# 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**

A customer with an existing WebCenter portal wants to expand his client device list to include a variety of mobile devices beyond basic browser support. What Oracle products are available to enable this expansion?

A. OWC, OHS, ADF Mobile, and Java ME

B. OWCA, ADF Mobile, OPSS, and Java ME

C. OWC, OHS, and ADF Mobile

D. OWCIC, ADF Mobile, and Java ME

Correct Answer: A

Explanation:

Oracle HTTP Server (OHS) - provides a HTTP listener for Oracle WebLogic Server and the framework for

hosting static content, dynamic content, and applications over the Web.

Java Platform, Micro Edition (Java ME)(not C):meets the needs of developers creating applications for the

consumer and embedded markets. No other technology provides such robust applications across so many

types of size-constrained wireless and wireline devices, from mobile phones and PDAs to set-top boxes

and vehicle telematics.c

References:

**QUESTION 2**

A customer has two separate lines of business and each has its own unique resources that are controlled independently. The customer wants to provide a single user interface at the enterprise level that, at least from the user\\'s perspective, unifies the separate lines of business and presents a single consistent view. What is the most suitable architectural arrangement for such a federated deployment?

A. The enterprise implements full client stack and part of the service stack while each LoB deploys the remaining part of the service tierin order to expose uniform interface elements.

B. The client tier assimilates the data from the resource stack of each line of business.

C. The enterprise implements full client and service stacks while each LoB deploys a partial service. sufficient to expose uniform interface elements.

D. The client tier assimilates the data from the service stack of each line of business.

Correct Answer: A

Explanation: Each line of business has its own resources that are unique to the line of business and are controlled by that line of business. The enterprise wants to provide a single user interface that, at least from the user\\'s perspective, unifies the separate lines of business. In this example, the enterprise wide user interface deployment is a full featured

user interaction architecture (i.e. it contains all of the capabilities defined in the Logical View). Each line of business deploys limited functionality since the only functionality required is the functionality to create interface elements exposing the resources of that line of business. The enterprise wide user interface then uses the interface elements provided by the lines of business to create a unified user experience. The interface elements provided by the lines of business are Remote Providers to the enterprise user interface. This deployment allows the lines of business to maintain control of their respective resources since the only access to the resources is via the interface elements that they create.

References:

**QUESTION 3**

Which one of the following user classification schemes best reflects what function or function performs?

A. role-based classification

B. rule-based classification

C. group-based classification

D. attribute-based classification

E. rank-based classification

Correct Answer: A

Explanation: Given the potentially large number of users of a system, access privileges are generally not assigned at the user level. Instead, users are assigned to groups (mimicking the organizational structure of a company), or roles (defined based on job functions that users perform), or some combination of the two. Access privileges are then assigned to groups and/or roles. The most natural case is that they are assigned to roles, since roles align more closely with operations users naturally perform to accomplish their job. The industry term for this is Role-Based Access Control (RBAC). RBAC is more flexible than defining access rights based on usernames or static groups and enables an organization to be more versatile when allocating resources. With RBAC the system must determine if the subject (user or client) is associated with a role that has been granted access to a resource. This process of user to role ascertainment is called role mapping.

Incorrect answers

B: Rule-based access control is very similar to fine-grained access control, where access is controlled by rules defined in policies. The twist is that rules might refer to each other. For instance, access may be granted to resource/function A as long as it is not also granted to resource/function B. This form of control can be used to ensure that a group or individual is not given privileges that create a conflict of interest or inappropriate level of authority. For instance, the approver of expenses or purchases cannot be the same as the requestor.

C: Role is better here.

D: There are times when access should be based on characteristics the user has rather than the organization or roles to which the user belongs. For instance, a customer with premium status might be granted access to exclusive offers, and a sales representative that has achieved his target sales revenue might have access to certain perks. Such levels of status vary over time, making it difficult to manage access based on relatively static group or role assignments. Attribute-based access control offers a more dynamic method of evaluation. Decisions are based on attributes assigned to users, which are free to change as business events unfold. Access policies define the attributes and values a user must have, and access decisions are evaluated against the current values assigned to the user. Attributes can be used to support both course-grained and fine-grained authorization.

E: No such thing as rank-based classification

References:

**QUESTION 4**

Which statement best describes the relationship between the Logical View and the Development view of the Service-Oriented Integration architecture?

A. The two architectural views are Independent and there is no relationship between them.

B. The Logical View defines the rationale for layers within the architecture. The Development View specifies the developer tools used for each layer.

C. The Logical View defines the layers of the architecture and the capabilities within each layer. The Development View describes how aspects of the architecture impact developers following the architecture.

D. The Logical View defines the layers of the architecture and the capabilities within each layer. The Development View specifies the developer tools that provide the capabilities for each layer.

E. The Logical View specifies the developer tools required by each layer in the architecture. The Development View describes the developer impact of the tools specified.

Correct Answer: C

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 Development View of the architecture describes aspects of the architecture that are of interest to developers building assets that conform to and leverage the architecture. In a service-oriented integration architecture the primary developer artifacts are the SOA Services that are created to expose data and functionality contained in source systems.

References:

**QUESTION 5**

Which of the following is not a valid type of SAML assertion?

A. authentication assertion

B. authorization decision assertion

C. audit assertion

D. attribute assertion

Correct Answer: C

Explanation:

SAML defines the syntax and semantics for creating XML-encoded assertions to describe authentication,

attribute, and authorization (entitlement) information, and for the protocol messages to carry this

information between systems. A brief description of the three SAML assertions is provided below.

*

Authentication Assertion (not A) - Generated by the authority when a subject successfully authenticates. It includes identity of the issuer and the principal, time of authentication, and how long it is valid. Many authentication methods are supported, including: passwords, Kerberos, hardware tokens, certificate-based client authentication (SSL/TLS), X.509 public key, PGP, XML digital signature, etc.

*

Authorization Decision Assertion (not B) - Issued by a policy decision point (PDP) containing the result of an access control decision. Authentication and attribute assertions may be provided in order to make authorization decisions. The resulting authorization assertion is used to claim access to protected resources. It includes the decision (Permit or Deny), along with the resource URI being accessed, and the action that the principal is authorized to perform.

*

Attribute Assertion (not D)- Generally issued by the authority in response to a request containing an authentication assertion. It contains a collection of attribute name/value pairs, in addition to identity and other elements. Attribute assertions can be passed to the authority when authorization decisions need to be made.

References: