SALESFORCE-MULESOFT-DEVELOPER-II Q&As

Salesforce Certified MuleSoft Developer 2 (SP24)

Pass Salesforce SALESFORCE-MULESOFT-DEVELOPER-II Exam with 100% Guarantee

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

https://www.geekcert.com/salesforce-mulesoft-developer-ii.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A company deploys 10 public APIs to CloudHub. Each API has its individual health endpoint defined. The platform operation team wants to configure API Functional Monitoring to monitor the health of the APIs periodically while minimizing

operational overhead and cost.

How should API Functional Monitoring be configured?

A. From one public location with each API in its own schedule

B. From one private location with all 10 APIs in a single schedule

C. From one public location with all 10 APIs in a single schedule

D. From 10 public locations with each API in its own schedule

Correct Answer: C

To configure API Functional Monitoring to monitor the health of 10 public APIs periodically while minimizing operational overhead and cost, the developer should use one public location with all 10 APIs in a single schedule. A public location is a worker that runs in a CloudHub shared environment, which is cheaper and easier to maintain than a private location. A single schedule allows running all 10 APIs tests at the same time and frequency, which reduces complexity and resource consumption. https://docs.mulesoft.com/functional-monitoring/fm-create-monitor#create-a-monitor

QUESTION 2

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

Correct Answer: C

A cipher suite is a set of cryptographic algorithms that are used to secure the communication between a client and a server. A cipher suite consists of four components: a key exchange algorithm, an authentication algorithm, an encryption

algorithm, and a message authentication code (MAC) algorithm. During the cipher suite exchange, the client and the server agree on which encryption algorithm to use for encrypting and decrypting the data.

Reference:

https://docs.mulesoft.com/mule-runtime.3/tls-configuration#cipher-suites

QUESTION 3

A company with MuleSoft Titanium develops a Salesforce System API using MuleSoft out-of-the-box Salesforce Connector and deploys the API to CloudHub. Which steps provide the average number of requests and average response time of the Salesforce Connector?

A. Access Anypoint Monitoring\\'s built-in dashboard. Select a resource. Locate the information under the Connectors tab.

B. Access Anypoint Monitoring\\'s built-in dashboard Seclect a resource. Create a custom dashboard to retrieve the information.

C. Access Anypoint Monitoring built-in dashboard. Select a resource. Locate the information under Log Manager

D. Change the API Implementation to capture the information in the log. Retrieve the information from the log file.

Correct Answer: A

To get the average number of requests and average response time of the Salesforce Connector, the developer should access Anypoint Monitoring\\'s built-in dashboard, select a resource (such as an application or an API), and locate the information under the Connectors tab. The Connectors tab shows metrics for each connector used by the resource, such as average requests per minute, average response time, and failures. https:// docs.mulesoft.com/monitoring/built-indashboard-reference

QUESTION 4

Which properties are mandatory on the HTTP Connector configuration in order to use the OAuth 2.0 Authorization Code 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

Correct Answer: D

To use the OAuth 2.0 Authorization Code grant type for authentication, the HTTP Connector configuration requires the following properties: token URL, authorization URL, client ID, client secret, and local callback URL. The token URL is the endpoint of the authorization server that provides access tokens. The authorization URL is the endpoint of the authorization server that initiates the user consent flow. The client ID and client secret are the credentials of the Mule application registered with the authorization server. The local callback URL is the endpoint of the Mule application that receives the authorization code from the authorization server. Reference: https://docs.mulesoft.com/http-connector.6/http-authentication#oauth-2-0

QUESTION 5

A Mule API receives a JSON payload and updates the target system with the payload. The developer uses JSON schemas to ensure the data is valid. How can the data be validation before posting to the target system?

A. Use a DataWeave 2.09 transform operation, and at the log of the DataWeave script, add: %dw 2.0 Import.json-

moduls

B. Using the DataWeave if Else condition test the values of the payload against the examples included in the schema

C. Apply the JSON Schema policy in API Manager and reference the correct schema in the policy configuration

D. Add the JSON module dependency and add the validate-schema operation in the flow, configured to reference the schema

Correct Answer: D

To validate the data before posting to the target system, the developer should add the JSON module dependency and add the validate-schema operation in the flow, configured to reference the schema. The JSON module provides a validate-schema operation that validates a JSON payload against a JSON schema and throws an error if the payload is invalid. https://docs.mulesoft.com/jsonmodule/1.1/json-validate-schema