Mark Wagner

Lab3

SDEV350

Security Rundown

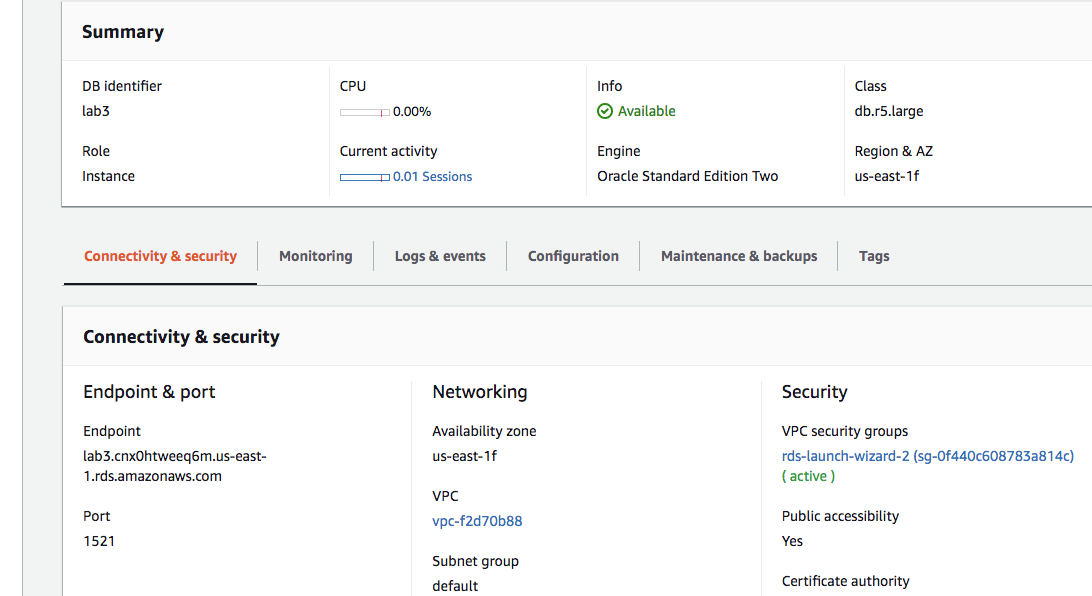
This database is designed to be both secure and structured form the best useability going forward. Rather than assign users permissions directly, as this is costly code-wise, roles are created to keep specifications controllable.

STIG, a federal department of defense standard for passwords requiring them to be 15 characters in length and contain an uppercase, a lowercase, a number, and a special character prevent password attacks on the database. (1)

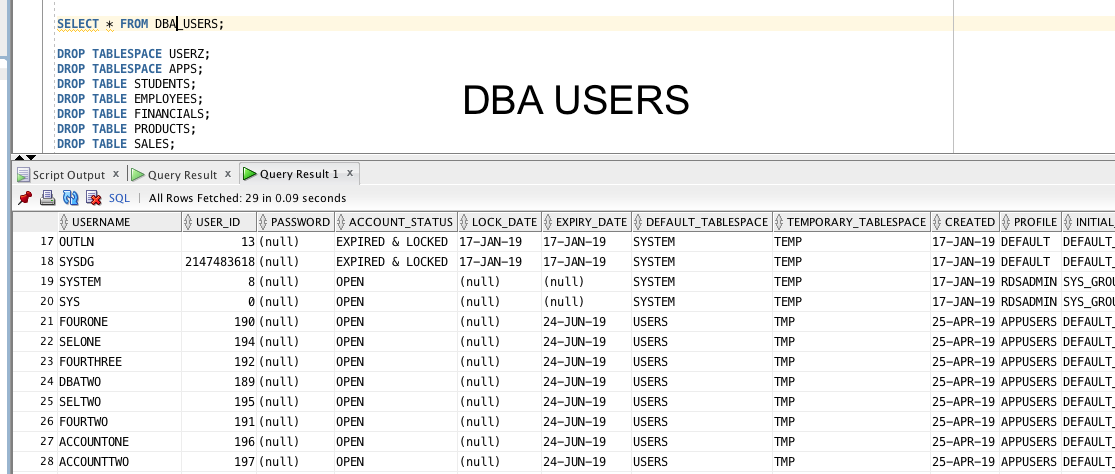
I have designed the SQL script to properly vacate the database space upon completion of running for hygiene reasons. The default profile, APPUSERS must be dropped last to avoid the use of a cascade clause.

The reason for limiting user permissions so strictly is to prevent allowing users who do not need to modify certain things from being able to do so. Therefore, should their application driving the queries be hacked, it would not be able to modify outside of an expected range of control.

I built this database from inside an RDS AWS service:



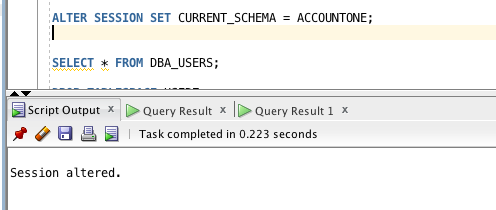
I also ran a dictionary command to list the dba users:



I plan to test this script by logging in as a user who can modify the payroll table and make both a modification to the table I am allowed to modify, and then attempt to modify a table I do not have access to as an account rep user.

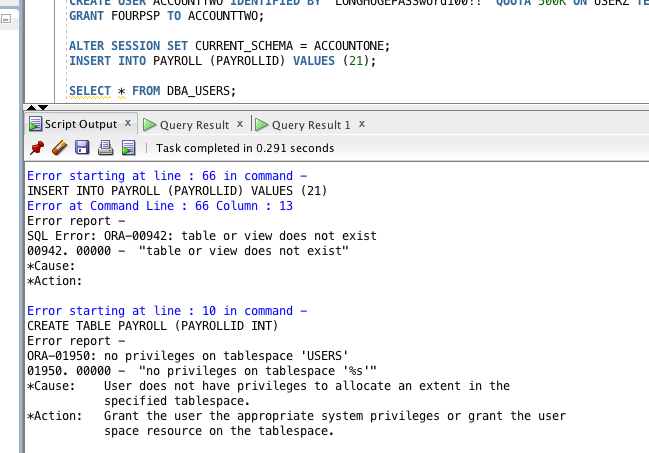
I changed to a user’s perspective with this command:

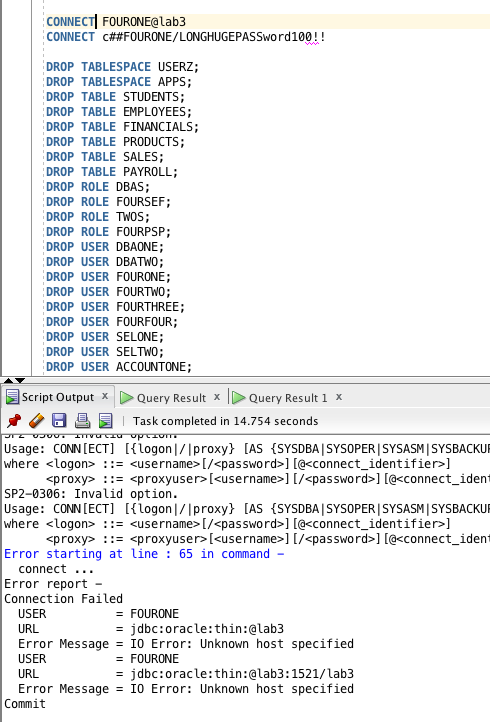
ALTER SESSION SET CURRENT\_SCHEMA = ACCOUNTONE;

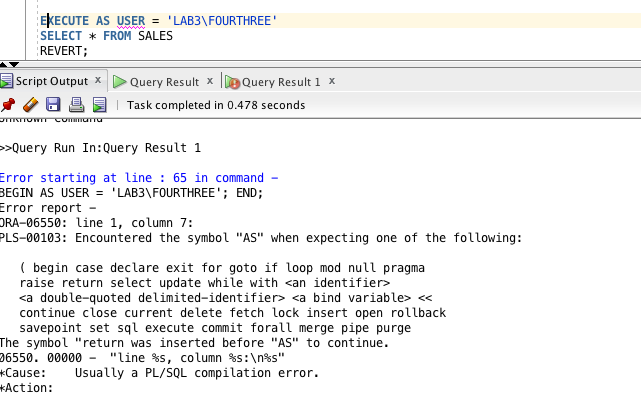


Here is the result:

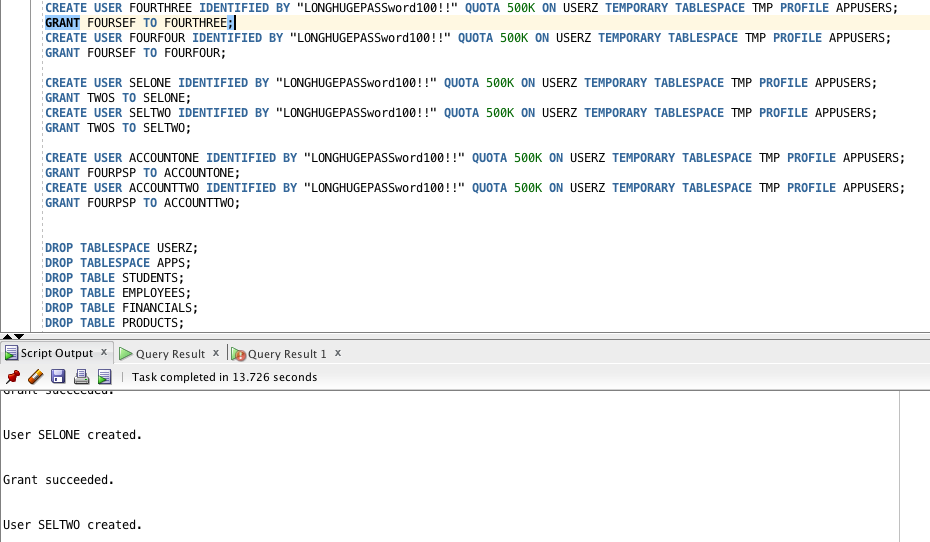
I am not sure why it will not let me make this modification. I may not be properly logged in to the user account.







Some successful screenshots:



I was unable to generate a successful spool file since, while testing the connectivity, I modified something behind the scenes and broke the database but if the SQL script were to be run on a new, empty, clean database, it would execute perfectly and if you were able to ssh into that database from a separate machine as a user with the STIG password, you would have the correct respective permissions.

Citations:

Defense Information System Agency. (2018, October 26). V-17689. Retrieved from https://vaulted.io/library/disa-stigs-srgs/video\_services\_policy\_stig/V-17689