

Oracle 1z0-545

Identity Administration and Analytics 11g Essentials

Version: 5.2

QUESTION NO: 1

You selected a group of 200 users. The users are distributed among 10 business structures. Next, you selected to certify as 'Business unit manager'. How many certifications will be created?

- A. 1
- B. 5
- C. 10
- D. 100
- E. 200

Answer: A

Explanation:

QUESTION NO: 2

Identify four main benefits of the Identity Audit functionality provided by OIA.

- A. Meeting compliance needs
- B. performing actual account screening
- C. Enterprise role life cycle management
- D. Monitoring audits using dashboards
- E. consolidating roles

Answer: A,C,D,E

Explanation: A: Oracle Identity Analytics (OIA), formerly Sun Role Manager (SRM) provides comprehensive

enterprise rolifecycle management and identity compliance capabilities to streamline operations, enhance compliance, and reduce costs.

C: Enterprise role lifecycle management includes the business processes and technologies governing the creation and maintenance of roles and their assignments to users.

D: Oracle Identity Analytics provides comprehensive dashboards and reporting capabilities based on user identity, access and audit data residing in the Identity Warehouse. Oracle Identity Analytics provides various compliance and operational dashboards for a quick review of compliance and operational status in context of roles, segregation of duty policies, audit policies and other controls

E: The use of roles lowers costs by simply reducing the number of objects that have to be managed for certification reviews and SoD monitoring. Instead of attempting to manage tens of thousands of individual entitlements across thousands of

applications, Oracle Identity Analytics can be used to define and manage far fewer roles into which those individuals fit

Reference: Oracle Identity Analytics Architecture, Oracle Technical White Paper

Reference: Oracle Identity Analytics, Business Overview, Oracle White Paper

QUESTION NO: 3

You have developed OIA in an environment where the provisioning engine is provided by another vendor.

How would you configure OIA to work with this third-party provisioning engine?

- A. OIA can work only with OIM and legacy SUN IDM.
- B. Add another entry and bean in conf-context.xml.
- C. Establish user mapping in iam-context.xml.
- D. Uncomment the corresponding entry bean in iam-context.xml.
- E. Add an additional entry and bean in Rolemanagement-context.xml.

Answer: D

Explanation: Oracle Identity Analytics integrates with third-party products to pull in user, account and entitlement data, and to provide closed-loop remediation.

In the Role Manager user interface, the Administration > Configuration > Provisioning Servers tab displays "file" and "sun" as the available options. To display Oracle Identity Manager as a supported provisioning server, edit iam-context.xml in the RBACX_Home/WEB-INF folder as follows.

Uncomment the oracle key entry in the iamSolutions property map lines in iam-context.xml

Reference: To Enable Oracle Identity Manager as a Provisioning Server Option

QUESTION NO: 4

For a typical OIA implementation, identify the correct two sequences of tasks.

- A. Review candidate roles > Analyze/Review role exceptions > analyze candidate roles
 B. Analyze/Review role exceptions > finalize candidate roles > finalize role exceptions and certify them
 C. Review candidate roles > Finalize candidate roles > Analyze/Review role exceptions
 D. Build Entitlement Warehouse > Perform role discovery > Review candidate roles

Answer: C,D

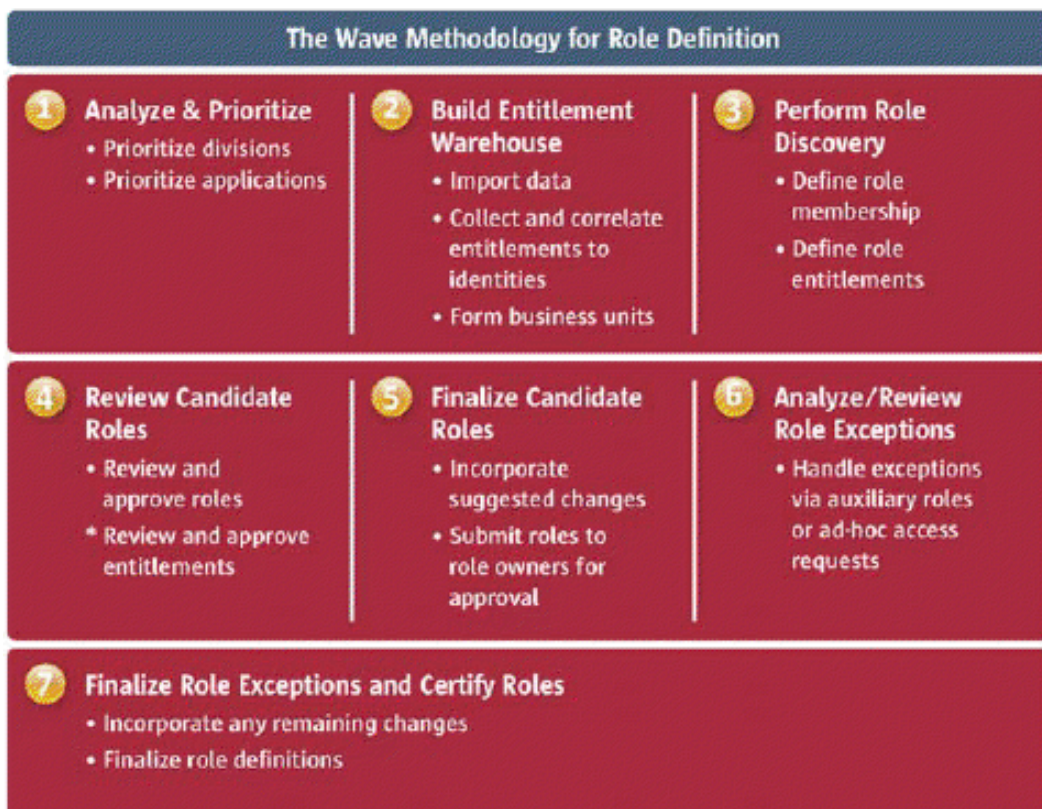
Explanation: Oracle's wave methodology separates large numbers of users into more manageable groups, or

"waves," for the purpose of defining roles. This is accomplished by first dividing users into business

units based on their managers, departments, divisions, or other commonalities. These business units

are then grouped into waves (usually four to six business units per wave), which are then prioritized

based on the needs of the business. Each wave requires a seven-step process for role definition. The figure summarizes the process



Reference: Wave Methodology: A Practical Approach to Defining Roles for Access Control, Oracle White Paper

QUESTION NO: 5

You have chosen to share policies across multiple roles in order to reduce the number of policies to manage. Here is the role composition:

Role A - Policy 1, Policy 2

Role B - Policy 1

Role C - Policy 1, Policy 2, Policy 3

Initially, all roles and policies are Active. Now Policy 1 is modified. The modification for Policy 1 is approved and Policy 1 moves from the Active state. How many role workflows are launched?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

Answer: B

Explanation: One for policy modification and second for role membership activation

The following table describes the eight workflows that are included with Oracle Identity Analytics.

Role Creation: Runs when a role is created.

Role Modification: Runs when a role is modified. For example, when a policy is added.

Role Membership: Runs when users are added or removed from the role.

Mass Modification: Runs when many roles are created or modified.

Policy Creation: Runs when a policy is created.

Policy Modification: Runs when a policy is modified.

Role Membership Rule Creation: Runs when role provisioning rule is created.

Role Membership Rule Modification: Runs when a role provisioning rule is modified.

Note: A workflow is a specific sequence of actions or tasks that are related to a business process.

In Oracle Identity Analytics, workflows enumerate each step involved in the various processes, such as role and policy creation, role and policy modification, and so on. It lists all the actors, who play a pivotal role in the management of roles and policies, and their function.

Oracle Identity Analytics has a robust and an easy-to-configure workflow engine. Workflows can be configured to any environment as they are based on the Open Source Open Symphony Workflow engine. Each workflow can be customized to support diverse requirements, such as role approval paths, policy approval paths, email integration, exposed web services to communicate with third-party applications, and so on.

Reference: Oracle Fusion Middleware Administrator's Guide for Oracle Identity Analytics:

Oracle Identity Analytics Workflows

QUESTION NO: 6

In OIA, business structure can be flat or hierarchical. What are the four logical groups you can group user in a business structure?

- A. Organizational structure
- B. Reporting structure
- C. Application Access structure
- D. Any custom logical group
- E. Roles structure

Answer: A,B,C,E

Explanation: Business structures are logical groupings of users. They can reflect the current organizational structure and hierarchy.

A *business structure* in Oracle Identity Analytics is defined as a department or sub-department within an organization. An organization can be segregated into as many business structures, with as many levels of hierarchy as is required to represent teams and sub-teams within the organization.

Only **Any custom logical group** is not a name of a logical group.

Reference: The Identity Warehouse, Best Practices, Oracle White Paper

QUESTION NO: 7

Which four represent out-of-the-box ad hoc report categories provided by OIA?

- A. Business structure reports
- B. System reports
- C. Identity audit reports
- D. Custom reports

- E. User reports
- F. Role reports

Answer: A,B,C,D

Explanation: The Ad Hoc Reports page has four subtabs: Business Structure Reports, System Reports, Identity Audit Reports, and Custom Reports. These reports can be run at any given time.

Reports are broadly classified as follows:

- * Business structure reports: Out-of-the-box reports that run on selected business structures.
- * System reports: Out-of-the-box reports that are run on all users, roles, or policies in Oracle Identity Analytics.
- * Identity Audit reports: Open-audit exception reports based on audit policy scans.
- * Custom reports: Reports customized according to the requirements of your organization

Reference: Oracle Identity Analytics User's Guide

Reports

QUESTION NO: 8

Identify four changes a typical upgrade process for OIA may involve.

- A. Change in database
- B. Change in Java code
- C. Additional .jrxml and .jasper files
- D. Patch in the Spring Framework
- E. Upgrades in the .rbx and xml schema files for imports

Answer: A,B,C,E

Explanation: A: consider the following: Upgrade the database schema if this step is required in the current release.

The necessary files are provided in the distribution package inside the db folder.

B: Rebuild any custom Java classes and utilities against the target product libraries.

C: Third-party files need to be downloaded prior to upgrading. Downloaded files should be saved to a library folder, which will be referred to as RM_LIB. For example, Download the jasper-jdt.jar file from this site.

E:To Import Accounts

Add the LDAP_accounts.rbx file.

For Windows - C:\Oracle\OIA_11gR1\import\schema

Reference: Oracle Identity Analytics Installation and Upgrade Guide

Upgrading Oracle Identity Analytics

QUESTION NO: 9

You have started to install OIA on Windows. You have created the database a schema for OIA as a prerequisite step for OIA installation. But when you run install 1.bat, the installer fails to connect to the database. To troubleshoot this problem, what three activities should you do?

- A. Check whether the database drivers are present in the WEB INF/lib folder.
- B. Check the configuration in thejdbc .properties file for the database.
- C. Check the configuration in the conf-context .xml file in the WEB INF folder
- D. The configuration in the iam-context .xml file In the WEB INF folder.
- E. Check the configuration in dataaccess-context .xml in the Web-INF folder

Answer: A,C,E

Explanation: This error occurs when Oracle Identity Analytics is unable to connect to the database.

E: Check the jdbc.properties configuration file in the \$RBACX_HOME/conf folder.

C: Check the conf-context.xml file in the /WEB-INF/ folder.

A: Ensure that JDBC drivers corresponding to the database type are present in /WEB-INF/lib. Verify that database server connectivity can be established from the application server.

And:

A: For Oracle Database Server you may need to copy the JDBC driver JARfile (ojdbc5.jar or ojdbc6.jar, depending on which JDK you are using) into the appropriate location (WEB-INF/lib or your application server's global lib directory).

C: Open conf-context.xml (located in the WEB-INF directory inside the WAR file) forediting.

E: Opendataaccess-context.xml(located in theWEB-INFdirectory inside the WAR file) for editing.

Reference: Oracle Fusion Middleware Administrator's Guide for Oracle Identity Analytics:

Oracle Identity Analytics Troubleshooting, JDBCConnection Error

QUESTION NO: 10

Which two tables in the OIA database may get updated as result of a certification?

- A. Id_certs
- B. Id_cert_users
- C. ldc_policies
- D. ldc_policy_attributes

Answer: A,B

Explanation: A: Each certification created in the Oracle Identity Analytics identity certification module is stored in the ID_CERTS table

B: Every user who is certified in the certification process appears in the ID_CERT_USERS table. This table includes a CERT_ID column that maps to the ID field of the ID_CERTS table. A USER_ID is also assigned to the user. The REPORTS_TO field associates a user with the user's manager, and the CERTIFIED_BY field captures the username of the person updating the certification.

Reference: Oracle Identity Analytics Database Administrator's Guide

Tables in the Identity Certification Module

QUESTION NO: 11

For a user-to-account correlation, choose four valid correlation rules.

-\$account.LastName"

- A. @IdentityCorrelationRule rule= \$globalUser.userName= [defaultuser] "
- B. @IdentityCorrelationRule rule="\$globaluser.userName=\$account. FirstName (-1.1) \$account.LastName"
- C. @IdentityCorrelationRule rule="globaluser.userName (-10) =\$account .name"
- D. @IdentityCorrelationRule rule="\$globaluser.userName=\$account. userName"
- E. @IdentityCorrelationRule rule="\$globaluser.userName="\$account. FirstName(-1.1)

Answer: A,B,D,E

Explanation: The error in C is that globaluser.userName is used instead of