## 5. Connect to and consume Azure services and third-party services

## **□** 5.1 Implement API Management

## **□** 5.1.4 Implement policies for APIs

- 1. What are API Management policies and where can they be applied?
- 2. How do you use the set-header policy to manipulate request/response headers?
- 3. How does the validate-jwt policy work for token validation?
- 4. How do you apply rate limiting using the rate-limit policy?
- 5. What's the difference between quota and rate-limit policies?
- 6. How do you rewrite URLs using rewrite-uri or set-backend-service?
- 7. How do you handle conditional logic in policies using choose and when?
- 8. How can you transform request or response bodies using set-body?
- 9. What tools are used to author, test, and debug APIM policies?
- 10. What are best practices for policy organization and reuse?

# 1. What are API Management policies and where can they be applied?

- XML-based logic executed at runtime.
- Applied at four scopes: inbound, backend, outbound, and on-error.
- Can be configured at global, product, API, or operation levels.

#### 2. How do you use the set-header policy to manipulate request/response headers?

- Adds or updates headers.
- Example:

```
<set-header name="X-Custom-Header" exists-action="override">
<value>my-value</value>
</set-header>
```

### 3. How does the validate-jwt policy work for token validation?

- Validates JWT tokens in Authorization header.
- Requires configuration of issuer, audience, and signing keys.
- Example:

```
<validate-jwt header-name="Authorization" require-scheme="Bearer">
  <openid-config url="https://login.microsoftonline.com/<tenant>/v2.0/.well-known/openid-configuration" />
  <required-claims><claim name="aud"><value>api-client-id</value></claim></required-claims>
  </validate-jwt>
```

## 4. How do you apply rate limiting using the rate-limit policy?

- Restricts number of calls in a time window.
- Example:

<rate-limit calls="100" renewal-period="60" />
Limits client to 100 calls per minute.

#### 5. What's the difference between quota and rate-limit policies?

- rate-limit: short-term throttle (e.g., per minute).
- quota: long-term usage limit (e.g., daily/weekly).
- Both can be used together for layered control.

#### 6. How do you rewrite URLs using rewrite-uri or set-backend-service?

• rewrite-uri: Changes request path.

Example:

<rewrite-uri template="/v2/resource" />

set-backend-service: Redirects to a different backend.

Example:

<set-backend-service base-url="https://api.contoso.com/v2" />

## 7. How do you handle conditional logic in policies using choose and when?

Enables branching logic based on conditions.

#### Example:

```
<choose>
    <when condition="@(context.Request.Headers["x-version"] == "v2")">
        <set-backend-service base-url="https://api-v2.contoso.com" />
        </when>
    <otherwise>
        <set-backend-service base-url="https://api-v1.contoso.com" />
        </otherwise>
    </otherwise>
</choose>
```

## 8. How can you transform request or response bodies using set-body?

Overwrites the payload.

Example (JSON):

<set-body>@("{\"message\": \"Access denied\"}")</set-body>

• Can also use Liquid templates for dynamic content.

## 9. What tools are used to author, test, and debug APIM policies?

- Azure Portal policy editor with IntelliSense.
- Test console in Azure Portal.
- Developer portal (limited testing).
- Trace/debug by enabling "trace" and reviewing trace logs in the test console.

## 10. What are best practices for policy organization and reuse?

- Keep logic centralized at product/API level when possible.
- Use named values for reusable values.
- Document policy use with <comment> blocks.
- Avoid deep nesting for readability.