MCPA-LEVEL1 Q&As

MuleSoft Certified Platform Architect - Level 1

Pass Mulesoft MCPA-LEVEL1 Exam with 100% Guarantee

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

https://www.geekcert.com/mulesoft-certified-platform-architect-level-1.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

An organization has several APIs that accept JSON data over HTTP POST. The APIs are all publicly available and are associated with several mobile applications and web applications.

The organization does NOT want to use any authentication or compliance policies for these APIs, but at the same time, is worried that some bad actor could send payloads that could somehow compromise the applications or servers running the API implementations.

What out-of-the-box Anypoint Platform policy can address exposure to this threat?

A. Shut out bad actors by using HTTPS mutual authentication for all API invocations

B. Apply an IP blacklist policy to all APIs; the blacklist will Include all bad actors

C. Apply a Header injection and removal policy that detects the malicious data before it is used

D. Apply a JSON threat protection policy to all APIs to detect potential threat vectors

Correct Answer: D

Apply a JSON threat protection policy to all APIs to detect potential threat vectors

****

>> Usually, if the APIs are designed and developed for specific consumers (known consumers/customers) then we would IP Whitelist the same to ensure that traffic only comes from them. >> However, as this scenario states that the APIs are

publicly available and being used by so many mobile and web applications, it is NOT possible to identify and blacklist all possible bad actors.

>> So, JSON threat protection policy is the best chance to prevent any bad JSON payloads from such bad actors.

QUESTION 2

How are an API implementation, API client, and API consumer combined to invoke and process an API?

A. The API consumer creates an API implementation, which receives API invocations from an API such that they are processed for an API client

B. The API client creates an API consumer, which receives API invocations from an API such that they are processed for an API implementation

C. The ApI consumer creates an API client, which sends API invocations to an API such that they are processed by an API implementation

D. The ApI client creates an API consumer, which sends API invocations to an API such that they are processed by an API implementation

Correct Answer: C

The API consumer creates an API client, which sends API invocations to an API such that they are processed by an API

implementation ********** Terminology:

>> API Client - It is a piece of code or program the is written to invoke an API >> API Consumer - An owner/entity who owns the API Client. API Consumers write API clients. >> API - The provider of the API functionality. Typically an API

Instance on API Manager where they are managed and operated. >> API Implementation - The actual piece of code written by API provider where the functionality of the API is implemented. Typically, these are Mule Applications running on

Runtime Manager.

QUESTION 3

Say, there is a legacy CRM system called CRM-Z which is offering below functions:

1.

Customer creation

2.

Amend details of an existing customer

3.

Retrieve details of a customer

4.

Suspend a customer

A. Implement a system API named customerManagement which has all the functionalities wrapped in it as various operations/resources

B. Implement different system APIs named createCustomer, amendCustomer, retrieveCustomer and suspendCustomer as they are modular and has seperation of concerns

C. Implement different system APIs named createCustomerInCRMZ, amendCustomerInCRMZ, retrieveCustomerFromCRMZ and suspendCustomerInCRMZ as they are modular and has seperation of concerns

Correct Answer: B

Implement different system APIs named createCustomer, amendCustomer, retrieveCustomer and suspendCustomer as they are modular and has seperation of concerns **********

>> It is quite normal to have a single API and different Verb + Resource combinations. However, this fits well for an Experience API or a Process API but not a best architecture style for System APIs. So, option with just one

customerManagement API is not the best choice here.

>> The option with APIs in createCustomerInCRMZ format is next close choice w.r.t modularization and less maintenance but the naming of APIs is directly coupled with the legacy system. A better foreseen approach would be to name your

APIs by abstracting the backend system names as it allows seamless replacement/migration of any backend system

anytime. So, this is not the correct choice too. >> createCustomer, amendCustomer, retrieveCustomer and

suspendCustomer is the right approach and is the best fit compared to other options as they are both modular and same time got the names decoupled from backend system and it has covered all requirements a System API needs.

QUESTION 4

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 5

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 APIs 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 API producer should be requested to run the old version in parallel with the new one

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

C. The API client code only needs to be changed if it needs to take advantage of the new features

D. The API clients need to update the code on their side and need to do full regression

Correct Answer: C