



Salesforce

Exam Questions Salesforce-MuleSoft-Developer-II

Salesforce Certified MuleSoft Developer 2 (SP24)

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

A Mule application includes a subflow containing a Scatter.Gather scope. Within each leg of the Scatter.Gather, an HTTP connector calls a PUT endpoint to modify records in different upstream system. The subflow is called inside an Unit successful scope to retry if a transitory exception is raised.

A technical spike is being performed to increase reliability of the Mule application. Which steps should be performed within the Mule flow above the ensure idempotent behavior?

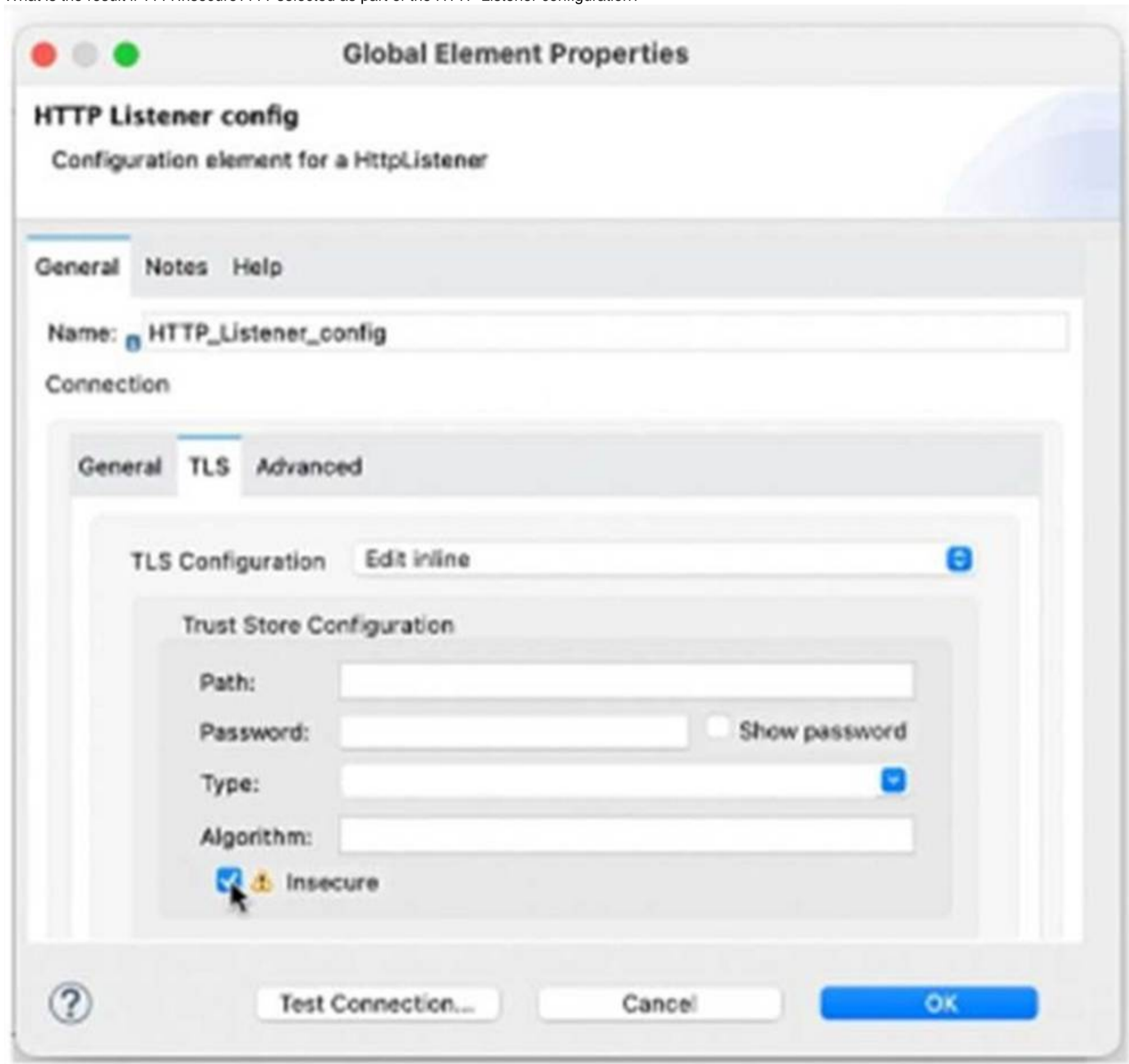
- A. Change the PUT requests inside the Scatter-Gather to POST requests
- B. Ensure an error-handling flow performs corrective actions to roll back all changes if any leg of the Scatter-Gather fails
- C. Remove the Put requests from the Scatter-Getter and perform them sequentially
- D. None, the flow already exhibits idempotent behavior

Answer: B

NEW QUESTION 2

Refer to the exhibit.

What is the result if Insecure selected as part of the HTTP Listener configuration?



- A. The HTTP Listener will trust any certificate presented by the HTTP client
- B. The HTTP Listener will accept any unauthenticated request
- C. The HTTP listener will only accept HTTP requests
- D. Mutual TLS authentication will be enabled between this HTTP Listener and an HTTP client

Answer: C

NEW QUESTION 3

When implementing a synchronous API where the event source is an HTTP Listener, a developer needs to return the same correlation ID back to the caller in the HTTP response header.
How can this be achieved?

- A. Enable the auto-generate CorrelationID option when scaffolding the flow
- B. Enable the CorrelationID checkbox in the HTTP Listener configuration
- C. Configure a custom correlation policy
- D. NO action is needed as the correlation ID is returned to the caller in the response header by default

Answer: D

NEW QUESTION 4

A developer deploys an API to CloudHub and applies an OAuth policy on API Manager. During testing, the API response is slow, so the developer reconfigures the API so that the out-of-the-box HTTP Caching policy is applied first, and the OAuth API policy is applied second.
What will happen when an HTTP request is received?

- A. In case of a cache hit, both the OAuth and HTTP Caching policies are evaluated; then the cached response is returned to the caller
- B. In case of a cache hit, only the HTTP Caching policy is evaluating; then the cached response is returned to the caller
- C. In case of a cache miss, only the HTTP Caching policy is evaluated; then the API retrieves the data from the API implementation, and the policy stores the data to be cached in Object Store
- D. In case of a cache miss, both the OAuth and HTTP Caching policies are evaluated; then the API retrieves the data from the API implementation, and the policy does not store the data in Object Store

Answer: B

NEW QUESTION 5

A mule application exposes an API for creating payments. An Operations team wants to ensure that the Payment API is up and running at all times in production.
Which approach should be used to test that the payment API is working in production?

- A. Create a health check endpoint that listens on a separate port and uses a separate HTTP Listener configuration from the API
- B. Configure the application to send health data to an external system
- C. Create a health check endpoint that reuses the same port number and HTTP Listener configuration as the API itself
- D. Monitor the Payment API directly sending real customer payment data

Answer: A

Explanation:

To test that the payment API is working in production, the developer should create a health check endpoint that listens on a separate port and uses a separate HTTP Listener configuration from the API. This way, the developer can isolate the health check endpoint from the API traffic and avoid affecting the performance or availability of the API.

The health check endpoint should return a simple response that indicates the status of the API, such as OK or ERROR. References: <https://docs.mulesoft.com/api-functionalmonitoring/afm-create-monitor#create-a-monitor>

NEW QUESTION 6

An organization uses CloudHub to deploy all of its applications.
How can a common-global-handler flow be configured so that it can be reused across all of the organization's deployed applications?

- A. Create a Mule plugin project. Create a common-global-error-handler flow inside the plugin project.
- B. Use this plugin as a dependency in all Mule applications. Import that configuration file in Mule applications.
- C. Create a common-global-error-handler flow in all Mule Applications. Refer to it flow-ref wherever needed.
- D. Create a Mule Plugin project. Create a common-global-error-handler flow inside the plugin project.
- E. Use this plugin as a dependency in all Mule applications.
- F. Create a Mule domain project. Create a common-global-error-handler flow inside the domain project.
- G. Use this domain project as a dependency.

Answer: C

NEW QUESTION 7

Which command is used to convert a JKS keystore to PKCS12?

- A. `keytool-importkeystore -srckeystore keystore.p12 -srcstoretype PKCS12 -destkeystore keystore.jks -deststoretype JKS`
- B. `keytool-importkeystore -srckeystore keystore.p12 -srcstoretype JKS -destkeystore keystore.p12 -deststoretype PKCS12`
- C. `keytool-importkeystore -srckeystore keystore.jks -srcstoretype JKS -destkeystore keystore.p13 -deststoretype PKCS12`
- D. `keytool-importkeystore -srckeystore keystore.jks -srcstoretype PKCS12 -destkeystore keystore.p12 -deststoretype JKS`

Answer: B

Explanation:

To convert a JKS keystore to PKCS12, the developer needs to use the `keytool-importkeystore` command with the following options: `-srckeystore keystore.jks -srcstoretype JKS -destkeystore keystore.p12 -deststoretype PKCS12`. This command imports all entries from a source JKS keystore (`keystore.jks`) into a destination PKCS12 keystore (`keystore.p12`). References:

<https://docs.oracle.com/en/java/javase/11/tools/keytool.html#GUID-5990A2E4-78E3-47B7-AE75-6D1826259549>

NEW QUESTION 8

What is the MuleSoft recommended method to encrypt sensitive property data?

- A. The encryption key and sensitive data should be different for each environment
- B. The encryption key should be identical for all environments
- C. The encryption key should be identical for all environments and the sensitive data should be different for each environment
- D. The encryption key should be different for each environment and the sensitive data should be the same for all environments

Answer: A

NEW QUESTION 9

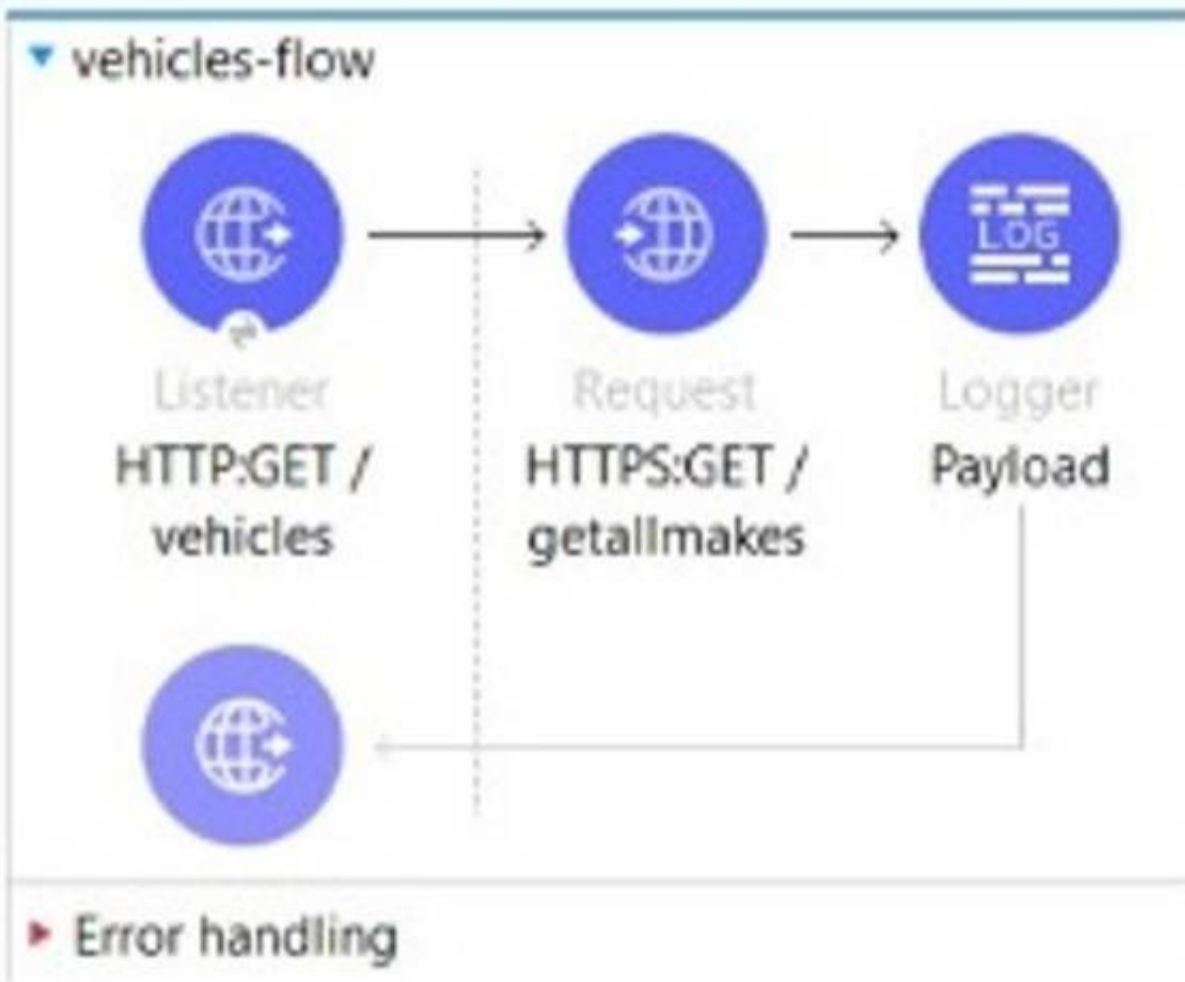
An order processing system is composed of multiple Mule application responsible for warehouse, sales and shipping. Each application communication using Anypoint MQ. Each message must be correlated against the original order ID for observability and tracing. How should a developer propagate the order ID as the correlation ID across each message?

- A. Use the underlying HTTP request of Anypoint MQ to set the `X-CORRELATION_ID` header to the order ID
- B. Set a custom Anypoint MQ user property to propagate the order ID and set the correlation ID in the receiving applications.
- C. Use the default correlation ID, Anypoint MQ will automatically propagate it.
- D. Wrap all Anypoint MQ Publish operations within a `With CorrelationID` scope from the Tracing module, setting the correlation ID to the order ID

Answer: D

NEW QUESTION 10

The flow is invoicing a target API. The API's protocol is HTTPS. The TLS configuration in the HTTP Request Configuration global element is set to None. A web client submits a request to `http://localhost:8081/vehicles`.



Configuration

Protocol:

Host:

Port:

Use persistent connections

Max connections:

Connection idle timeout:

Stream response

Response buffer size:

TLS Configuration

If the certificate of the target API is signed by a certificate authority (CA), what is true about the HTTP Request operation when the flow executes?

- A. The HTTP Request operation will succeed if the CA's certificate is present in the JRE's default keystore
- B. The HTTP Request operation will succeed if the CA's certificate is present in the JRE's default truststore.
- C. The HTTP Request operation will always succeed regardless of the CA
- D. The HTTP Request operation will always fail regardless of the CA

Answer: B

NEW QUESTION 10

Two APIs are deployed to a two-node on-prem cluster. Due to a requirements change, the two APIs must communicate to exchange data asynchronously.

- A. If the two APIs use the same domain, the VM Connector can be leveraged
- B. The VM Connector is used to inter-application communication, so it is not possible to use the VM Connector
- C. Instead of using the VM Connector use `<flow-ref>` directly
- D. It is not possible to use the VM Connector since the APIs are running in a cluster mode and each mode has its own set of VM Queues

Answer: A

NEW QUESTION 12

When a client and server are exchanging messages during the mTLS handshake, what is being agreed on during the cipher suite exchange?

- A. A protocol
- B. The TLS version
- C. An encryption algorithm
- D. The Public key format

Answer: C

NEW QUESTION 15

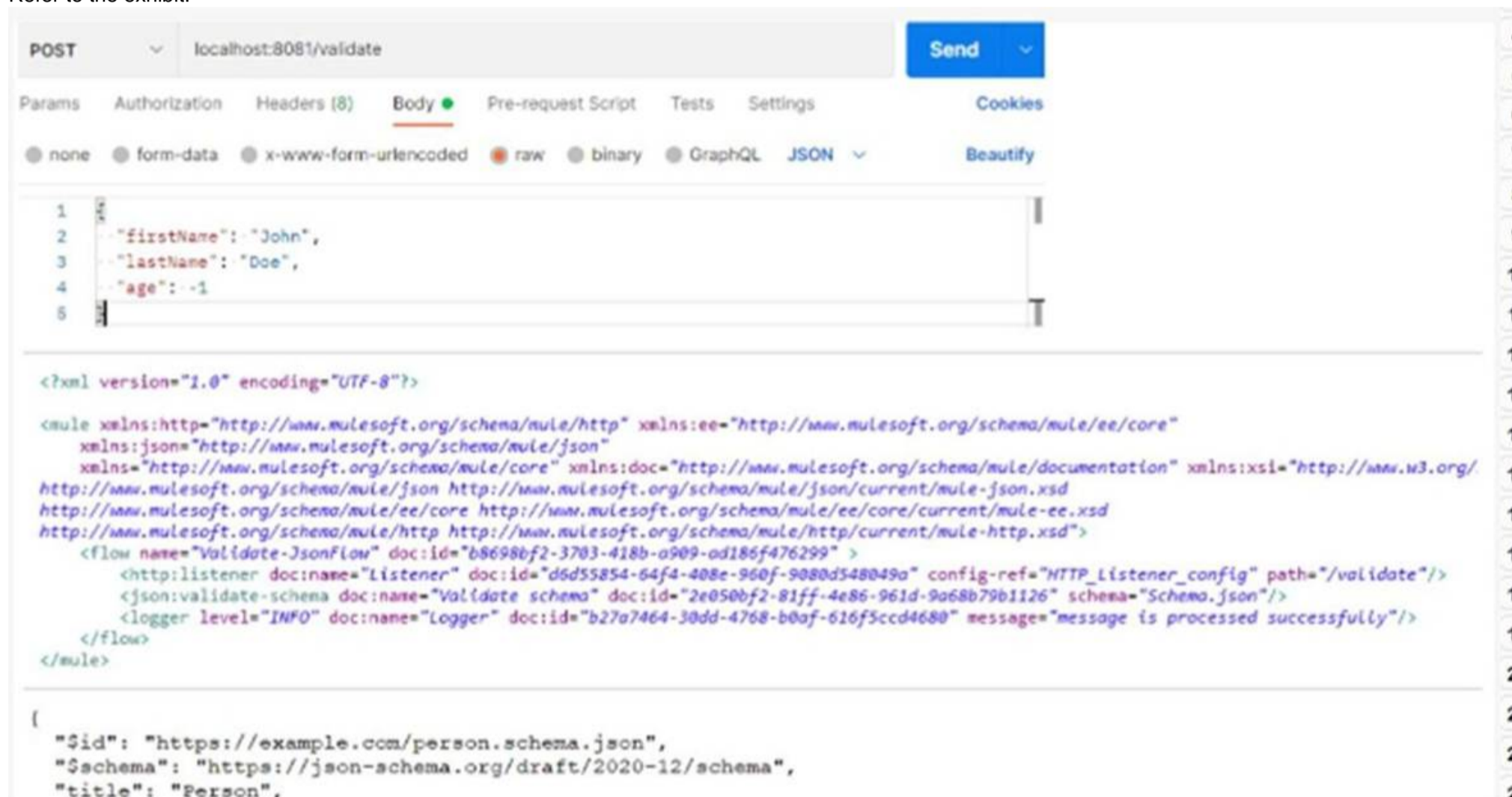
Which properties are mandatory on the HTTP Connector configuration in order to use the OAuth 2.0 AuthorizationCode grant type for authentication?

- A. External callback URL, access token URL, client ID response access token
- B. Token URL, authorization URL, client ID, client secret local callback URL
- C. External callback URL, access token URL, client ID, response refresh token
- D. External callback URL, access token URL, local authorization URL, authorization URL, client ID, client secret

Answer: D

NEW QUESTION 19

Refer to the exhibit.



```

POST localhost:8081/validate
Body
JSON
{
  "firstName": "John",
  "lastName": "Doe",
  "age": -1
}

<?xml version="1.0" encoding="UTF-8"?>
<mule xmlns:http="http://www.mulesoft.org/schema/mule/http" xmlns:ee="http://www.mulesoft.org/schema/mule/ee/core"
  xmlns:json="http://www.mulesoft.org/schema/mule/json"
  xmlns="http://www.mulesoft.org/schema/mule/core" xmlns:doc="http://www.mulesoft.org/schema/mule/documentation" xmlns:xsi="http://www.w3.org/
  http://www.mulesoft.org/schema/mule/json http://www.mulesoft.org/schema/mule/json/current/mule-json.xsd
  http://www.mulesoft.org/schema/mule/ee/core http://www.mulesoft.org/schema/mule/ee/core/current/mule-ee.xsd
  http://www.mulesoft.org/schema/mule/http http://www.mulesoft.org/schema/mule/http/current/mule-http.xsd">
  <flow name="Validate-JsonFlow" doc:id="b8698bf2-3703-418b-a909-ad186f476299" >
    <http:listener doc:name="Listener" doc:id="d6d55854-64f4-408e-960f-9080d548049a" config-ref="HTTP_Listener_config" path="/validate"/>
    <json:validate-schema doc:name="Validate schema" doc:id="2e050bf2-81ff-4e86-961d-9a68b79b1126" schema="Schema.json"/>
    <logger level="INFO" doc:name="Logger" doc:id="b27a7464-30dd-4768-b0af-616f5ccd4680" message="message is processed successfully"/>
  </flow>
</mule>

{
  "$id": "https://example.com/person.schema.json",
  "$schema": "https://json-schema.org/draft/2020-12/schema",
  "title": "Person",

```

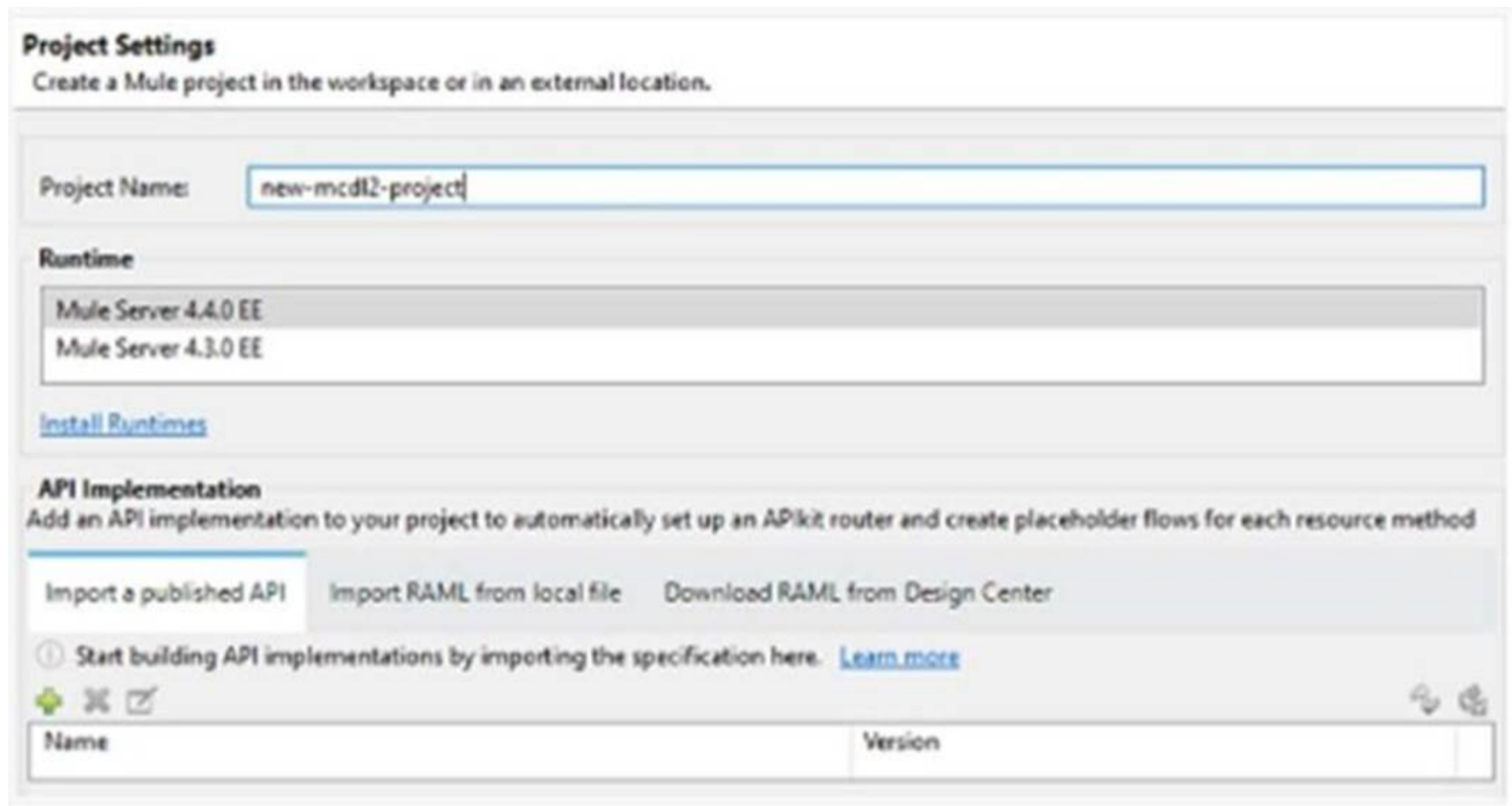
Based on the code snippet, schema.json file, and payload below, what is the outcome of the given code snippet when a request is sent with the payload?

- A. The Mule flow will execute successfully with status code 200, and the response will be the JSON sent in request
- B. The Mule flow will execute successfully with status code 204
- C. The Mule flow will throw the exception ??JSON:SCHEMA_NOT_HONOURED
- D. The Mule flow will execute successfully with status code 200m and a response will display themessage ??? Age in years which must equal to or greater than zero.????

Answer: C

NEW QUESTION 23

Refer to the exhibit.



When creating a new project, which API implementation allows for selecting the correct API version and scaffolding the flows from the API specification?

- A. Import a published API
- B. Generate a local RAML from anypoint Studio
- C. Download RAML from Design Center
- D. Import RAML from local file

Answer: C

NEW QUESTION 27

A Mule application deployed to multiple Cloudhub 2.0 replicas needs to temporarily persist large files over 10MB between flow executions, and routinely needs to query whether the file data exists on separate executions. How can this be achieved?

- A. Store the contents of the file on separate storage, and store the key and location of the file Object using Object Store v2
- B. Use an in-memory Object Store
- C. Store the key and full contents of the file in an Object Store
- D. Store the key and full contents of the file, caching the filename and location between requests

Answer: A

NEW QUESTION 32

Which plugin or dependency is required to unit test modules created with XML SDK?

- A. XMLUnit
- B. Junit
- C. MUnit Extensions Maven plugin
- D. MUnit Maven plugin

Answer: C

NEW QUESTION 37

.....

Relate Links

100% Pass Your Salesforce-MuleSoft-Developer-II Exam with ExamBible Prep Materials

<https://www.exambible.com/Salesforce-MuleSoft-Developer-II-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>