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.certbus.com/1z0-574.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which of the following are types of policy considerations designed to affect the way privileges are assigned to users?

A. Principle of Alternating Privilege

B. Separation of Duties

C. DefenseinDepth

D. Vacation, Job Rotation, and Transfer

E. Principle of Least Privilege

Correct Answer: BDE

Explanation:

B: Separation of duties is a classic security principle that restricts the amount of power held by any one individual in order to prevent conflict of interest, the appearance of conflict of interest, fraud, and errors. Separation of duties is one of the fundamental principles of many regulatory mandates such as Sarbanes-Oxley (SOX) and the Gramm-Leach-Bliley Act (GLBA), and as a result IT organizations are placing greater emphasis on separation of duties across all IT functions, especially database administration.

D: Vacation, Job Rotation, and Transfer are policy considerations.. Once way to detect and deter misuse of systems is to have a new person perform the duties of an existing worker. The new person might notice irregularities or questionable circumstances and be able to report it. The new worker might be there temporarily, i.e. filling in for someone on vacation, or might be a replacement as a result of periodic job rotations and transfers. In addition, workers that expect periodic rotations are less likely to misuse systems as they know others following behind them will eventually discover it and report them. E:Each user should have only those privileges appropriate to the tasks she needs to do, an idea termed the principle of least privilege. Least privilege mitigates risk by limiting privileges, so that it remains easy to do what is needed while concurrently reducing the ability to do inappropriate things, either inadvertently or maliciously. Note: The principle of least privilege. Users are given the least amount of privileges necessary in order to carry out their job functions. This applies to interactions between systems as well as user interactions. This reduces the opportunity for unauthorized access to sensitive information. References:

QUESTION 2

Which statement best describes the role of the Data Movement Layer within the logical view of the Service-Oriented Integration (SOI) architecture?

A. The Data Movement Layer provides access to persistent data storage for the architecture.

B. All write operations on persistent data are performed via the Data Movement Layer.

C. All read operations on persistent data are performed via the Data Movement Layer.

D. All create, read, update, and delete operations on persistent data are performed via the Data Movement Layer.

E. The Data Movement Layer provides batch and bulk data operations for the architecture.

Correct Answer: E

Explanation: The Data Movement Layer provides the batch and bulk data handling for the architecture. This layer exists primarily to offload bulk data movement from the upper layers in the architecture. Bulk data movement is a necessary evil in many enterprises, and therefore, the architecture must provide a mechanism to provide this capability in an efficient, controlled manner. Without this layer, the other layers in the architecture might be misused to move large blocks of data, a task for which the other layers are ill suited.

References:

QUESTION 3

Which of the following statements are true?

A. The MVC pattern became very popular when the client-server architecture was in common use.

B. MVC was developed to map to three tiers of an n-tier architecture.

C. Federation, as applied to user interfaces, means that all security standards must only be applied at a level at which government security agencies are able to decrypt communications.

D. Federation, as applied to user interfaces, is the concept that parts of the user interface arecreatedand controlled by an organization that is separate from the organization creating the user interface.

E. When in a disconnected state, the Data Management capability in the client tier may act temporarily as the model allowing the user interface to function.

F. Federation, as applied to a user interfaces, means that data must be replicated.

Correct Answer: AD

Explanation:

A: When the MVC pattern came into prominence, client-server was the system architecture de rigueur. Note: The model-view-controller (MVC) pattern separates the three major elements in the user interface; thereby providing separation of concerns which results in code that is more easily understood, reused, modified, and maintained. The three major elements in the user interface are: model, view, and controller.

D: Whereas the MVC pattern and modular programming are relatively old concepts (at least as far as software development is concerned), federation is a relatively new concept closely related to service orientation. Applied to user interfaces, federation is the concept that parts of the user interface are created and controlled by an organization (authority) that is separate from the organization (authority) creating the user interface.

References:

QUESTION 4

What are the benefits of the browser over traditional user Interfaces (for example, client-server GUI)?

A. HTML provides a richer interface for end users.

B. Development, maintenance, and support costs are reduced.

C. The browser simplifies application deployment compared to dedicated client server GUI applications.

D. There is more variety among browsers than among client-server GUIs.

E. The browser provides a richer graphical environment than client-server GUIs.

F. Browsers can support more diverse devices than dedicated client-server GUI application.

Correct Answer: BCF

Explanation:

QUESTION 5

Which of the following statements are true about an end-to-end security strategy?

A. End-to-end security and point-to-point security are virtually identical strategies proposed by different security vendors.

B. End-to-end security strives to protect data at rest, even in temporary queues.

C. End-to-end security often involves some form of message-level protection.

D. When end-to-end security is enabled. Point-to-point transport-level encryption should be disabledin order to avoid cryptography conflicts between layers.

E. End to-end security is highly beneficial for distributed computing environments where many point- point connections and intermediaries exist, because it offers seamless data protection.

Correct Answer: BCE

Explanation:

B:End to end security is an information-centric perspective of security where information is protected

throughout the entire computing environment. That is, from the points where system interactions originate,

through all points of integration, processing, and persistence.

End to end security is often associated with the secure transmission, processing, and storage of data,

where at no time are data unprotected Note:

For a typical web-based application, end to end security generally begins at the client/browser, and ends at

the application database and all external dependencies of the application.

A common challenge in providing end to end security is finding a suitable way to secure data in all states

and points along the processing path that does not interfere with any transmission, routing, processing,

and storage functions that need to occur along the way. Sensitive data will usually need to be decrypted at

certain points in order for processing or message routing to occur.

QUESTION 6

Which statement best describes the role of the Data Normalization Layer within the Logical view of the Service-Oriented Integration (SOI) architecture?

A. The Data Normalization Layer converts all data formats to third normal form to facilitate database access.

B. The Data Normalization Layer converts all data formats to XML to facilitate platform independent.

C. The Data Normalization Layer hides the complexity of the multiple data formats used by back end systems by converting data to standardized formats.

D. The Data Normalization Layer stores persistent data in a normalized format.

E. The Data Normalization Layer provides normalized access to all databasesiIncluded as back-end systems in the architecture.

Correct Answer: C

Explanation:

The Data Normalization Layer provides a standardized format for data entities. Each EIS stores data in its

own (usually proprietary) format. This layer transforms the data to a form that is readily consumable by the

upper layers in the architecture.

The primary purpose of this layer in the architecture is to encapsulate and hide the complexity of the data

models and formats used by the back-end systems. This allows the upper layers in the architecture to

operate on data entities that match the needs of the business rather than operating on data that match the

storage approach of the back-end systems.

References:

QUESTION 7

Which of the following token profiles is not included in the WS-Security standard as a standard type of identity token?

A. XACML token profile

B. SAML token profile

C. username token profile

D. Kerberos token profile

E. X.500 token profile

Correct Answer: A

Explanation:

TheWS-Securityspecification allows a variety of signature formats, encryption algorithms and multiple trust domains, and is open to various security token models, such as:

*

X.509 certificates (not E)

*

Kerberos tickets (not D) *UserID/Password credential (not C)

*

SAML Assertions (not B) *custom-defined tokens.

Note: WS-Security (Web Services Security, short WSS) is a flexible and feature-rich extension to SOAP to apply security to web services. It is a member of the WS-* family of web service specifications and was published by OASIS.

QUESTION 8

Which of the following are examples of the management and visibility gap between the traditionally monitored IT Infrastructure resources and the Services?

A. On-going Shift to Move to an Agile Shared Service Computing Environment

B. On-going Shift to Manage IT from an End-User Experience Perspective

C. Loosening of Corporate Policies and Regulations

D. Increasing Number of Heterogeneous IT Infrastructure Components to Manage

E. Complex Distributed Environments Requiring Access to Consolidated Information

Correct Answer: ABDE

Explanation:

Examples of the management and visibility gap are listed below:

*

On-going Shift to Move to an Agile Shared Service Computing Environment

*

On-going Shift to Manage IT from an End User Experience Perspective

*

Increasing Need to Enforce Regulatory and Corporate Policies (not C)

*

Increasing Number of Heterogeneous IT Infrastructure Components to Manage

*

Complex Distributed Environments Require Access to Consolidated Information

Note: Many companies today are deploying enterprise technology strategies (ETS) such as Service-Oriented Architectures (SOA), Business Process Management (BPM), and Cloud Computing, which are designed to make functions, processes, information, and computing resources more available. While these ETSs offer additional benefits and sophistication, they have created a management and visibility gap between the traditionally monitored IT infrastructure resources and the services that contribute to the overall experience encountered by the end user.

References:

QUESTION 9

Conceptually, management and monitoring capabilities consist of which of the following?

A. consolidating administration tasks for a variety of infrastructure components

B. homogeneous support for IT management environments

C. skilled architects to perform root-cause analysis

D. allowing enterprises to define, model, capture, and consolidate monitoringinformation into a single framework

Correct Answer: AD

Explanation:

QUESTION 10

A modular approach has been taken to document the Oracle Reference Architecture (ORA). Select the statements that are true for this modular approach?

A. The ORA library has a document dedicated to each Oracle product suite.

B. ORA is a collection of reference architectures, some based on specific technologies (Technology Perspectives), and some on industry verticals (Industry Perspectives).

C. ORA is a single-reference architecture but is documented via different views of the architects-some focused on specific technologies (Technology Perspectives), and some on industry verticals (Industry Perspectives).

D. The number of Technology Perspectives and Industry Perspectives will increase over time.

E. The technology Perspectives are complete, but the Industry Perspectives will increase over time as more verticals are Included.

Correct Answer: ACD

Explanation:

A: The scope of ITSO is all of Oracle\\'s product families. However, the Oracle technology real estate is extremely large and evolves as new products are introduced. Thus, the ITSO material will continue to grow as more ORA documents are created, additional ETSs are covered, and additional ESDs are created. C, D:Technology perspectives extend the core material by adding the unique capabilities, components, standards, and approaches that a specific technology strategy offers. SOA, BPM, EPM/BI, and EDA are examples of perspectives for ORA. Each technology strategy presents unique requirements to architecture that includes specific capabilities, principles, components, technologies, standards, etc. Rather than create another reference architecture for each strategy, ORA was designed to be extensible to incorporate new computing strategies as they emerge in the industry.

In order to present the reference architecture in the most effective manner, each new technology strategy adds a perspective to ORA. This enables the reference architecture to evolve holistically. New computing strategies extend the core material, providing further insight and detail as needed. A perspective extends the ORA core collateral by providing views, principles, patterns, and guidelines that are significant to that technology domain yet cohesive with the overall ORA. The perspective includes:

*

A foundation document describing the terms, concepts, standards, principles, etc. that are important to the ETS.

*

An infrastructure document that defines a reference architecture built using the technologies pertinent to the ETS.

An industry reference architecture is a set of high level architectural representations which characterize the current state architecture of an enterprise and a desired state, or architectural vision, based on the ORA.

References:

QUESTION 11

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 12

Which statement best describes the relationship between a SOA Service and service Infrastructure?

A. Service infrastructure is a primary part of an SOA Service.

B. Service Infrastructure exposes the Service Interface and may satisfy some capabilities of the Service Implementation.

C. Service infrastructure fulfills the Service Contract.

D. A SOA Service depends on the service infrastructure to satisfy some required capabilities.

E. A SOA Service uses the service infrastructure to generate the Service Interface.

Correct Answer: B

Explanation:

The Service Infrastructure side typically provides the Service enablement capabilities for the

implementation. These capabilities may include, exposing the interface as a Web Service, handling SLA

enforcement, security, data formatting, and others. Service infrastructure should be utilized when possible,

as it reduces the burden on Service providers, from an implementation standpoint.

References:

QUESTION 13

Oracle Reference Architecture uses multiple views (as defined by standard IEEE 1471) to describe the architecture. Which statement best describes the use of views within ORA?

A. Each view within ORA focuses on a particular set of Oracle products.

B. ORA provides multiple views (for example, Conceptual, Logical, Deployment) to describe the architecture to various stakeholders.

C. Each view within ORA focuses on a particular set of industry standards.

D. ORA provides multiple views (for example, Product Mapping, Deployment) to illustrate how Oracle products must be installed and configured.

E. ORS uses views to illustrate industry standards and document architecture guidelines.

Correct Answer: B

Explanation: It is important that the service-oriented reference architecture documents the architecture from multiple views. Each view might include multiple models to illustrate the concepts, capabilities, etc. important for that view. The particular choice of views depends on what material is being covered and which views best convey the information. Example views include conceptual, logical, product mapping, and deployment views.

References:

QUESTION 14

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.

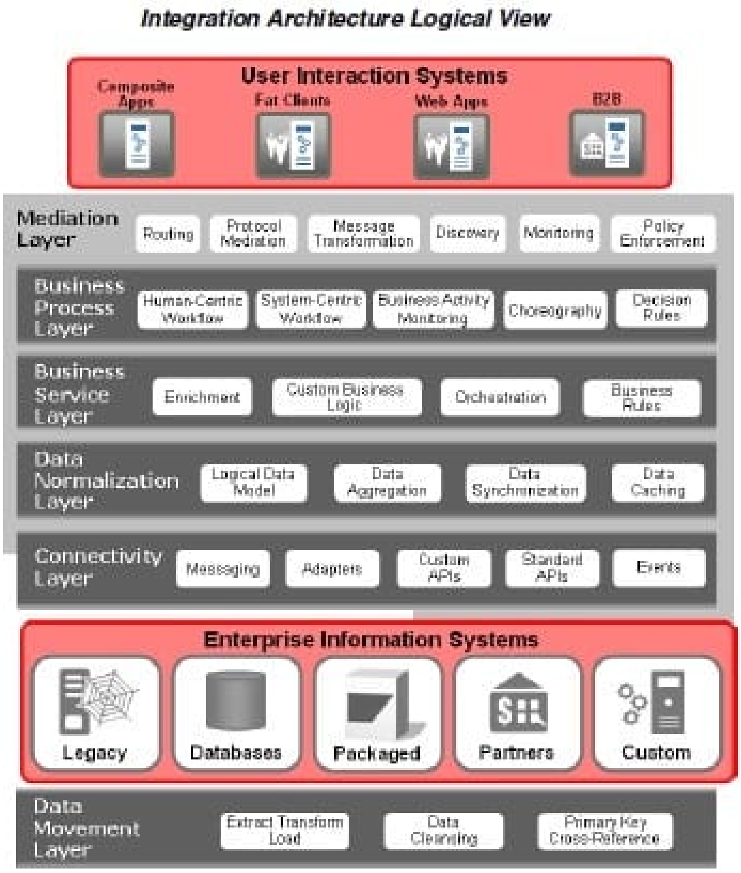
F. The layers are used to partition the capabilities of the architecture, but otherwise have no architectural significance.

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 15

Which of the following statements are true about the XACML standard and architecture?

A. The Policy Enforcement Point (PEP) is where permit / deny access decisions are made.

B. The Policy Information Point (PIP) provides information such as user attributes or environmental data that may be used to make access control decisions.

C. XACML defines an XML schema used to represent rules for access control.

D. XACML defines a TCP protocol used to communicate messages between Policy Enforcement Points.

E. SAML assertions can be used to carry XACML authorization decisions.

Correct Answer: ABCE

Explanation:

A: PEP - Policy Enforcement Point, where permit/deny access decisions are enforced.

B: PIP - Policy Information Point, where information can be retrieved to evaluate policy conditions. For example, a user\\'s role or time of day may be needed by the PDP to make a policy decision.

C: eXtensible Access Control Markup Language (XACML) provides a standard way to represent access control policy information using XML. XAMCL defines access control policies in terms of rules, which in turn are defined to include a target, an effect, and a set of conditions. XACML defines an XML schema used to represent rule

E: The SAML 2.0 profile of XACML 2.0 defines SAML assertions used to carry policies, policy queries and responses, authorization decisions, authorization query decisions and responses, and attribute assertions. In this way SAML authentication, attribute, and authorization assertions are incorporated into the security framework to complement XACML.

References: