Question #27 *Topic 3*

You are a developer for a SaaS company that offers many web services.
All web services for the company must meet the following requirements:
- Use API Management to access the services
- Use OpenID Connect for authentication
- Prevent anonymous usage

A recent security audit found that several web services can be called without any authentication.
Which API Management policy should you implement?

A. jsonp

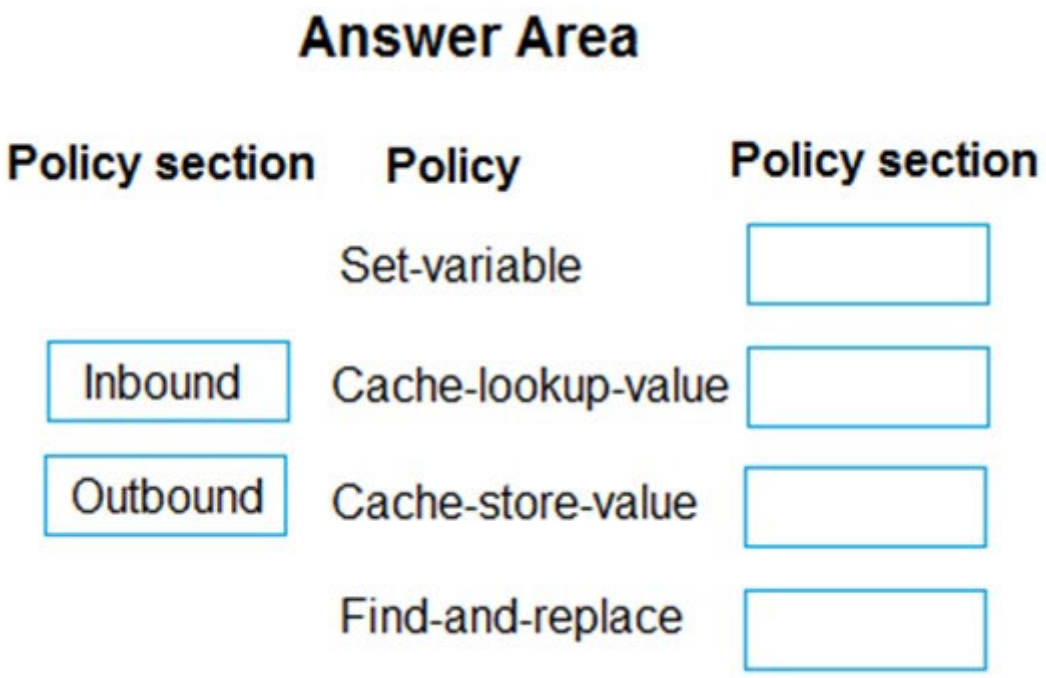
B. authentication-certificate

C. check-header

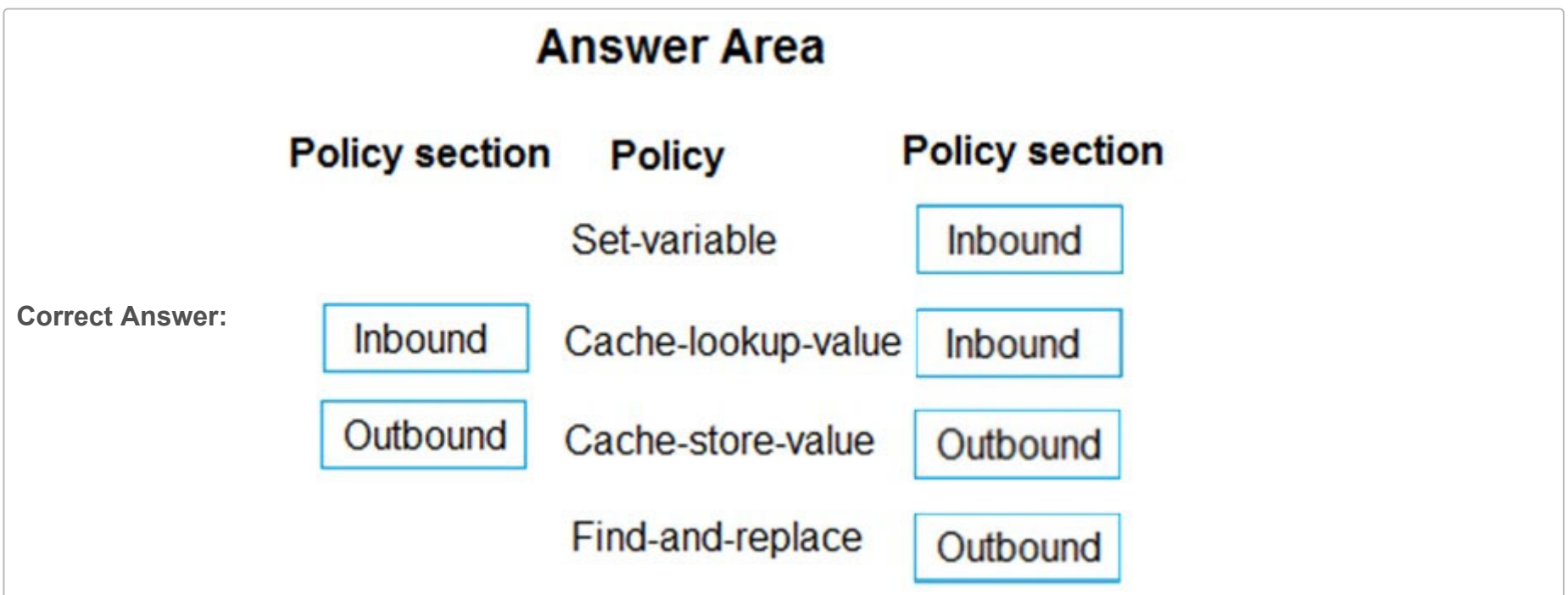
D. validate-jwt

Correct Answer: *D*
Add the validate-jwt policy to validate the OAuth token for every incoming request.
Incorrect Answers:
A: The jsonp policy adds JSON with padding (JSONP) support to an operation or an API to allow cross-domain calls from JavaScript browser-based clients.
JSONP is a method used in JavaScript programs to request data from a server in a different domain. JSONP bypasses the limitation enforced by most web browsers where access to web pages must be in the same domain.
JSONP - Adds JSON with padding (JSONP) support to an operation or an API to allow cross-domain calls from JavaScript browser-based clients.
Reference:
https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad

DRAG DROP -
Contoso, Ltd. provides an API to customers by using Azure API Management (APIM). The API authorizes users with a JWT token.
You must implement response caching for the APIM gateway. The caching mechanism must detect the user ID of the client that accesses data for a given location and cache the response for that user ID.
You need to add the following policies to the policies file:
☞ a set-variable policy to store the detected user identity
☞ a cache-lookup-value policy
☞ a cache-store-value policy
☞ a find-and-replace policy to update the response body with the user profile information
To which policy section should you add the policies? To answer, drag the appropriate sections to the correct policies. Each section 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:



Correct Answer:



Box 1: Inbound.
A set-variable policy to store the detected user identity.
Example:
<policies>
<inbound>
<!-- How you determine user identity is application dependent -->
<set-variable
name="enduserid"
value="@(context.Request.Headers.GetValueOrDefault("Authorization","").Split(' ')[1].AsJwt()?.Subject)" />

Box 2: Inbound -

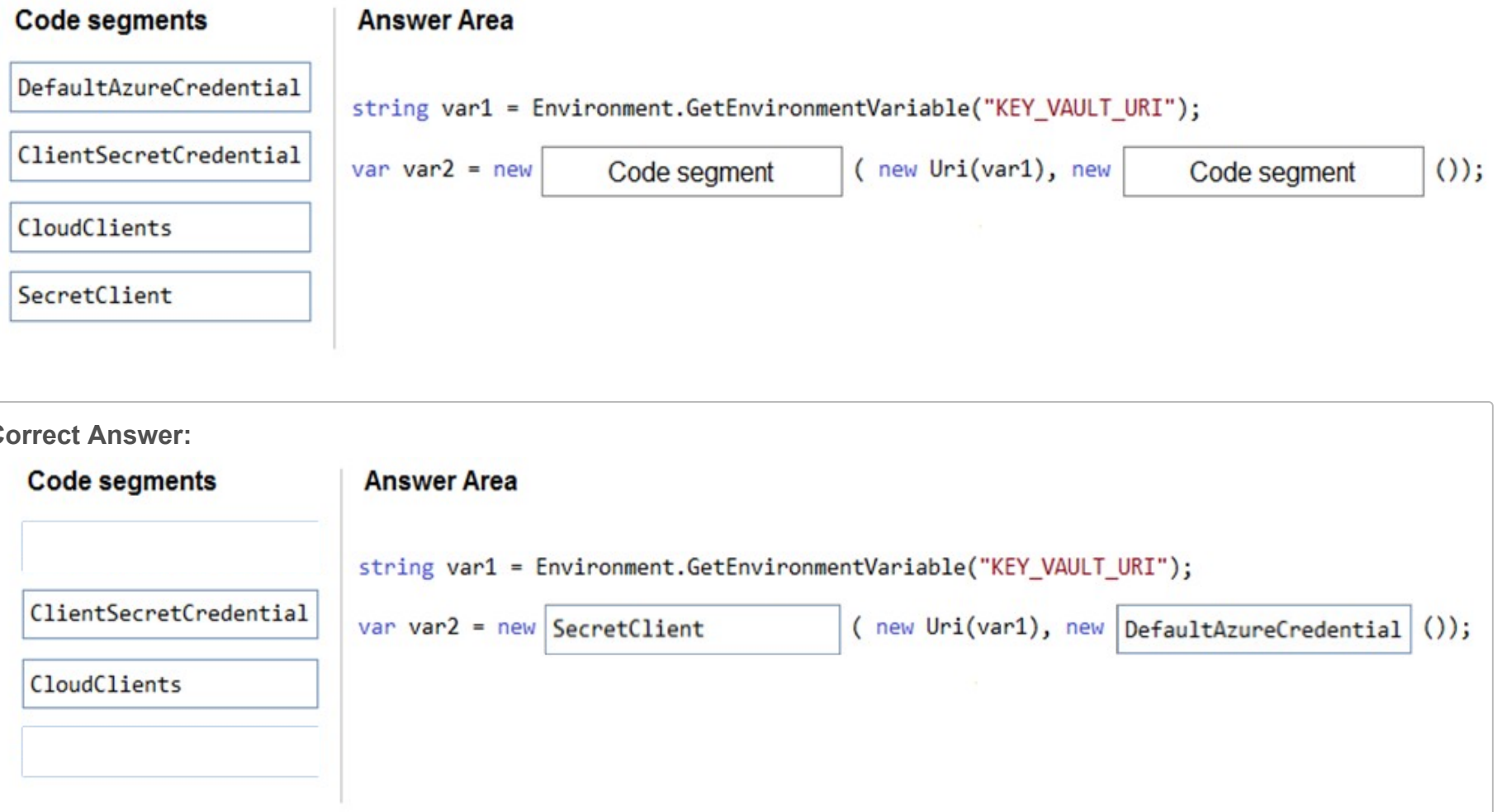
A cache-lookup-value policy -

Example:
<inbound>
<base />
<cache-lookup vary-by-developer="true | false" vary-by-developer-groups="true | false" downstream-caching-type="none | private | public" must- revalidate="true | false">
<vary-by-query-parameter>parameter name</vary-by-query-parameter> <!-- optional, can repeated several times -->
</cache-lookup>
</inbound>

Box 3: Outbound -
A cache-store-value policy.
Example:
<outbound>
<base />
<cache-store duration="3600" />
</outbound>

Box 4: Outbound -
A find-and-replace policy to update the response body with the user profile information.
Example:
<outbound>
<!-- Update response body with user profile-->
<find-and-replace
from="'$userprofile$"'
to="@((string)context.Variables["userprofile"])" />
<base />
</outbound>
Reference:
https://docs.microsoft.com/en-us/azure/api-management/api-management-caching-policies https://docs.microsoft.com/en-us/azure/api-management/api-management-sample-cache-by-key

DRAG DROP -
You are developing an Azure solution.
You need to develop code to access a secret stored in Azure Key Vault.
How should you complete the code segment? To answer, drag the appropriate code segments to the correct location. Each code segment 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:



Correct Answer:

Box 1: SecretClient -

Box 2: DefaultAzureCredential -
In below example, the name of your key vault is expanded to the key vault URI, in the format "https://<your-key-vault-name>.vault.azure.net". This example is using 'DefaultAzureCredential()' class from Azure Identity Library, which allows to use the same code across different environments with different options to provide identity. string keyVaultName = Environment.GetEnvironmentVariable("KEY_VAULT_NAME"); var kvUri = "https://" + keyVaultName + ".vault.azure.net"; var client = new SecretClient(new Uri(kvUri), new DefaultAzureCredential());
Reference:
https://docs.microsoft.com/en-us/azure/key-vault/secrets/quick-create-net

Question #30 *Topic 3*

You are developing an Azure App Service REST API.
The API must be called by an Azure App Service web app. The API must retrieve and update user profile information stored in Azure Active Directory (Azure AD).
You need to configure the API to make the updates.
Which two tools should you use? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. Microsoft Graph API

B. Microsoft Authentication Library (MSAL)

C. Azure API Management

D. Microsoft Azure Security Center

E. Microsoft Azure Key Vault SDK

Correct Answer: *AC*
A: You can use the Azure AD REST APIs in Microsoft Graph to create unique workflows between Azure AD resources and third-party services.
Enterprise developers use Microsoft Graph to integrate Azure AD identity management and other services to automate administrative workflows, such as employee onboarding (and termination), profile maintenance, license deployment, and more.
C: API Management (APIM) is a way to create consistent and modern API gateways for existing back-end services.
API Management helps organizations publish APIs to external, partner, and internal developers to unlock the potential of their data and services.
Reference:
https://docs.microsoft.com/en-us/graph/azuread-identity-access-management-concept-overview

Question #31 *Topic 3*

You develop a REST API. You implement a user delegation SAS token to communicate with Azure Blob storage.
The token is compromised.
You need to revoke the token.
What are two possible ways to achieve this goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Revoke the delegation key.

B. Delete the stored access policy.

C. Regenerate the account key.

D. Remove the role assignment for the security principle.

Correct Answer: *AB*

A: Revoke a user delegation SAS -
To revoke a user delegation SAS from the Azure CLI, call the az storage account revoke-delegation-keys command. This command revokes all of the user delegation keys associated with the specified storage account. Any shared access signatures associated with those keys are invalidated.
B: To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it.
Reference:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/blobs/storage-blob-user-delegation-sas-create-cli.md
https://docs.microsoft.com/en-us/rest/api/storageservices/define-stored-access-policy#modifying-or-revoking-a-stored-access-policy

Previous Questions Next Questions