1Z0-574 Q&As

Oracle IT Architecture Release 3 Essentials

Pass Oracle 1Z0-574 Exam with 100% Guarantee

QUESTION 1

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 2

Which of the following statements are true about perimeter security?

A. Though it is often associated with network security, it also applies to physical security measures as fences and locked doors.

B. It is most effective when there is only one perimeter. For example, when inner perimetersare established, they reduce the effectiveness of outer perimeters.

C. The Demilitarized Zone (DMZ) is the most protected zone of the network, which should be reserved for only the most sensitive data.

D. Connections should not be permitted to span more than one perimeter or firewall.

E. Perimeter security can be a component of a defense-in-depth strategy.

F. Perimeter security is most effective for protection against insider threats.

Correct Answer: ADE

Explanation:

A: Your inner perimeter consists of the doors, windows and walls of your building(s). Protecting your inner perimeter is usually accomplished with locks, keys and alarm systems.

D:

E: Defense in depth is a security strategy in which multiple, independent, and mutually reinforcing security controls are leveraged to secure an IT environment. 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. Defense in depth is compatible with perimeter security in that network perimeters (or more generically, protection zones) can make up part of the defense in depth strategy.

References:

QUESTION 3

Select the most appropriate reason why three-tier architecture is a better architectural choice than simple client-server architecture for complex enterprise applications.

A. Three-tier architecture uses three threads to run the applications, so performance is better.

B. Three-tier architecture combines presentation, business logic, and data processing of business logic, data, and presentation. This allows the tiers to be independently scaled to maximize the investment.

C. Three-tier architecture combines presentation, business logic, and data processing into a single layer to eliminate network latencies.

D. Three-tier architecture moves all processing to the client, thereby reducing the load on the server.

Correct Answer: B

Explanation: Three-tier architecture allows the data tier and middle tier to scale independently. 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. 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 4

Which of the following statements are true about point to point security?

A. It is often implemented using transport security protocols such as SSL/TLS.

B. It is designed to transport sensitive data over unprotected networks.

C. After data reaches an endpoint, it offers no further protection.

D. It can be combined with other forms of security such as perimeter security and defensein depth

E. SSL/TLS is used sparingly because it is difficult to set up.

Correct Answer: ABCE

Explanation:

A: The downside to TLS is that it only protects data in transit, or "point-to-point". Once data is received, it is no longer protected.

B: Point to point security is often used as a

default or minimal security option in order to protect messages over insecure networks.

C:A lesser alternative to end to end security is point to point security. This is used to protect messages in transit. It assumes that other means of security are used to protect messages during processing and persistence.

Generally, less effort is made to protect data behind the corporate firewall. This opens up a number of vulnerabilities and risks to an organization.

E: SSL/TLS is not so hard to set up. It is popular.

References:

QUESTION 5

Which of the following is not a key function of an identity management system?

A. user provisioning

B. password maintenance and self-service

C. approval workflow

D. LDAP integration

E. authentication

Correct Answer: BE

Explanation:

References:

1Z0-574 PDF Dumps 1Z0-574 Practice Test 1Z0-574 Braindumps