Oracle

1Z0-1118-23 Exam

Oracle Cloud Fusion Analytics Warehouse 2023 Implementation Professional

Questions & Answers
Demo

Version: 4.0

Question: 1

You must specify parameter values during the HCM Analytics' Reporting Configuration process.
Why are these parameters required as part of the implementation process?

A. The Reporting Configuration parameters are required to set the initial extract date for extracting the data from the source application.
B. The Reporting Configuration parameters help schedule reports required to be run at a defined time.
C. The Reporting Configuration parameters help specify how data is presented in KP1 decks, visualizations, analysis, dashboards, and reports in FAW.

Answer: C

Explanation:

The Reporting Configuration parameters are used to define how the data is displayed in the FAW user interface. They include settings such as currency, date format, decimal separator, number of decimals, and default dashboard. These parameters affect the presentation layer of the FAW semantic model and can be changed at any time without affecting the data pipeline or the data warehouse.
Verified Reference: Oracle Fusion HCM Analytics, page 9.

Question: 2

Fusion Analytics Warehouse (FAW) allows you to select the Descriptive Flexfields (DFFs) you want to move to your data warehouse.
What setup must you ensure in your Fusion Application for FAW to perform this operation7

A. Ensure that the DFFs and their attributes are Bl-enabled in your Fusion Application.
B. Ensure the DFFs are configured and validated in your Fusion Application.
C. Create a BICC extract for DFFs and schedule the same in your Fusion Application.

Answer: A

Explanation:

The DFFs and their attributes must be BI-enabled in order to be extracted by the FAW data pipeline and loaded into the data warehouse. BI-enabling a DFF means that it is exposed as a column in a view object that is part of a subject area in Oracle Transactional Business Intelligence (OTBI). This allows FAW to access the DFF data through OTBI web services.
Verified Reference: Use Descriptive Flexfields, section 23.1; About Flexfields, section “Use Flexfields in Your Data Model”.

Question: 3

LBAC is enabled in your Fusion pod. You plan to provision your instance using password-based authentication to Fusion Application.
What configuration does your Fusion Application require to achieve this?

A. You need to identify the user who will be connected to the Fusion Application for pipeline orchestration. This user must be enabled for access from All IP Addresses.
B. Log an SR for your Fusion Application and mention the identified user to authenticate to Fusion Application. Oracle Support will disable LBAC for the identified user.
C. Custom roles need to be created for the user identified to authenticate access to the Fusion Application. These roles must to be enabled for access from All IP addresses.

Answer: A

Explanation:

LBAC (Location-Based Access Control) is a feature that restricts access to Fusion Applications based on IP addresses or ranges of IP addresses. If LBAC is enabled on your Fusion pod, you need to identify a user who will be used by FAW to connect to Fusion Applications using password-based authentication. This user must have access from All IP Addresses in order to allow FAW to extract data from any location.
Verified Reference: Securing Oracle Fusion Applications REST APIs with Location Based Access Control (LBAC), section “LBAC Configuration”.

Question: 4

In the FAW Security framework, which mapping paradigm best describes the mapping of Security Content to Data Roles?

A. Security Context to Data Role is one-to-one
B. Security Context to Data Role is many-to-many
C. Security Context to Data Role is one-to-many

Answer: B

Explanation:

The FAW Security framework allows a flexible and extensible mapping of Security Content to Data Roles. A Security Content is a predefined attribute that defines the boundaries of data access for a given subject area, such as Business Unit, Country, Department, Job Family, Legal Entity, and Worker Type. A Data Role is a custom role that grants access to specific subsets of data in the data warehouse based on the Security Content. A Security Content can be mapped to multiple Data Roles, and a Data Role can have multiple Security Content associated with it. For example, a Security Content of Country = US can be mapped to a Data Role of US HR Manager, and a Data Role of US HR Manager can have multiple Security Content such as Country = US, Business Unit = Sales, and Department = Marketing.
Verified Reference: Reference for Fusion HCM Analytics, page 9-10.

Question: 5

In Fusion HCM Analytics, which job-specific role/group provides access to all HCM data without security restrictions on the HCM data set?

A. Human Resource Analyst
B. Human Resource Specialist
C. Human Resource Manager

Answer: A

Explanation: