Lab 5

Security Auditing in Oracle

Overview:

In this lab, you will demonstrate to set-up and monitor audits using the Auditing features within Oracle.

You must connect to the provided AWS Oracle RDS environment and complete these task to earn credit for this lab.

Scenario:

A new manager at your company has some growing concerns that private customer data stored in an AWS Oracle instance is being leaked or at least is being accessed by those who might not need to view the data. You have been tasked with using Auditing features with Oracle to monitor, track and identify any user who reads, inserts, updates or deletes data in the following tables:

- Sales2019
- Projections2020
- Customers

The Tables have the following composition

Sales2019

- CustomerID – Not Null, Integer, References Customers. The ID of the customer.
- TransactionDate – Not Null, Date, Composite Primary Key with CustomerID. The date and time of the sale.
- SalesAmount – not null, number(10,2). The amount of the sale.
- ProfitAmount - not null, number(10,2). The amount of profit for this sale.

Projections2020

- CustomerID – Not Null, Integer, References Customers. The ID of the customer.
- QuarterlyPurchaseAmount – Not Null, number(10,2). Projected Quarterly purchases for this customer.
- QuarterlyProfitAmount – not null, number(10,2). The projected quarterly Profit from purchases from this customer
- Confidence – not null, number (4,2). The confidence (range 0.00 – 1.00) of this projection. Higher numbers indicate more confidence

Customers

- CustomerID - Not Null, Integer, Primary Key. The ID of the customer
- CustomerLastName – Not Null, varchar2(40), Lastname of the customer
- CustomerFirstName – Not Null, varchar2(40). Firstname of the customer
- CustomerEmail – Not Null, varchar2(80). Email address of the customer
- CustomerPhone – varchar2(12), Phone number of the customer.

- CustomerCellPhone - varchar2(12), Cell Phone number of the customer

Here are some suggestions that might help you get started:

1. You will need to create the tables and at least 3 users to test the audit functionality. Note, your developer/DBA just left the company and put this application together quickly. Essentially, he gave all 3 users read, insert, update and delete privileges on all 3 tables. You should do the same for this analysis.
2. You will need to populate the tables with real-looking data.
3. You will need to create Audit statements, as appropriate for each table and/or user.
4. You will need to login as each user to generate some data in the dba_audit_trail. To generate interesting results, I recommend conducting at least 10 different transactions for each user on each of the tables.
5. Users should be created using the similar nomenclature as before: Lab5_1FirstnameLastname, Lab5_2FirstnameLastname, Lab5_3FirstnameLastname. You should also create a role (e.g. R5FirstnameLastname) for the privileges.
6. As you are building your audit results, be sure to look in to the dba_audit_trail data dictionary view to watch the data grow.

Deliverables:

1. A complete SQL script that shows all of your SQL used for this project from the table creation through the queries of the dba_audit_trail. You should provide comments for each major SQL statement describing what the statement is doing. (50 points)
2. Use excel, SQL queries, or any tool you want to use to perform analysis of the dba_audit_trail for your specific users that clearly display the following results: (50 points)
    a. How many updates and deletes were performed by each user you created for each table. (Hint: A visual display pie chart, bar graph or similar, along with detailed descriptions would satisfy this requirement.)
    b. An x,y plot of the times each transaction was completed by each user on the Projections2020 table. (Hint: You will have to experiment with this to get a meaningful plot.) Be sure to describe and analyze the results.
    c. A sequential list of SQL statements used against the Customers table for each user along with the timestamps. Providing these results in a table will satisfy the requirement.