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.geekcert.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

Identify the true statements in the following list.

A. The core components of the ORA UI Logical view are grouped into the client tier and the server tier.

B. The components of the ORA UI Logical view are model, view, and controller.

C. The core components of the ORA UI Logical view are grouped into thedisplaytier and theresourcestier.

D. In addition to the core components, the Logical view also includes security, communication protocols, and development tools.

Correct Answer: AD

Explanation:

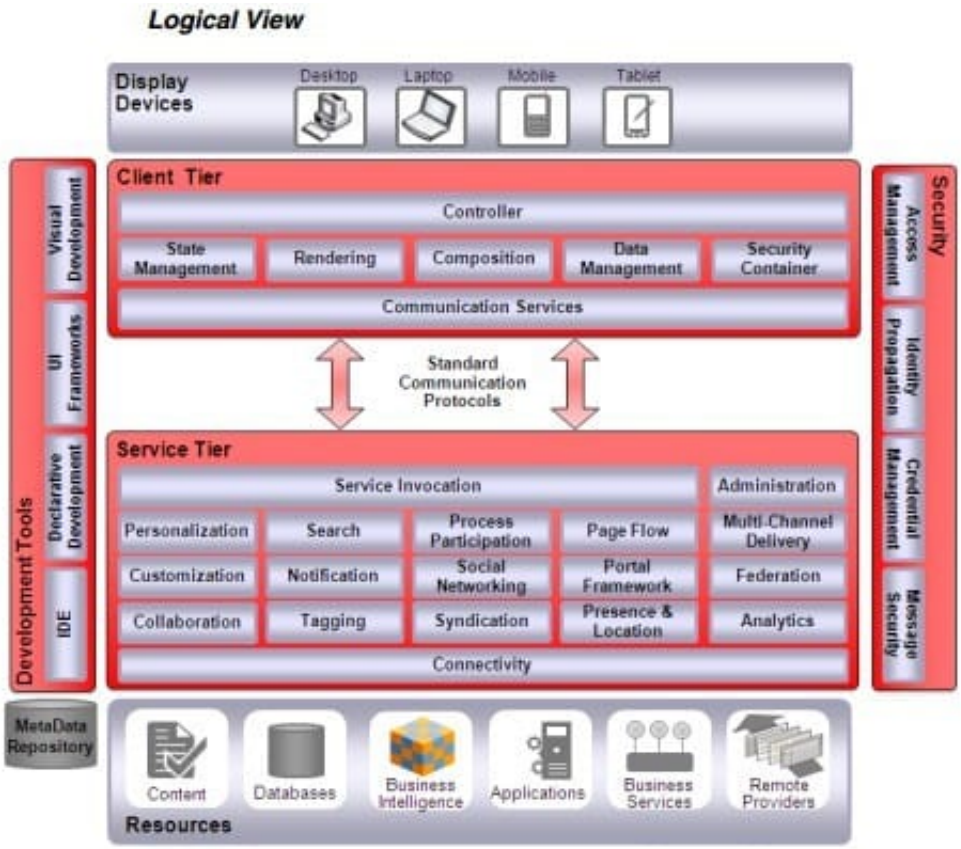
The Logical View of the architecture describes the various layers in the architecture. Each layer

encapsulates specific capabilities for the overall architecture. Upper layers in the architecture leverage the

capabilities provided by the lower layers.

The Client Tier is hosted on the display device.

The Service Tier hosts the capabilities that satisfy the requirements of the end user.



QUESTION 2

Which of the following are the implications of the architecture principle, "Asset-centric approach must be applied to engineering processes"?

A. The development Infrastructure must support asset-centric engineering.

B. Assets must be associated with meaningful metadata that can be used to discover and interpret the assets.

C. Solutions developed must beintegrated and tested early and often.

D. Existing assets must be reused to fulfill whole or part functionality when available.

Correct Answer: B

Explanation: The underlying core principle of ORA Engineering is asset sharing and enterprise development through an integrated asset management approach. Most organizations use a Software Configuration Management (SCM) or Version Control System (VCS) for managing the code and configuration assets. These tools are great for managing the versioning of assets produced but they don\\'t maintain the metadata of the assets. Without metadata assets are not organized in context and it is hard to discover them. ORA recommends an asset-centric engineering process, where an Asset Manager is used to address the challenges posed by the traditional approaches. The Asset Manager is typically an enterprise-scoped Metadata Repository working in concert with SCMs and other types of asset repositories.

References:

QUESTION 3

Which statements are correct with regard to the layers in the Logical View of Service-Oriented Integration (SOI)?

A. Upper layers in the architecture leverage capabilities provided by lower layers.

B. Upper layers are allowed to access capabilities in any lower layer.

C. Upper layers are allowed to access capabilities only in the next lower layer.

D. Each layer encapsulates specific capabilities required by the entire architecture.

E. Each layer encapsulates optional capabilities of the architecture; thus any layer can be omitted from the architecture.

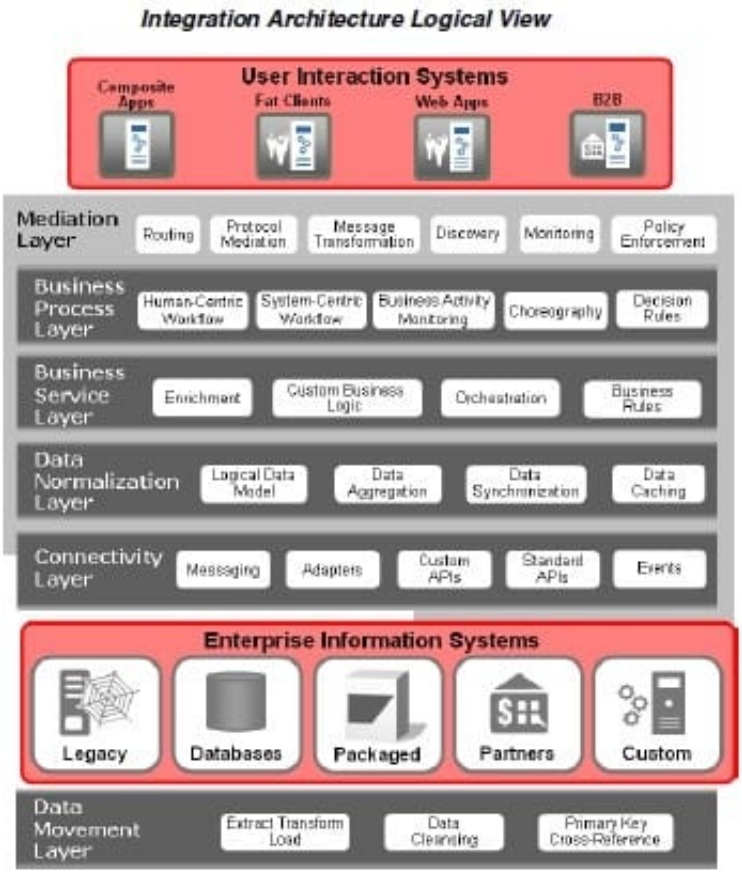
F. The layers are used to partition the capabilities of the architecture, but otherwise have no architectural significance.

Correct Answer: ACD

Explanation:

Each layer encapsulates specific capabilities for the overall architecture. Upper layers in the architecture

leverage the capabilities provided by the lower layers. Generally, upper layers call lower layers in the architecture and the reverse (i.e. lower levels calling upper layers) is prohibited.



References:

QUESTION 4

Which principle should be applied when considering display devices?

A. The architecture must provide distinct tooling for the unique development of every available device.

B. The architecture must support translation of standard browser code to all possible variations of display devices, allowing the developer to focus on functionality for the end user.

C. The architecture must provide for the development of user Interfaces for a variety of display devices.

D. Only display devices that support a full-featured user interaction are allowed with this architecture.

Correct Answer: C

Explanation:

The architecture must support multiple different display devices.

An architecture that supports only a single display device is prohibitively limiting in today\\'s connected

world. Even if only a single display device (e.g. personal computer) is the initial focus for a business

solution, the architecture must be designed to readily support additional display devices; otherwise the cost

of supporting another display device constrains the future flexibility of the solution.

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: