# MCD-LEVEL-2 Q&As

MuleSoft Certified Developer - Level 2 (Mule 4)

## Pass Mulesoft MCD-LEVEL-2 Exam with 100% Guarantee

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

**https://www.pass4itsure.com/mcd-level-2.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 a Mule project, Flow-1 contains a flow-ref to Flow-2 depends on data from Flow-1 to execute successfully.

Which action ensures the test suites and test cases written for Flow-1 and Flow-2 will executesuccessfully?

A. Chain together the test suites and test cases for Flow-1 and Flow-2

B. Use `\\'Set Event to pass the input that is needed, and keep the test cases for Flow-1 and Flow-2 independent

C. Use `\\'Before Test Case\\'\\' To collect data from Flow-1 test cases before running Flow-2 test cases

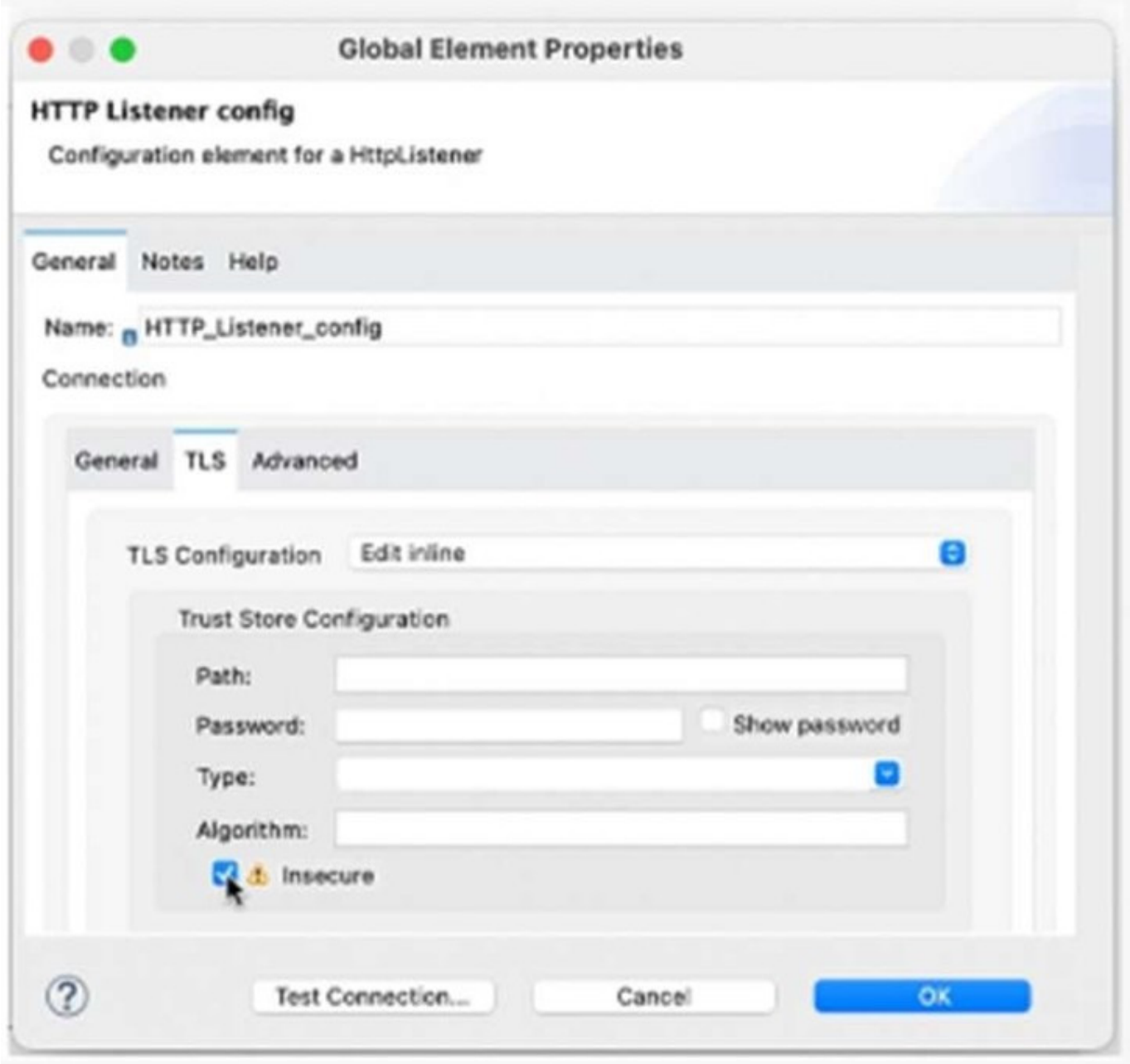
D. Use `After Test Case\\' to produce the data needed from Flow-1 test cases to pass to Flow-2 test cases

Correct Answer: B

To ensure the test suites and test cases written for Flow-1 and Flow-2 will execute successfully, the developer should use a Set Event processor to pass the input that is needed by Flow-2, and keep the test cases for Flow-1 and Flow-2 independent. This way, the developer can isolate the testing of each flow and avoid coupling them together. References:https://docs.mulesoft.com/munit/2.3/munit-test-flow

**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 Lister 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

Correct Answer: C

Based on the exhibit below, if `Insecure\\' is selected as part of the HTTP Listener configuration, the HTTP listener will only accept HTTP requests. This means that no TLS context will be configured for this listener and no encryption or authentication will be applied to incoming requests. The protocol attribute of this listener will be set to HTTP instead of HTTPS. References:https://docs.mulesoft.com/http-connector/1.6/http-listener-ref#insecure

**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

Correct Answer: D

When implementing a synchronous API where the event source is an HTTP Listener, Mule automatically propagates some message attributes between flows via outbound and inbound properties. One of these attributes is correlation ID,

which is returned to the caller in the response header by default as MULE_CORRELATION_ID.

References: https://docs.mulesoft.com/mule-runtime/4.3/about-mule-message#message-attributes

**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 it, 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 Cachingpolicies are evaluated; then the API retrieves the data from the API implementation, and the policy does not store the data in Object Store

Correct Answer: B

When an HTTP request is received and the HTTP Caching policy is applied first, it checks if there is a cached response for that request in Object Store. If there is a cache hit, meaning that a valid cached response exists, then only the HTTP Caching policy is evaluated and the cached response is returned to the caller without invoking the OAuth policy or the API implementation. If there is a cache miss, meaning that no valid cached response exists, then both the HTTP Caching policy and the OAuth policy are evaluated before invoking the API implementation.
References:https://docs.mulesoft.com/api-manager/2.x/http-caching-policy#policy-ordering

**QUESTION 5**

Mule application A is deployed to CloudHub and is using Object Store v2. Mute application B is also deployed to CloudHub.

Which approach can Mule application B use to remove values from Mule application A\\'S Object Store?

A. Object Storev2 REST API

B. CloudHub Connector

C. Object Store Connector

D. CloudHub REST API

Correct Answer: A

To remove values from Mule application A\\'s Object Store v2, Mule application B can use Object Store v2 REST API. This API allows performing operations on Object Store v2 resources using HTTP methods, such as GET, POST, PUT, and DELETE. Mule application B can use the DELETEmethod to remove values from Mule application A\\'s Object Store v2 by specifying the object store ID and the key of the value to delete.
References:https://docs.mulesoft.com/object-store/ osv2-apis