MCIA-LEVEL-1-MAINTENANCE Q&As

MuleSoft Certified Integration Architect - Level 1 MAINTENANCE

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

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

https://www.passapply.com/mcia-level-1-maintenance.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

What is true about automating interactions with Anypoint Platform using tools such as Anypoint Platform REST API\\'s, Anypoint CLI or the Mule Maven plugin?

A. By default, the Anypoint CLI and Mule Maven plugin are not included in the Mule runtime

B. Access to Anypoint Platform API;s and Anypoint CLI can be controlled separately thruough the roles and permissions in Anypoint platform, so that specific users can get access to Anypoint CLI while others get access to the platform API\\'s

C. Anypoint Platform API\\'s can only automate interactions with CloudHub while the Mule maven plugin is required for deployment to customer hosted Mule runtimes

D. API policies can be applied to the Anypoint platform API\\'s so that only certain LOS\\'s has access to specific functions

Correct Answer: A

Correct answer is By default, the Anypoint CLI and Mule Maven plugin are not included in the Mule runtime Maven is not part of runtime though it is part of studio. You do not need it to deploy in order to deploy your app. Same is the case with

CLI.

QUESTION 2

An organization is evaluating using the CloudHub shared Load Balancer (SLB) vs creating a CloudHub dedicated load balancer (DLB). They are evaluating how this choice affects the various types of certificates used by CloudHub deployed Mule applications, including MuleSoft-provided, customer-provided, or Mule application-provided certificates. What type of restrictions exist on the types of certificates for the service that can be exposed by the CloudHub Shared Load Balancer (SLB) to external web clients over the public internet?

A. Underlying Mule applications need to implement own certificates

B. Only MuleSoft provided certificates can be used for server side certificate

C. Only self signed certificates can be used

D. All certificates which can be used in shared load balancer need to get approved by raising support ticket

Correct Answer: B

Correct answer is Only MuleSoft provided certificates can be used for server side certificate

*

The CloudHub Shared Load Balancer terminates TLS connections and uses its own server-side certificate.

*

You would need to use dedicated load balancer which can enable you to define SSL configurations to provide custom certificates and optionally enforce two-way SSL client authentication.

*

To use a dedicated load balancer in your environment, you must first create an Anypoint VPC. Because you can associate multiple environments with the same Anypoint VPC, you can use the same dedicated load balancer for your different

environments.

Additional Info on SLB Vs DLB:

	Shared Load Balancer	Dedicated Load Balancer
VPC	Shared VPC (Mulesoft)	VPC (Customer)
Default Load Balancer	Cloudhub provides Deault Shared Load Balancer available in All Environment	Need to Purchase
Organization Use	Multiple Oragnization	Specific to Organization
Certificate	Mulesoft Certificate	Organization Certificate
TLS Support	Yes	Yes
URL Mapping	Fixed URL Mapping	Customer URL Mapping
Timeout	30 Sec Session Timeout	Custom Timeout
Ports	Public Port {80 : 8081, 443 : 8082}	Private Port {80 : 8091, 443 : 8092}
Fashion	Round Robin	Round Robin
Supports HTTPS Protocol	Yes	Yes
Worker Assignment	No	Yes
IP Blacklisting/ Whitelisting	No	Yes
	https://docs.mulesoft.com/runtime-manager/lb-whitelists	
Configure Custom Domain	No	Yes
Custom Certificate	No	Yes
Rate Limit	Lower Rate Limit and applied According to Region	Higher Rate Limit Threshold
VPC	Anypoint VPC optional	Can't Use DLB without Anypoint VPC

QUESTION 3

A new upstream API Is being designed to offer an SLA of 500 ms median and 800 ms maximum (99th percentile) response time. The corresponding API implementation needs to sequentially invoke 3 downstream APIs of very similar complexity. The first of these downstream APIs offers the following SLA for its response time: median: 100 ms, 80th percentile: 500 ms, 95th percentile: 1000 ms. If possible, how can a timeout be set in the upstream API for the

invocation of the first downstream API to meet the new upstream API\\'s desired SLA?

A. Set a timeout of 100 ms; that leaves 400 ms for the other two downstream APIs to complete

B. Do not set a timeout; the Invocation of this API Is mandatory and so we must wait until it responds

C. Set a timeout of 50 ms; this times out more invocations of that API but gives additional room for retries

D. No timeout is possible to meet the upstream API\\'s desired SLA; a different SLA must be negotiated with the first downstream API or invoke an alternative API

Correct Answer: D

Before we answer this question , we need to understand what median (50th percentile) and 80th percentile means. If the 50th percentile (median) of a response time is 500ms that means that 50% of my transactions are either as fast or faster than 500ms. If the 90th percentile of the same transaction is at 1000ms it means that 90% are as fast or faster and only 10% are slower. Now as per upstream SLA , 99th percentile is 800 ms which means 99% of the incoming requests should have response time less than or equal to 800 ms. But as per one of the backend API , their 95th percentile is 1000 ms which means that backend API will take 1000 ms or less than that for 95% of. requests. As there are three API invocation from upstream API , we can not conclude a timeout that can be set to meet the desired SLA as backend SLA\\'s do not support it. Let see why other answers are not correct. 1) Do not set a timeout --> This can potentially violate SLA\\'s of upstream API 2) Set a timeout of 100 ms; ---> This will not work as backend API has 100 ms as median meaning only 50% requests will be answered in this time and we will get timeout for 50% of the requests. Important thing to note here is, All APIs need to be executed sequentially, so if you get timeout in first API, there is no use of going to second and third API. As a service provider you wouldn\\'t want to keep 50% of your consumers dissatisfied. So not the best option to go with. *To quote an example: Let\\'s assume you have built an API to update customer contact details.

-First API is fetching customer number based on login credentials

-Second API is fetching Info in 1 table and returning unique key

-Third API, using unique key provided in second API as primary key, updating remaining details * Now consider, if API times out in first API and can\\'t fetch customer number, in this case, it\\'s useless to call API 2 and 3 and that is why question mentions specifically that all APIs need to be executed sequentially. 3) Set a timeout of 50 ms --> Again not possible due to the same reason as above Hence correct answer is No timeout is possible to meet the upstream API\\'s desired SLA; a different SLA must be negotiated with the first downstream API or invoke an alternative API

QUESTION 4

An insurance company is using a CIoudHub runtime plane. As a part of requirement, email alert should be sent to internal operations team every time of policy applied to an API instance is deleted As an integration architect suggest on how this requirement be met?

A. Use audit logs in Anypoint platform to detect a policy deletion and configure the Audit logs alert feature to send an email to the operations team

B. Use Anypoint monitoring to configure an alert that sends an email to the operations team every time a policy is deleted in API manager

C. Create a custom connector to be triggered every time of policy is deleted in API manager

D. Implement a new application that uses the Audit log REST API to detect the policy deletion and send an email to operations team the SMTP connector

Correct Answer: D

QUESTION 5

An organization is designing a mule application to support an all or nothing transaction between serval database operations and some other connectors so that they all roll back if there is a problem with any of the connectors. Besides the database connector , what other connector can be used in the transaction.

A. VM

B. Anypoint MQ

C. SFTP

D. ObjectStore

Correct Answer: A

Correct answer is VM VM support Transactional Type. When an exception occur, The transaction rolls back to its original state for reprocessing. This feature is not supported by other connectors. Here is additional information about Transaction management:

	Shared Load Balancer	Dedicated Load Balancer
VPC	Shared VPC (Mulesoft)	VPC (Customer)
Default Load Balancer	Cloudhub provides Deault Shared Load Balancer available in All Environment	Need to Purchase
Organization Use	Multiple Oragnization	Specific to Organization
Certificate	Mulesoft Certificate	Organization Certificate
TLS Support	Yes	Yes
URL Mapping	Fixed URL Mapping	Customer URL Mapping
Timeout	30 Sec Session Timeout	Custom Timeout
Ports	Public Port {80 : 8081, 443 : 8082}	Private Port {80 : 8091, 443 : 8092}
Fashion	Round Robin	Round Robin
Supports HTTPS Protocol	Yes	Yes
Worker Assignment	No	Yes
IP Blacklisting/ Whitelisting	No	Yes
	https://docs.mulesoft.com/runtime-manager/lb-whitelists	
Configure Custom Domain	No	Yes
Custom Certificate	No	Yes
Rate Limit	Lower Rate Limit and applied According to Region	Higher Rate Limit Threshold
VPC	Anypoint VPC optional	Can't Use DLB without Anypoint VPC

Latest MCIA-LEVEL-1-MAINTENANCE Dumps | MCIA-LEVEL-1-MAINTENANCE PDF Dumps | MCIA-LEVEL-1-MAINTENANCE Braindumps