Mark Wagner
Lab3
SDEV350

Security Rundown

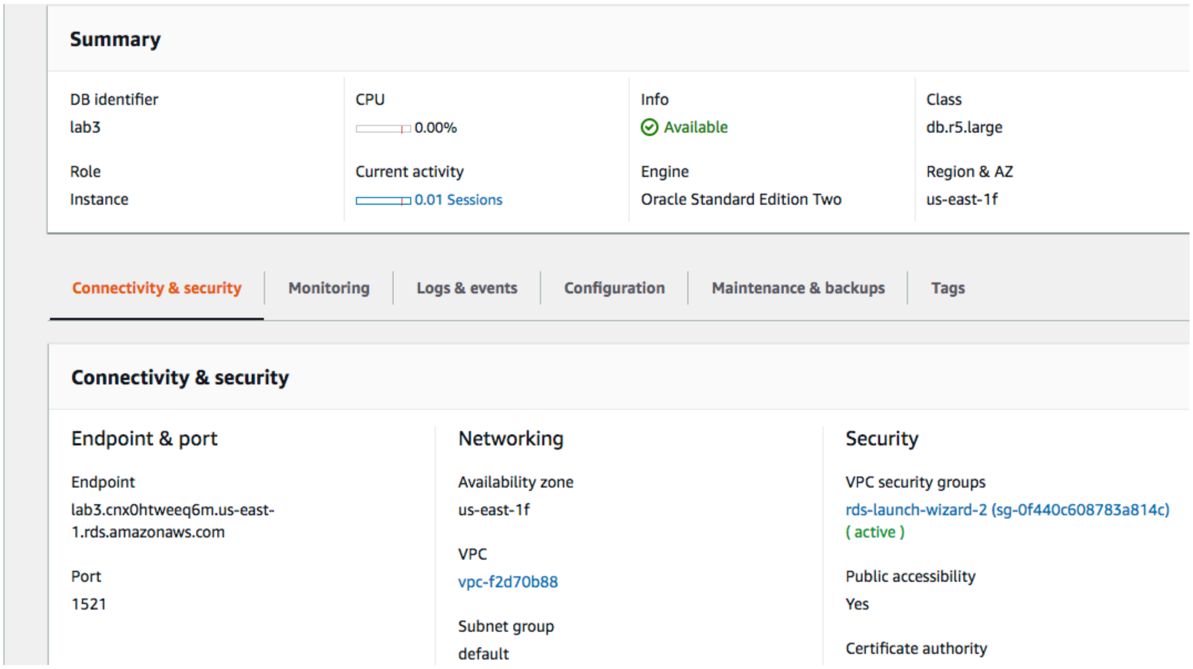
This database is designed to be both secure and structured form the best useability going forward. Rather than assign users permissions directly, as this is costly code-wise, roles are created to keep specifications controllable.

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:



Summary

DB identifier
lab3

CPU
0.00%

Info
Available

Class
db.r5.large

Role
Instance

Current activity
0.01 Sessions

Engine
Oracle Standard Edition Two

Region & AZ
us-east-1f

Connectivity & security

Endpoint & port

Endpoint
lab3.cnx0htweeq6m.us-east-1.rds.amazonaws.com

Port
1521

Networking

Availability zone
us-east-1f

VPC
vpc-f2d70b88

Subnet group
default

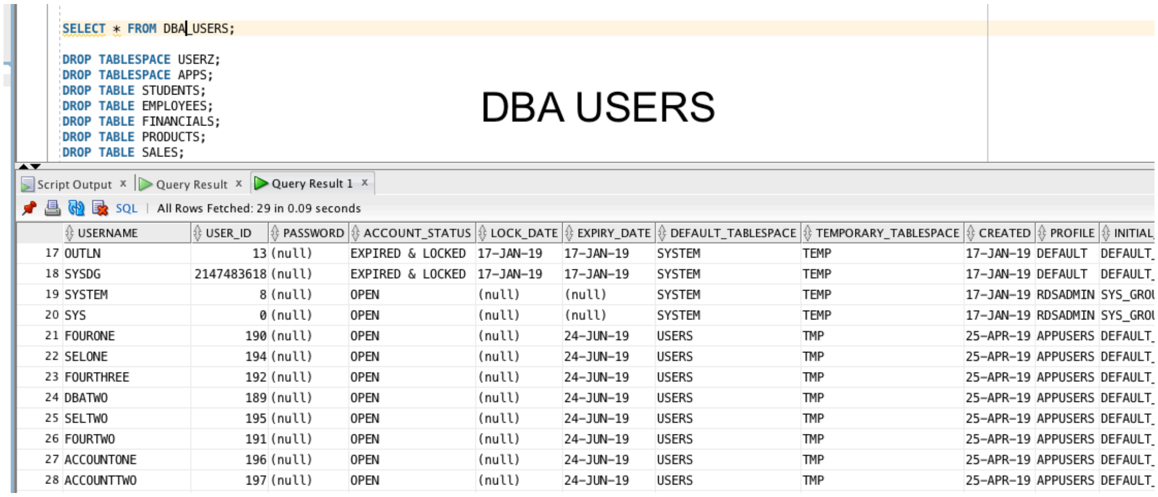
Security

VPC security groups
rds-launch-wizard-2 (sg-0f440c608783a814c)
(active)

Public accessibility
Yes

Certificate authority

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



```
SELECT * FROM DBA_USERS;

DROP TABLESPACE USERZ;
DROP TABLESPACE APPS;
DROP TABLE STUDENTS;
DROP TABLE EMPLOYEES;
DROP TABLE FINANCIALS;
DROP TABLE PRODUCTS;
DROP TABLE SALES;
```

DBA USERS

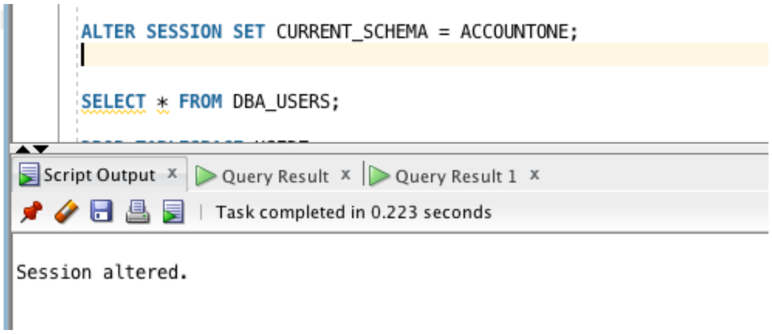
All Rows Fetched: 29 in 0.09 seconds

	USERNAME	USER_ID	PASSWORD	ACCOUNT_STATUS	LOCK_DATE	EXPIRY_DATE	DEFAULT_TABLESPACE	TEMPORARY_TABLESPACE	CREATED	PROFILE	INITIAL_
17	OUTLN	13	(null)	EXPIRED & LOCKED	17-JAN-19	17-JAN-19	SYSTEM	TEMP	17-JAN-19	DEFAULT	DEFAULT_
18	SYSDG	2147483618	(null)	EXPIRED & LOCKED	17-JAN-19	17-JAN-19	SYSTEM	TEMP	17-JAN-19	DEFAULT	DEFAULT_
19	SYSTEM	8	(null)	OPEN	(null)	(null)	SYSTEM	TEMP	17-JAN-19	RDSADMIN	SYS_GROU
20	SYS	0	(null)	OPEN	(null)	(null)	SYSTEM	TEMP	17-JAN-19	RDSADMIN	SYS_GROU
21	FOURONE	190	(null)	OPEN	(null)	24-JUN-19	USERS	TMP	25-APR-19	APPUSERS	DEFAULT_
22	SELONE	194	(null)	OPEN	(null)	24-JUN-19	USERS	TMP	25-APR-19	APPUSERS	DEFAULT_
23	FOURTHREE	192	(null)	OPEN	(null)	24-JUN-19	USERS	TMP	25-APR-19	APPUSERS	DEFAULT_
24	DBATWO	189	(null)	OPEN	(null)	24-JUN-19	USERS	TMP	25-APR-19	APPUSERS	DEFAULT_
25	SELTWO	195	(null)	OPEN	(null)	24-JUN-19	USERS	TMP	25-APR-19	APPUSERS	DEFAULT_
26	FOURTWO	191	(null)	OPEN	(null)	24-JUN-19	USERS	TMP	25-APR-19	APPUSERS	DEFAULT_
27	ACCOUNTONE	196	(null)	OPEN	(null)	24-JUN-19	USERS	TMP	25-APR-19	APPUSERS	DEFAULT_
28	ACCOUNTTWO	197	(null)	OPEN	(null)	24-JUN-19	USERS	TMP	25-APR-19	APPUSERS	DEFAULT_

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;



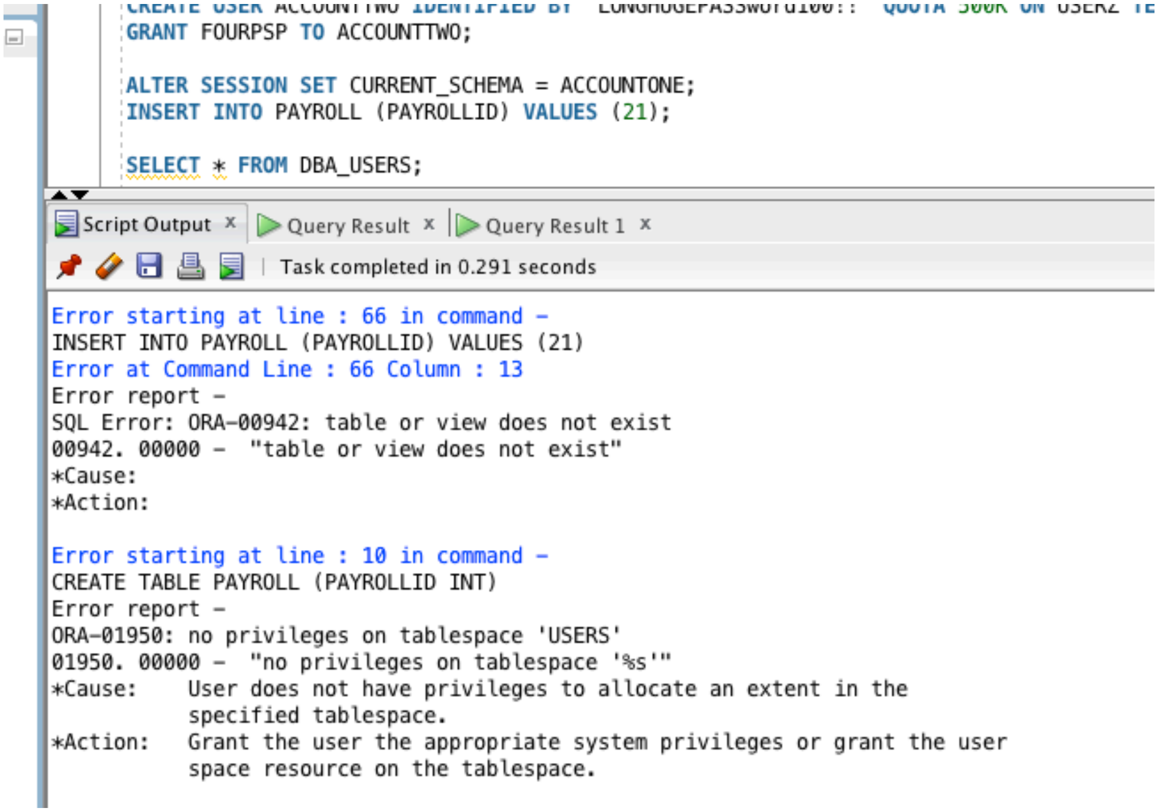
```
ALTER SESSION SET CURRENT_SCHEMA = ACCOUNTONE;

SELECT * FROM DBA_USERS;
```

Task completed in 0.223 seconds

```
Session altered.
```

Here is the result:

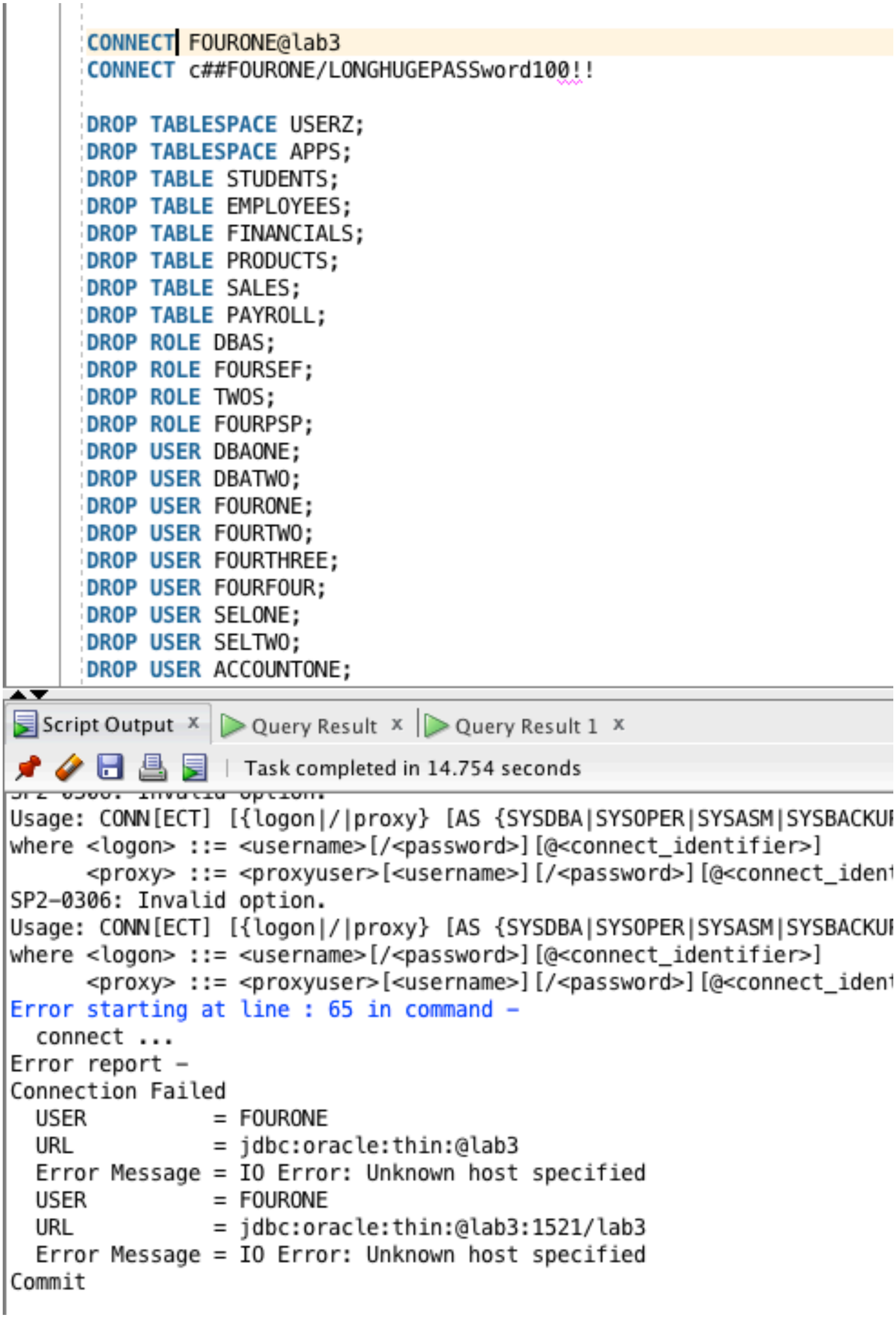
I am not sure why it will not let me make this modification. I may not be properly logged in to the user account.



```
CREATE USER ACCOUNTTWO IDENTIFIED BY "LONGHUGEPASSWord100!!" QUOTA 500K ON USERS TE
GRANT FOURPSP TO ACCOUNTTWO;

ALTER SESSION SET CURRENT_SCHEMA = ACCOUNTONE;
INSERT INTO PAYROLL (PAYROLLID) VALUES (21);

SELECT * FROM DBA_USERS;
```

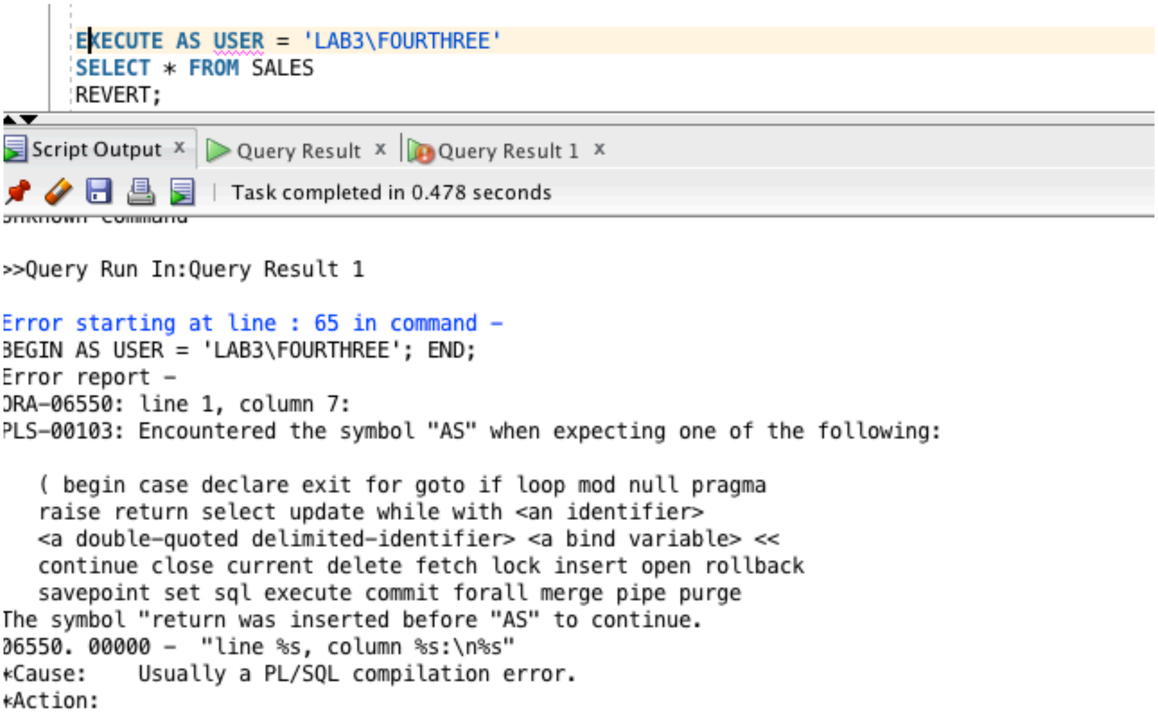
Task completed in 0.291 seconds

```
Error starting at line : 66 in command -
INSERT INTO PAYROLL (PAYROLLID) VALUES (21)
Error at Command Line : 66 Column : 13
Error report -
SQL Error: ORA-00942: table or view does not exist
00942. 00000 -  "table or view does not exist"
*Cause:
*Action:

Error starting at line : 10 in command -
CREATE TABLE PAYROLL (PAYROLLID INT)
Error report -
ORA-01950: no privileges on tablespace 'USERS'
01950. 00000 -  "no privileges on tablespace '%s'"
*Cause:    User does not have privileges to allocate an extent in the
           specified tablespace.
*Action:   Grant the user the appropriate system privileges or grant the user
           space resource on the tablespace.
```



```
CONNECT FOURONE@lab3
CONNECT c##FOURONE/LONGHUGEPASSword100!!

DROP TABLESPACE USERZ;
DROP TABLESPACE APPS;
DROP TABLE STUDENTS;
DROP TABLE EMPLOYEES;
DROP TABLE FINANCIALS;
DROP TABLE PRODUCTS;
DROP TABLE SALES;
DROP TABLE PAYROLL;
DROP ROLE DBAS;
DROP ROLE FOURSEF;
DROP ROLE TWOS;
DROP ROLE FOURPSP;
DROP USER DBAONE;
DROP USER DBATWO;
DROP USER FOURONE;
DROP USER FOURTWO;
DROP USER FOURTHREE;
DROP USER FOURFOUR;
DROP USER SELONE;
DROP USER SELTWO;
DROP USER ACCOUNTONE;
```

```
SP2-0306: Invalid option.
Usage: CONN[ECT] [{logon|/|proxy} [AS {SYSDBA|SYSOPER|SYSASM|SYSBACKU
where <logon> ::= <username>[/<password>][@<connect_identifier>]
      <proxy> ::= <proxyuser>[<username>][/<password>][@<connect_iden
SP2-0306: Invalid option.
Usage: CONN[ECT] [{logon|/|proxy} [AS {SYSDBA|SYSOPER|SYSASM|SYSBACKU
where <logon> ::= <username>[/<password>][@<connect_identifier>]
      <proxy> ::= <proxyuser>[<username>][/<password>][@<connect_iden
Error starting at line : 65 in command -
  connect ...
Error report -
Connection Failed
  USER          = FOURONE
  URL           = jdbc:oracle:thin:@lab3
  Error Message = IO Error: Unknown host specified
  USER          = FOURONE
  URL           = jdbc:oracle:thin:@lab3:1521/lab3
  Error Message = IO Error: Unknown host specified
Commit
```

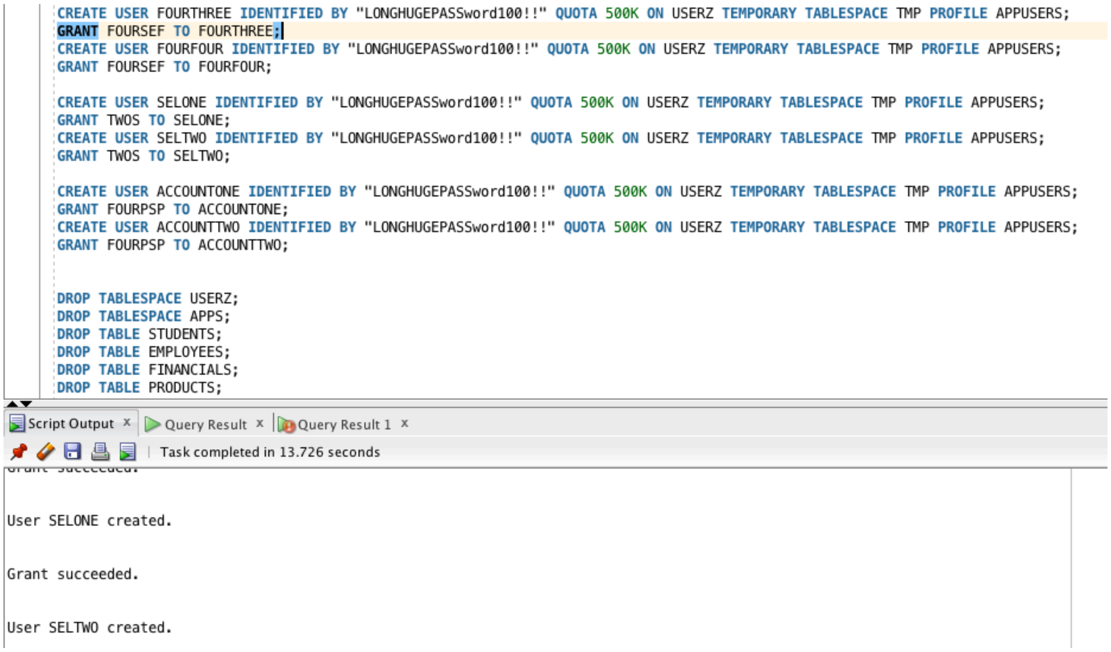


```
EXECUTE AS USER = 'LAB3\FOURTHREE'
SELECT * FROM SALES
REVERT;
```

Task completed in 0.478 seconds

```
Unknown Command

>>Query Run In:Query Result 1

Error starting at line : 65 in command -
BEGIN AS USER = 'LAB3\FOURTHREE'; END;
Error report -
ORA-06550: line 1, column 7:
PLS-00103: Encountered the symbol "AS" when expecting one of the following:

   ( begin case declare exit for goto if loop mod null pragma
   raise return select update while with <an identifier>
   <a double-quoted delimited-identifier> <a bind variable> <<
   continue close current delete fetch lock insert open rollback
   savepoint set sql execute commit forall merge pipe purge
The symbol "return was inserted before "AS" to continue.
06550. 00000 -  "line %s, column %s:\n%s"
*Cause:    Usually a PL/SQL compilation error.
*Action:
```

Some successful screenshots:



```
CREATE USER FOURTHREE IDENTIFIED BY "LONGHUGEPASSword100!!" QUOTA 500K ON USERZ TEMPORARY TABLESPACE TMP PROFILE APPUSERS;
GRANT FOURSEF TO FOURTHREE;
CREATE USER FOURFOUR IDENTIFIED BY "LONGHUGEPASSword100!!" QUOTA 500K ON USERZ TEMPORARY TABLESPACE TMP PROFILE APPUSERS;
GRANT FOURSEF TO FOURFOUR;

CREATE USER SELONE IDENTIFIED BY "LONGHUGEPASSword100!!" QUOTA 500K ON USERZ TEMPORARY TABLESPACE TMP PROFILE APPUSERS;
GRANT TWOS TO SELONE;
CREATE USER SELTWO IDENTIFIED BY "LONGHUGEPASSword100!!" QUOTA 500K ON USERZ TEMPORARY TABLESPACE TMP PROFILE APPUSERS;
GRANT TWOS TO SELTWO;

CREATE USER ACCOUNTONE IDENTIFIED BY "LONGHUGEPASSword100!!" QUOTA 500K ON USERZ TEMPORARY TABLESPACE TMP PROFILE APPUSERS;
GRANT FOURPSP TO ACCOUNTONE;
CREATE USER ACCOUNTTWO IDENTIFIED BY "LONGHUGEPASSword100!!" QUOTA 500K ON USERZ TEMPORARY TABLESPACE TMP PROFILE APPUSERS;
GRANT FOURPSP TO ACCOUNTTWO;


DROP TABLESPACE USERZ;
DROP TABLESPACE APPS;
DROP TABLE STUDENTS;
DROP TABLE EMPLOYEES;
DROP TABLE FINANCIALS;
DROP TABLE PRODUCTS;
```

Task completed in 13.726 seconds

```
Grant succeeded.

User SELONE created.


Grant succeeded.


User SELTWO created.
```

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