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.pass2lead.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 statements are true about defense-in-depth strategy?

A. It saves money by allowing organizations to remove costly perimeter security Infrastructure.

B. It is a strategy designed to win the battle by attrition. It consists of multiple security measures at various levels as opposed to a single barrier.

C. It includes security measures for the network, the operating system, the application, and data.

D. Due to network overhead issues, it should not be used in a distributed computing environment such as SOA or cloud computing.

E. It is a good strategy to protect an organization from insider threats.

Correct Answer: BCE

Explanation:

Defense in depth is a security strategy in which multiple, independent, and mutually reinforcing security

controls are leveraged to secure an IT environment.

The basic premise is that a combination of mechanisms, procedures and policies at different layers within

a system are harder to bypass than a single or small number security mechanisms. An attacker may

penetrate the outer layers but will be stopped before reaching the target, which is usually the data or

content stored in the \\'innermost\\' layers of the environment. Defense in depth is also adopted from military

defense strategy, where the enemy is defeated by attrition as it battles its way against several layers of

defense.

Defense in depth should be applied so that a combination of firewalls, intrusion detection and prevention,

user management, authentication, authorization, and encryption mechanisms are employed across tiers

and network zones.

The strategy also includes protection of data persisted in the form of backups and transportable/mobile

devices. Defense in depth should take into account OS and VM hardening as well as configuration control

as means of preventing attackers from thwarting the system by entering via the OS or by tampering with

application files.

References:

QUESTION 2

The Oracle Reference Architecture (ORA) includes the central layers as well as Technology Perspectives and Industry perspectives. Which statements best describe how these are related within ORA?

A. The Technology Perspectives are reference architectures incorporating specific technologies, products, and standards.

B. The Technology Perspectives provide a view of ORA focused on specific technologies, product and standards.

C. The Industry Perspectives are reference architectures for specificindustries, for example, Telco, Pharma.

D. The Industry Perspectives extend the central layers of ORA toincludeindustry-specific capabilities, components, and so on.

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

Correct Answer: BD

Explanation:

The core ORA material is extended via architecture perspectives. There are two types of perspectives:

Technology and Industry(not E).

B: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.

Industry perspectives extend the core material by adding the business functions, business processes, data entities, software capabilities and components that an industry vertical requires. Retail, Financial, Telco, and Pharma are examples of industry perspectives for ORA.

References:

QUESTION 3

A company is building a new customer self-service website. The company has an existing CRM application that

contains customer information that needs to be integrated into the self-service website. The CRM application provides a synchronous interface to access the needed customer information. The CRM application takes 5 to 30 seconds to respond to the request for customer information. The requirements for the new customer self-service website is to respond within 3 seconds 90% of the time. What integration pattern would you suggest that the company use to integrate the CRM application into the new customer self-service website?

A. Use the request-response message exchange pattern to access the synchronous interface provided by the CRM application. The request-response message exchange pattern matches the synchronous interface provided by the CRM application, so this is the simplest and best approach for integration.

B. When customer information from the CRM application is needed, asynchronously fetch the information by using the store-and-forward integration pattern. This approach allows the self-service website to respond quickly to customer requests without waiting for the CRM application. The website can display the fetched customer information when it is available.

C. Use the request optional-response message exchange pattern to access the CRM application. If the CRM application responds quickly (for example, in 5 seconds) use that response. If the CRM application does not respond quickly, then the optional response was not returned and processing continues.

D. When customer information from the CRM application is needed, post a message to a topic queue by using the publish-and-subscribe integration pattern. This approach allows the CRMapplication or any other application subscribing to the topic queue to respond with customer information.

E. Use the polling integration pattern to find the necessary customer information in the CRM application database. Obviously the data exists in the CRM application database. Obliviously the data exists in the CRM application database, so the slow response from the CRM application can be eliminated by polling directly from the CRM application database.

Correct Answer: B

Explanation:

An asynchronous exchange patternwould be good here. Asynchronous communication can be used when

the response time for the source system is too slow to support the timelines of the calling systems.

Note: Store-and-forward is a special case of asynchronous communication. In the store-and-forward

pattern, the request message is put onto a queue for later retrieval by the target of the request message.

Similarly, the response message is put onto a response queue for later retrieval. This is a very common

approach used by messaging systems (e.g. MQ Series) to integrate with legacy systems. The architecture

must support this integration pattern to facilitate integration with legacy systems and existing messaging

systems.

References:

QUESTION 4

Why is it necessary to have Integration of Metadata Repository to the Source Code Management (SCM) server?

A. The SCM needs to access the asset metadata for reporting purposes.

B. The Metadata Repository links the asset metadata to the asset payload, which may be archived in the SCM.

C. The Metadata Repository promotes the assets to the SCM.

D. The Metadata Repository stores the asset metadata in the SCM.

Correct Answer: B

Explanation: SCM server manages the code base and configuration. It uses file store or database for maintaining the asset payload and to manage the versioning of the assets. Note: The metadata repository is primarily a human interface for asset capture and presentment. It has integration with the service registry to promote the service interfaces and with the security framework for repository security like authentication and access control. It also has integration with other enterprise asset sources like Source Code Management (SCM) tools and file servers. Source Code Management (SCM) is the management of changes to documents, programs, and other information artifacts.

References:

QUESTION 5

Which one of the following statements best describes authentication as a service?

A. Authentication is a service offered by the local computing platform to the application it is hosting. The application uses this service to authenticate users with a local LDAP.

B. Authentication is a service offered by the enterprise security framework. Applications access it directly, bypassing local platform security. The authentication service provides a level of abstraction between applications and the various instances of infrastructure (LDAPs, databases) that can be used to verify credentials.

C. Authentication is a service offered by both the local computing platform and the enterprise security framework. The local platform can be configured to direct requests to local LDAPs or common enterprise services, depending on the operating environment (dev/test/production). Meanwhile, the enterprise security framework services can virtualize several shared credential stores into a single shared service.

D. Authentication is not a valid example of a security service.

Correct Answer: C

Explanation: ORA Security is one of the series of documents that comprise Oracle Reference Architecture. ORA Security describes important aspects of the enterprise security layer including identity, role, and entitlement management, authentication, authorization, and auditing (AAA), and transport, message, and data security.

A desktop SSO solution is one that lives on the user\\'s personal computer and handles authentication challenges on behalf of the user. The user logs into his desktop environment, which in turn works on his behalf to authenticate to the applications he accesses. The user is no longer prompted for credentials they are provided automatically by a process running on the desktop.

References:

QUESTION 6

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. AIAis 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 7

Which of the following are benefits of three-tier distributed computing?

A. It allows separation and independent scaling of the data tier and middle/business tier

B. Management of security, transaction, and connection are handled in the middle tier.

C. It allows the client to query the database directly.

D. It improves the performance of the application tenfold.

Correct Answer: AB

Explanation: Three-tier architecture allows the data tier and middle tier to scale independently (A). It also allows multiple clients to share the business logic running in the middle tier. This makes distribution of the application a lot easier. Since security, transactions management, and connection management are handled in the middle tier, it gives better control of the resources (B). Three-tier architecture is more scalable than the simple client-server model and requires less powerful client side machines. Due to these characteristics this architecture is suitable for small to medium enterprise deployments.

Note: Distributed programming typically falls into one of several basic architectures or categories such as Client-server, three-tier architecture, and N-tier architecture. In the three tier architecture, business logic is handled in the middle tier, presentation rendering is handled on the client and data management is handled in the backend. This architecture allows multiple clients to access centrally deployed business logic components. This allows centralized distribution and management of resources.

References:

QUESTION 8

The Mediation Layer in the Logical View of the Service-Oriented Integration architecture provides several capabilities. Which of the following are capabilities provided by the Mediation Layer?

A. enrichment - adding data elements to a data entity to give the entity increased Information

B. routing - sending the client request to the appropriate provider (s) based on some criteria

C. message transformation - converting the request message format to a different message form, appropriate for the provider

D. choreography - defining the messages that flow back and forth between systems that are participating in a business process

E. protocol mediation - converting a client request from one protocol to a different protocol used by provider

Correct Answer: BCE

Explanation:

The Mediation Layer provides loose coupling for the entire architecture. It decouples the layers of the

architecture as well as decoupling external users of the layers from the specific layers in the architecture.

The key capabilities in this layer include:

*

Routing - Routing provides the ability to send the client request to the appropriate provider based on

some criteria. The routing may even include sending the client request to multiple providers. This capability

facilitates location transparency, versioning, scalability, partitioning, request pipelining, SLA management,

etc.

*

Protocol Mediation - Protocol mediation is the ability to handle a client request using one protocol (e.g.

WS*, JMS, REST) with a provider using a different protocol. This provides protocol decoupling between the

provider and the consumer.

Message Transformation - Message transformation allows a client request using one message format to

be handled by a provider that expects a different message format. This provides message format

decoupling between the provider and the consumer.

*

Discovery - Discovery is the mechanism by which a client finds a provider of a particular SOA Service.

Discovery can occur at design time or runtime.

*

Monitoring - Monitoring captures runtime information about the messages flowing through the mediation layer. Since the mediation layer is an intermediary for message traffic, it provides a centralized monitoring capability.

*

Policy Enforcement - Policy enforcement provides consistent application of policies (e.g. WS-SecurityPolicy) across all messages flowing through the mediation layer. Since the mediation layer is an intermediary for message traffic, it provides a centralized policy enforcement capability.

References:

QUESTION 9

The Oracle Reference Architecture (ORA) contains both horizontal and vertical architectural layers. Which statements best describe the layers within ORA?

A. Lavers only provide a means to partition the capabilities encompassed by ORA and have no significance.

B. Horizontal layers are used to depict that upper layers build on the capabilities provided by lower layers

C. Vertical layers are used to depict capabilities applied across all the horizontal layers.

D. Horizontal layers are used to signify that the lower layers can be accessed only via the upper layers.

E. Vertical layers are used to depict enterprise-wide capabilities, whereas horizontal layers departmental capabilities.

F. Horizontal layers are stateful, whereas vertical layers are stateless.

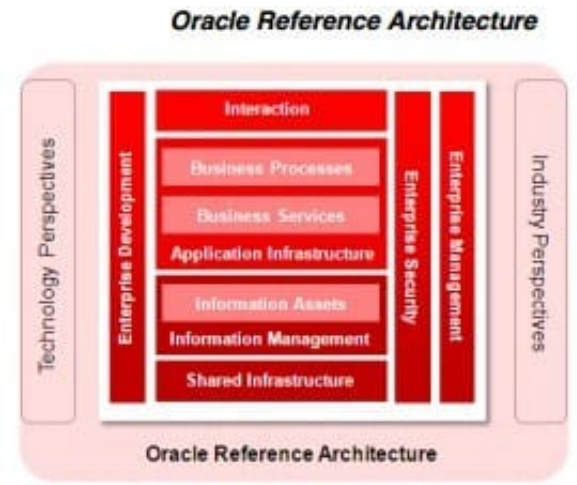
Correct Answer: BC

Explanation:

B: The horizontal layers illustrate that upper layers build upon or use the capabilities of lower layers. Examples: Shared Infrastructure, Information Management, Information Assets, Application Infrastructure C:Layers depicted vertically are orthogonal to the horizontal layers and apply across the entire platform, working in conjunction with horizontal layers to provide a complete solution.

Examples: Enterprise Development, Enterprise Security, Enterprise Management

Note: In order to promote modularity and encapsulation, an architecture will usually be divided into layers. Each layer has a specific purpose and leverages technologies, standards, and products designed specifically to address that purpose. Layers generally build upon the layers below and provide benefits and capabilities to the layers above. The ORA diagram in the figure below illustrates the many aspects of enterprise computing in the form of horizontal and vertical layers



QUESTION 10

What are the three primary delivery models of Cloud computing?

A. Infrastructure as a Service

B. Application as a Service

C. Software as a Service

D. Platform as a Service

Correct Answer: ACD

Explanation:

Regarding the Cloud Provider Perspective.Many resources can be offered as services but the ORA

conceptual model defines three broad categories of services listed below.

*

Infrastructure as a Service (IaaS)

*

Software as a Service (SaaS)

*

Platform as a Service (PaaS)

References:

QUESTION 11

Which of the following are true statements about the benefits of standardizing on a common security framework?

A. Security requirements no longer need to be specified for eachindividual application; the framework will automatically determine what security needs to be applied.

B. A common set of security services and information can be used across the organization, promoting Infrastructure reuseand minimizing inconsistencies.

C. Secure application integrationis made easier via standardization on a preferred subset of technologies and options.

D. Administration and auditing are improved due to rationalization and standardization of identities, attributes, roles, policies, and so on.

E. Interoperability amid federation are easier to achieve via the adoption of common security and technology standards.

Correct Answer: ABE

Explanation:

In order to provide security in a consistent manner, a common set of infrastructure, e.g. a security

framework, must be used. The purpose of this framework is to rationalize security across the enterprise by:

*

Establishing a master set of security data that reflect the policies, IT resources, participants and their attributes across the entire domain of security

*

Mapping organizational structures, computing resources, and users to roles in a way that clearly depicts access privileges for the organization

*

Maintaining fine-grained access rules based on roles that have been established for the organization

*

Propagating the master security data to individual applications and systems that enforce security (A)

*

Detecting changes to security data residing on systems that have not been propagated from the master source of record, and sending alerts regarding these inconsistencies

*

Providing common security services, such as authentication, authorization, credential mapping, auditing, etc. that solutions can leverage going forward in place of custom-developed and proprietary functions (B)

*

Facilitating interoperability between systems and trust between security domains by acting as a trusted authority and brokering credentials as needed(E)

*

Centrally managing security policies for SOA Service interactions

The security framework should provide these types of capabilities as a value-add to the existing infrastructure. The intent is not to discard the capabilities built into current applications, but rather to provide a common foundation that enhances security across the enterprise. Security enforcement can still be performed locally, but security data should be modeled and managed holistically.

Incorrect:

C: Not a main goal.

D: Ease of administration and auditing is not a main goal here.

References:

QUESTION 12

What does Lifecycle Management Provisioning refer to?

A. The process of preparing and equipping a network to allow it to provide (new) services to its users.

B. Automation of the Installation and configuration of operating systems, infrastructure software, applications, services, virtual servers, and hosts across different platforms, environments, and locations

C. Demonstration and enforcement of regulatory standards. Industry standards, and internal best practices

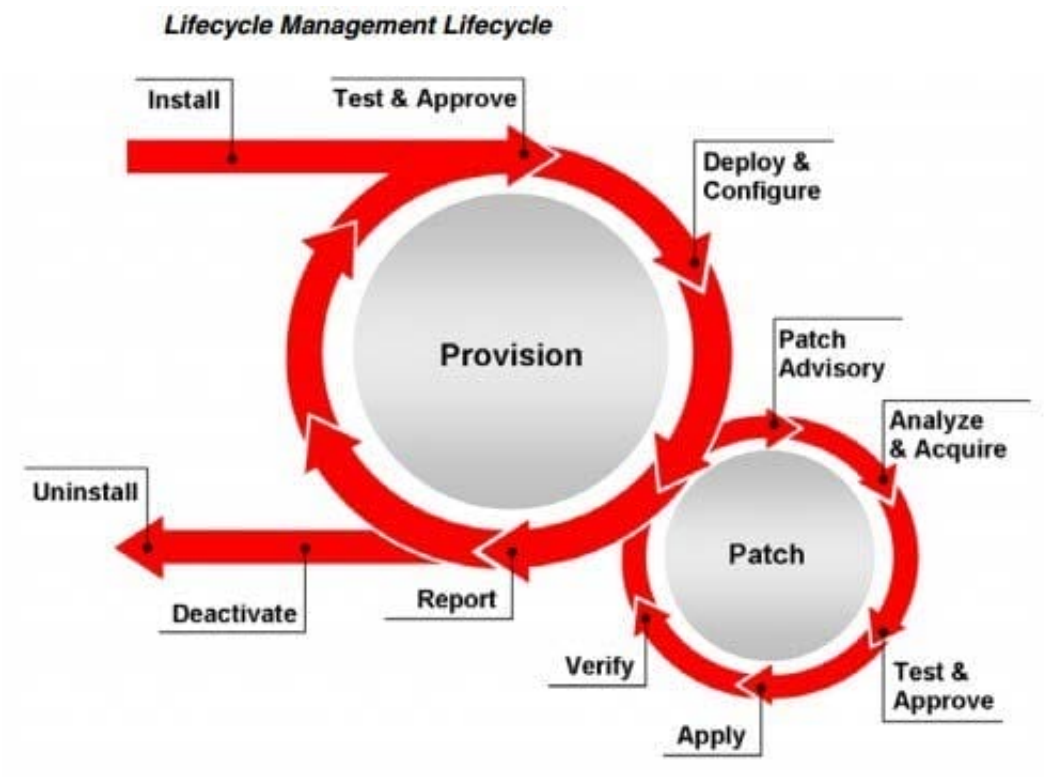
D. A comprehensive management and monitoring solution that helps to effectively manage services from an overview level to theindividual component

Correct Answer: B

Explanation:

Provisioning deals with automation of the installation and configuration of operating systems, infrastructure software, applications, services, virtual servers, and hosts across different platforms, environments, and locations.

Note: Lifecycle Management focuses on managing the lifecycle of software, applications, services, virtual servers, and hosts by automating deployment procedures to not only assist in the deployment of software, applications, services, and servers but also the maintenance of these deployments. This makes critical IT operations easy, efficient, and scalable resulting in lower operational risk and cost of ownership. Two key capabilities within lifecycle management is provisioning and patching.



References:

QUESTION 13

Which statement best describes synchronous versus asynchronous communications in a Service Oriented Integration (SOI) architecture?

A. Both synchronous and asynchronous communication should be supported by SOI. Synchronous communication provides an easier programming paradigm. Asynchronous communication provides greater decoupling between the requester and the responder.

B. The SOI architecture should use only synchronous communication because SOA Services are inherently synchronous. If a back end system supports only asynchronous communications, the "bridging synchronous and asynchronous communications" integration pattern can be used to convert from asynchronous communication to synchronous communication.

C. The SOI architecture should use only asynchronous communication because asynchronous communication provides greater decoupling in the architecture. If a back-end system supports only synchronous communications, the "bridging synchronous and asynchronous communications" integration pattern can be used to convert from synchronous communication to asynchronous communication.

D. The SOA Services in the SOI architecture should use only synchronous communication because SOA Services are inherently synchronous. All communication with back-end system should be asynchronous to decouple the SOA Services from the back-end systems.

E. The communication within the SOI architecture should be asynchronous and should follow the publishand-subscribe integration pattern. The publish-and-subscribe pattern is the most flexible and provides the greatest decoupling and message throughput.

Correct Answer: A

Explanation:

When using synchronous communication the service consumer blocks until the service provider responds.

This is usually the easiest type of communication to program in the consumer application. Thus,

synchronous communication must be supported by the architecture.

Many applications included in integration scenarios do not provide a synchronous interface. Asynchronous

communication is also used when the response time for the source system is too slow to support the

timelines of the calling systems. Thus the architecture must support asynchronous communications.

References:

QUESTION 14

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 15

Which of the following are capabilities required for the Integration subsystem of the Oracle Reference Architecture Management and Monitoring Framework?

A. Data Exchange

B. Extensibility Framework

C. Patch Monitoring

D. Alert and Notification Integration

E. Reporting

Correct Answer: ABD

Explanation:

Key integration capabilities:

*

Data Exchange

*

Extensibility Framework

*

Alert and Notification Integration

Note: While it is preferable to have a single management and monitoring solution it is unrealistic that a single management and monitoring framework can support every available infrastructure component now and in the future. Two-way integration capabilities that cater for message exchange, bulk data exchange and extending the framework are key in addressing the needs of the modern IT environment.