



# 1Z0-574<sup>Q&As</sup>

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

Audit logging is a form of what type of access control mechanism?

- A. detective control
- B. preventive control
- C. deterrent control
- D. corrective control
- E. compensating control
- F. recovery control

Correct Answer: A

Explanation:

There are many different forms of access control, which in turn can be classified into one or more categories.

Detective - Detective controls are meant to record all activities. They are passive systems that are aware of events but are not designed to prevent them from happening. Audit logging is a form of detective access control.

References:

---

### QUESTION 2

How do you enable risk profiling on the Authentication Service?

- A. Risk profiling is a feature of Oracle Identity Manager (OIM). It can be performed on any collection of users, groups, and/or roles. Risk profiling is an available option for OIM 11g. An administrator must install the license and configure the set of identities to profile.
- B. Risk profiling is a standard feature of Oracle Access Manager (OAM). It is enabled by default, but configured to only profile administrative identities. The OAM administrator can configure additional identities individually, or by group, or enable profiling on all users.
- C. Risk profiling is a feature of Oracle Adaptive Access Manager (OAAM), OAAM works in conjunction with OAM to provide value-add authentication features. OAAM will assess anomalies based on configurable rules, behavior, and risk analysis and will challenge users when risks are detected.
- D. Risk profiling is a feature of Oracle Advanced Security. This comprehensive suite provides value-add authentication and authorization capabilities including multi-factor authentication and rule-based authorization. OAS is a separately installed product that integrates with OAM, OIM, and Oracle Entitlements Server (OES).
- E. Risk profiling is a feature of Oracle Virtual Directory (OVD). It will assess risk based on login attempts, login devices,



login locations, and so on, and take action based on configurable rules. Possible actions include denying access, terminating sessions, and raising alerts. Sample rules are provided out of the box, and additional rules can be added via the IVD administrative console.

Correct Answer: C

Explanation:

The Oracle Adaptive Access Manager (OAAM) is part of the Oracle Identity Management product suite that provides access control services to web and other online applications.

The premise was simple in that the existing authentication technologies were unsatisfactory and easy to compromise. No authentication technology can really provide its full and intended security benefits unless the computer and computer network are re-designed from the grounds up. Oracle Adaptive Access Manager has two components, the strong Authentication-agnostic security component and the application-agnostic Risk component. One simple example of the Strong Authentication component is that a User can choose a personalized keypad and use mouse clicks to enter password to prevent passwords being stolen with key loggers and being phished or pharmed. The Risk Component analyzes the authentication and transaction data for abnormalities and anomalies in real-time to prevent fraud and also in off-line mode to identify and detect internet fraud.

Note:

Oracle Access Manager (OAM) - OAM provides an identity management and access control system that is shared by all applications. It offers a centralized and automated single sign-on (SSO) solution for managing who has access to what information across IT infrastructure.

Oracle Adaptive Access Manager (OAAM) - OAAM provides superior protection for businesses and their customers through strong yet easy-to-deploy multifactor authentication and proactive, real-time fraud prevention. Oracle Identity Manager (OIM) - OIM is a user provisioning and administration solution that automates the process of adding, updating, and deleting user accounts from applications and directories; and improves regulatory compliance by providing granular reports that attest to who has access to what resources Oracle Virtual Directory (OVD) - OVD virtually aggregates identity information from multiple sources and presents a real-time unified view without storing or copying the identity data itself.

---

### QUESTION 3

You are developing an Integration component that uses customer data. The source system defines customer data in a



different format than expected. Which of the following options best describes how you would develop the component?

- A. Create an object representation of customer data and use it in the component.
- B. Externalize the data transformation by mapping the source data format to a canonical data format.
- C. The data formats are different, so it is not possible to develop the component.
- D. Write data from the source system into a database and read it back in the expected format.

Correct Answer: A

Explanation:

Note: It is quite common to encounter use cases that require transformation of information from one format to another, especially in the area of enterprise integration. Source systems and target systems may use very different representations of data and in some cases, a canonical data model might be used as a common intermediate format. In some cases, the transformation is a simple field-to-field mapping whereas in other cases it is a complex manipulation and conversion of data. It should be possible to visually map the source and target representations with the ability to enrich the elements to support both simple and complex data transformations.

---

#### QUESTION 4

Which of the following statements is true with respect to virtualization?

- A. Visualization creates a layer of abstraction that allows the underlying resources to be managed independently of the applications that run on them.
- B. Virtualization is a hardware appliance that allows the applications to run faster.
- C. Virtualization is a technology used for creating clusters to support scalability of the infrastructure.
- D. Visualization may lead to server sprawl and decrease the overall data center utilization.

Correct Answer: AC

Explanation:

A: Computer hardware virtualization (or hardware virtualisation) is the virtualization of computers or operating systems. It hides the physical characteristics of a computing platform from users, instead showing another abstract computing platform.

C: Computer clusters have historically run on separate physical computers with the same operating system. With the advent of virtualization, the cluster nodes may run on separate physical computers with different operating systems which are painted above with a virtual layer to look similar. The cluster may also be virtualized on various configurations as maintenance takes place.

References:

---

#### QUESTION 5

Which of the following are capabilities provided by the Monitoring Engine within the Logical view of the Management and Monitoring architecture?

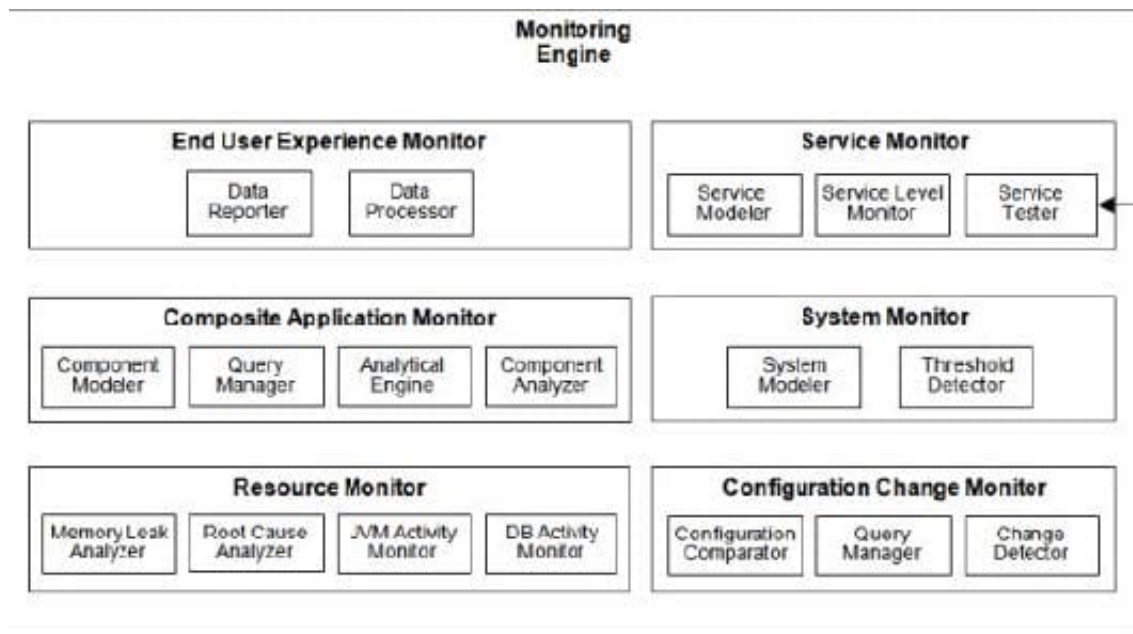


- A. Resource Monitor
- B. System Monitor
- C. Collection Monitor
- D. Service Monitor

Correct Answer: ABD

Explanation:

Logocal View, Monitoring Engine:



Note: The Monitoring Engine contains a number of monitoring sub-systems which respond to scheduled events, and specific user actions within the management console in making various requests for data to be collected from various managed targets. In addition, these monitoring sub-systems integrate with each other to offer the administrator full discovery and drill down capabilities.

References:

[Latest 1Z0-574 Dumps](#)

[1Z0-574 PDF Dumps](#)

[1Z0-574 Practice Test](#)