EXAMTOPICS

- Expert Verified, Online, **Free**.

Custom View Settings

Question #7 *Topic 3*

DRAG DROP -

You are developing an application to securely transfer data between on-premises file systems and Azure Blob storage. The application stores keys, secrets, and certificates in Azure Key Vault. The application uses the Azure Key Vault APIs.

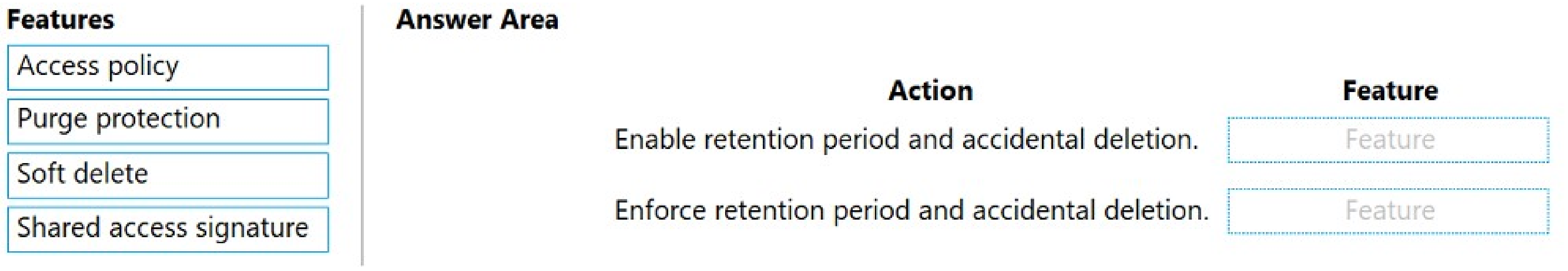
The application must allow recovery of an accidental deletion of the key vault or key vault objects. Key vault objects must be retained for 90 days after deletion.

You need to protect the key vault and key vault objects.

Which Azure Key Vault feature should you use? To answer, drag the appropriate features to the correct actions. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



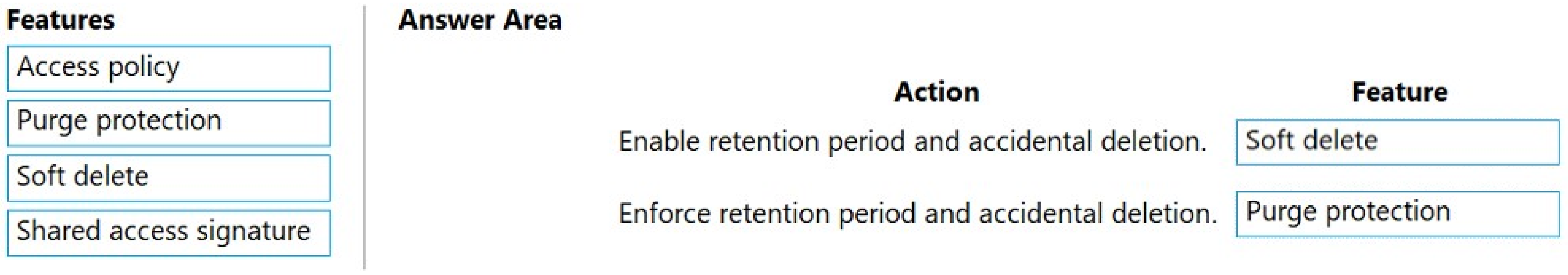
Features

- Access policy
- Purge protection
- Soft delete
- Shared access signature

Answer Area

Action	Feature
Enable retention period and accidental deletion.	Feature
Enforce retention period and accidental deletion.	Feature

Correct Answer:



Features

- Access policy
- Purge protection
- Soft delete
- Shared access signature

Answer Area

Action	Feature
Enable retention period and accidental deletion.	Soft delete
Enforce retention period and accidental deletion.	Purge protection

Box 1: Soft delete -

When soft-delete is enabled, resources marked as deleted resources are retained for a specified period (90 days by default). The service further provides a mechanism for recovering the deleted object, essentially undoing the deletion.

Box 2: Purge protection -

Purge protection is an optional Key Vault behavior and is not enabled by default. Purge protection can only be enabled once soft-delete is enabled.

When purge protection is on, a vault or an object in the deleted state cannot be purged until the retention period has passed. Soft-deleted vaults and objects can still be recovered, ensuring that the retention policy will be followed.

Reference:

https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview

Question #8 *Topic 3*

You provide an Azure API Management managed web service to clients. The back-end web service implements HTTP Strict Transport Security (HSTS).
Every request to the backend service must include a valid HTTP authorization header.
You need to configure the Azure API Management instance with an authentication policy.
Which two policies can you use? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Basic Authentication

B. Digest Authentication

C. Certificate Authentication

D. OAuth Client Credential Grant

Correct Answer: *CD*

Question #9 *Topic 3*

DRAG DROP -

You are developing an ASP.NET Core website that can be used to manage photographs which are stored in Azure Blob Storage containers. Users of the website authenticate by using their Azure Active Directory (Azure AD) credentials.

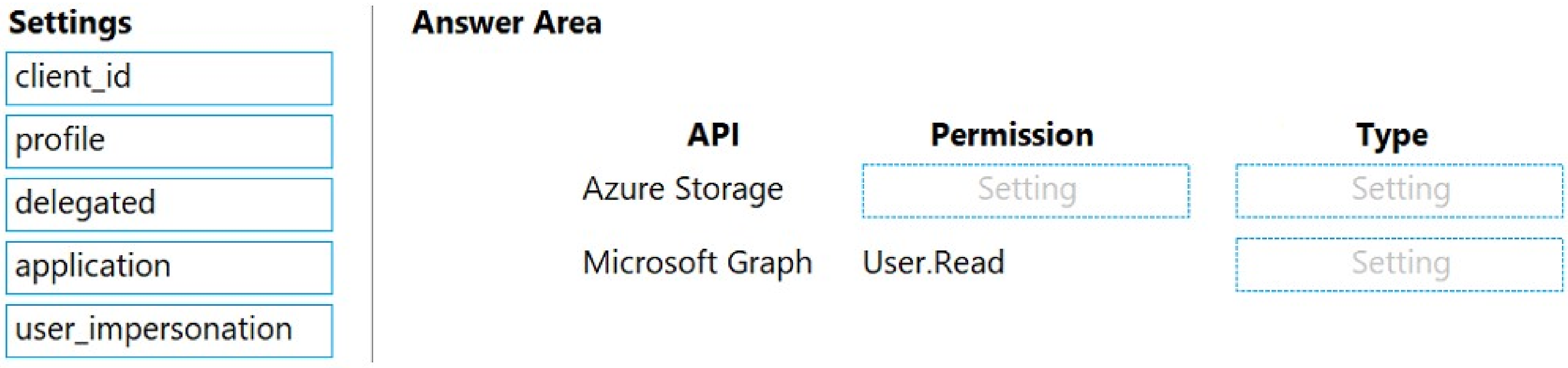
You implement role-based access control (RBAC) role permissions on the containers that store photographs. You assign users to RBAC roles.

You need to configure the website's Azure AD Application so that user's permissions can be used with the Azure Blob containers.

How should you configure the application? To answer, drag the appropriate setting to the correct location. Each setting can be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:



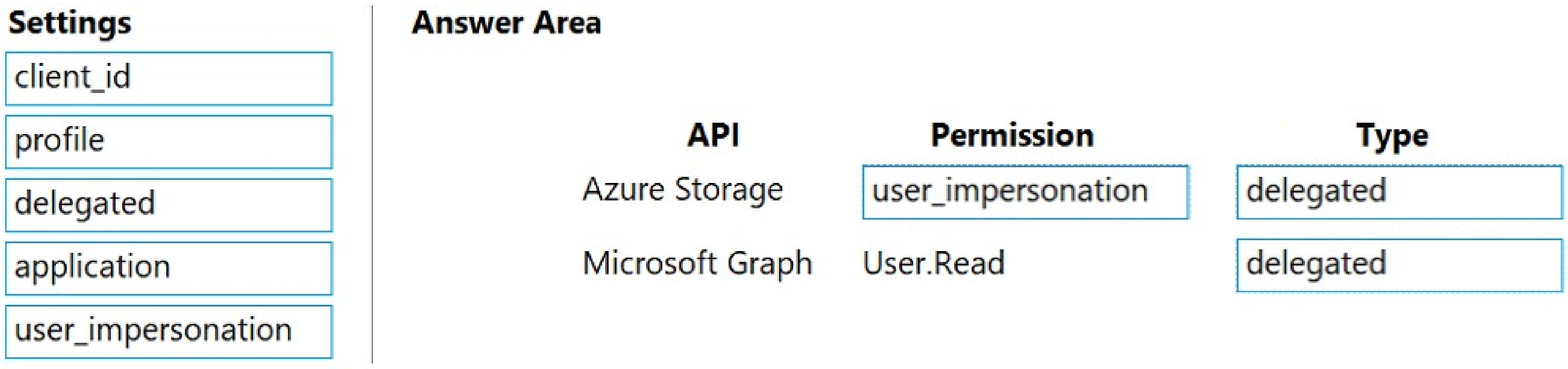
Settings

- client_id
- profile
- delegated
- application
- user_impersonation

Answer Area

API	Permission	Type
Azure Storage	Setting	Setting
Microsoft Graph	User.Read	Setting

Correct Answer:



Settings

- client_id
- profile
- delegated
- application
- user_impersonation

Answer Area

API	Permission	Type
Azure Storage	user_impersonation	delegated
Microsoft Graph	User.Read	delegated

Box 1: user_impersonation -

Box 2: delegated -

Example:

1. Select the API permissions section
2. Click the Add a permission button and then:

Ensure that the My APIs tab is selected

3. In the list of APIs, select the API TodoListService-aspnetcore.
4. In the Delegated permissions section, ensure that the right permissions are checked: user_impersonation.
5. Select the Add permissions button.

Box 3: delegated -

Example -

1. Select the API permissions section
2. Click the Add a permission button and then,

Ensure that the Microsoft APIs tab is selected

3. In the Commonly used Microsoft APIs section, click on Microsoft Graph
4. In the Delegated permissions section, ensure that the right permissions are checked: User.Read. Use the search box if necessary.
5. Select the Add permissions button

Reference:

https://docs.microsoft.com/en-us/samples/azure-samples/active-directory-dotnet-webapp-webapi-openidconnect-aspnetcore/calling-a-web-api-in-an-aspnet-core- web-application-using-azure-ad/

Question #10 *Topic 3*

HOTSPOT -

You are developing an ASP.NET Core app that includes feature flags which are managed by Azure App Configuration. You create an Azure App Configuration store named AppFeatureFlagStore that contains a feature flag named Export.

You need to update the app to meet the following requirements:

✑ Use the Export feature in the app without requiring a restart of the app.

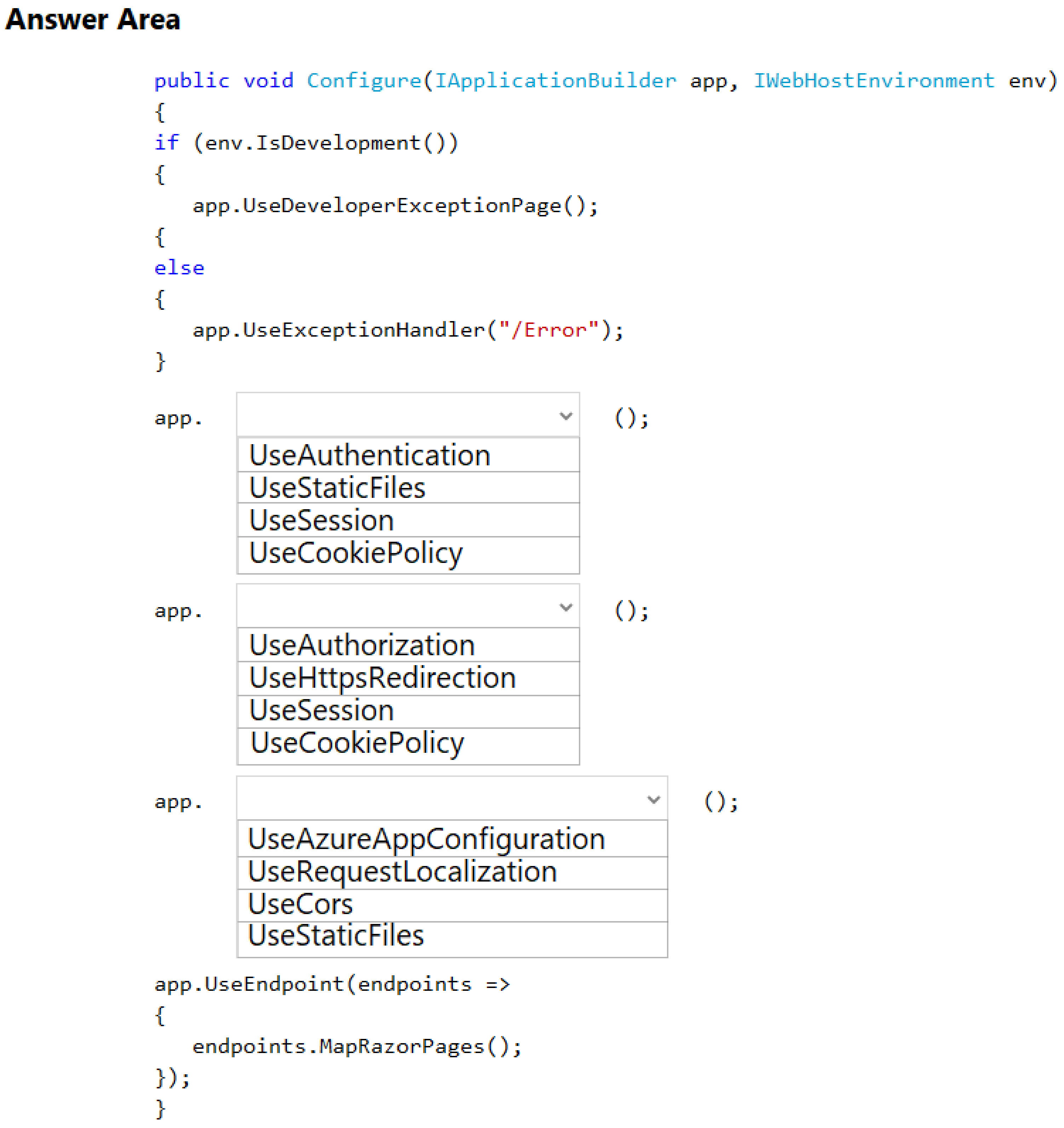
✑ Validate users before users are allowed access to secure resources.

✑ Permit users to access secure resources.

How should you complete the code segment? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

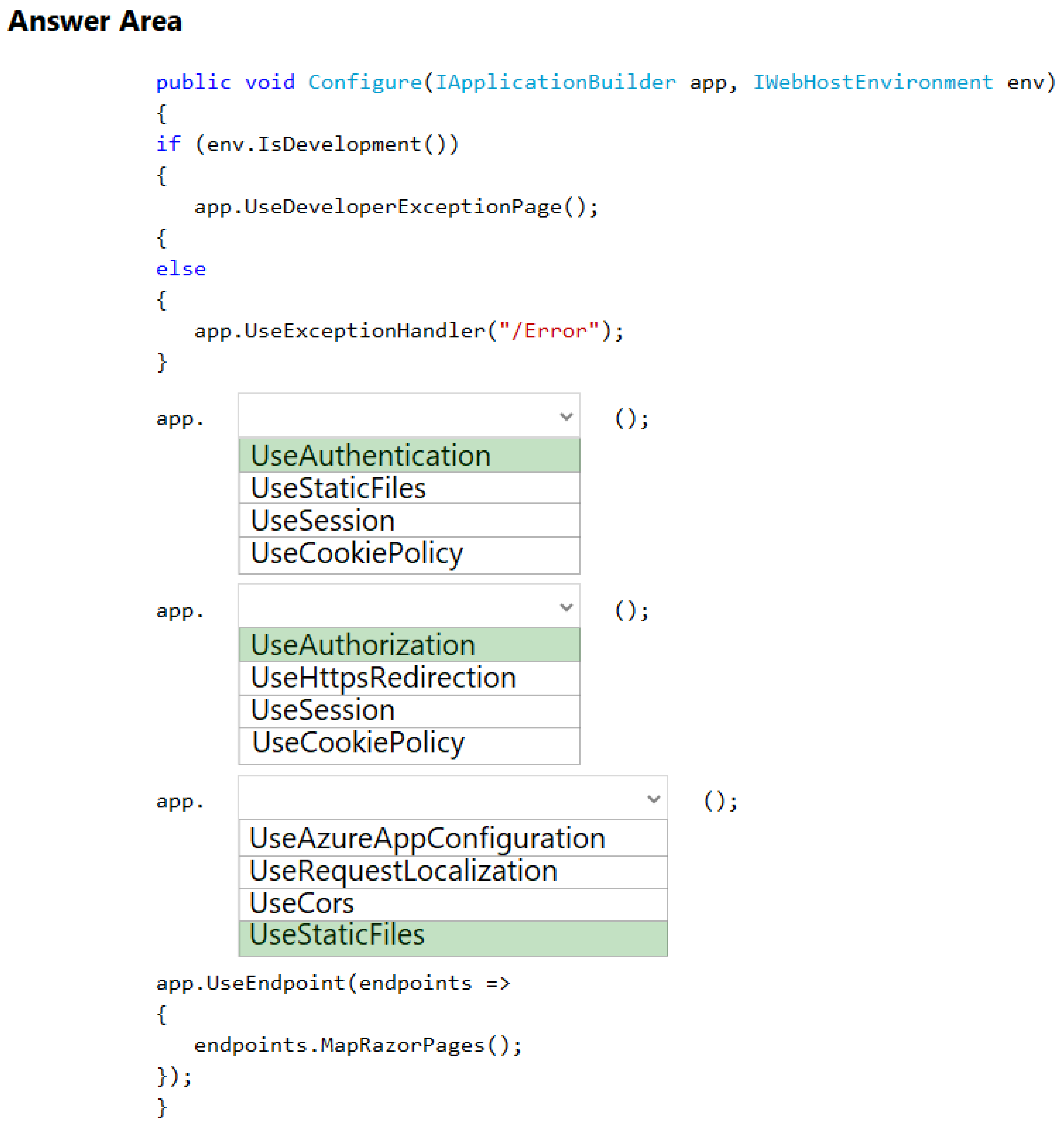
Hot Area:



Answer Area

```
public void Configure(IApplicationBuilder app, IWebHostEnvironment env)
{
if (env.IsDevelopment())
{
   app.UseDeveloperExceptionPage();
{
else
{
   app.UseExceptionHandler("/Error");
}

app. [                    ] ();
      UseAuthentication
      UseStaticFiles
      UseSession
      UseCookiePolicy

app. [                    ] ();
      UseAuthorization
      UseHttpsRedirection
      UseSession
      UseCookiePolicy

app. [                         ] ();
      UseAzureAppConfiguration
      UseRequestLocalization
      UseCors
      UseStaticFiles

app.UseEndpoint(endpoints =>
{
   endpoints.MapRazorPages();
});
}
```

Correct Answer:



Answer Area

```
public void Configure(IApplicationBuilder app, IWebHostEnvironment env)
{
if (env.IsDevelopment())
{
   app.UseDeveloperExceptionPage();
{
else
{
   app.UseExceptionHandler("/Error");
}

app.                          ();
```

[✓ UseAuthentication]
UseStaticFiles
UseSession
UseCookiePolicy

```
app.                          ();
```

[✓ UseAuthorization]
UseHttpsRedirection
UseSession
UseCookiePolicy

```
app.                          ();
```

UseAzureAppConfiguration
UseRequestLocalization
UseCors
[✓ UseStaticFiles]

```
app.UseEndpoint(endpoints =>
{
   endpoints.MapRazorPages();
});
}
```

Box 1: UseAuthentication -

Need to validate users before users are allowed access to secure resources.

UseAuthentication adds the AuthenticationMiddleware to the specified IApplicationBuilder, which enables authentication capabilities.

Box 2: UseAuthorization -

Need to permit users to access secure resources.

UseAuthorization adds the AuthorizationMiddleware to the specified IApplicationBuilder, which enables authorization capabilities.

Box 3: UseStaticFiles -

Need to use the Export feature in the app without requiring a restart of the app.

UseStaticFiles enables static file serving for the current request path

Reference:

https://docs.microsoft.com/en-us/dotnet/api/microsoft.aspnetcore.builder.iapplicationbuilder?view=aspnetcore-5.0

Question #11 *Topic 3*

You have an application that includes an Azure Web app and several Azure Function apps. Application secrets including connection strings and certificates are stored in Azure Key Vault.

Secrets must not be stored in the application or application runtime environment. Changes to Azure Active Directory (Azure AD) must be minimized.

You need to design the approach to loading application secrets.

What should you do?

A. Create a single user-assigned Managed Identity with permission to access Key Vault and configure each App Service to use that Managed Identity.

B. Create a single Azure AD Service Principal with permission to access Key Vault and use a client secret from within the App Services to access Key Vault.

C. Create a system assigned Managed Identity in each App Service with permission to access Key Vault.

D. Create an Azure AD Service Principal with Permissions to access Key Vault for each App Service and use a certificate from within the App Services to access Key Vault.

Correct Answer: *C*

Use Key Vault references for App Service and Azure Functions.

Key Vault references currently only support system-assigned managed identities. User-assigned identities cannot be used.

Reference:

https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references

← Previous Questions Next Questions →