



1Z0-574^{Q&As}

Oracle IT Architecture Release 3 Essentials

Pass Oracle 1Z0-574 Exam with 100% Guarantee

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

<https://www.passapply.com/1z0-574.html>

100% Passing Guarantee
100% Money Back Assurance

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

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

Which of the following environments are typically clustered?

- A. Development Environment
- B. User Acceptance Testing (UAT) Environment
- C. Staging Environment
- D. Nonfunctional Testing Environment

Correct Answer: B

Explanation:

UAT (also known as beta testing) : Formal testing with respect to user needs, requirements, and business processes conducted to determine whether or not a system satisfies the acceptance criteria and to enable the user, customers or other authorized entity to determine whether or not to accept the system.

Incorrect answer:

The staging tier is a environment that is as identical to the production environment as possible. The purpose of the Staging environment is to simulate as much of the Production environment as possible. The Staging environment can also double as a Demonstration/Training environment.

References:

QUESTION 2

Which statement best describes the relationship between the Service-Oriented Integration (SOI) architecture and the Application Integration Architecture (AIA) product from Oracle?

- A. AIA is a product specific Implementation of the SOI architecture.
- B. AIA is a traditional Enterprise Application Integration (EAI) architecture; therefore AIA does not follow the SOI architecture.
- C. AIA is an Oracle product that maps to some of the layers and capabilities defined by the SOI architecture.
- D. AIA is an Oracle product and the SOI architecture is a product-agnostic architecture; therefore there is no relationship between the two.
- E. AIA is one of many Oracle products that maps onto SOI architecture.

Correct Answer: E

Explanation:



There are two categories of Oracle products that map into the service-oriented integration architecture, Fusion Middleware products and the Application Integration Architecture (AIA) products.

References:

QUESTION 3

AAPML and CARML are part of what standards effort?

- A. WS-Security
- B. Web Services Interoperability
- C. JCA and JAAS
- D. Identity Governance Framework

Correct Answer: D

Explanation:

Identity Governance Framework (IGF) consists of:

*

An identity attribute service that supports access to many different sources of PII and enforces administrative policy.

*

Client Attribute Requirements Markup Language (CARML): declarative syntax used by clients to specify their requirements for PII.

*

Attribute Authority Policy Markup Language (AAPML): declarative syntax which enables providers of identity-related data to express policy on the usage of information.

*

A multi-language API (Java, .NET, Perl) for reading and writing identity-related attributes.

References:

QUESTION 4

Which three primary types of materials form an Enterprise Technology Strategy?

- A. ORA Technology Perspective
- B. ORA Industry Perspective
- C. Practitioner Guides



D. Maturity Model

E. Business Processes

F. Data Entities

Correct Answer: ACD

Explanation:

There are three primary types of collateral provided for each ETS:

*

ORA Technology Perspective

*

Practitioner Guides

*

Maturity Model

References:

QUESTION 5

Which of the following is least effective at deterring man-in-the-middle attacks?

A. encrypting network traffic

B. issuing single-use access tokens

C. mutual authentication

D. biometric authentication

E. using time stamps or transaction IDs to detect and discard replay attempts

Correct Answer: C

Explanation:

In order to avoid man-in-the-middle attacks a security framework must have capabilities such as:

*

Logging in users without the need to type passwords or PINs (not D)

*

Dynamically challenging the user for different information, e.g., asking a random question for which only the user will know the answer



*

Encrypting and signing transmissions from the client to the back end server (not A)

*

Detecting replays using embedded transaction ids or timestamps (not E)

*

Presenting proof to the user that the site they are visiting is authentic

Propagating a single proof object, or assertion, can be susceptible to man-in-the-middle attacks and replay attacks. If a rogue entity observes an assertion, it could reuse that assertion for illegitimate requests. Possible solutions include:

*

(notB) Invalidate the assertion after every request. In the case of chained SOA Services, service providers must verify each assertion they receives with the authority. The authority can invalidate assertions in its internal cache. Any future verifications with the same assertion would fail. SOA Service providers would need to obtain a new assertion in order to make subsequent service requests. This solves both types of problems mentioned above.

*

(notE) Reduce and enforce the assertion's time to live attribute. This would narrow the window of opportunity to reuse an assertion. The assertion would have to be captured and reused in a short period of time (programmatically vs. manually). While this limits the potential for man-in-the-middle attacks, it's not as effective for replay attacks

*

Require the signature of a trusted service consumer (client application) in addition to the signed assertion. The caller's signature should cover the assertion to bind it to the message. If all service consumers are required to sign their request messages, then service providers can be shielded from rogue clients, thereby preventing man-in-the-middle attacks.

This solution would need to be enhanced to solve replay attacks. One option is to include a unique request id, timestamp, or sequence number in the request. The target resource could maintain a cache of ids and refuse duplicate requests. A common request id service could be created to issue unique request ids and validate all requests that are received within the security domain

References:

[1Z0-574 PDF Dumps](#)

[1Z0-574 VCE Dumps](#)

[1Z0-574 Exam Questions](#)