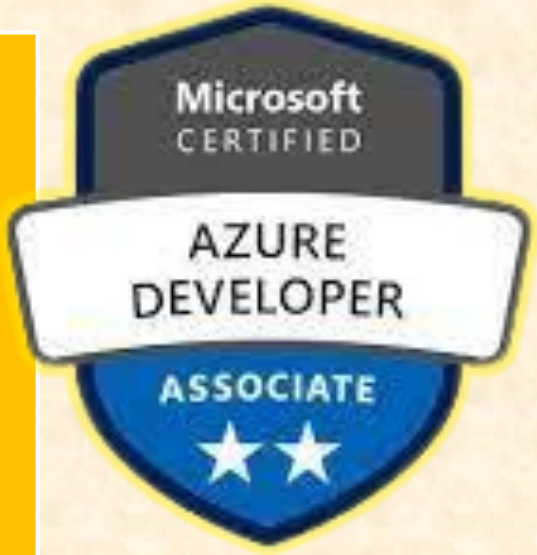
Clearcat.net
#Technology@Cloud

Latest Q&A

AZ-204 Exam

100

Questions & Answers



Best Practice Questions & Answers by 2023

AZ-204 Exam

Clearcat.net
#Technology@Cloud

100 Questions (Latest Version)

Other Suggested Azure Exam Dumps -

- **AZ-900 427 Questions PDF :** https://youtu.be/xafXsFbqvxU
- **AZ-104 368 Questions PDF:** https://youtu.be/DuwNgSuCtcc

Refer Video Description Section to Links for the same

You need to create a container in a container group and mount an Azure file share as volume.
Which code segment should you use?

- `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`
- `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`
- `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`
- `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`

Exam: AZ-204 Best Practice Questions 2023

You need to create a container in a container group and mount an Azure file share as volume.
Which code segment should you use?

- [x] `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`
- [ ] `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`
- [ ] `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`
- [ ] `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`

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.
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
az container | Microsoft Learn

You create an Azure Resource Manager (ARM) template.
You need to configure the template to generate a unique virtual machine name.
Which ARM template section should you use?

- parameters
- variables
- user-defined functions
- resources

You create an Azure Resource Manager (ARM) template.
You need to configure the template to generate a unique virtual machine name.
Which ARM template section should you use?

- ○ parameters
- ○ variables
- ○ user-defined functions
- ● resources

User-defined functions allow you to create functions for complicated expressions that are used repeatedly in the ARM template. Parameters provide values during deployment that allow the same template to be used with different environments. Variables are used to simplify a template, not to repeat complicated expressions throughout the template. A variable can be defined that contains the complicated expression. The resources section is used to deploy resources through an ARM template. Parameters, variables, and resources cannot be used to uniquely generate a unique name during a deployment.
Create and deploy Azure Resource Manager templates - Training | Microsoft Learn
User-defined functions in templates - Azure Resource Manager | Microsoft Learn
Declare resources in templates - Azure Resource Manager | Microsoft Learn

You plan to deploy five virtual machines (VMs) in Azure as part of an availability set.
You need to limit the impact of physical hardware failures, network outages, and power interruptions affecting the VMs.
Which solution should you use?

- Configure the VMs with five update domains.
- Configure the VMs with two fault domains.
- Configure the VMs with five fault domains.
- Configure the VMs with three update domains.

You plan to deploy five virtual machines (VMs) in Azure as part of an availability set.
You need to limit the impact of physical hardware failures, network outages, and power interruptions affecting the VMs.
Which solution should you use?

- ○ Configure the VMs with five update domains.
- ● Configure the VMs with two fault domains.
- ○ Configure the VMs with five fault domains.
- ○ Configure the VMs with three update domains.

Fault domains define the group of VMs that share a common power source and network switch, and there is a limit of three fault domains per availability set. Update domains indicate groups of VMs and underlying physical hardware that can be rebooted at the same time. Update domains do not protect from physical outages. There is a limit of 20 update domains per availability set.
Provision virtual machines in Azure - Training | Microsoft Learn
Availability sets overview - Azure Virtual Machines | Microsoft Learn

You plan to use the Azure CLI to deploy an Azure Resource Manager (ARM) template. The ARM template targets a resource group named **RG1**. RG1 has existing resources.
You need to ensure that the resources in the target resource group will be automatically deleted if they are not included in the template.
What should you use?

- the `--mode` parameter of the az deployment group `create` command
- the `--parameters` parameter of the az deployment group `create` command
- the `$schema` section of the template
- the `parameters` section of the template

You plan to use the Azure CLI to deploy an Azure Resource Manager (ARM) template. The ARM template targets a resource group named **RG1**. RG1 has existing resources.
You need to ensure that the resources in the target resource group will be automatically deleted if they are not included in the template.
What should you use?

- (●) the `--mode` parameter of the az deployment group `create` command
- ( ) the `--parameters` parameter of the az deployment group `create` command
- ( ) the `$schema` section of the template
- ( ) the `parameters` section of the template

The value of **the --mode parameter determines whether the deployment** is incremental or complete. The latter will result in deletion of resources that are not included in the template. The --parameters parameter allows for modifying the deployment behavior, but regardless of parameter values, will not result in deletion of existing resources. The $schema section controls the schema of the template, but regardless of its value, its modification will not result in deletion of existing resources. The parameters section allows for modifying the deployment behavior, but regardless of the parameter values, its modification will not result in deletion of existing resources.
Set the correct deployment mode - Training | Microsoft Learn
Deployment modes - Azure Resource Manager | Microsoft Learn

You develop a web application hosted on the Web Apps feature of Microsoft Azure App Service.

You need to enable and configure Azure Web Service Local Cache with 1.5 GB.

Which two code segments should you use? Each correct answer presents part of the solution.

- [ ] `"WEBSITE_LOCAL_CACHE_OPTION": "Always"`
- [ ] `"WEBSITE_LOCAL_CACHE_SIZEINMB": "1500"`
- [ ] `"WEBSITE_LOCAL_CACHE_OPTION": "Enable"`
- [ ] `"WEBSITE_LOCAL_CACHE_SIZEINMB": "1.5"`

You develop a web application hosted on the Web Apps feature of Microsoft Azure App Service.

You need to enable and configure Azure Web Service Local Cache with 1.5 GB.

Which two code segments should you use? Each correct answer presents part of the solution.

- [x] `"WEBSITE_LOCAL_CACHE_OPTION": "Always"`
- [x] `"WEBSITE_LOCAL_CACHE_SIZEINMB": "1500"`
- [ ] `"WEBSITE_LOCAL_CACHE_OPTION": "Enable"`
- [ ] `"WEBSITE_LOCAL_CACHE_SIZEINMB": "1.5"`

By using WEBSITE_LOCAL_CACHE_OPTION = Always, local cache will be enabled. WEBSITE_LOCAL_CACHE_SIZEINMB will properly configure Local Cache with 1.5 GB of size. WEBSITE_LOCAL_CACHE_OPTION = Enable is not a valid value. 1.5 will not configure 1.5 GB for the local cache.
Configure web app settings - Training | Microsoft Learn
Local cache - Azure App Service | Microsoft Learn

A company uses Azure App Service.
You need to secure the web app.
What are three possible ways to achieve this goal? Each correct answer presents a complete solution.

- [ ] Redirect HTTP to HTTPS.
- [ ] Use Microsoft Defender for App Service.
- [ ] Set the TLS version to 1.0.
- [ ] Secure application secrets.
- [ ] Install the latest version of an antivirus solution in Azure App Service.

A company uses Azure App Service.
You need to secure the web app.
What are three possible ways to achieve this goal? Each correct answer presents a complete solution.

- [x] Redirect HTTP to HTTPS.
- [x] Use Microsoft Defender for App Service.
- [ ] Set the TLS version to 1.0.
- [x] Secure application secrets.
- [ ] Install the latest version of an antivirus solution in Azure App Service.

This item tests the candidate's knowledge of following the best practices for Azure App Service.
Redirecting HTTPS uses the SSL/TLS protocol to provide a secure connection. **Defender** for Cloud assesses the resources covered by your App Service plan and generates security recommendations based on its findings. Application secrets must not be stored in application code or configuration files. **Azure App Service** apps use TLS 1.2. Newer versions of TLS include security improvements over older protocol versions, and version 1.0 is considered insecure. Installing an antivirus solution in Azure App Service is not allowed.
Configure web app settings - Training | Microsoft Learn
Security recommendations - Azure App Service | Microsoft Learn

You manage an Azure App Service web app named **app1**. App1 uses a service plan based on the Standard pricing tier.
You need to ensure app1 can host WebJobs that are triggered by using a CRON expression.
Which setting should you use?

- Always on
- ARR affinity
- Managed pipeline version
- WebSocket protocol

You manage an Azure App Service web app named **app1**. App1 uses a service plan based on the Standard pricing tier.
You need to ensure app1 can host WebJobs that are triggered by using a CRON expression.
Which setting should you use?

- (●) Always on
- ( ) ARR affinity
- ( ) Managed pipeline version
- ( ) WebSocket protocol

The **Always on** setting is required to support WebJobs that are triggered by using a CRON expression. The ARR affinity setting ensures that requests from a given client are routed to the same App Service web app instance for the duration of a session. The managed pipeline version setting allows choosing between the IIS and classic pipeline mode, with the latter intended for legacy apps. The WebSocket protocol setting provides the ability to implement Azure SignalR Service and socket.IO support. The ARR affinity, managed pipeline version, and WebSocket protocol settings has no relevance regarding support for WebJobs that are triggered by using a CRON expression.
Configure general settings - Training | Microsoft Learn
Run background tasks with WebJobs - Azure App Service | Microsoft Learn

You need to build a web app that meets the following requirements:

- Is hosted in Azure App Service.
- Restricts requests coming from users belonging to tenants other than the organization's own Azure Active Directory tenant.
- Keeps secrets external to the application.

Which three elements should you use? Each correct answer presents part of the solution.

- [ ] Service principal
- [ ] Managed identity
- [ ] Azure Key Vault
- [ ] Custom domain name
- [ ] Hybrid connection
- [ ] Virtual network integration

You need to build a web app that meets the following requirements:

- Is hosted in Azure App Service.
- Restricts requests coming from users belonging to tenants other than the organization's own Azure Active Directory tenant.
- Keeps secrets external to the application.

Which three elements should you use? Each correct answer presents part of the solution.

- [x] Service principal
- [x] Managed identity
- [x] Azure Key Vault
- [ ] Custom domain name
- [ ] Hybrid connection
- [ ] Virtual network integration

A **service principal** must establish the connection to the Microsoft identity provider. A **managed identity** needs to be associated with the web app and granted permission to the key vault. This is needed so it has access to the service principal secret used for the identity provider integration. **Azure Key Vault** is needed to keep the service principal secret external to the application. This will be referred to by a configuration setting in the app, with a reference to the key vault. A custom domain is not needed to fill the requirements. Virtual network integration is the access to the Azure Active Directory tenant. It is not done through the virtual network. This is needed when the function app accesses resources sitting inside a virtual network.

AZ-204: Create Azure App Service web apps - Training | Microsoft Learn

az webapp auth microsoft | Microsoft Learn

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?

- ○ WebSocket
- ○ Always on
- ○ HTTP version
- ○ ARR Affinity

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?

- ○ WebSocket
- ○ Always on
- ○ HTTP version
- ● ARR Affinity

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
Announcing HTTP/2 support in Azure App Service | Azure Blog and Updates | Microsoft Azure

You plan to create an Azure function 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?

- ◯ App Service
- ◯ App Service Environment
- ◯ Consumption
- ◯ Functions Premium

You plan to create an Azure function 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?

- ○ App Service
- ○ App Service Environment
- ● Consumption
- ○ Functions Premium

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
Azure Functions scale and hosting | Microsoft Learn

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 function app is deleted.
- Use native alerting.
- Minimize costs.

You need to select a hosting plan.

Which hosting plan should you use?

- Consumption
- Basic
- Premium
- Free

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 function app is deleted.
- Use native alerting.
- Minimize costs.

You need to select a hosting plan.

Which hosting plan should you use?

- ○ Consumption
- ● Basic
- ○ Premium
- ○ Free

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

Microsoft Defender for App Service - the benefits and features | Microsoft Learn

Securing Azure Functions | Microsoft Learn

App Service Pricing | Microsoft Azure

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?

- `@Microsoft.KeyVault(Secret=MyConnection;VaultName=MyVault)`
- `@Microsoft.KeyVault(SecretName=MyConnection;VaultName=MyVault)`
- `@Microsoft.KeyVault(Secret=MyConnection;Vault=MyVault)`
- `@Microsoft.KeyVault(SecretName=MyConnection;Vault=MyVault)`

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?

- `@Microsoft.KeyVault(Secret=MyConnection;VaultName=MyVault)`
- ● `@Microsoft.KeyVault(SecretName=MyConnection;VaultName=MyVault)`
- `@Microsoft.KeyVault(Secret=MyConnection;Vault=MyVault)`
- `@Microsoft.KeyVault(SecretName=MyConnection;Vault=MyVault)`

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

Use Key Vault references - Azure App Service | Microsoft Learn

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?

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

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?

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

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
Timer trigger fo r Azure Functions | Microsoft Learn

You manage an Azure App Service web app named **app1**. App1 is registered as an application in Azure Active Directory (Azure AD).

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

What should you configure?

- ◯ appRoles
- ◯ application permissions
- ◯ groupMembershipClaims
- ◯ delegated permissions

You manage an Azure App Service web app named **app1**. App1 is registered as an application in Azure Active Directory (Azure AD).

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

What should you configure?

- ○ appRoles
- ○ application permissions
- ○ groupMembershipClaims
- ● delegated permissions

Delegated permissions are used by apps that have a signed-in user present. For these apps, either the user or an administrator consents to the permissions that the app requests and the app can function as the signed-in user when making calls to Microsoft Graph. **appRoles** is an attribute in the application manifest of the registered application that specifies the collection of roles that an app may declare. These roles can be assigned to users, groups, or service principals. **Application permissions** are used by apps that run without a signed-in user present. For example, apps that run as background services or daemons. An administrator can only permit application permissions. **groupMembershipClaims** is an attribute in the application manifest of the registered application that configures the groups claim issued in a user or OAuth 2.0 access token that the app expects. AppRoles, application permissions, and groupMembershipClaims will not allow signed-in user information to be retrieved in the code.

Access User Data from Microsoft Graph - Training | Microsoft Learn
Understanding the Azure Active Directory app manifest - Microsoft Entra | Microsoft Learn
Authentication and authorization basics - Microsoft Graph | Microsoft Learn

You have an Azure Storage account.

You need to provide external users the ability to create and update blobs.

Which enum value of BlobSasPermissions should you use?

- Add
- Create
- Read
- Write

You have an Azure Storage account.

You need to provide external users the ability to create and update blobs.

Which enum value of BlobSasPermissions should you use?

- ○ Add
- ○ Create
- ○ Read
- ● Write

This item tests the candidate's knowledge of creating and implementing blobs.
The Write permission will allow users to create and update blobs. The Add permission is only applicable for append blobs. The Create permission only allows users to create blobs. It does not allow users to update blobs.
The Read permission does not allow users to create and update blobs.
Control access to Azure Storage with shared access signatures - Training | Microsoft Learn
Create a service SAS for a container or blob - Azure Storage | Microsoft Learn

You manage an Azure App Service web app named **app1**. App1 is registered as a multi-tenant application in an Azure Active Directory (Azure AD) tenant named **tenant1**.

You need to grant app1 the permission to access the Microsoft Graph API in tenant1.

Which service principal should you use?

- legacy
- system-assigned managed identity
- application
- user-assigned managed identity

You manage an Azure App Service web app named **app1**. App1 is registered as a multi-tenant application in an Azure Active Directory (Azure AD) tenant named **tenant1**.

You need to grant app1 the permission to access the Microsoft Graph API in tenant1.

Which service principal should you use?

- ○ legacy
- ○ system-assigned managed identity
- ● application
- ○ user-assigned managed identity

An **Azure AD application** is defined by its one and only application object, which resides in the Azure AD tenant where the application was registered (known as the application's home tenant). The application service principal is used to configure permission for app1 in tenant1 to access the Microsoft Graph API. The legacy service principal is a legacy app, which is an app created before app registrations were introduced or an app created through legacy experiences. Managed identities 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. Managed identities for Azure resources eliminate the need to manage credentials in code. A user-assigned managed identity can be created and assigned to one or more instances of an Azure service. The legacy, system-assigned managed identity, and user-assigned managed identity cannot be used to assign permission for app1 in tenant1 to access the Microsoft Graph API.

Explore the Microsoft identity platform - Training | Microsoft Learn
Explore service principals - Training | Microsoft Learn
Apps & service principals in Azure AD - Microsoft Entra | Microsoft Learn

You have blobs in an Azure storage account.
You need to implement a stored access policy that will apply to shared access signatures generated for the blobs.
To which type of storage resource should you associate the policy?

- ○ the storage account
- ○ the blob service of the storage account
- ○ the container that is hosting blobs
- ○ each individual blob

You have blobs in an Azure storage account.
You need to implement a stored access policy that will apply to shared access signatures generated for the blobs.
To which type of storage resource should you associate the policy?

- ○ the storage account
- ○ the blob service of the storage account
- ● the container that is hosting blobs
- ○ each individual blob

The container that is hosting blobs is used for associating the corresponding stored access policies. The storage account can be associated with shared access signatures keys but not stored access policies. The blob service of the storage account can be associated with shared access signatures keys but not stored access policies. Each individual blob can be associated with shared access signatures keys but not stored access policies.
Use stored access policies to delegate access to Azure Storage - Training | Microsoft Learn
Define a stored access policy - Azure Storage | Microsoft Learn

You develop an application. The application will be accessed by a supplier.

The supplier requires a shared access signature (SAS) to access Azure services in your company's subscription.

You need to secure the SAS.

Which three actions should you take? Each correct answer presents a complete solution.

- [ ] Always use HTTPS.
- [ ] Grant permission to multiple resources.
- [ ] Use Azure Monitor and Azure Storage logs to monitor the application.
- [ ] Define a stored access policy for a service SAS.
- [ ] Set a long expiration time.

You develop an application. The application will be accessed by a supplier.

The supplier requires a shared access signature (SAS) to access Azure services in your company's subscription.

You need to secure the SAS.

Which three actions should you take? Each correct answer presents a complete solution.

- [x] Always use HTTPS.
- [ ] Grant permission to multiple resources.
- [x] Use Azure Monitor and Azure Storage logs to monitor the application.
- [x] Define a stored access policy for a service SAS.
- [ ] Set a long expiration time.

The recommendation of **always using HTTPS** is valid and should be followed. **Azure Monitor and storage analytics logging** should be used to observe any spike in these types of authorization failures. **Stored access policies** will give the option to revoke permissions for a service SAS without having to regenerate the storage account keys. A security best practice is to provide a user with the minimum required privileges. It is best to use near-term expiration times on an ad-hoc SAS service or account SAS so that even if a SAS is compromised it is valid only for a short time.

Control access to Azure Storage with shared access signatures - Training | Microsoft Learn

Grant limited access to data with shared access signatures (SAS) - Azure Storage | Microsoft Learn

You manage an Azure Active Directory 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?

- ◯ Authorization code
- ◯ On-Behalf-Of
- ◯ Client credentials
- ◯ Implicit

You manage an Azure Active Directory 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?

- ○ Authorization code
- ● On-Behalf-Of
- ○ Client credentials
- ○ Implicit

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
Microsoft identity platform and OAuth2.0 On-Behalf-Of flow - Microsoft Entra | Microsoft LearnOAuth 2.0 client credentials flow on the Microsoft identity platform - Microsoft Entra | Microsoft Learn

You plan to generate a shared access signature (SAS) token for read access to a blob in a storage account.

You need to secure the token from being compromised.

What should you use?

- ◯ Primary account key
- ◯ Secondary account key
- ◯ Azure AD credentials assigned the Contributor role
- ◯ Azure AD credentials assigned the Reader role

You plan to generate a shared access signature (SAS) token for read access to a blob in a storage account.

You need to secure the token from being compromised.

What should you use?

- ○ Primary account key
- ○ Secondary account key
- ● Azure AD credentials assigned the Contributor role
- ○ Azure AD credentials assigned the Reader role

Azure AD credentials are required to generate the SAS token. The account used must have the Microsoft.Storage/storageAccounts/blobServices/generateUserDelegationKey permission, which is present in the following built-in roles: Contributor, Storage Account Contributor, Storage Blob Data Contributor, Storage Blob Data Owner, Storage Blob Data Reader, and Storage Blob Delegator. The account key can be used to generate the SAS token, but it can be more easily compromised.

Discover shared access signatures - Training | Microsoft Learn

Create a user delegation SAS - Azure Storage | Microsoft Learn

You need to generate a shared access signature token that grants the Read permission to a blob container.
Which code segment should you use?

```
BlobSasBuilder sasBuilder = new BlobSasBuilder() { BlobContainerName = containerClient.Name, Resource = "b" };
sasBuilder.ExpiresOn = DateTimeOffset.UtcNow.AddHours(1);
sasBuilder.SetPermissions(BlobContainerSasPermissions.Read); Uri sasUri =
containerClient.GenerateSasUri(sasBuilder);
```

```
BlobSasBuilder sasBuilder = new BlobSasBuilder() { BlobContainerName = containerClient.Name, Resource = "c" };
sasBuilder.ExpiresOn = DateTimeOffset.UtcNow.AddHours(1);
sasBuilder.SetPermissions(BlobContainerSasPermissions.Read); Uri sasUri =
containerClient.GenerateSasUri(sasBuilder);
```

```
BlobSasBuilder sasBuilder = new BlobSasBuilder() { BlobContainerName = containerClient.Name, Resource = “c” };
sasBuilder.ExpiresOn = DateTimeOffset.UtcNow.AddHours(1);
sasBuilder.SetPermissions(BlobContainerSasPermissions.Create); Uri sasUri =
containerClient.GenerateSasUri(sasBuilder);
```

```
BlobSasBuilder sasBuilder = new BlobSasBuilder() { BlobContainerName = containerClient.Name, Resource = "b" };
sasBuilder.ExpiresOn = DateTimeOffset.UtcNow.AddHours(1);
sasBuilder.SetPermissions(BlobContainerSasPermissions.Create); Uri sasUri =
containerClient.GenerateSasUri(sasBuilder);
```

You need to generate a shared access signature token that grants the Read permission to a blob container.
Which code segment should you use?

- `BlobSasBuilder sasBuilder = new BlobSasBuilder() { BlobContainerName = containerClient.Name, Resource = "b" }; sasBuilder.ExpiresOn = DateTimeOffset.UtcNow.AddHours(1); sasBuilder.SetPermissions(BlobContainerSasPermissions.Read); Uri sasUri = containerClient.GenerateSasUri(sasBuilder);`

- `BlobSasBuilder sasBuilder = new BlobSasBuilder() { BlobContainerName = containerClient.Name, Resource = "c" }; sasBuilder.ExpiresOn = DateTimeOffset.UtcNow.AddHours(1); sasBuilder.SetPermissions(BlobContainerSasPermissions.Read); Uri sasUri = containerClient.GenerateSasUri(sasBuilder);`

- `BlobSasBuilder sasBuilder = new BlobSasBuilder() { BlobContainerName = containerClient.Name, Resource = “c” }; sasBuilder.ExpiresOn = DateTimeOffset.UtcNow.AddHours(1); sasBuilder.SetPermissions(BlobContainerSasPermissions.Create); Uri sasUri = containerClient.GenerateSasUri(sasBuilder);`

- `BlobSasBuilder sasBuilder = new BlobSasBuilder() { BlobContainerName = containerClient.Name, Resource = "b" }; sasBuilder.ExpiresOn = DateTimeOffset.UtcNow.AddHours(1); sasBuilder.SetPermissions(BlobContainerSasPermissions.Create); Uri sasUri = containerClient.GenerateSasUri(sasBuilder);`

The code segment that includes **Resource = "c"** and **sasBuilder.SetPermissions(BlobContainerSasPermissions.Read)**; will generate the shared access signatures token that grants the Read permission to a blob container. The code segment that includes resource = ‘b’ will generate a shared access signatures token at the blob level. The code segments that include **sasBuilder.SetPermissions(BlobContainerSasPermissions.Create**); will generate a shared access signatures token with the Create permission at the blob level.

Store data in Azure learning path - Training | Microsoft Learn
Create a service SAS for a container or blob - Azure Storage | Microsoft Learn

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?

- ◯ system-assigned managed identities
- ◯ user-assigned managed identity
- ◯ service principal with permissions to Azure App Configuration
- ◯ developer's credentials in code

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?

- ○ system-assigned managed identities
- ● user-assigned managed identity
- ○ service principal with permissions to Azure App Configuration
- ○ developer's credentials in code

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
Managed identities - Azure App Service | Microsoft Learn

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.

- [ ] Use Azure role-based access control. Grant the Read permission to read keys that belong to the application.
- [ ] Organize keys by using key prefixes.
- [ ] Use managed identity. Grant the Read permission to read keys that belong to the application.
- [ ] Organize keys by using labels.

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.

- [ ] Use Azure role-based access control. Grant the Read permission to read keys that belong to the application.
- [x] Organize keys by using key prefixes.
- [ ] Use managed identity. Grant the Read permission to read keys that belong to the application.
- [x] Organize keys by using labels.

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

Azure App Configuration best practices | Microsoft Learn

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?

- ○ user-assigned managed identity
- ○ service principal and secret
- ○ service principal and certificate
- ○ system-assigned managed identity

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?

- ○ user-assigned managed identity
- ○ service principal and secret
- ○ service principal and certificate
- ● system-assigned managed identity

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
Azure Key Vault soft-delete | Microsoft Learn
Assign an Azure Key Vault access policy (CLI) | Microsoft Learn

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?

- `<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>`
- `<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>`
- `<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>`
- `<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>`

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?

- `<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>`
- `<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>`
- **(correct)** `<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>`
- `<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>`

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
Azure API Management transformation policies | Microsoft Learn

You manage an instance of Azure API Management. You define policies to multiple scopes.

You need to enforce a policy evaluation order.

What should you use?

- the `<base />` element
- the `<when />` element
- the `follow-redirects` attribute
- the `condition` attribute

You manage an instance of Azure API Management. You define policies to multiple scopes.

You need to enforce a policy evaluation order.

What should you use?

- (●) the `<base />` element
- ( ) the `<when />` element
- ( ) the `follow-redirects` attribute
- ( ) the `condition` attribute

The **<base />** element provides the ability to enforce policy evaluation order. The <when /> element is part of the choose policy and is evaluated in order of its appearance within the policy. The follow-redirects attribute is part of the forward request policy, so it does not have any impact on the policy evaluation order. The condition attribute is part of the retry policy, so it does not have any impact on the policy evaluation order.

Explore API Management policies - Training | Microsoft Learn

How to set or edit Azure API Management policies | Microsoft Learn

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?

- `EventHubConsumerClient`
- `EventProcessorHost`
- `EventHubProducerClient`
- `EventProcessorClient`

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?

- `EventHubConsumerClient`
- `EventProcessorHost`
- `EventHubProducerClient`
- `EventProcessorClient`

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
Scale your processing application - Training | Microsoft Learn
EventHubProducerClient class | Microsoft Learn

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?

- Create an endpoint.
- Create an event handler.
- Enable the Azure Event Grid resource provider.
- Configure filtering.

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?

- (●) Create an endpoint.
- ( ) Create an event handler.
- ( ) Enable the Azure Event Grid resource provider.
- ( ) Configure filtering.

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
Quickstart: Send custom events with Event Grid and Azure CLI - Azure Event Grid | Microsoft Learn

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.)

```
1  var connectionString = "<< CONNECTION STRING FOR THE EVENT HUBS NAMESPACE >>";
2  var eventHubName = "<< NAME OF THE EVENT HUB >>";
3  string consumerGroup = EventHubConsumerClient.DefaultConsumerGroupName;
4  await using (var consumer = new EventHubConsumerClient(consumerGroup, connectionString, eventHubName))
5  {
6
 7
8    using var cancellationSource = new CancellationTokenSource(); 9    cancellationSource.CancelAfter(TimeSpan.FromSeconds(45));
10   await foreach (PartitionEvent receivedEvent in consumer.ReadEventsFromPartitionAsync(partitionId,
11 . startingPosition, cancellationSource.Token))
12   {
 13    // At this point, the loop will wait for events to be available in the partition. When an event is available, the loop will iterate with the event that was
received.
14   }
16 }
```

You need to complete the code.
Which two actions should you perform? Each correct answer presents part of the solution.

- [ ] Insert the following code segment at line 6: `EventPosition startingPosition = EventPosition.Earliest;`
- [ ] Insert the following code segment at line 6: `EventPosition startingPosition = EventPosition.Latest;`
- [ ] Insert the following code segment at line 7: `string partitionId = (await consumer.GetPartitionIdsAsync()).First();`
- [ ] Insert the following code segment at line 7: `int partitionId = (await consumer.GetPartitionIdsAsync()).First();`

helpful for you.

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.)

```
1  var connectionString = "<< CONNECTION STRING FOR THE EVENT HUBS NAMESPACE >>";
2  var eventHubName = "<< NAME OF THE EVENT HUB >>
3  string consumerGroup = EventHubConsumerClient.Def
4  await using (var consumer = new EventHubConsumerC
5  {
6
 7
8    using var cancellationSource = new CancellationToker
10   await foreach (PartitionEvent receivedEvent in consu
11 . startingPosition, cancellationSource.Token))
12   {
 13    // At this point, the loop will wait for events to be a
received.
14   }
16 }
```

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
EventHubProducerClient.GetPartitionIdsAsync(CancellationToken) Method (Azure.Messaging.EventHubs.Producer) - Azure for .NET Developers | Microsoft Learn
EventPosition.Earliest Property (Azure.Messaging.EventHubs.Consumer) - Azure for .NET Developers | Microsoft Learn

You need to complete the code.
Which two actions should you perform? Each correct answer presents part of the solution.

- [x] Insert the following code segment at line 6: `EventPosition startingPosition = EventPosition.Earliest;`
- [ ] Insert the following code segment at line 6: `EventPosition startingPosition = EventPosition.Latest;`
- [x] Insert the following code segment at line 7: `string partitionId = (await consumer.GetPartitionIdsAsync()).First();`
- [ ] Insert the following code segment at line 7: `int partitionId = (await consumer.GetPartitionIdsAsync()).First();`

You need to capture events streaming from Azure Event Hubs.
To which three locations can you capture data? Each correct answer presents a complete solution.

- [ ] Azure Blob storage
- [ ] Azure Data Lake Storage Gen1
- [ ] Azure Functions
- [ ] Azure Stream Analytics
- [ ] Azure Data Lake Storage Gen2

You need to capture events streaming from Azure Event Hubs.
To which three locations can you capture data? Each correct answer presents a complete solution.

- [x] Azure Blob storage
- [x] Azure Data Lake Storage Gen1
- [ ] Azure Functions
- [ ] Azure Stream Analytics
- [x] Azure Data Lake Storage Gen2

Azure Event Hubs Capture can automatically deliver the streaming data in Event Hubs to **Azure Blob storage**. Azure Event Hubs Capture can automatically deliver the streaming data in Event Hubs to **Azure Data Lake Storage Gen1**. Azure Event Hubs Capture can automatically deliver the streaming data in Event Hubs to **Azure Data Lake Storage Gen2**. Azure Functions and Azure Stream Analytics cannot be used to capture events from Azure Event Hubs.
Introduction to Event Hubs - Training | Microsoft Learn
Event Hubs - Capture streaming events using Azure portal - Azure Event Hubs | Microsoft Learn

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?

- ○ simple request/reply
- ○ multicast request/reply
- ○ multiplexing
- ○ multiplexed request/reply

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?

- ○ simple request/reply
- ● multicast request/reply
- ○ multiplexing
- ○ multiplexed request/reply

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
Azure Service Bus messages, payloads, and serialization - Azure Service Bus | Microsoft Learn

You are developing a .NET project that will manage messages in Azure Storage queues.

You need to verify the presence of messages in a queue without removing them from the queue.

Which method should you use?

- `Peek`
- `PeekMessages`
- `ReceiveMessages`
- `ReceiveMessageAsync`

You are developing a .NET project that will manage messages in Azure Storage queues.

You need to verify the presence of messages in a queue without removing them from the queue.

Which method should you use?

- ○ `Peek`
- ● `PeekMessages`
- ○ `ReceiveMessages`
- ○ `ReceiveMessageAsync`

Messages can be **peek**ed at in the queue without removing them from the queue by calling the **PeekMessages** method of the QueueClient class. The Peek method of the QueueClient class is used with Azure Service Bus, not Azure Queue Storage. The **ReceiveMessages** method of the QueueClient class removes them from the queue. The **ReceiveMessageAsync** method of the QueueClient class is used with Azure Service Bus, not Azure Queue Storage.

Create and manage Azure Queue Storage and messages by using .NET - Training | Microsoft Learn
Get started with Azure Queue Storage using .NET - Azure Storage | Microsoft Learn

You need to sign a shared access signature (SAS) token with a key created by using Azure Active Directory (Azure AD) credentials.

Which type of SAS should you use?

- ○ user delegation
- ○ service
- ○ account
- ○ stored access policy

You need to sign a shared access signature (SAS) token with a key created by using Azure Active Directory (Azure AD) credentials.

Which type of SAS should you use?

- (●) user delegation
- ( ) service
- ( ) account
- ( ) stored access policy

A user delegation SAS is authenticated with Azure AD. A service SAS is authenticated using a shared key. An account SAS is authenticated using a shared key. A user delegation SAS must be used because it is the only one that is authenticated by using Azure AD credentials. Stored access policies are not supported with a user delegation SAS.

Implement shared access signatures - Training | Microsoft Learn

Grant limited access to data with shared access signatures (SAS) - Azure Storage | Microsoft Learn

You develop a multitenant web application named **App1**. You plan to register App1 with multiple Azure Active Directory (Azure AD) tenants.

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

Which relationship should you identify?

- ○ App1 will have multiple application objects and multiple service principals.
- ○ App1 will have multiple application objects and a single service principal.
- ○ App1 will have a single application object and multiple service principals.
- ○ App1 will have a single application object and a single service principal.

You develop a multitenant web application named **App1**. You plan to register App1 with multiple Azure Active Directory (Azure AD) tenants.

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

Which relationship should you identify?

- ○ App1 will have multiple application objects and multiple service principals.
- ○ App1 will have multiple application objects and a single service principal.
- ● App1 will have a single application object and multiple service principals.
- ○ App1 will have a single application object and a single service principal.

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
Apps & service principals in Azure AD - Microsoft Entra | Microsoft Learn

You plan to enable a user to create a managed identity for an Azure virtual machine (VM).

You need to ensure the following requirements are met:

•The user account must have sufficient permissions to create the managed identity.

•The principle of least privilege must be used.

Which permission role should you assign?

- ○ Virtual Machine Administrator Login
- ○ Virtual Machine Contributor
- ○ Global Administrator
- ○ Security Administrator

You plan to enable a user to create a managed identity for an Azure virtual machine (VM).

You need to ensure the following requirements are met:

•The user account must have sufficient permissions to create the managed identity.

•The principle of least privilege must be used.

Which permission role should you assign?

- ○ Virtual Machine Administrator Login
- ● Virtual Machine Contributor
- ○ Global Administrator
- ○ Security Administrator

Virtual Machine Contributor is the least privileged built-in role required to create a managed identity for an Azure VM. Virtual Machine Administrator Login is not sufficient to create a managed identity for an Azure VM. Global Administrator and Security Administrator have excessive permissions to Azure Active Directory, which does not follow the principle of least privilege. Global Administrator and Security Administrator do not provide sufficient permissions to the Azure resources.

Configure managed identities - Training | Microsoft Learn

Configure managed identities using the Azure portal - Azure AD - Microsoft Entra | Microsoft Learn

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?

- ○ system-assigned managed identities
- ○ user-assigned managed identity
- ○ service principal with permissions to Azure App Configuration
- ○ developer's credentials in code

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?

- ○ system-assigned managed identities
- ● user-assigned managed identity
- ○ service principal with permissions to Azure App Configuration
- ○ developer's credentials in code

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

Managed identities - Azure App Service | Microsoft Learn

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.

- [ ] Azure App Configuration Free tier
- [ ] Azure App Configuration Standard tier
- [ ] Azure Key Vault Standard tier
- [ ] Azure Key Vault Premium tier

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.

- [x] Azure App Configuration Free tier
- [ ] Azure App Configuration Standard tier
- [ ] Azure Key Vault Standard tier
- [x] Azure Key Vault Premium tier

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
Azure Managed HSM Overview - Azure Managed HSM | Microsoft Learn

You manage an Azure Key Vault named **vault1**.

You need to ensure that an accidental deletion of a secret can be automatically recovered for a period of 60 days.

Which setting should you configure?

- ○ access policy
- ○ purge
- ○ soft-delete
- ○ backup

You manage an Azure Key Vault named **vault1**.

You need to ensure that an accidental deletion of a secret can be automatically recovered for a period of 60 days.

Which setting should you configure?

- ○ access policy
- ○ purge
- ● soft-delete
- ○ backup

The Azure Key Vault **soft-delete** feature allows for the recovery of the deleted vaults and deleted key vault objects. If no configuration is specified, the default recovery period will be set to 90 days.
A key vault access policy determines whether a given security principal, namely a user, application, or user group, can perform different operations on key vault secrets, keys, and certificates. Purge is used to permanently delete a soft-deleted secret. Purge access policy permission is not granted by default to any service principal, including key vault and subscription owners, and must be deliberately set. An access policy and purge cannot configure the recovery of secret deletion. Backup creates regular backups of a key vault that are updated, deleted, and created within a vault, but the backups need to be configured manually.
Discover Azure Key Vault best practices - Training | Microsoft Learn
Azure Key Vault soft-delete | Microsoft Learn

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?

- Deployment Center
- Deployment slot setting
- Managed identity
- Scale up

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?

- ○ Deployment Center
- ● Deployment slot setting
- ○ Managed identity
- ○ Scale up

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 Azure Active Directory 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
Set up staging environments - Azure App Service | Microsoft Learn
Configure deployment credentials - Azure App Service | Microsoft Learn

You need to configure a web app to allow external requests from https://myapps.com.

Which Azure CLI command should you use?

- `az webapp cors add -g MyResourceGroup -n MyWebApp --allowed-origins https://myapps.com`
- `az webapp identity add -g MyResourceGroup -n MyWebApp --allowed-origins https://myapps.com`
- `az webapp traffic-routing set --distribution myapps=100 --name MyWebApp --resource-group MyResourceGroup`
- `az webapp config access-restriction add -g MyResourceGroup -n MyWebApp --rule-name external --action Allow -ids myapps --priority 200`

You need to configure a web app to allow external requests from https://myapps.com.

Which Azure CLI command should you use?

- ● `az webapp cors add -g MyResourceGroup -n MyWebApp --allowed-origins https://myapps.com`
- ○ `az webapp identity add -g MyResourceGroup -n MyWebApp --allowed-origins https://myapps.com`
- ○ `az webapp traffic-routing set --distribution myapps=100 --name MyWebApp --resource-group MyResourceGroup`
- ○ `az webapp config access-restriction add -g MyResourceGroup -n MyWebApp --rule-name external --action Allow -ids myapps --priority 200`

The code segment that includes the **cors** add will configure CORS to allow requests from https://myapps.com. The code segment that includes identity add will add a managed identity to a web app. The code segment that includes traffic-routing-set will configure a traffic routing to a deployment slot named **myapps**. The code segment that includes access-restriction add will add an access restriction on a web app.
Control Azure services with the CLI - Training | Microsoft Learn
az webapp config access-restriction | Microsoft Learn

You plan to create a durable function named **app1** by using C#.

You need to define the order in which actions are executed.

Which function should you use?

- ○ activity
- ○ entity
- ○ orchestrator
- ○ client

You plan to create a durable function named **app1** by using C#.

You need to define the order in which actions are executed.

Which function should you use?

- ○ activity
- ○ entity
- ● orchestrator
- ○ client

Orchestrator functions describe how actions are executed and the order in which actions are executed. Orchestrator functions describe the orchestration in code (e.g., C#, Python, or JavaScript). Activity functions are the basic unit of work in a durable function orchestration. Entity functions define operations for reading and updating small pieces of state. Client functions are non-orchestrator functions. Activity, entity, and client functions cannot be used to define the execution order of actions.

Create a long-running serverless workflow with Durable Functions - Training | Microsoft Learn

Function types in Azure Durable Functions | Microsoft Learn

You plan to use Azure API Management for Hybrid and multicloud API management.

You need to create a self-hosted gateway for production.

Which container image tag should you use?

- `2.0.1`
- `v3`
- `latest`
- `V3-preview`

You plan to use Azure API Management for Hybrid and multicloud API management.

You need to create a self-hosted gateway for production.

Which container image tag should you use?

- [x] `2.0.1`
- [ ] `v3`
- [ ] `latest`
- [ ] `V3-preview`

In production, the version must be pinned. The only way to achieve that is by using a tag that follows the convention {major}.{minor}.{patch}. The v3 tag will result in always running a major version with every new feature and patch. The latest tag is used for evaluating the self-hosted gateway. The V3-preview tag should be used to run the latest preview container image.
Explore API Management - Training | Microsoft Learn
Self-hosted gateway overview | Microsoft Learn

You have an Azure event hub.
You need to add partitions to the event hub.
Which code segment should you use?

- `az eventhubs eventhub consumer-group update --resource-group MyResourceGroupName --namespace-name MyNamespaceName --eventhub-name MyEventHubName --set partitioncount=12`
- `az eventhubs eventhub consumer-group create --resource-group MyResourceGroupName --namespace-name MyNamespaceName --eventhub-name MyEventHubName --set partitioncount=12`
- `az eventhubs eventhub update --resource-group MyResourceGroupName --namespace-name MyNamespaceName --name MyEventHubName --partition-count 12`
- `az eventhubs eventhub create --resource-group MyResourceGroupName --namespace-name MyNamespaceName --name MyEventHubName --partition-count 12`

You have an Azure event hub.
You need to add partitions to the event hub.
Which code segment should you use?

- `az eventhubs eventhub consumer-group update --resource-group MyResourceGroupName --namespace-name MyNamespaceName --eventhub-name MyEventHubName --set partitioncount=12`
- `az eventhubs eventhub consumer-group create --resource-group MyResourceGroupName --namespace-name MyNamespaceName --eventhub-name MyEventHubName --set partitioncount=12`
- ● `az eventhubs eventhub update --resource-group MyResourceGroupName --namespace-name MyNamespaceName --name MyEventHubName --partition-count 12`
- `az eventhubs eventhub create --resource-group MyResourceGroupName --namespace-name MyNamespaceName --name MyEventHubName --partition-count 12`

The code segment that includes az eventhubs eventhub update adds partitions to an existing event hub. The code segment that includes az eventhubs eventhub consumer-group update updates the event hub consumer group. The code segment that includes az eventhubs eventhub consumer-group create will create an event hub consumer group. The code segment that includes az eventhubs eventhub create --resource-group segment will create an event hub with partitions, not change an existing one
Control Azure services with the CLI - Training | Microsoft Learn
az eventhubs eventhub | Microsoft Learn

You have an Azure Service Bus instance.

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

What should you configure?

- dead-letter queue
- message deferral
- message sessions
- scheduled delivery

You have an Azure Service Bus instance.

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

What should you configure?

- ○ dead-letter queue
- ○ message deferral
- ● message sessions
- ○ scheduled delivery

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

Azure Service Bus message sessions - Azure Service Bus | Microsoft Learn

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.

- [ ] SQL
- [ ] Boolean
- [ ] Size
- [ ] Correlation
- [ ] Content

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.

- [x] SQL
- [x] Boolean
- [ ] Size
- [x] Correlation
- [ ] Content

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
Azure Service Bus topic filters - Azure Service Bus | Microsoft Learn

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

Which rule action should you use?

- delete
- enableAutoTierToHotFromCool
- tierToArchive
- tierToCool

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

Which rule action should you use?

- [x] delete
- [ ] enableAutoTierToHotFromCool
- [ ] tierToArchive
- [ ] tierToCool

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
Optimize costs by automatically managing the data lifecycle - Azure Storage | Microsoft Learn

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?

- ○ access key
- ○ instrumentation key
- ○ system-assigned managed identity
- ○ user-assigned managed identity

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?

- ○ access key
- ● instrumentation key
- ○ system-assigned managed identity
- ○ user-assigned managed identity

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. Azure Active Directory system-assigned managed identities and Azure Active Directory user-assigned managed identities are not supported as an authorization mechanism by Application Insights.
Explore Application Insights - Training | Microsoft Learn
Create a new Azure Application Insights resource - Azure Monitor | Microsoft Learn

A company uses Application Insights to instrument an application hosted in Azure App Service.

Instrumentation data that is collected by using API calls in the code is not available in Application Insights.

You need to ensure the collected data is available in Application Insights.

What should you do?

- ◯ Enable auto-instrumentation.
- ◯ Enable manual instrumentation.
- ◯ Verify the health of Application Insights.
- ◯ Verify the health of Azure App Service.

A company uses Application Insights to instrument an application hosted in Azure App Service.

Instrumentation data that is collected by using API calls in the code is not available in Application Insights.

You need to ensure the collected data is available in Application Insights.

What should you do?

- ○ Enable auto-instrumentation.
- ● Enable manual instrumentation.
- ○ Verify the health of Application Insights.
- ○ Verify the health of Azure App Service.

Manual instrumentation must be enabled to emit telemetry using API calls. Because some data is being collected, Application Insights is available. Because the application is running, Azure App Service is available.
Instrument an app for monitoring - Training | Microsoft Learn
Monitor Azure App Service performance - Azure Monitor | Microsoft Learn

You need to capture user actions by using the Azure Application Insights API.

Which API call should you use?

- `TrackEvent`
- `TrackMetric`
- `TrackRequest`
- `TrackTrace`

You need to capture user actions by using the Azure Application Insights API.

Which API call should you use?

- (●) `TrackEvent`
- ( ) `TrackMetric`
- ( ) `TrackRequest`
- ( ) `TrackTrace`

The `TrackEvent` API call tracks user actions and other events. It is used to track user behavior or to monitor performance. The `TrackMetric` API call is used to track performance measurements such as queue length. The `TrackRequest` API call is used to log the frequency and duration of server requests for performance analysis. The `TrackTrace` API call is used to capture Resource Diagnostic log messages and can also be used to capture third-party logs.
Instrument an app for monitoring - Training | Microsoft Learn
Application Insights API for custom events and metrics - Azure Monitor | Microsoft Learn

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?

- `GetMetric`
- `TrackMetric`
- `SetMetric`
- `LogMetric`

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?

- (●) `GetMetric`
- ( ) `TrackMetric`
- ( ) `SetMetric`
- ( ) `LogMetric`

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
Get-Metric in Azure Monitor Application Insights - Azure Monitor | Microsoft Learn

You plan to use Application Insights to monitor the performance of an on-premises web application.

You need to identify a configuration that satisfies the following requirements:

- Minimize the volume of data ingested into Application Insights.
- Maximize the accuracy of the collected metrics.

What should you do?

- ◯ Apply sampling.
- ◯ Apply filtering.
- ◯ Use log-based metrics.
- ◯ Use standard metrics.

You plan to use Application Insights to monitor the performance of an on-premises web application.

You need to identify a configuration that satisfies the following requirements:

- Minimize the volume of data ingested into Application Insights.
- Maximize the accuracy of the collected metrics.

What should you do?

- ○ Apply sampling.
- ○ Apply filtering.
- ○ Use log-based metrics.
- ● Use standard metrics.

Using **standard metrics** both minimizes the volume of data ingested into Application Insights and maximizes the accuracy of the collected metrics. Applying sampling and filtering would negatively affect the accuracy of the collected metrics. Using log-based metrics does not minimize the volume of data ingested into Application Insights.
Discover log-based metrics - Training | Microsoft Learn
Log-based and pre-aggregated metrics in Application Insights - Azure Monitor | Microsoft Learn

You need to generate a new version of a key stored in Azure Key Vault.

Which code segment should you use?

- `az keyvault key rotation-policy update -n mykey --vault-name mykeyvault --value path/to/policy.json`
- `az keyvault key purge --name mykey --vault-name mykeyvault`
- `az keyvault key rotate --vault-name mykeyvault --name mykey`
- `az keyvault key set-attributes --vault-name mykeyvault --name mykey -policy path/to/policy.json`

You need to generate a new version of a key stored in Azure Key Vault.

Which code segment should you use?

- `az keyvault key rotation-policy update -n mykey --vault-name mykeyvault --value path/to/policy.json`
- `az keyvault key purge --name mykey --vault-name mykeyvault`
- ● `az keyvault key rotate --vault-name mykeyvault --name mykey`
- `az keyvault key set-attributes --vault-name mykeyvault --name mykey -policy path/to/policy.json`

The **Rotate** operation will generate a new version of the key based on the key policy. The **Rotation Policy** operation updates the rotation policy of a key vault key. The **Purge** Deleted Key operation is applicable for soft-delete enabled vaults or HSMs. The Set Attributes operation changes specified attributes of a stored key.
Control Azure services with the CLI - Training | Microsoft Learn
az keyvault key | Microsoft Learn

You manage an Azure Key Vault named **vault1**.

You need to ensure that an accidental deletion of a secret can be automatically recovered for a period of 60 days.

Which setting should you configure?

- ○ access policy
- ◯ purge
- ◯ soft-delete
- ○ backup

You manage an Azure Key Vault named **vault1**.

You need to ensure that an accidental deletion of a secret can be automatically recovered for a period of 60 days.

Which setting should you configure?

- ○ access policy
- ○ purge
- ● soft-delete
- ○ backup

The Azure Key Vault **soft-delete** feature allows for the recovery of the deleted vaults and deleted key vault objects. If no configuration is specified, the default recovery period will be set to 90 days.
A key vault **access policy** determines whether a given security principal, namely a user, application, or user group, can perform different operations on key vault secrets, keys, and certificates. **Purge** is used to permanently delete a soft-deleted secret. Purge access policy permission is not granted by default to any service principal, including key vault and subscription owners, and must be deliberately set. An access policy and purge cannot configure the recovery of secret deletion. **Backup** creates regular backups of a key vault that are updated, deleted, and created within a vault, but the backups need to be configured manually.
Discover Azure Key Vault best practices - Training | Microsoft Learn
Azure Key Vault soft-delete | Microsoft Learn

You have an Azure App Configuration instance named **AppConfig1** and an Azure key vault named **KeyVault1**.

You plan to encrypt data stored in AppConfig1 by using your own key stored in KeyVault1.

You need to grant permissions in KeyVault1 to the identity assigned to AppConfig1.

Which three key-specific permissions should you use? Each correct answer presents part of the solution.

- [ ] DECRYPT
- [ ] ENCRYPT
- [ ] GET
- [ ] UNWRAP
- [ ] WRAP

You have an Azure App Configuration instance named **AppConfig1** and an Azure key vault named **KeyVault1**.

You plan to encrypt data stored in AppConfig1 by using your own key stored in KeyVault1.

You need to grant permissions in KeyVault1 to the identity assigned to AppConfig1.

Which three key-specific permissions should you use? Each correct answer presents part of the solution.

- [ ] DECRYPT
- [ ] ENCRYPT
- [x] GET
- [x] UNWRAP
- [x] WRAP

To use the custom key stored in KeyVault1, the identity assigned to AppConfig1 needs to have **GET**, **WRAP**, and **UNWRAP** permissions to the custom key. The DECRYPT and ENCRYPT permissions are not required to use the custom key stored in KeyVault1 in this scenario.
Secure app configuration data - Training | Microsoft Learn
Use customer-managed keys to encrypt your configuration data | Microsoft Learn

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?

- bounded staleness
- consistent prefix
- eventual
- session

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?

- ○ bounded staleness
- ○ consistent prefix
- ● eventual
- ○ session

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
Consistency levels in Azure Cosmos DB | Microsoft Learn

You create a new application. The application uses an Azure Cosmos DB database.

You need to ensure the application can use new Azure Cosmos DB features as soon as they are released.

Which API should you use?

- ○ Azure Cosmos DB for NoSQL API
- ○ Azure Cosmos DB for Apache Cassandra API
- ○ Azure Cosmos DB for MongoDB API
- ○ Azure Cosmos DB for Apache Gremlin API

You create a new application. The application uses an Azure Cosmos DB database.

You need to ensure the application can use new Azure Cosmos DB features as soon as they are released.

Which API should you use?

- [x] Azure Cosmos DB for NoSQL API
- [ ] Azure Cosmos DB for Apache Cassandra API
- [ ] Azure Cosmos DB for MongoDB API
- [ ] Azure Cosmos DB for Apache Gremlin API

Core (SQL) API offers the best end-to-end experience, with any new feature that is rolled out to Azure Cosmos DB becoming first available on SQL API accounts. Cassandra API should be used when there is a need to leverage Cassandra ecosystem skills and tools, while still taking advantage of the fully managed Azure Cosmos DB service. MongoDB API should be used when there is a need to leverage MongoDB ecosystem skills and tools, while still taking advantage of the fully managed Azure Cosmos DB service. **Gremlin API** should be used when there is a need to leverage Gremlin ecosystem skills and tools, with graph traversal query usage, while still taking advantage of the fully managed Azure Cosmos DB service.

AZ-204: Develop solutions that use Azure Cosmos DB - Training | Microsoft Learn

Choose an API in Azure Cosmos DB | Microsoft Learn

You need to read an Azure Cosmos DB change feed by using a reactive model.

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

- [ ] Azure Functions with an Azure Cosmos DB trigger
- [ ] Change feed processor library
- [ ] Azure Functions with an Azure Event Grid trigger
- [ ] Change feed pull model

You need to read an Azure Cosmos DB change feed by using a reactive model.

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

- [x] Azure Functions with an Azure Cosmos DB trigger
- [x] Change feed processor library
- [ ] Azure Functions with an Azure Event Grid trigger
- [ ] Change feed pull model

Azure Functions with an Azure Cosmos DB trigger allows you to select the container to connect, and the Azure Function is triggered whenever there is a change in the container. The change feed processor library follows the observer pattern, where the processing function is called by the library. The change feed processor library will automatically check for changes and, if changes are found, push them to the client. Azure Functions with an Event Grid trigger will execute the function when an Event Grid event is dispatched. It has no relationship with an Azure Cosmos DB change feed. A change feed pull model will use a pull model rather than a push model.
Consume an Azure Cosmos DB for NoSQL change feed using the SDK - Training | Microsoft Learn

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?

- ○ strong
- ○ bounded staleness
- ○ session
- ○ eventual

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?

- ○ strong
- ○ bounded staleness
- ● session
- ○ eventual

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
Consistency levels in Azure Cosmos DB | Microsoft Learn

A company has a blob in the Archive access tier.

You need to rehydrate the blob to an online tier.

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

- [ ] Copy the blob to a new blob in the Hot or Cool tier with the Copy Blob operation.
- [ ] Change the blob's tier using the Set Blob Properties operation.
- [ ] Change the blob's tier using the Set Blob Tier operation.
- [ ] Copy the blob to a new blob in the Hot or Cool tier with the Snapshot Blob operation.

A company has a blob in the Archive access tier.

You need to rehydrate the blob to an online tier.

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

- [x] Copy the blob to a new blob in the Hot or Cool tier with the Copy Blob operation.
- [ ] Change the blob's tier using the Set Blob Properties operation.
- [x] Change the blob's tier using the Set Blob Tier operation.
- [ ] Copy the blob to a new blob in the Hot or Cool tier with the Snapshot Blob operation.

The Copy Blob operation copies a blob to an online tier. The Set Blob Tier operation sets the access tier on a blob. The Set Blob Properties operation sets system properties on the blob. The Snapshot Blob operation creates a read-only snapshot of a blob.

Explore Azure Storage services - Training | Microsoft Learn

Blob rehydration from the Archive tier | Microsoft Learn

You have an Azure Storage account named **account1**.

You need to configure the storage account to meet the following requirements:

- Data should be copied to a secondary region.
- Data should be copied across multiple Azure availability zones in the primary region.
- Cost should be minimized.

Which Azure Storage redundancy solution should you use?

- ○ geo-zone-redundant storage (GZRS)
- ○ geo-redundant storage (GRS)
- ○ zone-redundant storage (ZRS)
- ○ read-access geo-redundant storage (RA-ZRS)

You have an Azure Storage account named **account1**.

You need to configure the storage account to meet the following requirements:

- Data should be copied to a secondary region.
- Data should be copied across multiple Azure availability zones in the primary region.
- Cost should be minimized.

Which Azure Storage redundancy solution should you use?

- ○ geo-zone-redundant storage (GZRS)
- ○ geo-redundant storage (GRS)
- ○ zone-redundant storage (ZRS)
- ○ read-access geo-redundant storage (RA-ZRS)

GZRS copies data synchronously across three Azure availability zones in the primary region using zone-redundant storage. It then copies data asynchronously to a single physical location in the secondary region. **GRS** copies data synchronously three times within a single physical location in the primary region using locally redundant storage. It then copies data asynchronously to a single physical location in a secondary region. **ZRS** replicates storage account data synchronously across three Azure availability zones in the primary region. **GZRS** copies data synchronously across three Azure availability zones in the primary region using zone-redundant storage. For read access to the secondary region, enable read-access geo-redundant storage (RA-GRS) or read-access geo-zone-redundant storage (RA-GZRS).
Create an Azure Storage account - Training | Microsoft Learn
Data redundancy - Azure Storage | Microsoft Learn

A company uses Azure Container Instances for an application.

You need to ensure that the containers are restarted when the process terminates with a nonzero exit code.

What should you do?

- ◯ Define a container restart policy of `Always`.
- ◯ Run the containers using a managed identity.
- ◯ Define a container restart policy of `Never`.
- ◯ Run an init container.

A company uses Azure Container Instances for an application.

You need to ensure that the containers are restarted when the process terminates with a nonzero exit code.

What should you do?

- [x] Define a container restart policy of `Always`.
- [ ] Run the containers using a managed identity.
- [ ] Define a container restart policy of `Never`.
- [ ] Run an init container.

Containers in the container group are always restarted with an **Always** policy in effect, regardless of their exit code. **Running containers using a managed identity** would simplify the access to external Azure resources but doing so has no effect on when a container restarts. When the processes in the container fail (terminating with a nonzero exit code), they will not restart and will only run once at most. Init containers are meant to perform initialization logic for app containers, running to completion before the application containers start.
Run container images in Azure Container Instances - Training | Microsoft Learn
Restart policy for run-once tasks - Azure Container Instances | Microsoft Learn

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?

- ◯ `WEBSITE_LOAD_CERTIFICATES`
- ◯ `WEBSITE_ROOT_CERTS_PATH`
- ◯ `WEBSITE_CORS_ALLOWED_ORIGINS`
- ◯ `WEBSITE_AUTH_TOKEN_CONTAINER_SASURL`

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?

- ● `WEBSITE_LOAD_CERTIFICATES`
- ○ `WEBSITE_ROOT_CERTS_PATH`
- ○ `WEBSITE_CORS_ALLOWED_ORIGINS`
- ○ `WEBSITE_AUTH_TOKEN_CONTAINER_SASURL`

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
Environment variables and app settings reference - Azure App Service | Microsoft Learn
Use a TLS/SSL certificate in code - Azure App Service | Microsoft Learn

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?

- ◯ Run `az webapp deploy` specifying `--clean true`.
- ◯ Run `az webapp deploy` specifying `--restart true`.
- ◯ Run `az webapp deploy` to a staging slot with auto swap on.
- ◯ Run `az webapp deploy` by using a high value for the `--timeout` parameter.

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?

- ○ Run `az webapp deploy` specifying `--clean true`.
- ○ Run `az webapp deploy` specifying `--restart true`.
- ● Run `az webapp deploy` to a staging slot with auto swap on.
- ○ Run `az webapp deploy` by using a high value for the `--timeout` parameter.

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

Deploy files to App Service - Azure App Service | Microsoft Learn

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

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

What should you do?

- ○ Create a function.json file for each function.
- ○ Create a host.json file for the function app.
- ○ Decorate methods of each function with C# attributes.
- ○ Decorate parameters of each function with C# attributes.

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

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

What should you do?

- [x] Create a function.json file for each function.
- [ ] Create a host.json file for the function app.
- [ ] Decorate methods of each function with C# attributes.
- [ ] Decorate parameters of each function with C# attributes.

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
Guidance for developing Azure Functions | Microsoft Learn

You create an Azure Service Bus topic with a default message time to live of 10 minutes.

You need to send messages to this topic with a time to live of 15 minutes. The solution must not affect other applications that are using the topic.

What should you recommend?

- ◯ Change the topic's default time to live to 15 minutes.
- ◯ Change the specific message's time to live to 15 minutes.
- ◯ Create a new topic with a default time to live of 15 minutes. Send the messages to this topic.
- ◯ Update the time to live for the queue containing the topic.

You create an Azure Service Bus topic with a default message time to live of 10 minutes.

You need to send messages to this topic with a time to live of 15 minutes. The solution must not affect other applications that are using the topic.

What should you recommend?

- ○ Change the topic's default time to live to 15 minutes.
- ○ Change the specific message's time to live to 15 minutes.
- ● Create a new topic with a default time to live of 15 minutes. Send the messages to this topic.
- ○ Update the time to live for the queue containing the topic.

To avoid affecting existing applications, the time to live of the existing topic must not be changed. A new topic needs to be created. Changing the topic's default time to live will affect other applications. A message-level time to live cannot be higher than the topic's time to live. To avoid affecting existing applications, the time to live of the existing topic or queue must not be changed.
Exercise: Send and receive message from a Service Bus queue by using .NET. - Training | Microsoft Learn

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?

- ◯ Azure Service Bus Premium tier
- ◯ Azure Service Bus Standard tier
- ◯ Azure Storage queues with locally redundant storage (LRS)
- ◯ Azure Storage queues with zone-redundant storage (ZRS)

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?

- (●) Azure Service Bus Premium tier
- ( ) Azure Service Bus Standard tier
- ( ) Azure Storage queues with locally redundant storage (LRS)
- ( ) Azure Storage queues with zone-redundant storage (ZRS)

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

You plan to create a key namespace hierarchy in Azure App Configuration.

You need to separate individual key names.

Which character should you use?

- ◯ :
- ◯ *
- ◯ ,
- ◯ \

You plan to create a key namespace hierarchy in Azure App Configuration.

You need to separate individual key names.

Which character should you use?

- [x] :
- [ ] *
- [ ] ,
- [ ] \

The colon character **(:)** is used to separate names of individual keys when creating a namespace hierarchy in Azure App Configuration. The asterisk character **(*)** is one of reserved characters in Azure App Configuration, so it cannot be used to separate names of individual keys when creating a namespace hierarchy in Azure App Configuration. The comma character **(,)** is one of reserved characters in Azure App Configuration, so it cannot be used to separate names of individual keys when creating a namespace hierarchy in Azure App Configuration. The backslash character **(\)** is one of reserved characters in Azure App Configuration, so it cannot be used to separate names of individual keys when creating a namespace hierarchy in Azure App Configuration.

Create paired keys and values - Training | Microsoft Learn

Understand Azure App Configuration key-value store | Microsoft Learn

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

Which code segment should you use?

- `using (var cache = ConnectionMultiplexer.Connect("")) { IDatabase db = cache.GetDatabase(); bool setValue = await db.StringSetAsync("test:key", "10"); }`
- `using (var cache = ConnectionMultiplexer.Connect("")) { IDatabase db = cache.GetDatabase(); bool setValue = await db.StringSetAsync("test:key", "10", TimeSpan.FromSeconds(10)); }`
- `using (var cache = ConnectionMultiplexer.Connect("")) { IDatabase db = cache.GetDatabase(); bool setValue = await db.StringSetAsync("test:key", "10", DateTime.UtcNow.AddSeconds(10)); }`
- `using (var cache = ConnectionMultiplexer.Connect("")) { IDatabase db = cache.GetDatabase(); bool setValue = await db.StringSetAsync("test:key", "10", DateTime.Now.AddSeconds(10)); }`

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

Which code segment should you use?

- `using (var cache = ConnectionMultiplexer.Connect("")) { IDatabase db = cache.GetDatabase(); bool setValue = await db.StringSetAsync("test:key", "10"); }`
- **`using (var cache = ConnectionMultiplexer.Connect("")) { IDatabase db = cache.GetDatabase(); bool setValue = await db.StringSetAsync("test:key", "10", TimeSpan.FromSeconds(10)); }`**
- `using (var cache = ConnectionMultiplexer.Connect("")) { IDatabase db = cache.GetDatabase(); bool setValue = await db.StringSetAsync("test:key", "10", DateTime.UtcNow.AddSeconds(10)); }`
- `using (var cache = ConnectionMultiplexer.Connect("")) { IDatabase db = cache.GetDatabase(); bool setValue = await db.StringSetAsync("test:key", "10", DateTime.Now.AddSeconds(10)); }`

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

Azure Redis Cache SDK for .NET - Azure for .NET Developers | Microsoft Learn

You need to read an Azure Cosmos DB change feed by using a reactive model.

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

- [ ] Azure Functions with an Azure Cosmos DB trigger
- [ ] Change feed processor library
- [ ] Azure Functions with an Azure Event Grid trigger
- [ ] Change feed pull model

You need to read an Azure Cosmos DB change feed by using a reactive model.

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

- [x] Azure Functions with an Azure Cosmos DB trigger
- [x] Change feed processor library
- [ ] Azure Functions with an Azure Event Grid trigger
- [ ] Change feed pull model

Azure Functions with an Azure Cosmos DB trigger allows you to select the container to connect, and the Azure Function is triggered whenever there is a change in the container. The change feed processor library follows the observer pattern, where the processing function is called by the library. The change feed processor library will automatically check for changes and, if changes are found, push them to the client. Azure Functions with an Event Grid trigger will execute the function when an Event Grid event is dispatched. It has no relationship with an Azure Cosmos DB change feed. A change feed pull model will use a pull model rather than a push model.
Consume an Azure Cosmos DB for NoSQL change feed using the SDK - Training | Microsoft Learn

You manage an Azure Cosmos DB container named **container1**.
You need to use the **ReadItemAsync** method to read an item from the Azure Cosmos service.
Which two parameters do you need to provide? Each correct answer presents part of the solution.

- [ ] `consistencyLevel`
- [ ] `eTag`
- [ ] `partitionKey`
- [ ] `sessionToken`
- [ ] `itemId`

You manage an Azure Cosmos DB container named **container1**.
You need to use the **ReadItemAsync** method to read an item from the Azure Cosmos service.
Which two parameters do you need to provide? Each correct answer presents part of the solution.

- [ ] `consistencyLevel`
- [ ] `eTag`
- [x] `partitionKey`
- [ ] `sessionToken`
- [x] `itemId`

The **ReadItemAsync** method of the container class of .NET SDK for Azure Cosmos DB has two mandatory parameters: partitionKey and itemId. The **consistencyLevel** parameter is part of the optional requestOptions parameter of the **ReadItemAsync**. The eTag and sessionToken parameters are part of the optional **requestOptions** parameter of the **ReadItemAsync** method.
Explore Microsoft .NET SDK v3 for Azure Cosmos DB - Training | Microsoft Learn
Container.ReadItemAsync<T> Method (Microsoft.Azure.Cosmos) - Azure for .NET Developers | Microsoft Learn

A company has Azure Cosmos DB accounts configured with multiple write regions.

You need to identify the conflict types used by Azure Cosmos DB.

Which three conflict types should you identify? Each correct answer presents a complete solution.

- [ ] Insert
- [ ] Replace
- [ ] Delete
- [ ] Last Write Wins
- [ ] First Write Wins

A company has Azure Cosmos DB accounts configured with multiple write regions.

You need to identify the conflict types used by Azure Cosmos DB.

Which three conflict types should you identify? Each correct answer presents a complete solution.

- [x] Insert
- [x] Replace
- [x] Delete
- [ ] Last Write Wins
- [ ] First Write Wins

The **Insert** conflict can occur when an application simultaneously inserts two or more items with the same unique index in two or more regions. For example, this conflict might occur with an ID property. The **Replace** conflict can occur when an application updates the same item simultaneously in two or more regions. The **Delete** conflict can occur when an application simultaneously deletes an item in one region and updates it in another region. **Last Write** Win is not an update conflict type but rather a conflict resolution policy. **First Write** Win is not an update conflict type.

Work with Azure Cosmos DB - Training | Microsoft Learn

Conflict resolution types and resolution policies in Azure Cosmos DB | Microsoft Learn

You plan to implement a storage mechanism for managing state across multiple change feed consumers.

You need to configure the change feed processor in the .NET SDK for Azure Cosmos DB for NoSQL API.

Which component should you use?

- Delegate
- Host
- Lease container
- Monitored container

You plan to implement a storage mechanism for managing state across multiple change feed consumers.

You need to configure the change feed processor in the .NET SDK for Azure Cosmos DB for NoSQL API.

Which component should you use?

- ○ Delegate
- ○ Host
- ● Lease container
- ○ Monitored container

The **lease container** component serves as a storage mechanism to manage state across multiple change feed consumers. The **delegate** component is the code within the client application that implements business logic for each batch of changes. The **host** component is a client application instance that listens for changes from the change feed. The **monitored container** component is monitored for any insert or update operations. It does not serve as a storage mechanism to manage state across multiple change feed consumers.

Understand change feed features in the SDK - Training | Microsoft Learn

How to use Azure Cosmos DB change feed with Azure Functions | Microsoft Learn

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?

- Append a suffix to the blob name by using the location and weather. Add a delimiter between them.
- Use metadata headers defined with a POST request.
- Use metadata headers defined with a PUT request.
- Create one container for each location. Inside each container, define the blob name as the weather type and a random suffix.

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?

- ○ Append a suffix to the blob name by using the location and weather. Add a delimiter between them.
- ○ Use metadata headers defined with a POST request.
- ● Use metadata headers defined with a PUT request.
- ○ Create one container for each location. Inside each container, define the blob name as the weather type and a random suffix.

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
Naming and Referencing Containers, Blobs, and Metadata - Azure Storage | Microsoft Learn

You have an Azure storage lifecycle policy for block blobs.

You need to create a prefixMatch filter rule that will contain an array of strings for prefixes to be matched.

What should be the first element of the prefix string?

- a block blob index tag
- a block blob name
- a container name
- a storage account name

You have an Azure storage lifecycle policy for block blobs.

You need to create a prefixMatch filter rule that will contain an array of strings for prefixes to be matched.

What should be the first element of the prefix string?

- ○ a block blob index tag
- ○ a block blob name
- ● a container name
- ○ a storage account name

When creating a prefixMatch filter rule for an Azure storage lifecycle policy for block blobs, the first element of the prefix string must be a **container name** not a block blob index tag, block blob name, or storage account name.
Discover Blob storage lifecycle policies - Training | Microsoft Learn
Optimize costs by automatically managing the data lifecycle - Azure Storage | Microsoft Learn

You create the following retention policy. (Line numbers are included for reference only.)

```
1  {
2    "rules": [
3      {
4        "name": "agingRule",
5        "enabled": true,
6        "type": "Lifecycle",
7        "definition": {
8          "filters": {
9            "blobTypes": [ "blockBlob" ],
10           "prefixMatch": [ "sample-container/blob1" ]
11         },
12         "actions": {
13           "baseBlob": {
14
15           }
16         }
17       }
18     }
19   ]
20 }
```

You need to transition blobs in the Hot access tier to an online tier if the blobs have not been modified in over 90 days.
Which code segment should you add to line 14?

- `"tierToArchive": { "daysAfterCreationGreaterThan": 90 }`
- `"tierToCool": { "daysAfterCreationGreaterThan": 90 }`
- `"tierToCool": { "daysAfterModificationGreaterThan": 90 }`
- `"tierToArchive": { "daysAfterModificationGreaterThan": 90 }`

You create the following retention policy. (Line numbers are included for reference only.)

```
1  {
2    "rules": [
3      {
4        "name": "agingRule",
5        "enabled": true,
6        "type": "Lifecycle",
7        "definition": {
8          "filters": {
9            "blobTypes": [ "blockBlob" ],
10           "prefixMatch": [ "sample-container/blob1" ]
11         },
12         "actions": {
13           "baseBlob": {
14
15           }
16         }
17       }
18     }
19   ]
20 }
```

You need to transition blobs in the Hot access tier to an online tier if the blobs have not been modified in over 90 days.
Which code segment should you add to line 14?

- ○ `"tierToArchive": { "daysAfterCreationGreaterThan": 90 }`
- ○ `"tierToCool": { "daysAfterCreationGreaterThan": 90 }`
- ● `"tierToCool": { "daysAfterModificationGreaterThan": 90 }`
- ○ `"tierToArchive": { "daysAfterModificationGreaterThan": 90 }`

The code segment **"tierToCool": { "daysAfterModificationGreaterThan": 90 }** moves the blobs not modified after 90 days to the Cool tier, as defined by the requirement. The code segments that include "tierToArchive": move the blobs to the Archive tier, which is not an online access tier; it is an offline tier. The code segment ***"tierToCool": { "daysAfterCreationGreaterThan": 90 }*** moves the blobs to the Cool tier 90 days after creation, which does not meet the requirement to move blobs after 90 days without modification.
Implement Blob storage lifecycle policies - Training | Microsoft Learn

You have blobs in an Azure storage account.

You need to implement a stored access policy that will apply to shared access signatures generated for the blobs.

To which type of storage resource should you associate the policy?

- ○ the storage account
- ○ the blob service of the storage account
- ○ the container that is hosting blobs
- ○ each individual blob

You have blobs in an Azure storage account.

You need to implement a stored access policy that will apply to shared access signatures generated for the blobs.

To which type of storage resource should you associate the policy?

- ○ the storage account
- ○ the blob service of the storage account
- ● the container that is hosting blobs
- ○ each individual blob

The **container** that is hosting blobs is used for associating the corresponding stored access policies. The **storage account** can be associated with shared access signatures keys but not stored access policies. The **blob service** of the storage account can be associated with shared access signatures keys but not stored access policies. **Each individual blob** can be associated with shared access signatures keys but not stored access policies.
Use stored access policies to delegate access to Azure Storage - Training | Microsoft Learn

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?

- ○ user-assigned managed identity
- ○ service principal and secret
- ○ service principal and certificate
- ○ system-assigned managed identity

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?

- ○ user-assigned managed identity
- ○ service principal and secret
- ○ service principal and certificate
- ● system-assigned managed identity

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

Azure Key Vault soft-delete | Microsoft Learn

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.

- [ ] Azure App Configuration Free tier
- [ ] Azure App Configuration Standard tier
- [ ] Azure Key Vault Standard tier
- [ ] Azure Key Vault Premium tier

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.

- [ ] Azure App Configuration Free tier
- [x] Azure App Configuration Standard tier
- [ ] Azure Key Vault Standard tier
- [x] Azure Key Vault Premium tier

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
Azure Managed HSM Overview - Azure Managed HSM | Microsoft Learn

You create an Azure Resource Manager (ARM) template.

You need to configure the template to generate a unique virtual machine name.

Which ARM template section should you use?

- parameters
- variables
- user-defined functions
- resources

You create an Azure Resource Manager (ARM) template.

You need to configure the template to generate a unique virtual machine name.

Which ARM template section should you use?

- ○ parameters
- ○ variables
- ○ user-defined functions
- ● resources

User-defined functions allow you to create functions for complicated expressions that are used repeatedly in the ARM template. **Parameters** provide values during deployment that allow the same template to be used with different environments. **Variables** are used to simplify a template, not to repeat complicated expressions throughout the template. A **variable** can be defined that contains the complicated expression. The **resources** section is used to deploy resources through an ARM template. Parameters, variables, and resources cannot be used to uniquely generate a unique name during a deployment.
Create and deploy Azure Resource Manager templates - Training | Microsoft Learn
User-defined functions in templates - Azure Resource Manager | Microsoft Learn

You need to delete an image with the tag `dev/nginx:latest` from an Azure container registry named **devregistry**.

Which code segment should you use?

- `az acr repository delete --name devregistry --image dev/nginx:latest`
- `az acr repository delete --name devregistry --suffix dev/nginx:latest`
- `az acr manifest delete --registry devregistry -n dev/nginx:latest`
- `az acr manifest delete --registry devregistry --suffix dev/nginx:latest --image dev/nginx:latest`

You need to delete an image with the tag `dev/nginx:latest` from an Azure container registry named **devregistry**.

Which code segment should you use?

- `az acr repository delete --name devregistry --image dev/nginx:latest`
- `az acr repository delete --name devregistry --suffix dev/nginx:latest`
- `az acr manifest delete --registry devregistry -n dev/nginx:latest`
- `az acr manifest delete --registry devregistry --suffix dev/nginx:latest --image dev/nginx:latest`

The code segment **az acr repository delete --name devregistry --image dev/nginx:latest** will delete the image from a container registry. The code segments that include the suffix parameter should be used if you are accessing the registry from a different subscription or have permission to access images but not permission to manage the registry resource. The code segments that include the manifest parameters delete the manifest of the artifact not the image.

Build and store container images with Azure Container Registry - Training | Microsoft Learn
az acr repository | Microsoft Learn

You plan to deploy three virtual machines located in different availability zones in a region.

You have the following requirements:

- Maximize application resiliency.
- Distribute Layer 4 (TCP/UDP) incoming traffic.
- Support client IP affinity.

What should you configure?

- ◯ Azure Load Balancer
- ◯ Azure Application Gateway
- ◯ Azure Traffic Manager
- ◯ Azure Front Door

You plan to deploy three virtual machines located in different availability zones in a region.

You have the following requirements:

- Maximize application resiliency.
- Distribute Layer 4 (TCP/UDP) incoming traffic.
- Support client IP affinity.

What should you configure?

- (●) Azure Load Balancer
- ( ) Azure Application Gateway
- ( ) Azure Traffic Manager
- ( ) Azure Front Door

Azure Load Balancer will support maximum application resiliency, Layer 4 TCP/UDP distribution of incoming traffic, and client IP affinity. **Azure Application Gateway** is a web traffic load balancer that enables you to manage traffic to your web applications and can make routing decisions based on additional attributes of an HTTP request. **Azure Traffic Manager** is a DNS-based traffic load balancer. This service allows you to distribute traffic to your public-facing applications across the global Azure regions. Traffic Manager also provides your public endpoints with high availability and quick responsiveness. It does not support Layer 4 (TCP/UDP) load balancing. **Azure Front Door** is Microsoft's modern cloud Content Delivery Network that provides fast, reliable, and secure access between users and applications' static and dynamic web content across the globe.

AZ-204: Implement infrastructure as a service solutions - Training | Microsoft Learn
What is Azure Load Balancer? - Azure Load Balancer | Microsoft Learn
Azure Load Balancer distribution modes | Microsoft Learn
What is Azure Application Gateway | Microsoft Learn
Azure Front Door | Microsoft Learn

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?

- ◯ Scale out app1.
- ◯ Scale up app1.
- ◯ Configure automated deployment of app1 with Azure DevOps.
- ◯ Configure automated deployment of app1 with GitHub.

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?

- ◯ Scale out app1.
- ◯ Scale up app1.
- ◯ Configure automated deployment of app1 with Azure DevOps.
- ◯ Configure automated deployment of app1 with GitHub.

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

Deployment best practices - Azure App Service | Microsoft Learn

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?

- ◯ Deployment Center
- ◯ Deployment slot setting
- ◯ Managed identity
- ◯ Scale up

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?

- ○ Deployment Center
- ● Deployment slot setting
- ○ Managed identity
- ○ Scale up

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 Azure Active Directory 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

A company plans to create an Azure function app.

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

- Executes multiple functions concurrently.
- Performs aggregation on the results from the functions.
- Avoids cold starts.
- Minimizes costs.

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

- [ ] The Consumption plan
- [ ] The Premium plan
- [ ] Fan-out/fan-in pattern
- [ ] Function chaining pattern

A company plans to create an Azure function app.

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

- Executes multiple functions concurrently.
- Performs aggregation on the results from the functions.
- Avoids cold starts.
- Minimizes costs.

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

- [ ] The Consumption plan
- [x] The Premium plan
- [x] Fan-out/fan-in pattern
- [ ] Function chaining pattern

The **Premium plan** avoids cold starts and offers unlimited execution duration. The **fan-out/fan-in pattern** enables multiple functions to be executed in parallel, waiting for all functions to finish. Often, some aggregation work is done on the results that are returned from the functions. The **Consumption plan** avoids paying for idle time but might face cold starts. Furthermore, each function run is limited to 10 minutes. **The function chaining pattern** is a sequence of functions that execute in a specific order. In this pattern, the output of one function is applied to the input of another function.
AZ-204: Implement Azure Functions - Training | Microsoft Learn
Azure Functions Premium plan | Microsoft Learn
Fan-out/fan-in scenarios in Durable Functions - Azure | Microsoft Learn

You manage an Azure Cache for Redis instance.

You need to load data on demand into the cache from a large database.

Which application architecture pattern should you use?

- ◯ content cache
- ◯ distributed transactions
- ◯ data cache
- ◯ session store

You manage an Azure Cache for Redis instance.

You need to load data on demand into the cache from a large database.

Which application architecture pattern should you use?

- ◯ content cache
- ◯ distributed transactions
- ● data cache
- ◯ session store

Databases often are too large to load directly into a cache, so it is common to **use data cache** pattern. **Session store** is used to store user-session information instead of storing too much data in a cookie that can adversely affect performance. **Distributed transactions** allow a series of commands to run on a back-end datastore as a single operation. By using **content cache**, you can provide quicker access to static content compared to back-end datastores. Session store, distributed transactions, and content cache cannot be used to load data on demand.
What is Azure Cache for Redis? - Training | Microsoft Learn
Cache-Aside pattern - Azure Architecture Center | Microsoft Learn

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.

- ◯ Standard
- ◯ Premium
- ◯ Enterprise
- ◯ Enterprise Flash

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.

- ○ Standard
- ○ Premium
- ○ Enterprise
- ● Enterprise Flash

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
Pricing - Azure Cache for Redis | Microsoft Azure

A company uses Application Insights to instrument an application hosted in Azure App Service.

Instrumentation data that is collected by using API calls in the code is not available in Application Insights.

You need to ensure the collected data is available in Application Insights.

What should you do? Select only one answer.

- ◯ Enable auto-instrumentation.
- ◯ Enable manual instrumentation.
- ◯ Verify the health of Application Insights.
- ◯ Verify the health of Azure App Service.

A company uses Application Insights to instrument an application hosted in Azure App Service.

Instrumentation data that is collected by using API calls in the code is not available in Application Insights.

You need to ensure the collected data is available in Application Insights.

What should you do? Select only one answer.

- ◯ Enable auto-instrumentation.
- ● Enable manual instrumentation.
- ◯ Verify the health of Application Insights.
- ◯ Verify the health of Azure App Service.

Manual instrumentation must be enabled to emit telemetry using API calls. Because some data is being collected, Application Insights is available. Because the application is running, Azure App Service is available.
Instrument an app for monitoring - Training | Microsoft Learn
Monitor Azure App Service performance - Azure Monitor | Microsoft Learn

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.

- ◯ Azure portal
- ◯ Azure CLI
- ◯ Visual Studio
- ◯ Visual Studio Code

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.

- ◯ Azure portal
- ◯ Azure CLI
- ● Visual Studio
- ◯ Visual Studio Code

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
Monitor with multistep web tests - Application Insights - Azure Monitor | Microsoft Learn

You manage an Azure API Management instance.

You need to limit the maximum number of API calls allowed from a single source for a specific time interval.

What should you configure? Select only one answer.

- ◯ Product
- ◯ Policy
- ◯ Subscription
- ◯ API

You manage an Azure API Management instance.

You need to limit the maximum number of API calls allowed from a single source for a specific time interval.

What should you configure? Select only one answer.

- ○ Product
- ● Policy
- ○ Subscription
- ○ API

API publishers can change API behavior through configuration using policies. **Policies** are a collection of statements that run sequentially on the request or response of an API. A **product** has one or more APIs, a usage quota, and the terms of use and cannot be used to restrict the number of API calls. **Subscriptions** are the most common way for API consumers to access APIs published through an API Management instance. **API** is a representation of a back-end API and needs to be configured with a policy to implement a rate limit.
How Azure API Management Works - Training | Microsoft Learn
Subscriptions in Azure API Management | Microsoft Learn

You create an Azure Service Bus topic with a default message time to live of 10 minutes.

You need to send messages to this topic with a time to live of 15 minutes. The solution must not affect other applications that are using the topic.

What should you recommend? Select only one answer.

- ◯ Change the topic's default time to live to 15 minutes.
- ◯ Change the specific message's time to live to 15 minutes.
- ◯ Create a new topic with a default time to live of 15 minutes. Send the messages to this topic.
- ◯ Update the time to live for the queue containing the topic.

You create an Azure Service Bus topic with a default message time to live of 10 minutes.

You need to send messages to this topic with a time to live of 15 minutes. The solution must not affect other applications that are using the topic.

What should you recommend? Select only one answer.

- ◯ Change the topic's default time to live to 15 minutes.
- ◯ Change the specific message's time to live to 15 minutes.
- ● Create a new topic with a default time to live of 15 minutes. Send the messages to this topic.
- ◯ Update the time to live for the queue containing the topic.

To avoid affecting existing applications, the time to live of the existing topic must not be changed. A **new topic needs to be created**. Changing the topic's default time to live will affect other applications. A message-level time to live cannot be higher than the topic's time to live. To avoid affecting existing applications, the time to live of the existing topic or queue must not be changed.

Exercise: Send and receive message from a Service Bus queue by using .NET. - Training | Microsoft Learn

ServiceBusMessage.TimeToLive Property (Azure.Messaging.ServiceBus) - Azure for .NET Developers | Microsoft Learn

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?

- ○ `WEBSITE_LOAD_CERTIFICATES`
- ○ `WEBSITE_ROOT_CERTS_PATH`
- ○ `WEBSITE_CORS_ALLOWED_ORIGINS`
- ○ `WEBSITE_AUTH_TOKEN_CONTAINER_SASURL`

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?

- (●) `WEBSITE_LOAD_CERTIFICATES`
- ( ) `WEBSITE_ROOT_CERTS_PATH`
- ( ) `WEBSITE_CORS_ALLOWED_ORIGINS`
- ( ) `WEBSITE_AUTH_TOKEN_CONTAINER_SASURL`

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
Environment variables and app settings reference - Azure App Service | Microsoft Learn
Use a TLS/SSL certificate in code - Azure App Service | Microsoft Learn

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?

- ◯ Basic
- ◯ Standard
- ◯ Premium
- ◯ Enterprise

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?

- ◯ Basic
- ◯ Standard
- ◯ Premium
- ● Enterprise

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
Explore Azure Cache for Redis - Training | Microsoft Learn
What is Azure Cache for Redis? | Microsoft Learn

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.

- ◯ Redis database (RDB) persistence with the soft-delete feature enabled on the associated storage account.
- ◯ Redis database (RDB) persistence with the soft-delete feature disabled on the associated storage account.
- ◯ Append only File (AOF) persistence with the soft-delete feature disabled on the associated storage account.
- ◯ Append only File (AOF) persistence with the soft-delete feature enabled on the associated storage account.

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.

- ◯ Redis database (RDB) persistence with the soft-delete feature enabled on the associated storage account.
- ◯ Redis database (RDB) persistence with the soft-delete feature disabled on the associated storage account.
- ◯ Append only File (AOF) persistence with the soft-delete feature disabled on the associated storage account.
- ◯ Append only File (AOF) persistence with the soft-delete feature enabled on the associated storage account.

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

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.

- [ ] `"enableDependencyTracking": true`
- [ ] `"dependencyTrackingOptions": { "enableSqlCommandTextInstrumentation": true },`
- [ ] `"enablePerformanceCountersCollection": true`
- [ ] `"logLevel": { "default": "Verbose" }`

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.

- [x] `"enableDependencyTracking": true`
- [x] `"dependencyTrackingOptions": { "enableSqlCommandTextInstrumentation": true },`
- [ ] `"enablePerformanceCountersCollection": true`
- [ ] `"logLevel": { "default": "Verbose" }`

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.

Instrument server-side web application code with Application Insights - Training | Microsoft Learn

Dependency tracking in Application Insights - Azure Monitor | Microsoft Learn

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.

- ◯ GetMetric
- ◯ TrackMetric
- ◯ SetMetric
- ◯ LogMetric

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.

- (●) GetMetric
- ( ) TrackMetric
- ( ) SetMetric
- ( ) LogMetric

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

Get-Metric in Azure Monitor Application Insights - Azure Monitor | Microsoft Learn

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.

- [ ] Upload static content to a storage container named **$web.**
- [ ] Use Azure Traffic Manager to route users to the closest region.
- [ ] Upload static content to a storage container named **web.**
- [ ] Use Azure Content Delivery Network for regional caching.

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.

- [x] Upload static content to a storage container named **$web.**
- [ ] Use Azure Traffic Manager to route users to the closest region.
- [ ] Upload static content to a storage container named **web.**
- [x] Use Azure Content Delivery Network for regional caching.

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
Static website hosting in Azure Storage | Microsoft Learn

You plan to use Microsoft Graph to retrieve a list of users in an Azure Active Directory (Azure AD) tenant.

You need to optimize query results.

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

- [ ] `$filter`
- [ ] `$count`
- [ ] `$select`
- [ ] `$expand`

You plan to use Microsoft Graph to retrieve a list of users in an Azure Active Directory (Azure AD) tenant.

You need to optimize query results.

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

- [x] `$filter`
- [ ] `$count`
- [ ] `$select`
- [x] `$expand`

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 $count query option is meant to retrieve the total count of matching resources. **$expand** query option is used to retrieve related resources.

Query Microsoft Graph by using REST - Training | Microsoft Learn

Paging Microsoft Graph data in your app - Microsoft Graph | Microsoft Learn

You manage an Azure Active Directory 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.

- ◯ Authorization code
- ◯ On-Behalf-Of
- ◯ Client credentials
- ◯ Implicit

You manage an Azure Active Directory 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.

- ○ Authorization code
- ● On-Behalf-Of
- ○ Client credentials
- ○ Implicit

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

Microsoft identity platform and OAuth2.0 On-Behalf-Of flow - Microsoft Entra | Microsoft

You plan to enable a user to create a managed identity for an Azure virtual machine (VM).

You need to ensure the following requirements are met:

The user account must have sufficient permissions to create the managed identity.
The principle of least privilege must be used.
Which permission role should you assign? Select only one answer.

- ○ Virtual Machine Administrator Login
- ○ Virtual Machine Contributor
- ○ Global Administrator
- ○ Security Administrator

You plan to enable a user to create a managed identity for an Azure virtual machine (VM).

You need to ensure the following requirements are met:

The user account must have sufficient permissions to create the managed identity.
The principle of least privilege must be used.
Which permission role should you assign? Select only one answer.

- ○ Virtual Machine Administrator Login
- ● Virtual Machine Contributor
- ○ Global Administrator
- ○ Security Administrator

Virtual Machine Contributor is the least privileged built-in role required to create a managed identity for an Azure VM. Virtual Machine Administrator Login is not sufficient to create a managed identity for an Azure VM. Global Administrator and Security Administrator have excessive permissions to Azure Active Directory, which does not follow the principle of least privilege. Global Administrator and Security Administrator do not provide sufficient permissions to the Azure resources.
Configure managed identities - Training | Microsoft Learn
Configure managed identities using the Azure portal - Azure AD - Microsoft Entra | Microsoft Learn

You manage Azure Cache for Redis by using classes in the .NET StackExchange.Redis namespace.

You need to retrieve a reference to a Redis database by using the GetDatabase method.

What do you need to do first? Select only one answer.

- ◯ Create a CdnManagementClient object.
- ◯ Create a ConnectionMultiplexer object.
- ◯ Call a StringSet method.
- ◯ Call a StringGet method.

You manage Azure Cache for Redis by using classes in the .NET StackExchange.Redis namespace.

You need to retrieve a reference to a Redis database by using the GetDatabase method.

What do you need to do first? Select only one answer.

- ○ Create a CdnManagementClient object.
- ● Create a ConnectionMultiplexer object.
- ○ Call a StringSet method.
- ○ Call a StringGet method.

Creating a ConnectionMultiplexer object is the first step required to retrieve a reference to a Redis database by using the GetDatabase method. Creating a CdnManagementClient object is required when using Azure Content Delivery Network caching, not Azure Cache for Redis. Calling a StringSet method allows you to manage the content of a Redis database, which happens once the ConnectionMultiplexer object, and the database have been created. Calling a StringGet method allows you to retrieve the content of a Redis database, which happens once the ConnectionMultiplexer object, and the database have been created.

Interact with Azure Cache for Redis by using .NET - Training | Microsoft Learn

Quickstart: Use Azure Cache for Redis in .NET Framework | Microsoft Learn

Thank you...

Please **LIKE** & **SUBSCRIBE** @Clearcatnet