FreeCram

FreeCram

Instant Download | 365 Days Free Updates | Money Back Guarantee | Security & Privacy

Full refund if you fail the corresponding exam in 60 days after purchasing. And Free get any another product.

We're not the only ones **happy** about FreeCram Practice Material ...

12514+ customers in 100+ countries use FreeCram Test Engine. Meet our customers.

https://www.freecram.com

Free Exam/Cram Practice Materials.

Exam : **MCPA-Level-1**

Title : MuleSoft Certified Platform Architect - Level 1

Vendor : MuleSoft

Version : DEMO

NO.1 Which scenario is suited for MUnit tests instead of integration tests?

A. For read-only interactions to any dependencies (such as other web APIs)

B. When testing does not require knowledge of implementation details

C. When no mocking is permissible

D. For tests that are implemented using SoapUI

Answer: A

Explanation:

MUnit is MuleSoft's testing framework for creating and running automated tests within Anypoint Studio. It is specifically designed for unit testing Mule applications and is best suited when testing doesn't require understanding the inner workings or implementation details of the components being tested.

* Ideal Use Cases for MUnit:
* MUnit is optimal when testing individual flows, functions, or components in isolation. This type of testing focuses on verifying the behavior of each unit without needing to understand the complete system.
* Since unit tests do not require external integrations or dependencies to be live, mocking is commonly used in MUnit to simulate the behavior of external services and APIs.
* Why Option B is Correct:
* Option B aligns with the concept of unit testing, where the emphasis is on testing functionality rather than system integration. Integration tests, on the other hand, would require implementation knowledge and live endpoints, making them unsuitable for MUnit's scope.
* Explanation of Incorrect Options:
* Option A (read-only interactions) and Option C (no mocking) do not suit MUnit's typical testing environment as MUnit is designed with mocking capabilities to simulate dependencies.
* Option D (SoapUI-based tests) suggests an external testing tool, while MUnit is specific to MuleSoft.
ReferencesFor more on MUnit best practices, refer to MuleSoft's MUnit documentation.

NO.2 Which statement is true about identity management and client management on Anypoint Platform?

A. If an external identity provider is configured, the SAML 2.0 bearer tokens issued by the identity provider cannot be used for invocations of the Anypoint Platform web APIs

B. If an external client provider is configured, it must be configured at the Anypoint Platform organization level and cannot be assigned to individual business groups and environments

C. Anypoint Platform supports configuring one external identity provider

D. Both client management and identity management require an identity provider

Answer: C

Explanation:

Anypoint Platform allows organizations to integrate one external identity provider (IdP) for identity and access management (IAM), supporting SSO and centralized user authentication.

* Identity Provider Limit:
* Anypoint Platform supports configuring a single IdP for the organization, which can be used to authenticate all users across business groups and environments within that Anypoint organization.
* Explanation of Correct Answer (C):
* Configuring one IdP ensures centralized and secure identity management, aligned with MuleSoft' s architecture.

* Explanation of Incorrect Options:
* Option A is incorrect because SAML 2.0 bearer tokens from external IdPs can indeed be used for invoking Anypoint Platform APIs.
* Option B is incorrect as client providers can be assigned to specific business groups and environments.
* Option D is incorrect since only identity management strictly requires an IdP; client management does not.
ReferencesFor further details on identity management options, consult MuleSoft documentation on Anypoint Platform's IAM capabilities.

NO.3 A Platinum customer uses the U.S. control plane and deploys applications to CloudHub in Singapore with a default log configuration.
The compliance officer asks where the logs and monitoring data reside?
A. Logs are held in:Singapore and monitoring data is held in the United States
B. Logs and monitoring data are held in the United States
C. Logs are held in the United States and monitoring data is held in Singapore
D. Logs and monitoring data are held in Singapore
Answer: B
Explanation:
For applications deployed on CloudHub in a foreign region (e.g., Singapore), MuleSoft handles log and monitoring data in the region where the control plane resides. This data storage policy is standard for CloudHub deployments to maintain centralized log and monitoring data.
* Data Location:
* For a U.S.-based control plane, all logs and monitoring data are stored in the United States, regardless of the deployment region.
* Although the application itself runs in Singapore, data related to application performance and logs is not localized to the deployment region.
* Explanation of Correct Answer (B):
* Since the control plane is based in the United States, all operational data like logs and monitoring will also be stored there, ensuring compliance with MuleSoft's data handling policies.
* Explanation of Incorrect Options:
* Option A and D are incorrect because MuleSoft does not store logs or monitoring data in the application deployment region when the control plane is located in the United States.
* Option C suggests mixed storage, which does not align with MuleSoft's data policy structure.
ReferencesFor details on data residency in CloudHub deployments, refer to MuleSoft's documentation on CloudHub control planes and data handling policies.

NO.4 An IT Security Compliance Auditor is assessing which nonfunctional requirements (NFRs) are already being implemented to meet security measures.
* The Web API has Rate-Limiting SLA
* Basic Authentication - LDAP
* JSON Threat Protection
* TP Allowlist policies applied
Which two NFRs-are enforced?
A. The API invocations are coming from a known subnet range
B. Username/password supported to validate login credentials

C. Sensitive data is masked to prevent compromising critical information

D. The API is protected against XML invocation attacks

E. Performance expectations are to be allowed up to 1,000 requests per second

Answer: A B

Explanation:

* Understanding Nonfunctional Requirements (NFRs):
* The NFRs in this context are related to security measures implemented for the Web API, such as rate limiting, LDAP-based authentication, JSON threat protection, and IP allowlist policies.
* Evaluating the Options:
* Option A (Correct Answer): The IP allowlist policy restricts access to known subnets, ensuring that API invocations come from a defined range of IPs.
* Option B (Correct Answer): Basic Authentication with LDAP enforces a username/password validation, satisfying an NFR for identity verification.
* Option C: Masking sensitive data is not part of the listed NFRs, as none of the mentioned policies address data masking.
* Option D: XML threat protection is not mentioned, so this option is incorrect.
* Option E: While rate-limiting implies performance control, it does not directly enforce a specific performance expectation.
* Conclusion:
* Options A and B are correct as they directly address the implemented security measures related to IP range restrictions and username/password authentication.

Refer to MuleSoft's documentation on API security policies for details on LDAP, rate limiting, and allowlist policies.

NO.5 An organization wants to create a Center for Enablement (C4E). The IT director schedules a series of meetings with IT senior managers.

What should be on the agenda of the first meeting?

A. Define C4E objectives, mission statement, guiding principles, a

B. Explore API monetization options based on identified use cases through MuleSoft

C. A walk through of common-services best practices for logging, auditing, exception handling, caching, security via policy, and rate limiting/throttling via policy

D. Specify operating model for the MuleSoft Integrations division

Answer: A

Explanation:

In the initial meeting for establishing a Center for Enablement (C4E), it's essential to lay the foundational vision, objectives, and guiding principles for the team. Here's why this is crucial:

* Clear Vision and Mission:
* Defining the mission statement and objectives at the start ensures alignment within the organization and clarifies the C4E's role in supporting API-led development and integration practices.
* Guiding Principles:
* Establishing guiding principles will help the C4E maintain consistent practices and strategies across projects. This serves as a framework for decisions and fosters shared understanding among IT leaders and stakeholders.
* Explanation of Correct Answer (A):
* By prioritizing the C4E's objectives and mission, the organization builds a solid foundation, paving

the way for subsequent meetings focused on technical standards, processes, and operating models.
* Explanation of Incorrect Options:
* Option B (API monetization) and Option C (common services best practices) are specific topics better suited for later discussions.
* Option D (specifying the operating model) is an important step but typically follows the establishment of the C4E's objectives and vision.
ReferencesFor more on C4E objectives and foundational setup, refer to MuleSoft's documentation on establishing a C4E and the roles and mission statements recommended for such initiatives.

NO.6 A REST API is being designed to implement a Mule application.
What standard interface definition language can be used to define REST APIs?
A. Web Service Definition Language(WSDL)
B. OpenAPI Specification (OAS)
C. YAML
D. AsyncAPI Specification
Answer: B

NO.7 In which layer of API-led connectivity, does the business logic orchestration reside?
A. System Layer
B. Experience Layer
C. Process Layer
Answer: C
Explanation:
Process Layer
****
>> Experience layer is dedicated for enrichment of end user experience. This layer is to meet the needs of different API clients/ consumers.
>> System layer is dedicated to APIs which are modular in nature and implement/ expose various individual functionalities of backend systems
>> Process layer is the place where simple or complex business orchestration logic is written by invoking one or many System layer modular APIs So, Process Layer is the right answer.

NO.8 A code-centric API documentation environment should allow API consumers to investigate and execute API client source code that demonstrates invoking one or more APIs as part of representative scenarios.
What is the most effective way to provide this type of code-centric API documentation environment using Anypoint Platform?
A. Enable mocking services for each of the relevant APIs and expose them via their Anypoint Exchange entry
B. Ensure the APIs are well documented through their Anypoint Exchange entries and API Consoles and share these pages with all API consumers
C. Create API Notebooks and include them in the relevant Anypoint Exchange entries
D. Make relevant APIs discoverable via an Anypoint Exchange entry
Answer: C
Explanation:

Create API Notebooks and Include them in the relevant Anypoint exchange entries
****
>> API Notebooks are the one on Anypoint Platform that enable us to provide code-centric API documentation

NO.9 Mule applications that implement a number of REST APIs are deployed to their own subnet that is inaccessible from outside the organization.
External business-partners need to access these APIs, which are only allowed to be invoked from a separate subnet dedicated to partners - called Partner-subnet. This subnet is accessible from the public internet, which allows these external partners to reach it.
Anypoint Platform and Mule runtimes are already deployed in Partner-subnet. These Mule runtimes can already access the APIs.
What is the most resource-efficient solution to comply with these requirements, while having the least impact on other applications that are currently using the APIs?
A. Implement (or generate) an API proxy Mule application for each of the APIs, then deploy the API proxies to the Mule runtimes
B. Redeploy the API implementations to the same servers running the Mule runtimes
C. Add an additional endpoint to each API for partner-enablement consumption
D. Duplicate the APIs as Mule applications, then deploy them to the Mule runtimes
Answer: A

NO.10 A TemperatureSensors API instance is defined in API Manager in the PROD environment of the CAR_FACTORY business group. An AcmelemperatureSensors Mule application implements this API instance and is deployed from Runtime Manager to the PROD environment of the CAR_FACTORY business group. A policy that requires a valid client ID and client secret is applied in API Manager to the API instance.
Where can an API consumer obtain a valid client ID and client secret to call the AcmeTemperatureSensors Mule application?
A. In secrets manager, request access to the Shared Secret static username/password
B. In API Manager, from the PROD environment of the CAR_FACTORY business group
C. In access management, from the PROD environment of the CAR_FACTORY business group
D. In Anypoint Exchange, from an API client application that has been approved for the TemperatureSensors API instance
Answer: D
Explanation:
When an API policy requiring a client ID and client secret is applied to an API instance in API Manager, API consumers must obtain these credentials through a registered client application. Here's how it works:
* Anypoint Exchange and Client Applications:
* To access secured APIs, API consumers need to create or register a client application in Anypoint Exchange. This process involves requesting access to the specific API, and once approved, the consumer can retrieve the client ID and client secret associated with the application.
* Why Option D is Correct:
* Option D accurately describes the process, as the client ID and client secret are generated and managed within Anypoint Exchange. API consumers can use these credentials to authenticate with

the TemperatureSensors API.
* Explanation of Incorrect Options:
* Option A (secrets manager) is incorrect because client credentials for API access are not managed via secrets manager.
* Option B (API Manager) is incorrect as API Manager manages policies but does not provide client-specific credentials.
* Option C (Access Management) does not apply, as Access Management is primarily used for user roles and permissions, not API client credentials.
ReferencesFor further details on managing client applications in Anypoint Exchange, consult MuleSoft documentation on client application registration and API security policies.

NO.11 Traffic is routed through an API proxy to an API implementation. The API proxy is managed by API Manager and the API implementation is deployed to a CloudHub VPC using Runtime Manager. API policies have been applied to this API. In this deployment scenario, at what point are the API policies enforced on incoming API client requests?

A. At the API implementation

B. At a MuleSoft-hosted load balancer

C. At both the API proxy and the API implementation

D. At the API proxy

Answer: D

NO.12 A company uses a hybrid Anypoint Platform deployment model that combines the EU control plane with customer-hosted Mule runtimes. After successfully testing a Mule API implementation in the Staging environment, the Mule API implementation is set with environment-specific properties and must be promoted to the Production environment. What is a way that MuleSoft recommends to configure the Mule API implementation and automate its promotion to the Production environment?

A. Bundle properties files for each environment into the Mule API implementation's deployable archive, then promote the Mule API implementation to the Production environment using Anypoint CLI or the Anypoint Platform REST APIsB.

B. Modify the Mule API implementation's properties in the API Manager Properties tab, then promote the Mule API implementation to the Production environment using API Manager

C. Modify the Mule API implementation's properties in Anypoint Exchange, then promote the Mule API implementation to the Production environment using Runtime Manager

D. Use an API policy to change properties in the Mule API implementation deployed to the Staging environment and another API policy to deploy the Mule API implementation to the Production environment

Answer: A
Explanation:
Bundle properties files for each environment into the Mule API implementation's deployable archive, then promote the Mule API implementation to the Production environment using Anypoint CLI or the Anypoint Platform REST APIs
****
>> Anypoint Exchange is for asset discovery and documentation. It has got no provision to modify the properties of Mule API implementations at all.
>> API Manager is for managing API instances, their contracts, policies and SLAs. It has also got no

provision to modify the properties of API implementations.
>> API policies are to address Non-functional requirements of APIs and has again got no provision to modify the properties of API implementations.
So, the right way and recommended way to do this as part of development practice is to bundle properties files for each environment into the Mule API implementation and just point and refer to respective file per environment.

NO.13 When using CloudHub with the Shared Load Balancer, what is managed EXCLUSIVELY by the API implementation (the Mule application) and NOT by Anypoint Platform?

A. The assignment of each HTTP request to a particular CloudHub worker

B. The logging configuration that enables log entries to be visible in Runtime Manager

C. The SSL certificates used by the API implementation to expose HTTPS endpoints

D. The number of DNS entries allocated to the API implementation

Answer: C

Explanation:
The SSL certificates used by the API implementation to expose HTTPS endpoints
****
>> The assignment of each HTTP request to a particular CloudHub worker is taken care by Anypoint Platform itself. We need not manage it explicitly in the API implementation and in fact we CANNOT manage it in the API implementation.
>> The logging configuration that enables log entries to be visible in Runtime Manager is ALWAYS managed in the API implementation and NOT just for SLB. So this is not something we do EXCLUSIVELY when using SLB.
>> We DO NOT manage the number of DNS entries allocated to the API implementation inside the code.
Anypoint Platform takes care of this.
It is the SSL certificates used by the API implementation to expose HTTPS endpoints that is to be managed EXCLUSIVELY by the API implementation. Anypoint Platform does NOT do this when using SLBs.

NO.14 A company wants to move its Mule API implementations into production as quickly as possible. To protect access to all Mule application data and metadata, the company requires that all Mule applications be deployed to the company's customer-hosted infrastructure within the corporate firewall. What combination of runtime plane and control plane options meets these project lifecycle goals?

A. Manually provisioned customer-hosted runtime plane and customer-hosted control plane

B. MuleSoft-hosted runtime plane and customer-hosted control plane

C. Manually provisioned customer-hosted runtime plane and MuleSoft-hosted control plane

D. iPaaS provisioned customer-hosted runtime plane and MuleSoft-hosted control plane

Answer: A

Explanation:
Manually provisioned customer-hosted runtime plane and customer-hosted control plane
****
There are two key factors that are to be taken into consideration from the scenario given in the question.

>> Company requires both data and metadata to be resided within the corporate firewall
>> Company would like to go with customer-hosted infrastructure.
Any deployment model that is to deal with the cloud directly or indirectly (Mulesoft-hosted or Customer's own cloud like Azure, AWS) will have to share atleast the metadata.
Application data can be controlled inside firewall by having Mule Runtimes on customer hosted runtime plane. But if we go with Mulsoft-hosted/ Cloud-based control plane, the control plane required atleast some minimum level of metadata to be sent outside the corporate firewall.
As the customer requirement is pretty clear about the data and metadata both to be within the corporate firewall, even though customer wants to move to production as quickly as possible, unfortunately due to the nature of their security requirements, they have no other option but to go with manually provisioned customer- hosted runtime plane and customer-hosted control plane.

NO.15 The application network is recomposable: it is built for change because it "bends but does not break"

A. TRUE

B. FALSE

Answer: A

Explanation:
****
>> Application Network is a disposable architecture.
>> Which means, it can be altered without disturbing entire architecture and its components.
>> It bends as per requirements or design changes but does not break