Security Auditing in Oracle within AWS

Overview: In this lab, you will use your AWS Oracle RDS account to set-up and monitor audits.

Important: This assignment requires you to use your AWS account.

Assignment: Total 100 points

Scenario:

A new manager at your company has some growing concerns that competition sensitive 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 updating the Oracle RDS instance running on AWS to enable Audits and monitor for and alert when any user reads, inserts, updates or deletes the data in the following tables:

- BidRates2017
- BidRates2018
- Proposals2017
- Proposals2018

In addition, you have been asked to monitor the Unified Audit Table to look for the creation of new users and audit trails additions.

A test plan should be developed to monitor and verify that audit information is correctly being recorded for all of the scenarios mentioned.

Finally, your manager wants reports on any suspicious or anomalous activity in the AWS Oracle logs, trace files or Audit files over the last two weeks.

Here are some hints that may help you:

1. You will need to create the tables and possibly some users to test the audit functionality
2. The test plan needs to verify each possible scenario
3. The log files for AWS are found in the AWS RDS instance

Deliverables:

1. A word (or PDF) document describing in detail how and why you decided on your audit design. This document should be well-written, using APA style guides and references and include screen captures of you successfully running all of the scripts. The word document should include a test plan and the results and explanations of running that test plan to verify all security components are functioning as expected. (Hint: Log in as users to perform each action, on each object and query the data dictionaries for results.) The document should also include your analysis of the logs available within AWS.
2. A complete SQL script that runs perfectly from start to finish that creates all tables, users and audit trail components.

Grading Components and Rubric:

Audit Design and Justification of Design (10 points)

Creation and use of Users (15 points)

Creation and use of Tables (15 points)

Modifying the AWS Instance to Enable Audits (15 points)

Includes detailed Test plan and results (10 points)

Describes and analyzes the RDS Log files and any anomalies (15 points)

Includes complete SQL script (10 points)

Document is well-organized, well-written and formatted in APA style (10 points)

Did not use AWS account (-100 points)