DirectCertify

Unlock Your Potential, Certify Your Success

Salesforce

Mule-Dev-301 Exam

Salesforce Certified MuleSoft Developer II

Exam Latest Version: 6.0

DEMO Version

Full Version Features:

• 90 Days Free Updates

• 30 Days Money Back Guarantee

• Instant Download Once Purchased

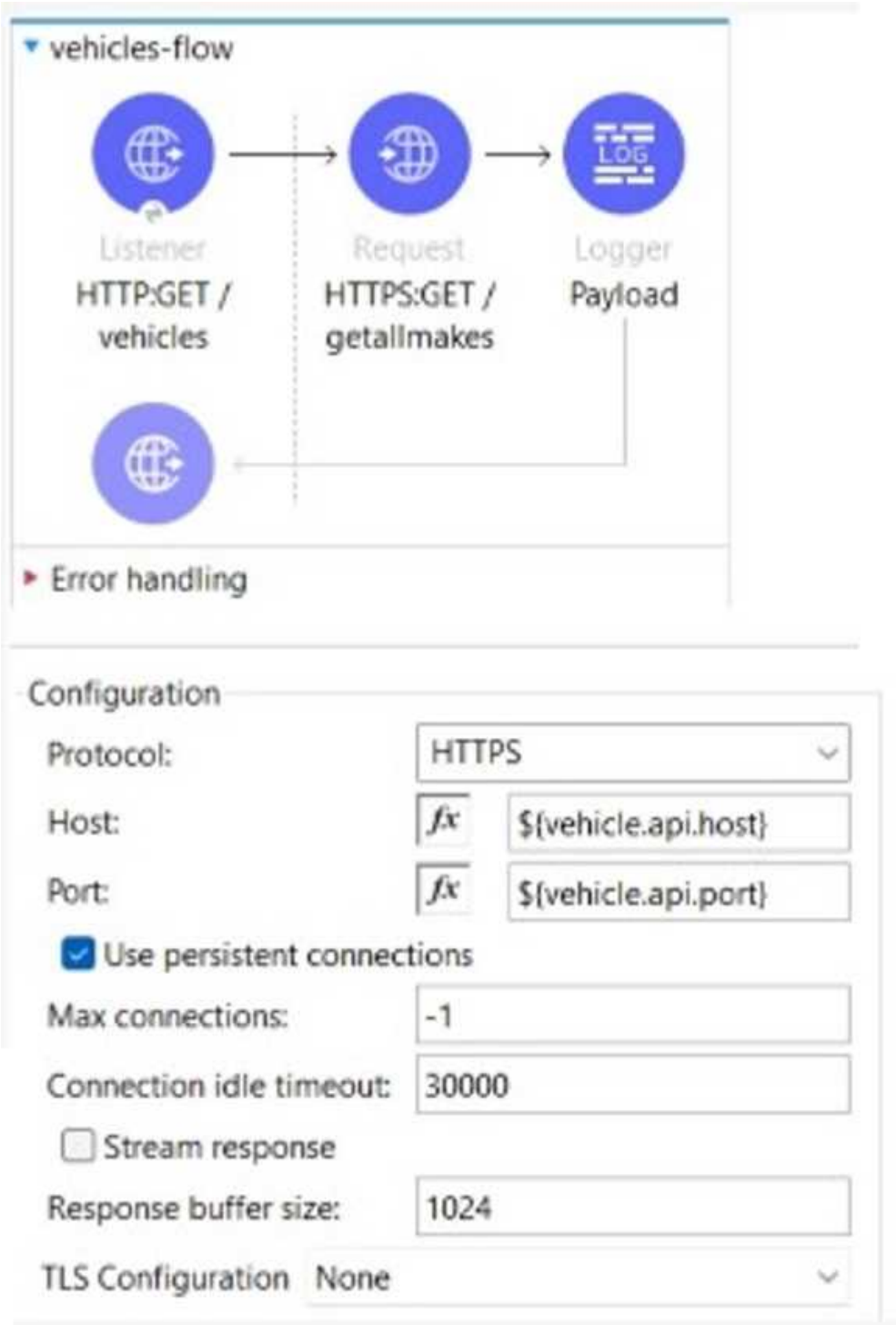
• 24 Hours Live Chat Support

Full version is available at link below with affordable price.

https://www.directcertify.com/salesforce/mule-dev-301

Question 1. (Single Select)

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.



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

Correct Answer: B

Explanation:

The HTTP Request operation will use the default truststore of the JRE to validate the certificate of the target API. If the CA's certificate is present in the truststore, the operation will succeed. Otherwise, it will fail with a handshake exception.
https://docs.mulesoft.com/mule-runtime/4.3/tls-configuration#tls-default

Question 2. (Single Select)

Which statement is true about using mutual TLS to secure an application?

A: Mutual TLS requires a hardware security module to be used
B: Mutual TLS authenticates the identity of the server before the identity of the client
C: Mutual TLS ensures only authorized end users are allowed to access an endpoint
D: Mutual TLS increases the encryption strength versus server-side TLS alone

Correct Answer: B

Explanation:

Mutual TLS (mTLS) is an extension of TLS that requires both parties (client and server) to present their certificates to each other during the handshake process. This way, both parties can verify each other's identity and establish a secure connection. The authentication of the server happens before the authentication of the client, as the server sends its certificate first and then

requests the client's certificate.
https://docs.mulesoft.com/mule-runtime/4.3/tls-configuration#mutual-authentication

Question 3. (Single Select)

Which statement is true when using XML SDK for creating custom message processors?

A: Properties are fields defined by an end user of the XML SDK component and serve as a global configuration for the entire Mule project in which they are used
B: An XML SDK provides both inbound and outbound operations
C: Operations can be reused in recursive calls
D: All operations are public

Correct Answer: A

Explanation:

When using XML SDK for creating custom message processors, all operations are public by default and can be used by any Mule application that imports them. There is no way to make an operation private or protected in XML SDK.
https://docs.mulesoft.com/mule-sdk/1.1/xml-sdk#operations

Question 4. (Single Select)

Which type of cache invalidation does the Cache scope support without having to write any additional code?

A: Write-through invalidation
B: White-behind invalidation
C: Time to live
D: Notification-based invalidation

Correct Answer: C

Explanation:

The Cache scope supports time to live (TTL) as a cache invalidation strategy without having to write any additional code. TTL specifies how long the cached response is valid before it expires and needs to be refreshed. The Cache scope also supports custom invalidation strategies using MEL or DataWeave expressions.
https://docs.mulesoft.com/mule-runtime/4.3/cache-scope#cache_invalidation

Question 5. (Single Select)

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

Correct Answer: A

Explanation:

The MuleSoft recommended method to encrypt sensitive property data is to use the Secure Properties Tool that comes with Anypoint Studio. This tool allows encrypting properties files with a secret key and then decrypting them at runtime using the same key. The encryption key and sensitive data should be different for each environment to ensure security and avoid accidental exposure of sensitive data.
https://docs.mulesoft.com/mule-runtime/4.3/secure-configuration-properties

DirectCertify

Unlock Your Potential, Certify Your Success

Full version is available at link below with affordable price.

https://www.directcertify.com/salesforce/mule-dev-301

30% Discount Coupon Code: LimitedTime2025