MCPA-LEVEL1 Q&As

MuleSoft Certified Platform Architect - Level 1

Pass Mulesoft MCPA-LEVEL1 Exam with 100% Guarantee

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

https://www.pass4itsure.com/mulesoft-certified-platform-architect-level-1.html

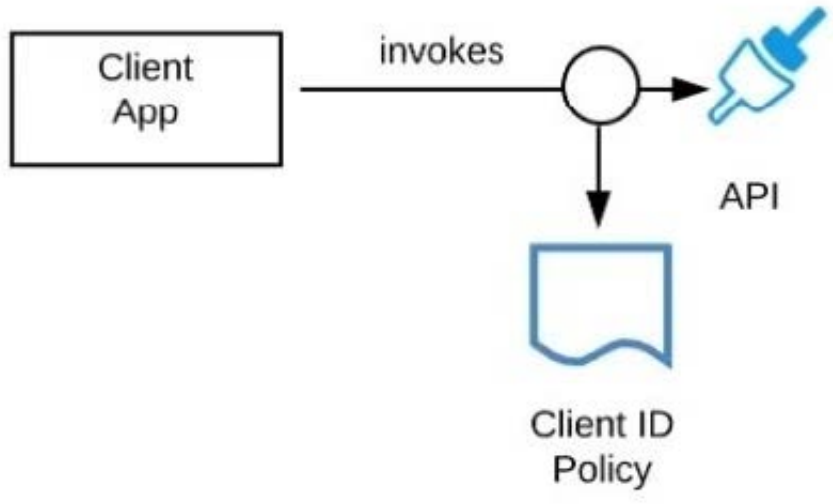
100% Passing Guarantee
100% Money Back Assurance

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

Refer to the exhibit.



A developer is building a client application to invoke an API deployed to the STAGING environment that is governed by a client ID enforcement policy.

What is required to successfully invoke the API?

A. The client ID and secret for the Anypoint Platform account owning the API in the STAGING environment

B. The client ID and secret for the Anypoint Platform account\\'s STAGING environment

C. The client ID and secret obtained from Anypoint Exchange for the API instance in the STAGING environment

D. A valid OAuth token obtained from Anypoint Platform and its associated client ID and secret

Correct Answer: C

The client ID and secret obtained from Anypoint Exchange for the API instance in the STAGING environment ********** >> We CANNOT use the client ID and secret of Anypoint Platform account or any individual environments for accessing the APIs >> As the type of policy that is enforced on the API in question is "Client ID Enforcment Policy", OAuth token based access won\\'t work. Right way to access the API is to use the client ID and secret obtained from Anypoint Exchange for the API instance in a particular environment we want to work on. References: Managing API instance Contracts on API Manager https://docs.mulesoft.com/api-manager/1.x/request-access-to-api-task https://docs.mulesoft.com/exchange/to-request-access https://docs.mulesoft.com/api-manager/2.x/policy-mule3-client-id-based-policies

QUESTION 2

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 3

An API implementation returns three X-RateLimit-* HTTP response headers to a requesting API client. What type of information do these response headers indicate to the API client?

A. The error codes that result from throttling

B. A correlation ID that should be sent in the next request

C. The HTTP response size

D. The remaining capacity allowed by the API implementation

Correct Answer: D

The remaining capacity allowed by the API implementation.

****

>> Reference: https://docs.mulesoft.com/api-manager/2.x/rate-limiting-and-throttling-sla-based-policies#response-headers

QUESTION 4

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

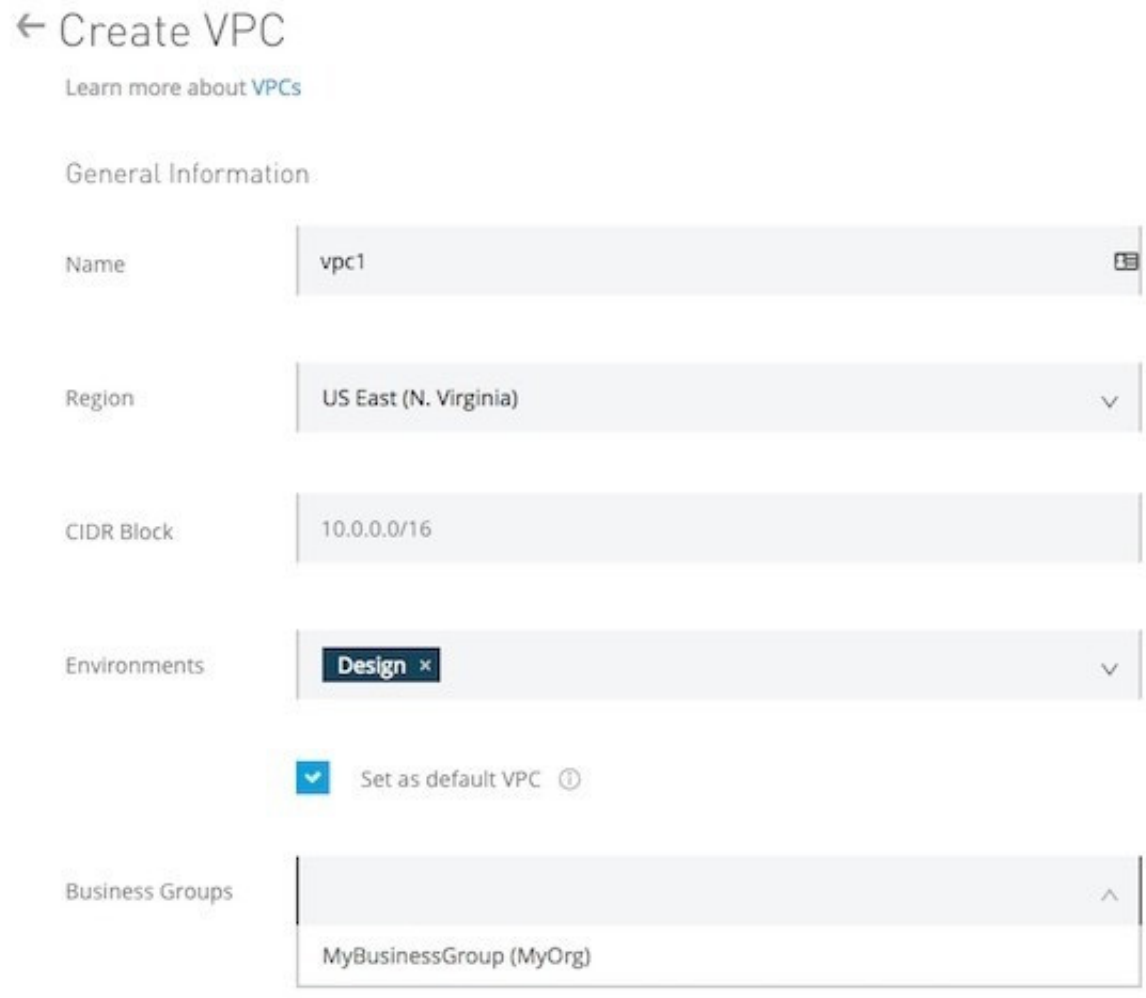
Correct Answer: B

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.



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

QUESTION 5

An organization makes a strategic decision to move towards an IT operating model that emphasizes consumption of reusable IT assets using modern APIs (as defined by MuleSoft). What best describes each modern API in relation to this new IT operating model?

A. Each modern API has its own software development lifecycle, which reduces the need for documentation and automation

B. Each modem API must be treated like a product and designed for a particular target audience (for instance, mobile app developers)

C. Each modern API must be easy to consume, so should avoid complex authentication mechanisms such as SAML or JWT D

D. Each modern API must be REST and HTTP based

Correct Answer: B

Each modern API must be treated like a product and designed for a particular target audience (for instance mobile app developers) **