MCPA-LEVEL1 Q&As

MuleSoft Certified Platform Architect - Level 1

QUESTION 1

An API has been updated in Anypoint exchange by its API producer from version 3.1.1 to 3.2.0 following accepted semantic versioning practices and the changes have been communicated via the APIs public portal. The API endpoint does NOT change in the new version. How should the developer of an API client respond to this change?

A. The API producer should be requested to run the old version in parallel with the new one

B. The API producer should be contacted to understand the change to existing functionality

C. The API client code only needs to be changed if it needs to take advantage of the new features

D. The API clients need to update the code on their side and need to do full regression

Correct Answer: C

QUESTION 2

The responses to some HTTP requests can be cached depending on the HTTP verb used in the request. According to the HTTP specification, for what HTTP verbs is this safe to do?

A. PUT, POST, DELETE

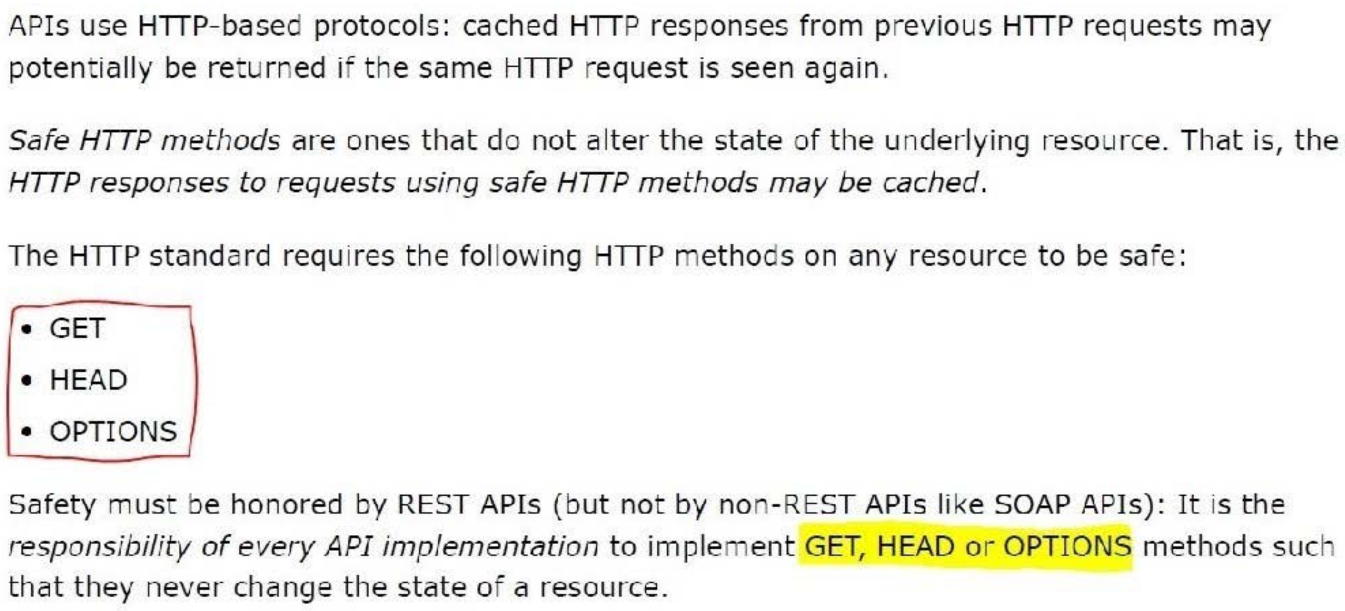
B. GET, HEAD, POST

C. GET, PUT, OPTIONS

D. GET, OPTIONS, HEAD

Correct Answer: D

GET, OPTIONS, HEAD



APIs use HTTP-based protocols: cached HTTP responses from previous HTTP requests may potentially be returned if the same HTTP request is seen again.

Safe HTTP methods are ones that do not alter the state of the underlying resource. That is, the *HTTP responses to requests using safe HTTP methods may be cached*.

The HTTP standard requires the following HTTP methods on any resource to be safe:

- GET
- HEAD
- OPTIONS

Safety must be honored by REST APIs (but not by non-REST APIs like SOAP APIs): It is the *responsibility of every API implementation* to implement GET, HEAD or OPTIONS methods such that they never change the state of a resource.

http://restcookbook.com/HTTP%20Methods/idempotency/

QUESTION 3

An Anypoint Platform organization has been configured with an external identity provider (IdP) for identity management and client management. What credentials or token must be provided to Anypoint CLI to execute commands against the Anypoint Platform APIs?

A. The credentials provided by the IdP for identity management

B. The credentials provided by the IdP for client management

C. An OAuth 2.0 token generated using the credentials provided by the IdP for client management

D. An OAuth 2.0 token generated using the credentials provided by the IdP for identity management

Correct Answer: A

The credentials provided by the IdP for identity management *** Reference: https://docs.mulesoft.com/runtime-manager/anypoint-platform- cli#authentication

>> There is no support for OAuth 2.0 tokens from client/identity providers to authenticate via Anypoint CLI. Only possible tokens are "bearer tokens" that too only generated using Anypoint Organization/Environment Client Id and Secret from https://anypoint.mulesoft.com/accounts/login. Not the client credentials of client provider. So, OAuth 2.0 is not possible. More over, the token is mainly for API Manager purposes and not associated with a user. You can NOT use it to call most APIs (for example Cloudhub and etc) as per this Mulesoft Knowledge article.

>> The other option allowed by Anypoint CLI is to use client credentials. It is possible to use client credentials of a client provider but requires setting up Connected Apps in client management but such details are not given in the scenario explained in the question.

>> So only option left is to use user credentials from identify provider

QUESTION 4

What is a best practice when building System APIs?

A. Document the API using an easily consumable asset like a RAML definition

B. Model all API resources and methods to closely mimic the operations of the backend system

C. Build an Enterprise Data Model (Canonical Data Model) for each backend system and apply it to System APIs

D. Expose to API clients all technical details of the API implementation\\'s interaction wifch the backend system

Correct Answer: B

Model all API resources and methods to closely mimic the operations of the backend system.

****

>> There are NO fixed and straight best practices while opting data models for APIs. They are completly contextual and depends on number of factors. Based upon those factors, an enterprise can choose if they have to go with Enterprise

Canonical Data Model or Bounded Context Model etc.

>> One should NEVER expose the technical details of API implementation to their API clients. Only the API interface/ RAML is exposed to API clients. >> It is true that the RAML definitions of APIs should be as detailed as possible and should

reflect most of the documentation. However, just that is NOT enough to call your API as best documented API. There should be even more documentation on Anypoint Exchange with API Notebooks etc. to make and create a developer

friendly API and repository.. >> The best practice always when creating System APIs is to create their API interfaces by modeling their resources and methods to closely reflect the operations and functionalities of that backend system.

QUESTION 5

What is true about the technology architecture of Anypoint VPCs?

A. The private IP address range of an Anypoint VPC is automatically chosen by CloudHub

B. Traffic between Mule applications deployed to an Anypoint VPC and on-premises systems can stay within a private network

C. Each CloudHub environment requires a separate Anypoint VPC

D. VPC peering can be used to link the underlying AWS VPC to an on-premises (non AWS) private network

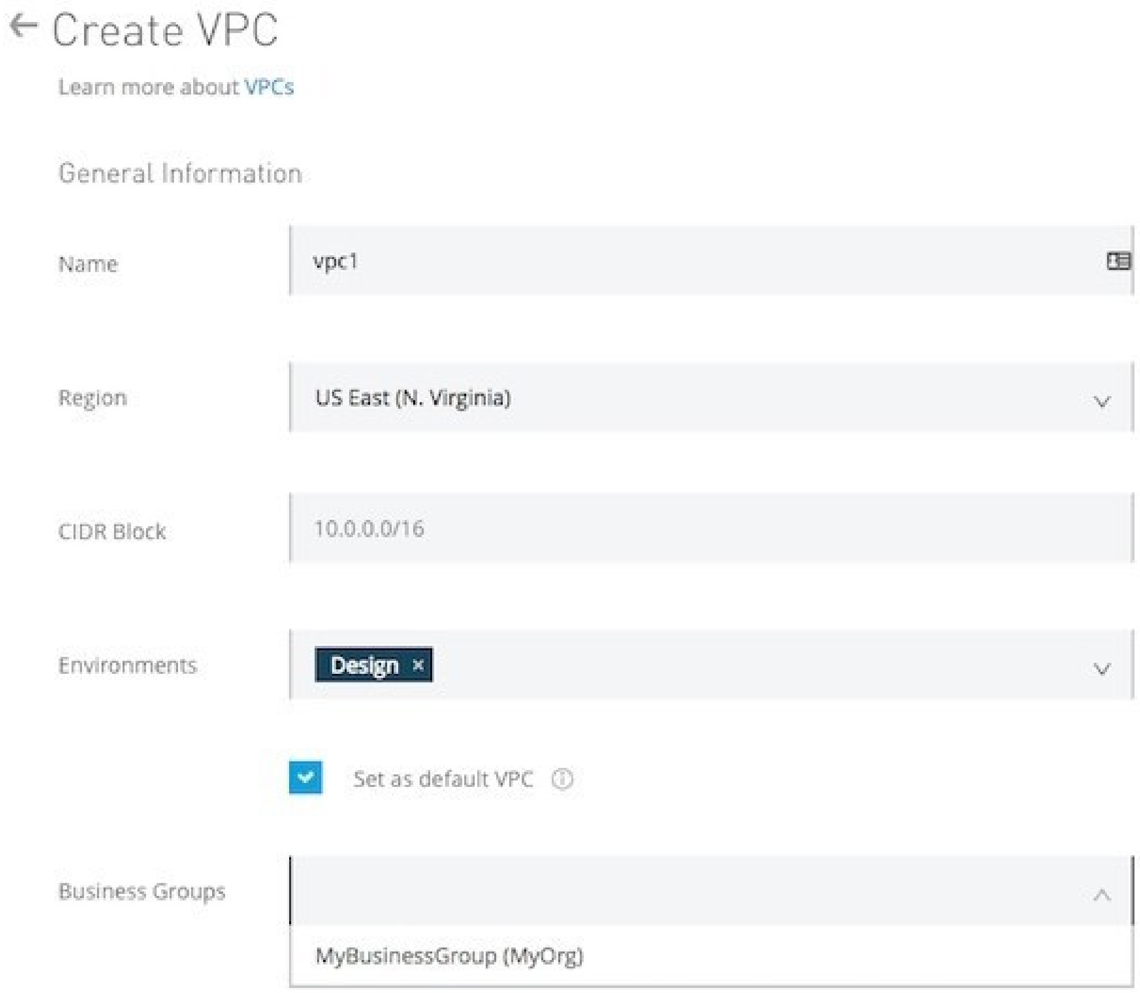
Correct Answer: B

Traffic between Mule applications deployed to an Anypoint VPC and on- premises systems can stay within a private network *** >> The private IP address range of an Anypoint VPC is NOT automatically

chosen by CloudHub. It is chosen by us at the time of creating VPC using thr CIDR blocks. CIDR Block: The size of the Anypoint VPC in Classless Inter-Domain Routing (CIDR) notation.

For example, if you set it to 10.111.0.0/24, the Anypoint VPC is granted 256 IP addresses from 10.111.0.0 to 10.111.0.255.

Ideally, the CIDR Blocks you choose for the Anypoint VPC come from a private IP space, and should not overlap with any other Anypoint VPC\\'s CIDR Blocks, or any CIDR Blocks in use in your corporate network.



← Create VPC

Learn more about VPCs

General Information

Name	vpc1
Region	US East (N. Virginia)
CIDR Block	10.0.0.0/16
Environments	Design ×
	☑ Set as default VPC
Business Groups	MyBusinessGroup (MyOrg)

that each CloudHub environment requires a separate Anypoint VPC. Once an Anypoint VPC is created, we can choose a same VPC by multiple environments. However, it is generally a best and recommended practice to always have

seperate Anypoint VPCs for Non-Prod and Prod environments.

>> We use Anypoint VPN to link the underlying AWS VPC to an on-premises (non AWS) private network. NOT VPC Peering.

Reference: https://docs.mulesoft.com/runtime-manager/vpn-about

Only true statement in the given choices is that the traffic between Mule applications deployed to an Anypoint VPC and on-premises systems can stay within a private network.

https://docs.mulesoft.com/runtime-manager/vpc-connectivity-methods-concept