Oracle

Exam 1z0-574

Oracle IT Architecture Essentials

Verson: Demo

[Total Questions: 10]

Question No : 1

Which statement best describes the relationship between the Oracle Reference Architecture (ORA) and Service-Oriented Architecture (SOA)?

A. ORAincludes many different technology perspectives (for example, BPM, BI) Including SOA. The SOA perspective provides a view of ORA focused on the products and technology applicable to SOA.
B. ORA embraces service orientation as a core tenet to consistently and uniformly deal with the complexity of a heterogeneous computing environment common to enterprise IT.
C. ORA embraces SOA as a core tenet; therefore, adopting ORA means that SOAis adopted as well.
D. ORA is a reference architecture based on architecture principles and best practices. SOA is a marketing term that has become widely and ambiguously used within the industry.
E. SOAis an architectural approach that isproduct- and vendor-independent,ORA is essentially a SOA implemented using Oracle products and technology.

Answer: B

Explanation: ORA does have a special relationship with SOA. ORA embraces service-orientation as a core tenet to improve agility, rationalize functions and data, and promote reuse in an effective manner. The entire strategy of SOA is not core to ORA (not C), but the concept of exposing data and functionality as interoperable SOA Services is core to ORA.
ORA must provide interoperability across all Oracle products and must also effectively deal with the heterogeneity that exists in IT environments. SOA Services provide a clean, consistent approach to deal with both of these complexities. This is the reason that ORA includes service orientation as a core tenet.

Stated as an architecture principle, this becomes:
* The architecture embraces services as the primary mechanism for interoperability and integration.

Reference: Oracle Reference Architectureand Service Orientation, Release 3.0

Question No : 2

Which statements are correct for service versioning within Service-Oriented Integration?

A. Only one production version of each SOA Service should be allowed. Multiple versions cause service sprawl.
B. Service consumers should be allowed to migrate to new versions of SOA Services over time as part of regular maintenance.
C. Service consumers should be automatically migrated to new versions of SOA Services by using the mediation layer to perform any necessary translations or transformations.
D. At most two versions of an SOA Service are allowed in production, one current and one that's deprecated.
E. The architecture must support multiple, concurrent production versions of SOA Services.

Answer: B,E

Explanation: B (not C): Service consumers are able to migrate to a newer version of a SOA Service gracefully.
Service consumers should migrate to a new version of a SOA Service as part of a normal maintenance process. The coordinated deployment of service consumers and service providers should not be necessary.
Implications:
* A service migration strategy needs to be established.
* The architecture must support graceful service migration.

E(not A, not D):There may be multiple versions of a SOA Service in production concurrently.
Invariably a SOA Service will require modifications to support new consumers or to expand functionality. Supporting concurrent versions of a SOA Service is essential for a sound service versioning approach.
Implications:
* A service versioning strategy needs to be established.
* The architecture must support multiple, concurrent versions of a SOA Service.

Reference: Oracle Reference Architecture, Service-Oriented Integration, Release 3.0

Question No : 3

How is Oracle Database Firewall (ODF) used to protect applications from attacks such as SQL-Injection?

A. ODF is an option for the Oracle Database. A DBA configures this option to inspect database commands and compare them with a set of known attacks. An ODF agent periodically downloads the latest signatures in order to keep up with the latest known types of attacks.
B. ODF is a feature of Oracle Advanced Security. A database security administrator configures each database realm with a set of acceptable ports and protocols from which database clients can connect. Valid connections are continuously monitored for suspicious activity.
C. ODF is an agent based secure connection component that is installed on the database and on the clients. It creates a VPN-like connection between the two that greatly reduces the likelihood of man-in-the-middle and SQL-injection attacks. An administrator installs ODF and configures it for a specific environment.
D. ODF is a stand-alone product that is installed in between the client and database. It monitors and/or blocks SQL statements, comparing them against a set of known good or known bad statements.

Answer: D

Explanation: Oracle Database Firewall (ODF) - ODF is the first line of defense for both Oracle
and non-Oracle databases. It monitors database activity on the network to help prevent unauthorized access, SQL injections, and other forms of attack. ODF uses positive (white list) and negative (black list) security models to validate SQL commands before they can reach the database.
The ODF instances act as a firewall for incoming SQL
traffic. Each instance can handle multiple downstream databases, and the instances are configured for high availability. SQL traffic must pass through the firewall boxes in order to reach the databases.
ODF protects Oracle, MySQL, Microsoft SQL Server, IBM DB2 for Linux, Unix, and Windows, and Sybase databases

Reference: Oracle Reference Architecture,Security, Release 3.1

Question No : 4

There are a number of ways to classify applications in order to assess business risks and assign appropriate security policies. Which of the following is not described as a primary means to classify an application?

A. by the user community it serves, such as HR, finance, all employees, general public,

and so on
B. by the information it handles, such as classified information, personal information, publicly availableinformation, and so on
C. by business criticality, such as revenue-generating applications versus informational applications
D. by technology and/or vendor, such as .NET versus Java, and so on
E. by the applicability of existing laws and regulations pertaining to privacy, auditing, and access control

Answer: D

Explanation: Applications can be classified in a number of ways, such as:
* By the user community it serves, such as HR, Finance, company executives, all employees, all persons working on behalf of the company (includes contractors and temporary workers), general public, etc. (not A)
* Based on information confidentiality. Some applications process personal information while others do not. Likewise, in military terms, an application might be targeted towards individuals with a specific level of clearance. (not B)
* Based on business criticality. Some applications may have a direct and severe contribution or impact to revenue. Examples include order processing, credit card processing, call processing, securities trading, and travel reservations. Others may have little or no impact. (not C)
* Based on the applicability of existing laws and regulations. For example, HIPPA puts more security emphasis on patient records than would otherwise exist. (not E)
* Based on network exposure. Levels might include: locked down (no network access), secure production environment access, general organization-wide intranet access, partner access, Internet access limited to a specific user community, and Internet access open to the public.

Reference: Oracle Reference Architecture,Security, Release 3.1

Question No : 5

What is meant by cache hit rate or ratio?

A. the percentage of times the cache was hit successfully over the total number of tries
B. the percentage of times the cache was refreshed from the back-end database
C. the number of servers the cache is replicated to
D. the ratio of cache objects in a server to the total number of cache objectsin the server cluster

Answer: A

Explanation: Cache hit rate or ratio: The percentage of times the cache was hit successfully over the total
number of tries is called the hit ratio.

Reference: Oracle Reference Architecture, Application Infrastructure Foundation, Release 3.0

Question No : 6

Which of the following is NOT defined as a primary ORA computing foundation component?

A. Distributed Computing
B. Utility Computing
C. Grid Computing
D. Caching

Answer: D

Explanation: Primary ORA computing foundation components:
Distributed Computing
On-Demand Computing
Utility Computing
Grid Computing
Cloud Computing
Elastic Computing
Virtualization

Reference: Oracle Reference Architecture, Application Infrastructure Foundation, Release 3.0

Question No : 7

Which statement best describes the relationship between a Service Contract and a Usage

Agreement as defined by the Oracle Reference Architecture (ORA)?

A. There is a one-to-one relationship between a Service Contract and a Usage Agreement. For each Service Contract there is a corresponding Usage Agreement.
B. There may be multiple Usage Agreements associated with a single Service Contract.
C. There may be multiple Service Contracts associated with a single Usage Agreement.
D. There is a many-to-many relationship between Service Contracts and Usage Agreements.
E. There is no defined relationship between a Service Contract and a Usage Agreement.

Answer: B

Explanation: The Service Contract defines what the SOA Service agrees to provide to the environment.

The service consumer Usage Agreement defines what a particular service consumer is entitled to consume.
Each service might have several consumers.
The Service provider must ensure that the Service will satisfy the aggregate specifications of all related usage agreements.

Note:
The usage agreement is not part of the Service; rather it defines what a particular service consumer is entitled to consume from the Service.
Having both a usage agreement and a service contract provides a decoupling between the service provider and service consumer. This not only facilitates reuse but also provides a separation of concerns. The service contract defines the totality of what the Service guarantees to provide, and can be written and validated independent of any knowledge of specific service consumers. The usage agreement is service consumer specific and defines what capabilities of the Service each consumer is allowed to consume.

Reference: Oracle Reference Architectureand Service Orientation, Release 3.0

Question No : 8

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.

Answer: B,C,E

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 No : 9

Which product provides the standard communication protocols (for example, HTTPS) between the Client Tier and the Service Tier as well as Message Security?

A. Oracle platform Security Services
B. Oracle WebCenter
C. Application Development Framework
D. Oracle HI IP Server

Answer: A

Explanation: Oracle Platform Security Services comprises Oracle WebLogic Server's internal security framework and Oracle's security framework (referred to as Oracle Platform Security). OPSS delivers security as a service within a comprehensive, standards-based security framework.
The Security Services includes SSL:Hypertext Transfer Protocol Secure (**HTTPS**) is a combination of Hypertext Transfer Protocol (**HTTP**) with **SSL**/TLS protocol.

Note:Oracle Platform Security Services (OPSS) provides enterprise product development teams, systems integrators (SIs), and independent software vendors (ISVs) with a standards-based, portable, integrated, enterprise-grade security framework for Java Standard Edition (Java SE) and Java Enterprise Edition (Java EE) applications.
OPSS provides an abstraction layer in the form of standards-based application programming interfaces (APIs) that insulate developers from security and identity management implementation details. With OPSS, developers don't need to know the details of cryptographic key management or interfaces with user repositories and other identity management infrastructures. Thanks to OPSS, in-house developed applications, third-party applications, and integrated applications benefit from the same, uniform security, identity management, and audit services across the enterprise.
OPSS is the underlying security platform that provides security to Oracle Fusion Middleware including products like WebLogic Server, SOA, WebCenter, ADF, OES to name a few. OPSS is designed from the ground up to be portable to third-party application servers. As a result, developers can use OPSS as the single security framework for both Oracle and third-party environments, thus decreasing application development, administration, and maintenance costs.

Reference: Oracle® Fusion Middleware Security Overview, 11g Release 1, About Oracle Platform Security Services

Question No : 10

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.

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.

Reference: Oracle Reference Architecture, Service-Oriented Integration, Release 3.0