MCPA-LEVEL-1-MAINTENANCE Q&As

MuleSoft Certified Platform Architect - Level 1 MAINTENANCE

Pass Mulesoft MCPA-LEVEL-1-MAINTENANCE Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/mcpa-level-1-maintenance.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Mulesoft Official Exam Center

QUESTION 1

How can the application of a rate limiting API policy be accurately reflected in the RAML definition of an API?

A. By refining the resource definitions by adding a description of the rate limiting policy behavior

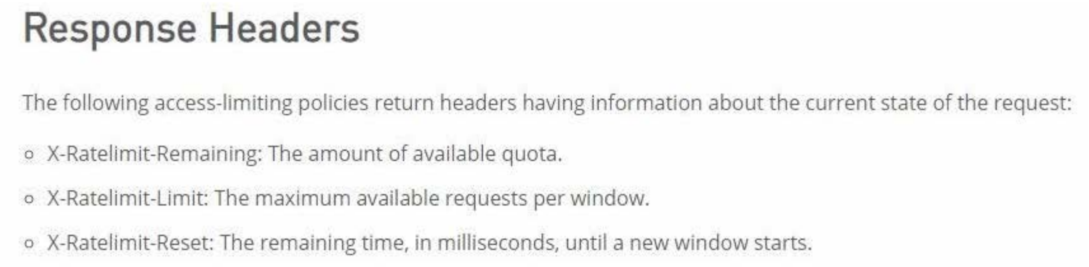
B. By refining the request definitions by adding a remaining Requests query parameter with description, type, and example

C. By refining the response definitions by adding the out-of-the-box Anypoint Platform rate- limit-enforcement securityScheme with description, type, and example

D. By refining the response definitions by adding the x-ratelimit-* response headers with description, type, and example

Correct Answer: D

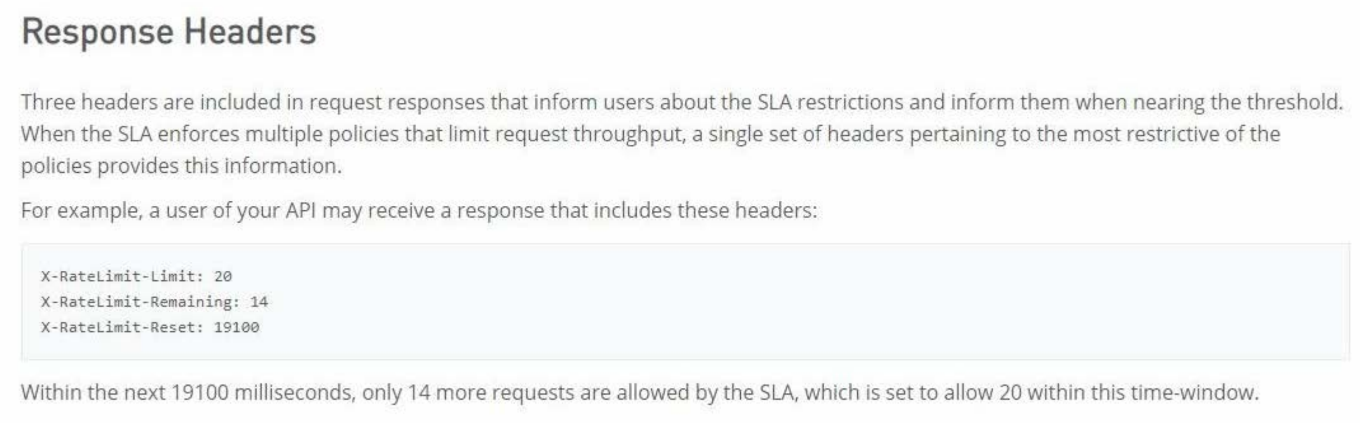
By refining the response definitions by adding the x-ratelimit-* response headers with description, type, and example
****



Response Headers

The following access-limiting policies return headers having information about the current state of the request:

- X-Ratelimit-Remaining: The amount of available quota.
- X-Ratelimit-Limit: The maximum available requests per window.
- X-Ratelimit-Reset: The remaining time, in milliseconds, until a new window starts.



Response Headers

Three headers are included in request responses that inform users about the SLA restrictions and inform them when nearing the threshold. When the SLA enforces multiple policies that limit request throughput, a single set of headers pertaining to the most restrictive of the policies provides this information.

For example, a user of your API may receive a response that includes these headers:

```
X-RateLimit-Limit: 20
X-RateLimit-Remaining: 14
X-RateLimit-Reset: 19100
```

Within the next 19100 milliseconds, only 14 more requests are allowed by the SLA, which is set to allow 20 within this time-window.

References: https://docs.mulesoft.com/api-manager/2.x/rate-limiting-and-throttling#response-headers https://docs.mulesoft.com/api-manager/2.x/rate-limiting-and-throttling-sla-based- policies#response-headers

QUESTION 2

An organization has created an API-led architecture that uses various API layers to integrate mobile clients with a backend system. The backend system consists of a number of specialized components and can be accessed via a REST API. The process and experience APIs share the same bounded-context model that is different from the backend data model. What additional canonical models, bounded-context models, or anti-corruption layers are best added to this architecture to help process data consumed from the backend system?

A. Create a bounded-context model for every layer and overlap them when the boundary contexts overlap, letting API developers know about the differences between upstream and downstream data models

B. Create a canonical model that combines the backend and API-led models to simplify and unify data models, and minimize data transformations.

C. Create a bounded-context model for the system layer to closely match the backend data model, and add an anti-corruption layer to let the different bounded contexts cooperate across the system and process layers

D. Create an anti-corruption layer for every API to perform transformation for every data model to match each other, and let data simply travel between APIs to avoid the complexity and overhead of building canonical models

Correct Answer: C

Create a bounded-context model for the system layer to closely match the backend data model, and add an anti-corruption layer to let the different bounded contexts cooperate across the system and process layers *** >> Canonical models are not an option here as the organization has already put in efforts and created bounded-context models for Experience and Process APIs. >> Anti-corruption layers for ALL APIs is unnecessary and invalid because it is mentioned that experience and process APIs share same bounded-context model. It is just the System layer APIs that need to choose their approach now. >> So, having an anti-corruption layer just between the process and system layers will work well. Also to speed up the approach, system APIs can mimic the backend system data model.

QUESTION 3

What Anypoint Connectors support transactions?

A. Database, JMS, VM

B. Database, 3MS, HTTP

C. Database, JMS, VM, SFTP

D. Database, VM, File

Correct Answer: A

QUESTION 4

An Anypoint Platform organization has been configured with an external identity provider (IdP) for identity management and client management. What credentials or token must be provided to Anypoint CLI to execute commands against the Anypoint Platform APIs?

A. The credentials provided by the IdP for identity management

B. The credentials provided by the IdP for client management

C. An OAuth 2.0 token generated using the credentials provided by the IdP for client management

D. An OAuth 2.0 token generated using the credentials provided by the IdP for identity management

Correct Answer: A

The credentials provided by the IdP for identity management *** Reference: https://docs.mulesoft.com/runtime-manager/anypoint-platform- cli#authentication >> There is no support for OAuth 2.0 tokens from client/identity providers to authenticate via Anypoint CLI. Only possible tokens are "bearer tokens" that too only generated using Anypoint Organization/Environment Client Id and Secret from https://anypoint.mulesoft.com/accounts/login. Not the client credentials of client provider. So, OAuth 2.0 is not possible. More over, the token is mainly for API Manager purposes and not associated with a user. You can NOT use it to call most APIs (for example Cloudhub and etc) as per this Mulesoft Knowledge article.

>> The other option allowed by Anypoint CLI is to use client credentials. It is possible to use client credentials of a client provider but requires setting up Connected Apps in client management but such details are not given in the scenario explained in the question.

>> So only option left is to use user credentials from identify provider

QUESTION 5

Version 3.0.1 of a REST API implementation represents time values in PST time using ISO 8601 hh:mm:ss format. The API implementation needs to be changed to instead represent time values in CEST time using ISO 8601 hh:mm:ss format. When following the semver.org semantic versioning specification, what version should be assigned to the updated API implementation?

A. 3.0.2

B. 4.0.0

C. 3.1.0

D. 3.0.1

Correct Answer: B

4.0.0

****

As per semver.org semantic versioning specification:

Given a version number MAJOR.MINOR.PATCH, increment the:

-MAJOR version when you make incompatible API changes.

-

MINOR version when you add functionality in a backwards compatible manner.

-

PATCH version when you make backwards compatible bug fixes. As per the scenario given in the question, the API implementation is completely changing its behavior. Although the format of the time is still being maintained as hh:mm:ss

and there is no change in schema w.r.t format, the API will start functioning different after this change as the times are going to come completely different. Example: Before the change, say, time is going as 09:00:00 representing the PST.

Now on, after the change, the same time will go as 18:00:00 as Central European Summer Time is 9 hours ahead of Pacific Time.

>> This may lead to some uncertain behavior on API clients depending on how they are handling the times in the API response. All the API clients need to be informed that the API functionality is going to change and will return in CEST

format. So, this considered as a MAJOR change and the version of API for this new change would be 4.0.0

QUESTION 6

What is a best practice when building System APIs?

A. Document the API using an easily consumable asset like a RAML definition

B. Model all API resources and methods to closely mimic the operations of the backend system

C. Build an Enterprise Data Model (Canonical Data Model) for each backend system and apply it to System APIs

D. Expose to API clients all technical details of the API implementation\\'s interaction wifch the backend system

Correct Answer: B

Model all API resources and methods to closely mimic the operations of the backend system.

****

>> There are NO fixed and straight best practices while opting data models for APIs. They are completly contextual and depends on number of factors. Based upon those factors, an enterprise can choose if they have to go with Enterprise

Canonical Data Model or Bounded Context Model etc.

>> One should NEVER expose the technical details of API implementation to their API clients. Only the API interface/ RAML is exposed to API clients. >> It is true that the RAML definitions of APIs should be as detailed as possible and should

reflect most of the documentation. However, just that is NOT enough to call your API as best documented API. There should be even more documentation on Anypoint Exchange with API Notebooks etc. to make and create a developer

friendly API and repository.. >> The best practice always when creating System APIs is to create their API interfaces by modeling their resources and methods to closely reflect the operations and functionalities of that backend system.

QUESTION 7

What is a key requirement when using an external Identity Provider for Client Management in Anypoint Platform?

A. Single sign-on is required to sign in to Anypoint Platform

B. The application network must include System APIs that interact with the Identity Provider

C. To invoke OAuth 2.0-protected APIs managed by Anypoint Platform, API clients must submit access tokens issued by that same Identity Provider

D. APIs managed by Anypoint Platform must be protected by SAML 2.0 policies

Correct Answer: C

https://www.folkstalk.com/2019/11/mulesoft-integration-and-platform.html To invoke OAuth 2.0-protected APIs managed by Anypoint Platform, API clients must submit access tokens issued by that same Identity Provider

****

>> It is NOT necessary that single sign-on is required to sign in to Anypoint Platform because we are using an external Identity Provider for Client Management >> It is NOT necessary that all APIs managed by Anypoint Platform must be

protected by SAML 2.0 policies because we are using an external Identity Provider for Client Management

>> Not TRUE that the application network must include System APIs that interact with the Identity Provider because we are using an external Identity Provider for Client Management Only TRUE statement in the given options is - "To invoke

OAuth 2.0-protected APIs managed by Anypoint Platform, API clients must submit access tokens issued by that same Identity Provider"

References:

https://docs.mulesoft.com/api-manager/2.x/external-oauth-2.0-token-validation-policy https://blogs.mulesoft.com/dev/api-dev/api-security-ways-to-authenticate-and-authorize/

QUESTION 8

What are 4 important Platform Capabilities offered by Anypoint Platform?

A. API Versioning, API Runtime Execution and Hosting, API Invocation, API Consumer Engagement

B. API Design and Development, API Runtime Execution and Hosting, API Versioning, API Deprecation

C. API Design and Development, API Runtime Execution and Hosting, API Operations and Management, API Consumer Engagement

D. API Design and Development, API Deprecation, API Versioning, API Consumer Engagement

Correct Answer: C

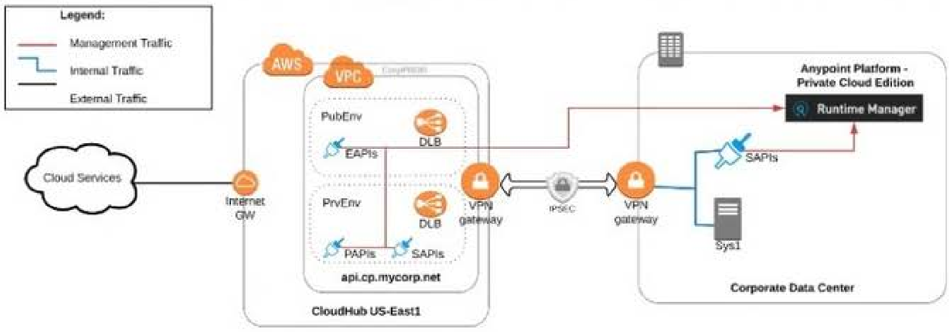
API Design and Development, API Runtime Execution and Hosting, API Operations and Management, API Consumer Engagement *** >> API Design and Development - Anypoint Studio, Anypoint Design Center, Anypoint Connectors >> API Runtime Execution and Hosting - Mule Runtimes, CloudHub, Runtime Services >> API Operations and Management - Anypoint API Manager, Anypoint Exchange >> API Consumer Management - API Contracts, Public Portals, Anypoint Exchange, API Notebooks

QUESTION 9

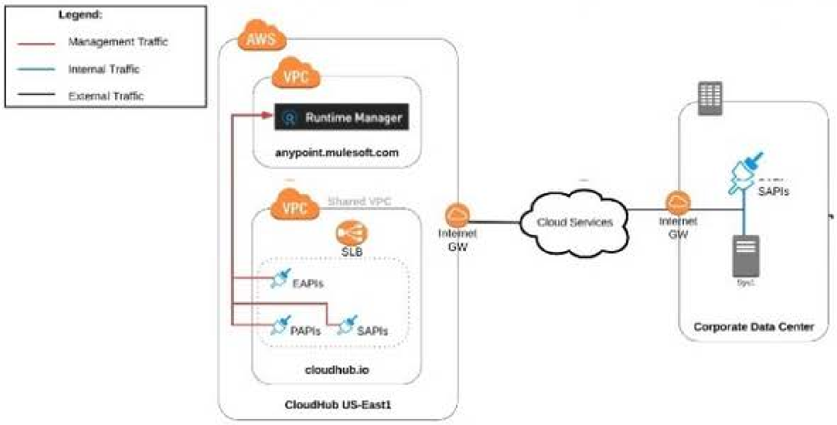
An organization uses various cloud-based SaaS systems and multiple on-premises systems. The on-premises systems are an important part of the organization\\'s application network and can only be accessed from within the organization\\'s intranet.

What is the best way to configure and use Anypoint Platform to support integrations with both the cloud-based SaaS systems and on-premises systems?

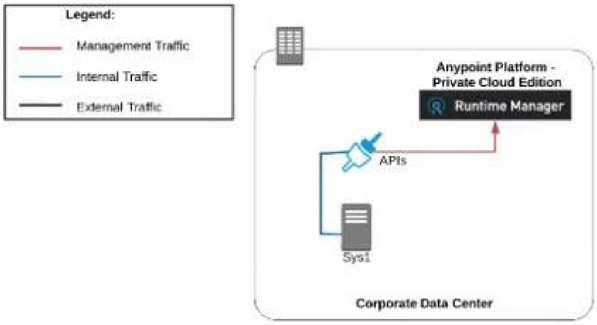
A. Use CloudHub-deployed Mule runtimes in an Anypoint VPC managed by Anypoint Platform Private Cloud Edition control plane



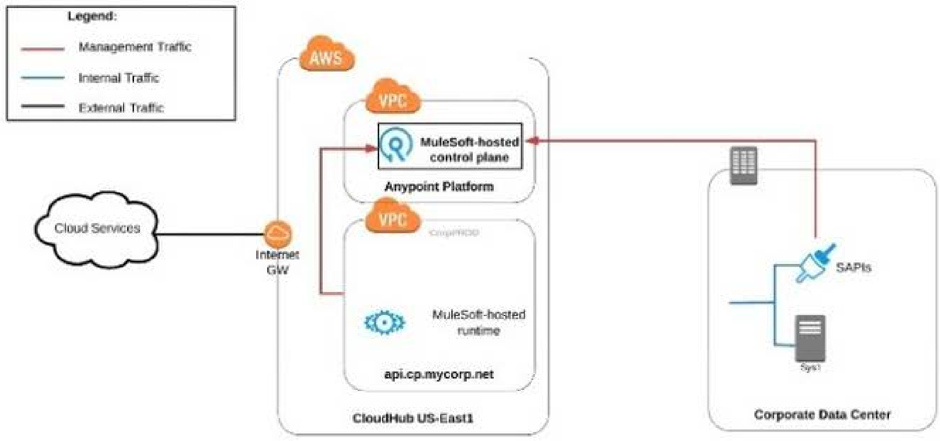
B. Use CloudHub-deployed Mule runtimes in the shared worker cloud managed by the MuleSoft-hosted Anypoint Platform control plane



C. Use an on-premises installation of Mule runtimes that are completely isolated with NO external network access, managed by the Anypoint Platform Private Cloud Edition control plane



D. Use a combination of Cloud Hub-deployed and manually provisioned on-premises Mule runtimes managed by the MuleSoft-hosted Anypoint Platform control plane



A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

Use a combination of CloudHub-deployed and manually provisioned on- premises Mule runtimes managed by the MuleSoft-hosted Platform control plane.

****

Key details to be taken from the given scenario:

>> Organization uses BOTH cloud-based and on-premises systems >> On-premises systems can only be accessed from within the organization\\'s intranet Let us evaluate the given choices based on above key details:

>> CloudHub-deployed Mule runtimes can ONLY be controlled using MuleSoft-hosted control plane. We CANNOT use Private Cloud Edition\\'s control plane to control CloudHub Mule Runtimes. So, option suggesting this is INVALID >> Using

CloudHub-deployed Mule runtimes in the shared worker cloud managed by the MuleSoft-hosted Anypoint Platform is completely IRRELEVANT to given scenario and silly choice. So, option suggesting this is INVALID

>> Using an on-premises installation of Mule runtimes that are completely isolated with NO external network access, managed by the Anypoint Platform Private Cloud Edition control plane would work for On-premises integrations. However,

with NO external access, integrations cannot be done to SaaS-based apps. Moreover CloudHub-hosted apps are best-fit for integrating with SaaS-based applications. So, option suggesting this is BEST WAY.

The best way to configure and use Anypoint Platform to support these mixed/hybrid integrations is to use a combination of CloudHub-deployed and manually provisioned on- premises Mule runtimes managed by the MuleSoft-hosted Platform

control plane.

QUESTION 10

What best describes the Fully Qualified Domain Names (FQDNs), also known as DNS entries, created when a Mule application is deployed to the CloudHub Shared Worker Cloud?

A. A fixed number of FQDNs are created, IRRESPECTIVE of the environment and VPC design

B. The FQDNs are determined by the application name chosen, IRRESPECTIVE of the region

C. The FQDNs are determined by the application name, but can be modified by an administrator after deployment

D. The FQDNs are determined by both the application name and the Anypoint Platform organization

Correct Answer: B

The FQDNs are determined by the application name chosen, IRRESPECTIVE of the region

****

>> When deploying applications to Shared Worker Cloud, the FQDN are always determined by application name chosen.

>> It does NOT matter what region the app is being deployed to. >> Although it is fact and true that the generated FQDN will have the region included in it (Ex: exp-salesorder-api.au-s1.cloudhub.io), it does NOT mean that the same name

can be used when deploying to another CloudHub region.

>> Application name should be universally unique irrespective of Region and Organization and solely determines the FQDN for Shared Load Balancers.

QUESTION 11

An organization wants to make sure only known partners can invoke the organization\\'s APIs. To achieve this security goal, the organization wants to enforce a Client ID Enforcement policy in API Manager so that only registered partner applications can invoke the organization\\'s APIs. In what type of API implementation does MuleSoft recommend adding an API proxy to enforce the Client ID Enforcement policy, rather than embedding the policy directly in the application\\'s JVM?

A. A Mule 3 application using APIkit

B. A Mule 3 or Mule 4 application modified with custom Java code

C. A Mule 4 application with an API specification

D. A Non-Mule application

Correct Answer: D

A Non-Mule application

****

>> All type of Mule applications (Mule 3/ Mule 4/ with APIkit/ with Custom Java Code etc) running on Mule Runtimes support the Embedded Policy Enforcement on them. >> The only option that cannot have or does not support embedded

policy enforcement and must have API Proxy is for Non-Mule Applications.

So, Non-Mule application is the right answer.

QUESTION 12

Which layer in the API-led connectivity focuses on unlocking key systems, legacy systems, data sources etc and exposes the functionality?

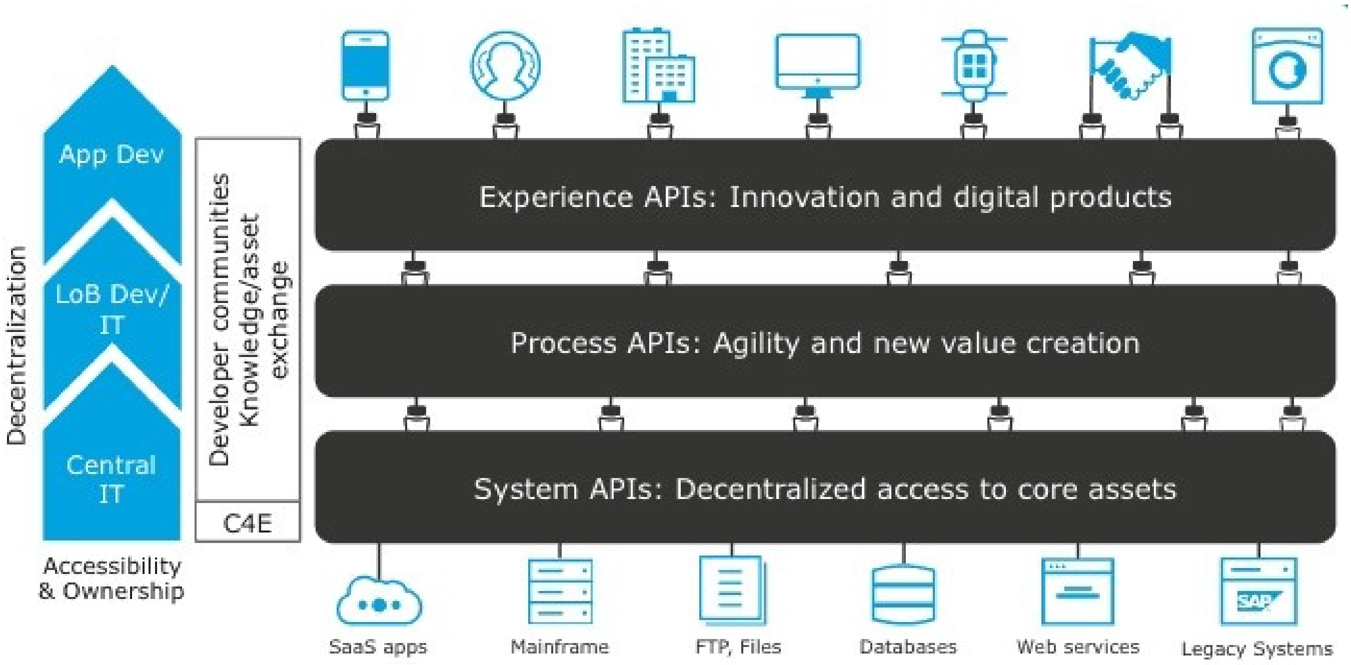
A. Experience Layer

B. Process Layer

C. System Layer

Correct Answer: C

System Layer


Decentralization
App Dev
LoB Dev/ IT
Central IT
Accessibility & Ownership
Developer communities Knowledge/asset exchange
C4E
Experience APIs: Innovation and digital products
Process APIs: Agility and new value creation
System APIs: Decentralized access to core assets
SaaS apps
Mainframe
FTP, Files
Databases
Web services
SAP
Legacy Systems

The APIs used in an API-led approach to connectivity fall into three categories:

System APIs -these usually access the core systems of record and provide a means of insulating the user from the complexity or any changes to the underlying systems. Once built, many users, can access data without any need to learn the

underlying systems and can reuse these APIs in multiple projects.

Process APIs -These APIs interact with and shape data within a single system or across systems (breaking down data silos) and are created here without a dependence on the source systems from which that data originates, as well as the

target channels through which that data is delivered.

Experience APIs -Experience APIs are the means by which data can be reconfigured so that it is most easily consumed by its intended audience, all from a common data source, rather than setting up separate point-to-point integrations for

each channel. An Experience API is usually created with API-first design principles where the API is designed for the specific user experience in mind.

QUESTION 13

A REST API is being designed to implement a Mule application.

What standard interface definition language can be used to define REST APIs?

A. Web Service Definition Language(WSDL)

B. OpenAPI Specification (OAS)

C. YAML

D. AsyncAPI Specification

Correct Answer: B

QUESTION 14

An API implementation is updated. When must the RAML definition of the API also be updated?

A. When the API implementation changes the structure of the request or response messages

B. When the API implementation changes from interacting with a legacy backend system deployed on-premises to a modern, cloud-based (SaaS) system

C. When the API implementation is migrated from an older to a newer version of the Mule runtime

D. When the API implementation is optimized to improve its average response time

Correct Answer: A

When the API implementation changes the structure of the request or response messages

****

>> RAML definition usually needs to be touched only when there are changes in the request/response schemas or in any traits on API.

>> It need not be modified for any internal changes in API implementation like performance tuning, backend system migrations etc..

QUESTION 15

An API has been updated in Anypoint Exchange by its API producer from version 3.1.1 to 3.2.0 following accepted semantic versioning practices and the changes have been communicated via the API\\'s public portal.

The API endpoint does NOT change in the new version.

How should the developer of an API client respond to this change?

A. The update should be identified as a project risk and full regression testing of the functionality that uses this API should be run

B. The API producer should be contacted to understand the change to existing functionality

C. The API producer should be requested to run the old version in parallel with the new one

D. The API client code ONLY needs to be changed if it needs to take advantage of new features

Correct Answer: D

Reference: https://docs.mulesoft.com/exchange/to-change-raml-version