be mentioned to the certificates and then be loaded in the code. The WEBSITE\_AUTH\_TOKEN\_CONTAINER\_SASURL app setting is used to instruct the auth module to store and load all encrypted tokens to the specified blob storage container. This setting is used for Azure Storage and cannot be used to load certificates inside a Windows custom container.

[Configure web app settings - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/configure-web-app-settings/)

[Environment variables and app settings reference - Azure App Service | Microsoft Learn](https://learn.microsoft.com/azure/app-service/reference-app-settings?tabs=kudu%2Cdotnet)

[Use a TLS/SSL certificate in code - Azure App Service | Microsoft Learn](https://learn.microsoft.com/azure/app-service/configure-ssl-certificate-in-code)

**Question 40 of 50**

You manage an Azure App Service web app named **app1**. App1 uses a service plan based on the Basic pricing tier.

You need to create a deployment slot for app1.

What should you do first?

Select only one answer.

1. Scale out app1.
2. Scale up app1. **This answer is correct.**
3. Configure automated deployment of app1 with Azure DevOps.
4. Configure automated deployment of app1 with GitHub.

**Notes:** This item tests the candidate’s knowledge of creating deployment slots, which ties directly to the pricing tier used by Azure App Service web apps. This is configured as part of the Azure App Service web app creation.

Deployment slots require at a minimum the Standard pricing tier, so to supply support for app1, it is necessary to scale it up. Scaling out app1 provisions more instances of app1, but it does not provide the ability to create its deployment slot. Automated deployment of app1 with Azure DevOps or GitHub is not a prerequisite of support for deployment slots, but it commonly is the reason for implementing them.

[Examine Azure App Service - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/introduction-to-azure-app-service/2-azure-app-service)

[Deployment best practices - Azure App Service | Microsoft Learn](https://learn.microsoft.com/azure/app-service/deploy-best-practices)

**Question 41 of 50**

You create an Azure web app locally. The web app consists of a ZIP package.

You need to deploy the web app by using the Azure CLI. The deployment must reduce the likelihood of locked files.

What should you do?

Select only one answer.

1. Run az webapp deploy specifying –-clean true.
2. Run az webapp deploy specifying –-restart true.
3. Run az webapp deploy to a staging slot with auto swap on. **This answer is correct.**
4. Run az webapp deploy by using a high value for the --timeout parameter.

**Notes** This item tests the candidate's knowledge of deploying Azure Web Apps using the Azure CLI.

Using a production and staging slot with auto swap enabled reduces the likelihood of locked files. If –clean true is used, the target folder is cleaned, but this has no effect on the likelihood of locked files. It is good to restart the app after deployment. This, however, is the default behavior of a ZIP deployment and has no effect on the reduced likelihood of locked files during deployment. The --timeout parameter has no effect on the likelihood of locked files.

[Deploy to App Service - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/introduction-to-azure-app-service/4-deploy-code-to-app-service?ns-enrollment-type=learningpath&ns-enrollment-id=learn.wwl.create-azure-app-service-web-apps)

[Deploy files to App Service - Azure App Service | Microsoft Learn](https://learn.microsoft.com/azure/app-service/deploy-zip?tabs=cli)

**Question 42 of 50**

You manage the staging and production deployment slots of an Azure App Service web app named **app1**.

You need to ensure a connection string is not swapped when swapping is performed.

Which configuration should you use?

Select only one answer.

1. Deployment Center
2. Deployment slot setting **This answer is correct.**
3. Managed identity
4. Scale up

**Notes:** This item tests the candidate’s knowledge of deploying code to Azure App Service, which is part of creating Azure App Service Web Apps.

Marking a setting as a deployment slot setting keeps it sticky to that deployment slot. For example, an app setting marked as a deployment slot setting on app1 will always stick with app1 and will never move to app1/staging during a swap. The Deployment Center setting is used to configure continuous deployment and manual deployment. Managed identity provides an identity for applications to use when connecting to resources that support Microsoft Entra ID authentication. Scale up will ensure the web app is entitled to get CPU, memory, disk space, and extra features such as dedicated virtual machines, custom domains and certificates, staging slots, and autoscaling. Deployment Center, Managed Identity, and Scale up cannot be used to ensure a connecting string is not swapped when swapping is performed.

[Host a web application with Azure App Service - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/host-a-web-app-with-azure-app-service/)

[Set up staging environments - Azure App Service | Microsoft Learn](https://learn.microsoft.com/azure/app-service/deploy-staging-slots)

[Configure deployment credentials - Azure App Service | Microsoft Learn](https://learn.microsoft.com/azure/app-service/deploy-configure-credentials?tabs=cli)

**Question 43 of 50**

You manage a multi-instance deployment of an Azure App Service web app named **app1**.

You need to ensure a client application is routed to the same instance for the life of the session.

Which platform setting should you use?

Select only one answer.

1. WebSocket
2. Always on
3. HTTP version
4. ARR Affinity **This answer is correct.**

**Notes:** This item tests the candidate’s knowledge of configuring web app settings, which is part of creating Azure App Service Web Apps.

In a multi-instance deployment, the ARR Affinity setting ensures a client application is routed to the same instance for the life of the session. WebSocket is a standardized protocol that provides full-duplex communication. Always on keeps the app loaded even when there is no traffic. In HTTP/2, a persistent connection can be used to service multiple simultaneous requests. WebSocket, Always on, and HTTP version are not used to ensure a client application is routed to the same instance for the life of the session.

[Configure web app settings - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/configure-web-app-settings/)

[Announcing HTTP/2 support in Azure App Service | Azure Blog and Updates | Microsoft Azure](https://azure.microsoft.com/blog/announcing-http-2-support-in-azure-app-service/)

**Question 44 of 50**

You plan to create an Azure Functions app named **app1**.

You need to ensure that app1 will satisfy the following requirements:

* Supports automatic scaling.
* Has event-based scaling behavior.
* Provides a serverless pricing model.

Which hosting plan should you use?

Select only one answer.

1. App Service
2. App Service Environment
3. Consumption **This answer is correct.**
4. Functions Premium

**Notes:** This item tests the candidate’s knowledge of selecting the appropriate hosting plan, which is part of the implementation of Azure Functions.

The Consumption hosting plan satisfies all requirements. It supports autoscaling, has event-based scaling behavior, and provides a serverless pricing model. The App Service, App Service Environment, and Functions Premium hosting plans support autoscaling but does not provide the serverless pricing model. Its scaling behavior is not event based but performance based.

[Compare Azure Functions hosting options - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/explore-azure-functions/3-compare-azure-functions-hosting-options)

[Azure Functions scale and hosting | Microsoft Learn](https://learn.microsoft.com/azure/azure-functions/functions-scale)

**Question 45 of 50**

A company plans to implement a Microsoft Defender for Cloud solution.

The company has the following requirements:

* Notifies when DNS domains are not deleted when a new Azure Functions app is deleted.
* Use native alerting.
* Minimize costs.

You need to select a hosting plan.

Which hosting plan should you use?

Select only one answer.

1. Consumption
2. Basic **This answer is correct.**
3. Premium
4. Free

**Notes:** This item tests the candidate's knowledge about securing Azure Functions.

The Basic plan supports both custom domains and Microsoft Defender for Cloud, which can automatically alert on dangling DNS domains. The Consumption plan is incorrect because it does not support Microsoft Defender for Cloud. This can automatically alert on dangling DNS domains. The Premium plan supports custom domains and Microsoft Defender for Cloud, which can automatically alert on dangling DNS domains. This, however, is not the lowest cost option. The Free plan does not support custom domains, although it does support Microsoft Defender for Cloud, which can automatically alert on dangling DNS domains.

[AZ-204: Implement Azure Functions - Training | Microsoft Learn](https://learn.microsoft.com/training/paths/implement-azure-functions/)

[Microsoft Defender for App Service - the benefits and features | Microsoft Learn](https://learn.microsoft.com/azure/defender-for-cloud/defender-for-app-service-introduction)

[Securing Azure Functions | Microsoft Learn](https://learn.microsoft.com/azure/azure-functions/security-concepts?tabs=v4)

[App Service Pricing | Microsoft Azure](https://azure.microsoft.com/pricing/details/app-service/windows/)

**Question 46 of 50**

You have an Azure Key Vault named **MyVault**.

You need to use a key vault reference to access a secret named **MyConnection** from MyVault.

Which code segment should you use?

Select only one answer.

1. @Microsoft.KeyVault(Secret=MyConnection;VaultName=MyVault)
2. @Microsoft.KeyVault(SecretName=MyConnection;VaultName=MyVault) **This answer is correct.**
3. @Microsoft.KeyVault(Secret=MyConnection;Vault=MyVault)
4. @Microsoft.KeyVault(SecretName=MyConnection;Vault=MyVault)

**Notes:** This item tests the candidate’s knowledge of retrieving secrets from Key Vault in Azure Functions.

The code segment @Microsoft.KeyVault(SecretName=MyConnection;VaultName=MyVault) segment reads the secret from Key Vault. The code segment that includes Secret uses an invalid parameter. The code segment that includes Secret and Vault use invalid parameters. The code segment that includes SecretName and Vault use invalid parameters.

[Create serverless applications learning path - Training | Microsoft Learn](https://learn.microsoft.com/training/paths/create-serverless-applications/)

[Use Key Vault references - Azure App Service | Microsoft Learn](https://learn.microsoft.com/azure/app-service/app-service-key-vault-references?toc=%2Fazure%2Fazure-functions%2Ftoc.json&tabs=azure-cli#reference-syntax)

**Question 47 of 50**

You plan to create a C# script-based Azure Functions app.

You need to configure the trigger and bindings for the functions of the Azure Functions app.

What should you do?

Select only one answer.

1. Create a function.json file for each function. **This answer is correct.**
2. Create a host.json file for the Azure Functions app.
3. Decorate methods of each function with C# attributes.
4. Decorate parameters of each function with C# attributes.

**Notes:** This item tests the candidate’s knowledge of configuring triggers and bindings.

When using scripting languages, such as C# script, the function.json file for each function contains its triggers and bindings, and it needs to be explicitly created. The file host.json has runtime-specific configurations, not definitions of triggers and bindings. Decorating methods and Decorating parameters are used to define triggers and bindings when using compiled languages, not scripted ones.

[Create triggers and bindings - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/develop-azure-functions/3-create-triggers-bindings)

[Guidance for developing Azure Functions | Microsoft Learn](https://learn.microsoft.com/azure/azure-functions/functions-reference?tabs=blob)

**Question 48 of 50**

You create a batch routine by using a timer trigger in Azure Functions.

You need to configure the batch routine to execute every 15 minutes.

Which code segment should you use?

Select only one answer.

1. [FunctionName("TimerTriggerCSharp")] public static void Run([TimerTrigger("0 \*/15 \* \* \* 1-5")]TimerInfo myTimer, ILogger log) { if (myTimer.IsPastDue) { log.LogInformation("Timer is running late!"); } log.LogInformation($"C# Timer trigger function executed at: {DateTime.Now}"); } **This answer is correct.**
2. [FunctionName("TimerTriggerCSharp")] public static void Run([TimerTrigger("\*/15 \* \* \* 0-4")]TimerInfo myTimer, ILogger log) { if (myTimer.IsPastDue) { log.LogInformation("Timer is running late!"); } log.LogInformation($"C# Timer trigger function executed at: {DateTime.Now}"); }
3. [FunctionName("TimerTriggerCSharp")] public static void Run([TimerTrigger("0 15 \* \* \* ")]TimerInfo myTimer, ILogger log) { if (myTimer.IsPastDue) { log.LogInformation("Timer is running late!"); } log.LogInformation($"C# Timer trigger function executed at: {DateTime.Now}"); }
4. [FunctionName("TimerTriggerCSharp")] public static void Run([TimerTrigger("\* 15 \* \* 1-5")]TimerInfo myTimer, ILogger log) { if (myTimer.IsPastDue) { log.LogInformation("Timer is running late!"); } log.LogInformation($"C# Timer trigger function executed at: {DateTime.Now}"); }

**Notes:** This item tests the candidate’s knowledge of working with timer triggers in Azure Functions.

The code segment that includes Run([TimerTrigger("0 \*/15 \* \* \* 1-5") executes the function every 15 minutes from Monday to Friday. The code segment that includes Run([TimerTrigger("\*/15 \* \* \* 0-4") is missing the second part, and it is not using the proper range for days of the week. The code segment that includes Run([TimerTrigger("0 15 \* \* \* ") executes only once at 15:00 (3 PM). The code segment that includes Run([TimerTrigger("\* 15 \* \* 1-5") is missing the seconds attribute and the step (‘/’) part for the minutes.

[Execute an Azure Function with triggers - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/execute-azure-function-with-triggers/)

[Timer trigger fo r Azure Functions | Microsoft Learn](https://learn.microsoft.com/azure/azure-functions/functions-bindings-timer?tabs=in-process&pivots=programming-language-csharp#ncrontab-expressions)

**Question 49 of 50**

You are developing a .NET application that includes multiple container images. The application will be deployed to Azure Container Instances (ACI).

You need to ensure that an Azure file share can be mapped to each container of the application.

Which configuration should you use?

Select only one answer.

1. pods
2. confidential containers
3. container group **This answer is correct.**
4. virtual network deployment

**Notes:** This item tests the candidate’s knowledge of running containers by using Azure Container Instances (ACI). The top-level resource in ACI is the container group. A container group is a collection of containers that get scheduled on the same host machine. You can specify external volumes to mount within a container group. You can map these volumes into specific paths within the individual containers in a group. A pod is a group of one or more containers with shared storage and network resources and specification for how to run the containers. Pods can be used in the Azure Kubernetes Service but not ACI. Confidential containers on ACI are used to ensure hardware-based confidentiality. ACI enables deployment of container instances into an Azure virtual network. A virtual network deployment cannot be used to map an Azure file share to each container in a multiple container scenario.

[Explore Azure Container Instances](https://learn.microsoft.com/training/modules/create-run-container-images-azure-container-instances/2-azure-container-instances-overview)

[What is Azure Container Instances?](https://learn.microsoft.com/azure/container-instances/container-instances-overview)

**Question 50 of 50**

A company has an App Service web app that requires a TLS/SSL certificate. The certificate will be used in other App Service apps. The certificate must be automatically renewed with the least management overhead.

You need to add the certificate.

What should you do?

Select only one answer.

1. Create a free App Service managed certificate.
2. Purchase an App Service certificate. **This answer is correct.**
3. Upload a certificate from a third party.
4. Import a certificate from a Key Vault.

**Notes:** This item tests the candidate’s knowledge of configuring web app settings including SSL, API settings, and connection strings. Purchasing an App Service certificate automates the process of requesting, renewing, and synchronizing the certificate with the App Service apps that use them. Free App Service certificates offer basic functionalities and cannot be exported. Obtaining the certificate from a third party and uploading it to Azure App Service is also an option but lacks the automation and integration offered by the App Service certificates. It is recommended to store certificates in and retrieve them from a Key Vault, but if they are obtained from a third party, the renewal and synchronization with the App Service apps need to be automated in other ways.

[Configure security certificates - Training | Microsoft Learn](https://learn.microsoft.com/training/modules/configure-web-app-settings/6-configure-security-certificates)

[Get started with Key Vault certificates | Microsoft Learn](https://learn.microsoft.com/azure/key-vault/certificates/certificate-scenarios)