MCIA-LEVEL-1-MAINTENANCE$^{Q\&As}$

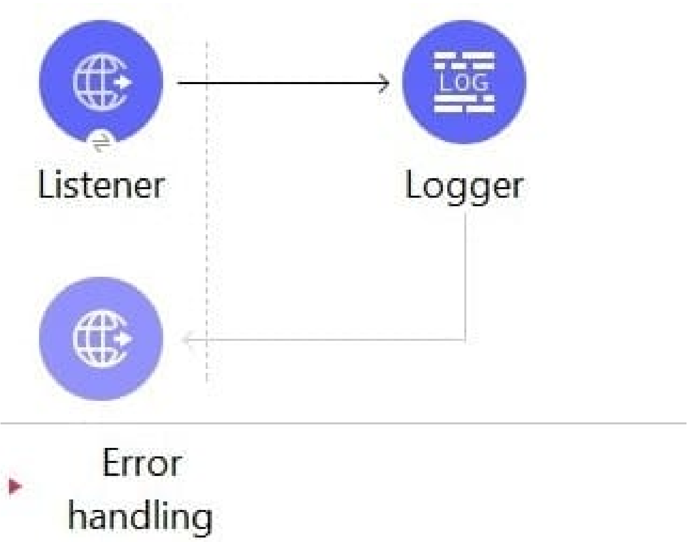
MuleSoft Certified Integration Architect - Level 1 MAINTENANCE

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

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

QUESTION 1

Refer to the exhibit.



The HTTP Listener and the Logger are being handled from which thread pools respectively?

A. CPU_INTENSIVE and Dedicated Selector pool

B. UBER and NONBLOCKING

C. Shared Selector Pool and CPU LITE

D. BLOCKING _IO and UBER

Correct Answer: C

QUESTION 2

A customer wants to use the mapped diagnostic context (MDC) and logging variables to enrich its logging and improve tracking by providing more context in the logs.

The customer also wants to improve the throughput and lower the latency of message processing.

As an Mulesoft integration architect can you advise, what should the customer implement to meet these requirements?

A. Use synchronous logging and use pattern layout with [%MDC] in the log4j2.xml configuration file and then configure the logging variables

B. Useasync logger at the level greater than INFO and use pattern layout with [%MDC] in the log4j2,xml configuration file and then configure the logging variables

C. Useasync logger at the level equal to DEBUG orTRACEand use pattern layout with [%MDC] in the log4j2.xml configuration file and then configure the logging variables

D. Use synchronous logging at the INFO DEBUG or Trace level and use pattern layout with [%MDC] in the log4j2.xml configuration file and then configure the logging variables

Correct Answer: B

QUESTION 3

A Mule application is running on a customer-hosted Mule runtime in an organization\\'s network. The Mule application acts as a producer of asynchronous Mule events. Each Mule event must be broadcast to all interested external consumers

outside the Mule application. The Mule events should be published in a way that is guaranteed in normal situations and also minimizes duplicate delivery in less frequent failure scenarios.

The organizational firewall is configured to only allow outbound traffic on ports 80 and 443. Some external event consumers are within the organizational network, while others are located outside the firewall.

What Anypoint Platform service is most idiomatic (used for its intended purpose) for publishing these Mule events to all external consumers while addressing the desired reliability goals?

A. CloudHub VM queues

B. Anypoint MQ

C. Anypoint Exchange

D. CloudHub Shared Load Balancer

Correct Answer: B

Set the Anypoint MQ connector operation to publish or consume messages, or to accept (ACK) or not accept (NACK) a message. Reference: https://docs.mulesoft.com/mq/

QUESTION 4

An organization has several APIs that accept JSON data over HTTP POST. The APIs are all publicly available and are associated with several mobile applications and web applications. The organization does NOT want to use any authentication or compliance policies for these APIs, but at the same time, is worried that some bad actor could send payloads that could somehow compromise the applications or servers running the API implementations. What out-of-thebox Anypoint Platform policy can address exposure to this threat?

A. Apply a Header injection and removal policy that detects the malicious data before it is used

B. Apply an IP blacklist policy to all APIs; the blacklist will Include all bad actors

C. Shut out bad actors by using HTTPS mutual authentication for all API invocations

D. Apply a JSON threat protection policy to all APIs to detect potential threat vectors

Correct Answer: D

We need to note few things about the scenario which will help us in reaching the correct solution. Point 1 : The APIs are all publicly available and are associated with several mobile applications and web applications. This means Apply an IP blacklist policy is not viable option. as blacklisting IPs is limited to partial web traffic. It can\\'t be useful for traffic from mobile application Point 2 : The organization does NOT want to use any authentication or compliance policies for these APIs. This means we can not apply HTTPS mutual authentication scheme. Header injection or removal will not help the purpose. By its nature, JSON is vulnerable to JavaScript injection. When you parse the JSON object, the malicious code inflicts its damages. An inordinate increase in the size and depth of the JSON payload can indicate injection. Applying the JSON threat protection policy can limit the size of your JSON payload and thwart recursive additions to the JSON hierarchy. Hence correct answer is Apply a JSON threat protection policy to all APIs to detect potential threat vectors

QUESTION 5

A company is building an application network and has deployed four Mule APIs: one experience API, one process API, and two system APIs. The logs from all the APIs are aggregated in an external log aggregation tool. The company wants to trace messages that are exchanged between multiple API implementations. What is the most idiomatic (based on its intended use) identifier that should be used to implement Mule event tracing across the multiple API implementations?

A. Mule event ID

B. Mule correlation ID

C. Client\\'s IP address

D. DataWeave UUID

Correct Answer: B

Correct answer is Mule correlation ID By design, Correlation Ids cannot be changed within a flow in Mule 4 applications and can be set only at source. This ID is part of the Event Context and is generated as soon as the message is received by the application. When a HTTP Request is received, the request is inspected for "X-Correlation-Id" header. If "X-Correlation-Id" header is present, HTTP connector uses this as the Correlation Id. If "X- Correlation-Id" header is NOT present, a Correlation Id is randomly generated. For Incoming HTTP Requests: In order to set a custom Correlation Id, the client invoking the HTTP request must set "X-Correlation-Id" header. This will ensure that the Mule Flow uses this Correlation Id. For Outgoing HTTP Requests: You can also propagate the existing Correlation Id to downstream APIs. By default, all outgoing HTTP Requests send "X- Correlation-Id" header. However, you can choose to set a different value to "X-Correlation- Id" header or set "Send Correlation Id" to NEVER.