Mark Wagner

SDEV350-7981 Lab4

Database Audit

5/6/19

Mr. Director of Global IT,

I have completed forming a database of Bid Rates and Proposals for FY2017-2018. Already, two employees and an external contractor have interacted with it to check the rates and make adjustments.

I performed a security audit by reviewing the audit logs, trace files and listener logs to ensure that proper permissions had been granted and that no unauthorized users were added or added and subsequently removed.

Rather than using command line queries for audit, I generated the reports using RDS from Amazon as they are already hosting this file system. From here I should be able to perform Statement, Privilege, and Object Audits. I will also set up an audit table via SQL command.

The database was designed to have two user types Employee and Contractor. The Employees should only have SELECT access to proposals but full S/I/U/D rights on Bid Rates and the Contractors should have Select only on Bid Rates and Insert Only permissions on proposals.

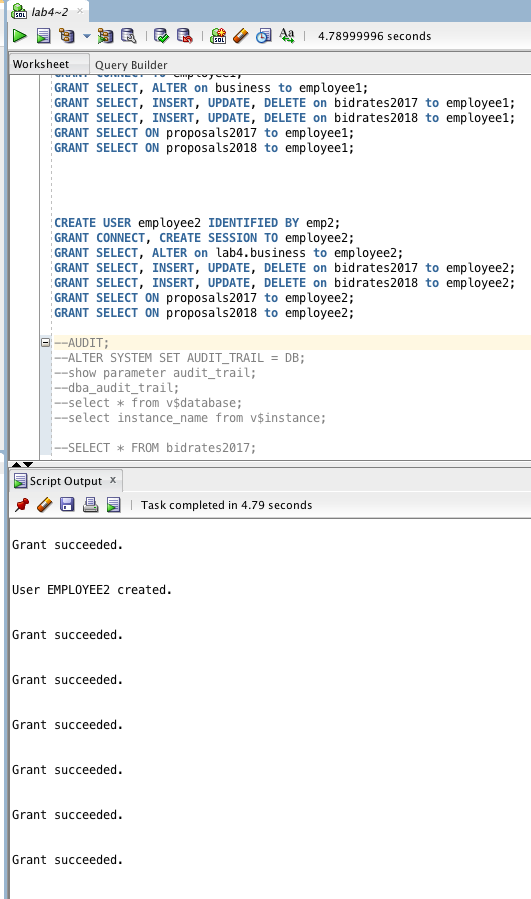
As there are only two employee accounts, I did not create roles to contain the permission parameters nor did I give anyone permission to generate more user accounts.

My test plan is to see which changes were made to which tables, by who and when, particularly if there were unusual hours.

Very important is the differentiation of Select or Modifying queries.

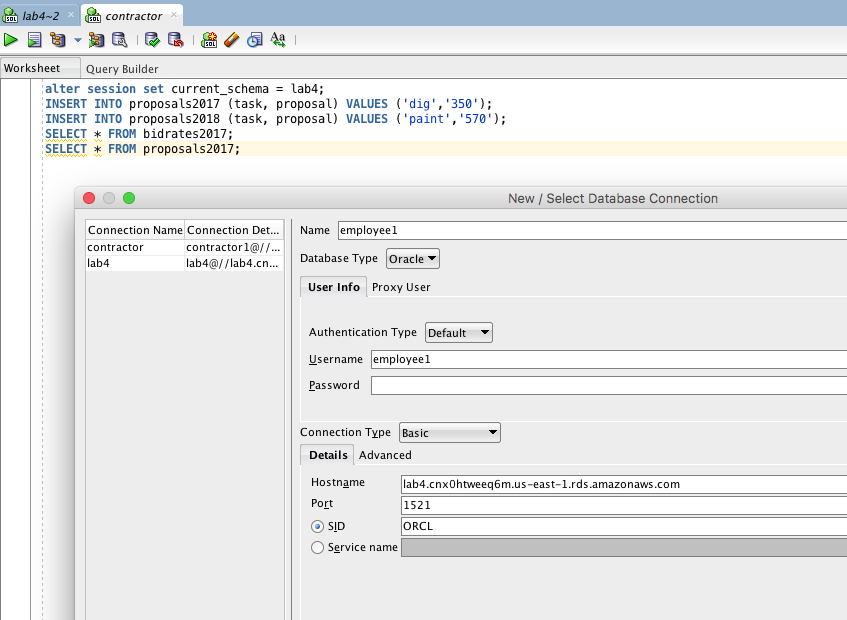
I also made an unsuccessful attempt to log in which should appear in logs.

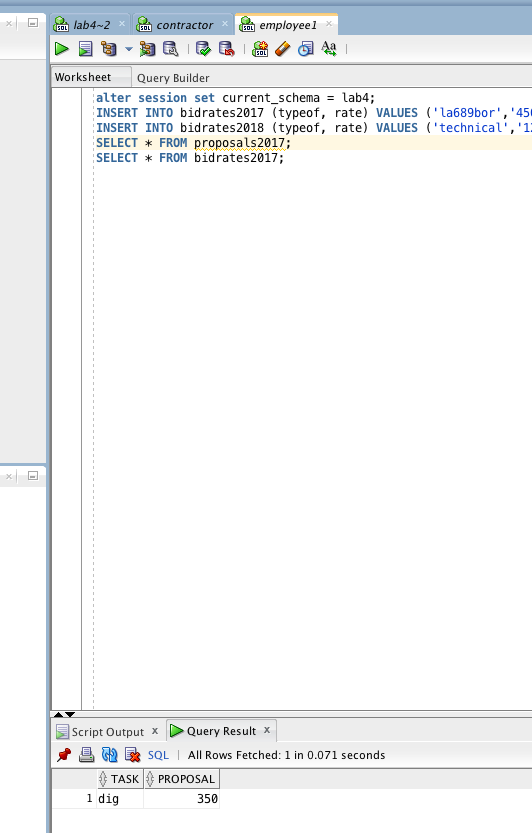
First, creating the database:

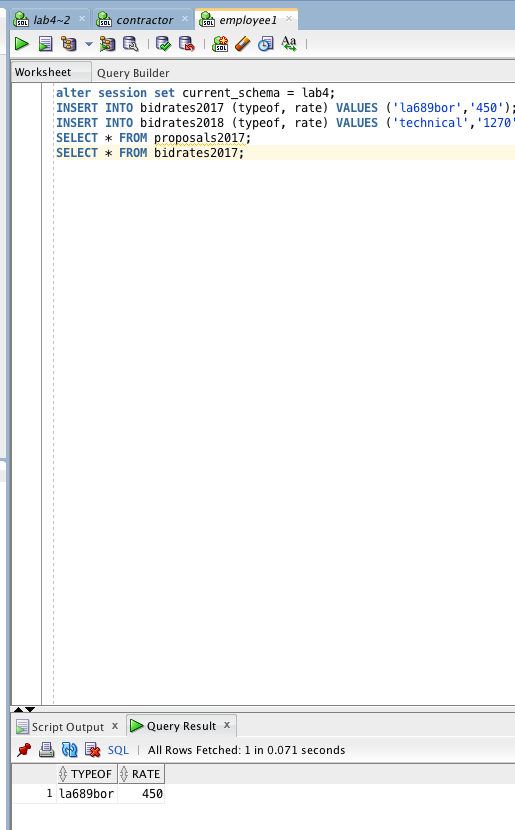


Then logging in as a user and making changes to main schema: Changing the schema is basically the ORACLE equivalent to “USE <dbNAME>” in mysql.

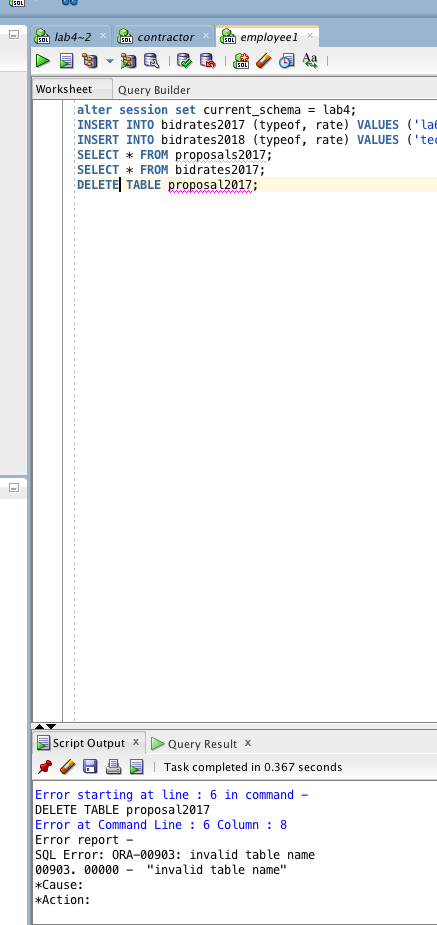


Then logging into another account:

Making more Changes:

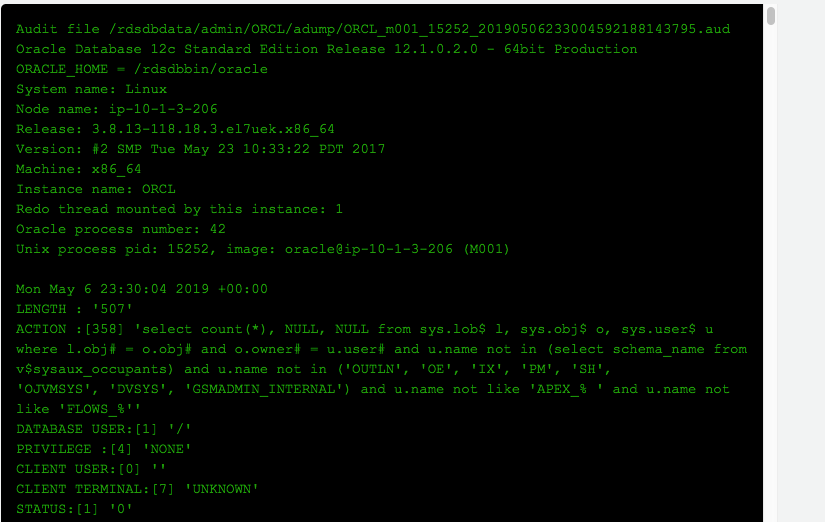


Queries come back okay above (inter-schema) and for some reason delete doesn’t work: below. But back to auditing…

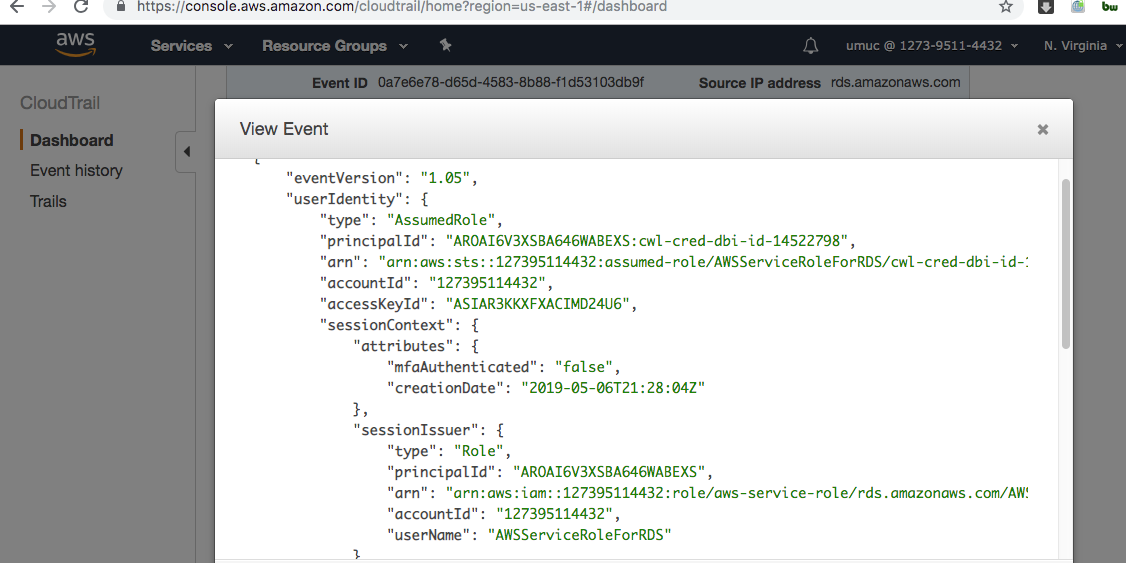


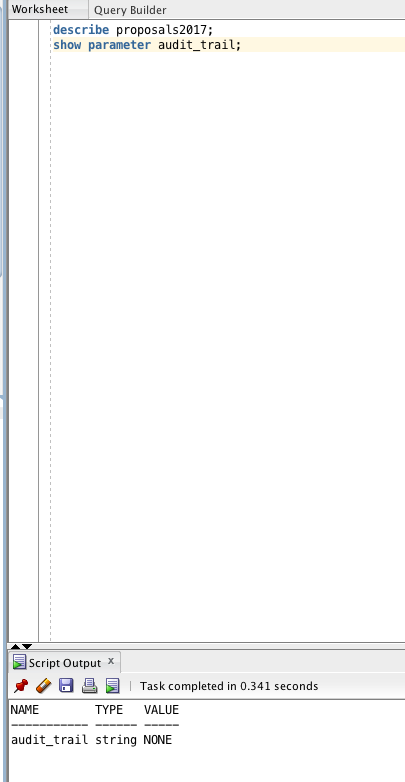
Here are Audit results from AWS Vies which basically put’s audit\_trail to ‘db’ for me and takes control and then queries the aud aux table.

I can check the basic log which is all internal RDS stuff:

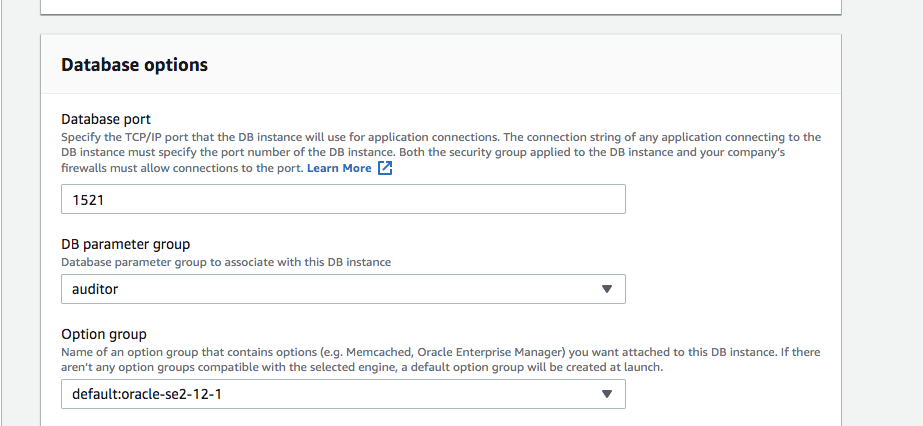


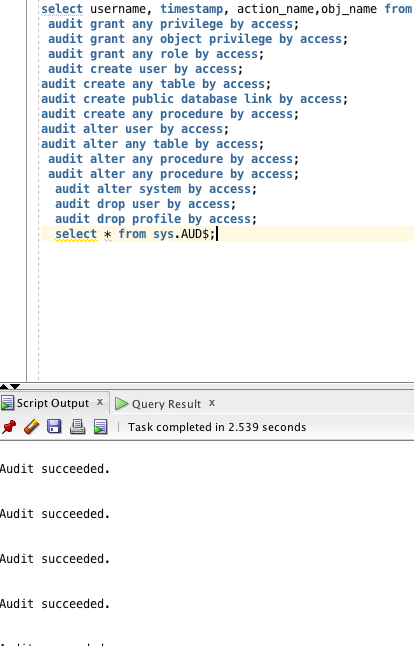
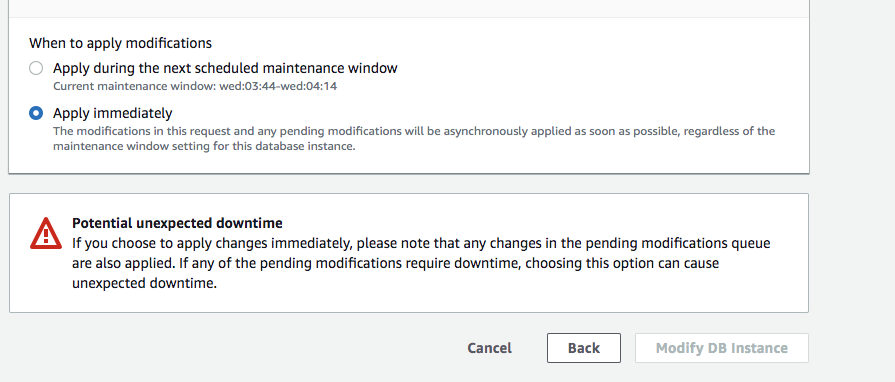
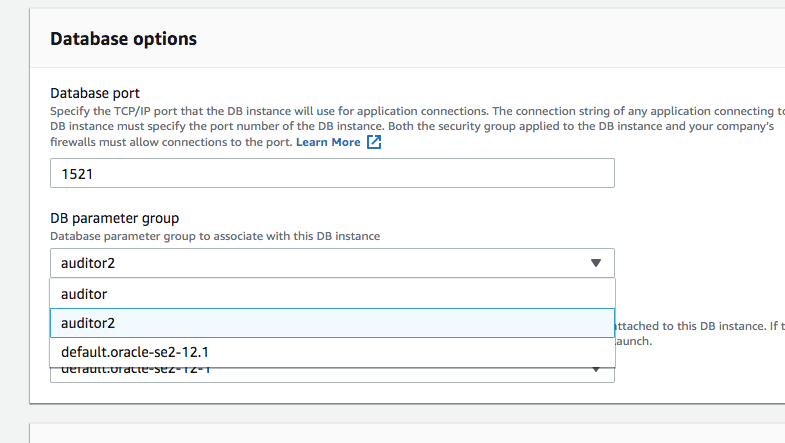
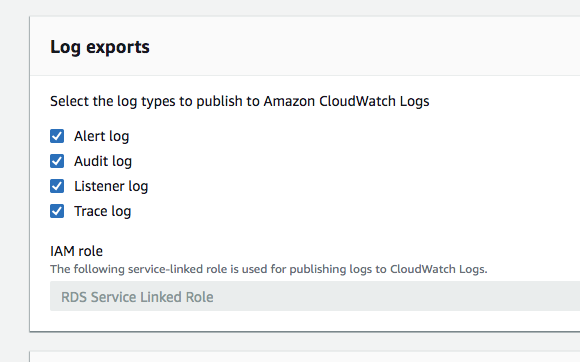
And the cloudtrail which mostly is internal from what I can see:



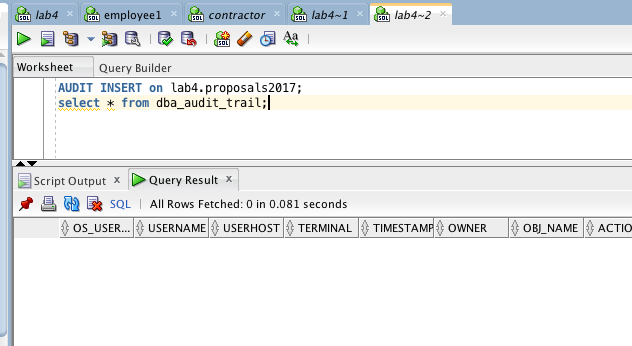


By modifying it to the default auditor parameter group I enabled when creating it, I can access more specific user generated events:

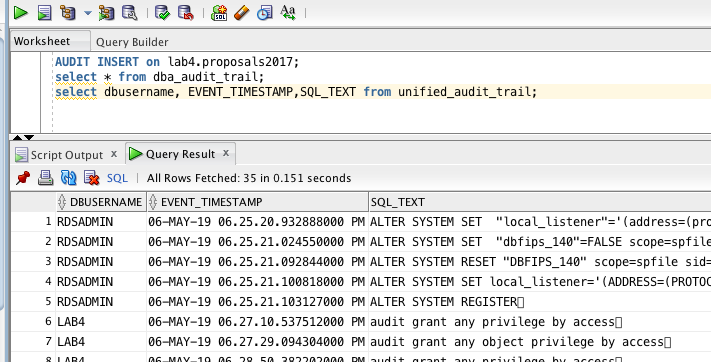


Although they have already been sent to cloudwatch.

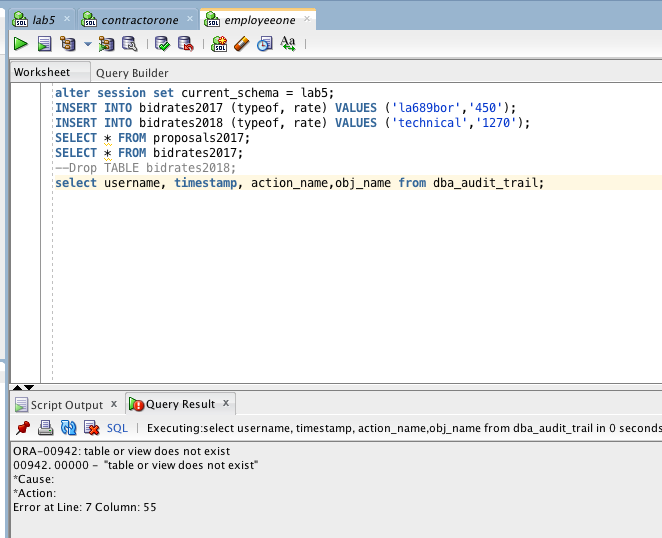
No matter what I try, the Audit result continue to come up blank:



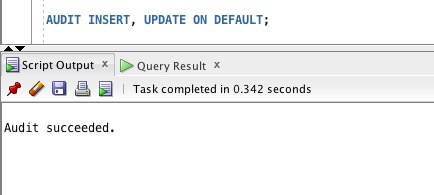
Now it seems to be tracking my audits:

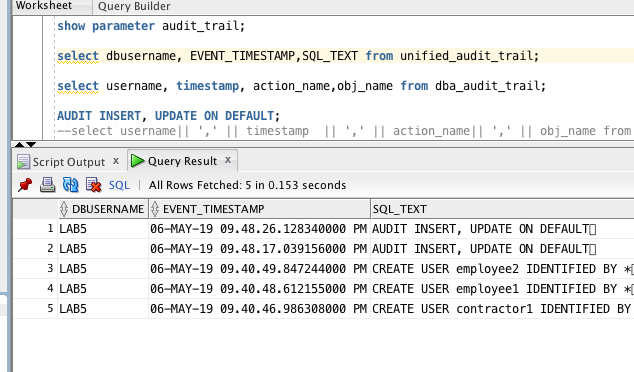


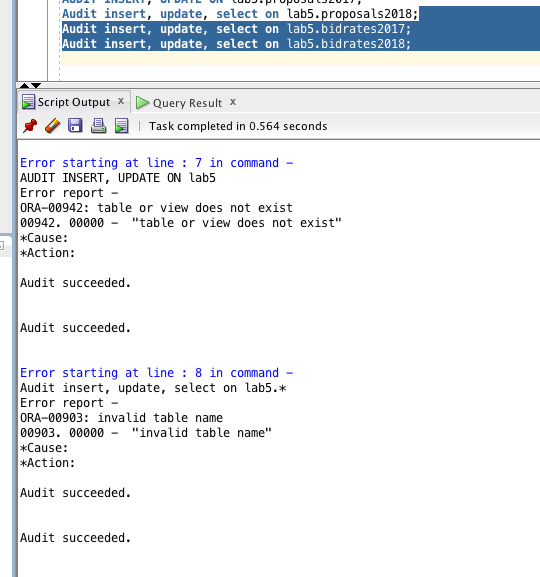
Upon rebuilding, I was able to simulate the same moves and see the user’s actions too. As shown below, the users cannot perform audits as only the admin has access.



Unfortunately, it seems I can only audit the actions I have taken..

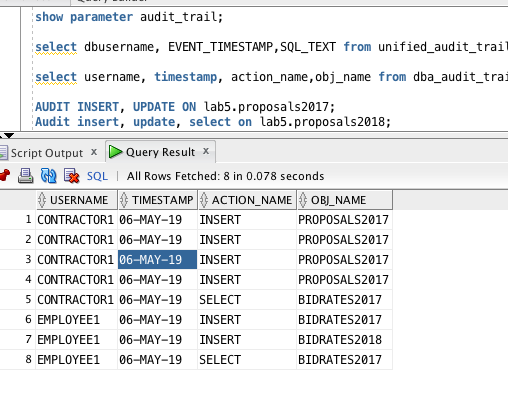






From here, I can see that some changes were made to the tables and selections by users. This lets me know that the employees have only been adjusting bid rates and the contractors have only been modifying their proposals. I can even see if something was modified late, past a due date, or on an off-day/hour.

Unfortunately, the details are not incredibly specific but even if I queried for deeper details, it does not show me attempts that were made to do things that failed.



An aside: What would be really neat is creating an Audit trigger for whenever someone performs a suspicious action.

CREATE TRIGGER audit\_emp\_salaries

I also wanted to see a trail view for USER\_AUDIT\_SESSION but this seems to not be supported by 12c or perhaps that is part of a larger command.