MCIA-LEVEL-1-MAINTENANCE Q&As

MuleSoft Certified Integration Architect - Level 1 MAINTENANCE

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

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

https://www.geekcert.com/mcia-level-1-maintenance.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

In one of the critical payment related mule application, transaction is being used . As an enhancement to implementation , scatter gather route is introduced which is also the part of transaction group. Scatter gather route has 4 routes.

What will be the behavior of the Mule application in case of error occurs in 4th route of the scatter-gather router and transaction needs to be rolled back?

A. Only errored route will be rolled back

B. All routes will be rolled back

C. Scatter Gather router cannot be part of transaction

Correct Answer: B

Scatter Gather: When running within a transaction, Scatter Gather does not execute in parallel. This means that the second route is executed after the first one is processed, the third after the second one, etc. In case of error, all routes will be rolled back

QUESTION 2

A leading e-commerce giant will use Mulesoft API\\'s on runtime fabric (RTF) to process customer orders. Some customer\\'s sensitive information such as credit card information is also there as a part of a API payload.

What approach minimizes the risk of matching sensitive data to the original and can convert back to the original value whenever and wherever required?

A. Apply masking to hide the sensitive information and then use API

B. manager to detokenize the masking format to return the original value

C. create a tokenization format and apply a tokenization policy to the API Gateway

D. Used both masking and tokenization

E. Apply a field level encryption policy in the API Gateway

Correct Answer: A

QUESTION 3

The implementation of a Process API must change. What is a valid approach that minimizes the impact of this change on API clients?

A. Implement required changes to the Process API implementation so that whenever possible, the Process API\\'s RAML definition remains unchanged

B. Update the RAML definition of the current Process API and notify API client developers by sending them links to the updated RAML definition

C. Postpone changes until API consumers acknowledge they are ready to migrate to a new Process API or API version

D. Implement the Process API changes in a new API implementation, and have the old API implementation return an HTTP status code 301 - Moved Permanently to inform API clients they should be calling the new API implementation

Correct Answer: A

*

Option B shouldn\\'t be used unless extremely needed, if RAML is changed, client needs to accommodate changes. Question is about minimizing impact on Client. So this is not a valid choice.

*

Option C isn\\'t valid as Business can\\'t stop for consumers acknowledgment.

*

Option D again needs Client to accommodate changes and isn\\'t viable option.

*

Best choice is A where RAML definition isn\\'t changed and underlined functionality is changed without any dependency on client and without impacting client.

QUESTION 4

An organization has chosen Mulesoft for their integration and API platform.

According to the Mulesoft catalyst framework, what would an integration architect do to create achievement goals as part of their business outcomes?

A. Measure the impact of the centre for enablement

B. build and publish foundational assets

C. agree upon KPI\\'s and help develop and overall success plan

D. evangelize API\\'s

Correct Answer: C

QUESTION 5

As a part of design , Mule application is required call the Google Maps API to perform a distance computation. The application is deployed to cloudhub. At the minimum what should be configured in the TLS context of the HTTP request configuration to meet these requirements?

A. The configuration is built-in and nothing extra is required for the TLS context

B. Request a private key from Google and create a PKCS12 file with it and add it in keyStore as a part of TLS context

C. Download the Google public certificate from a browser, generate JKS file from it and add it in key store as a part of

TLS context

D. Download the Google public certificate from a browser, generate a JKS file from it and add it in Truststore as part of the TLS context

Correct Answer: A

Latest MCIA-LEVEL-1-MAINTENANCE Dumps | MCIA-LEVEL-1-MAINTENANCE VCE Dumps | MCIA-LEVEL-1-MAINTENANCE Practice Test