

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.

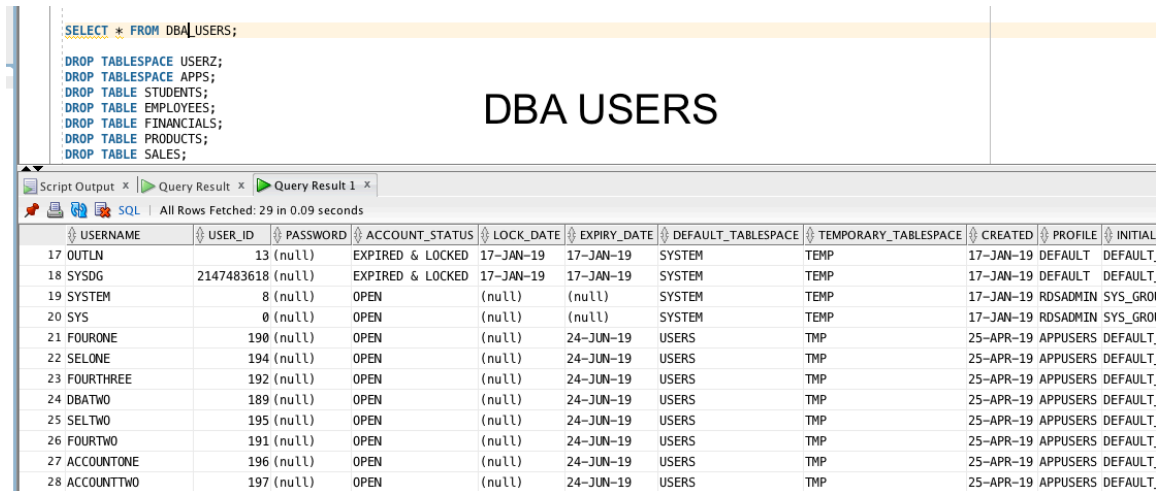
I built this database from inside an RDS AWS service:

The screenshot displays the AWS RDS console interface for a database instance named 'lab3'. The top section, titled 'Summary', provides key details about the instance: its identifier is 'lab3', the CPU usage is at 0.00%, the status is 'Available' (indicated by a green checkmark), and the class is 'db.r5.large'. It also shows the role as 'Instance', current activity as '0.01 Sessions', the engine as 'Oracle Standard Edition Two', and the region & availability zone as 'us-east-1f'. Below the summary, a navigation bar allows switching between 'Connectivity & security' (selected), 'Monitoring', 'Logs & events', 'Configuration', 'Maintenance & backups', and 'Tags'. The 'Connectivity & security' section is further divided into three columns: 'Endpoint & port' showing the endpoint 'lab3.cnx0htweeq6m.us-east-1.rds.amazonaws.com' and port '1521'; 'Networking' showing the availability zone 'us-east-1f', VPC 'vpc-f2d70b88', and subnet group 'default'; and 'Security' showing the VPC security group 'rds-launch-wizard-2 (sg-0f440c608783a814c)' as active, public accessibility set to 'Yes', and the certificate authority.

Summary			
DB identifier	CPU	Info	Class
lab3	0.00%	Available	db.r5.large
Role	Current activity	Engine	Region & AZ
Instance	0.01 Sessions	Oracle Standard Edition Two	us-east-1f

Connectivity & security		
Endpoint & port	Networking	Security
Endpoint	Availability zone	VPC security groups
lab3.cnx0htweeq6m.us-east-1.rds.amazonaws.com	us-east-1f	rds-launch-wizard-2 (sg-0f440c608783a814c) (active)
Port	VPC	Public accessibility
1521	vpc-f2d70b88	Yes
	Subnet group	Certificate authority
	default	

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



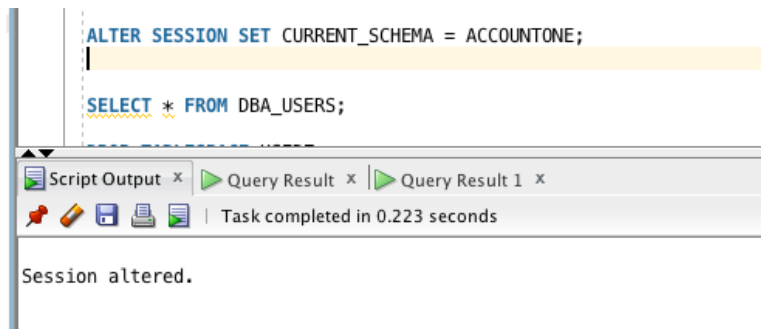
The screenshot shows a SQL Developer window with a script editor containing a dictionary command. The command is: `SELECT * FROM DBA_USERS;` followed by a series of `DROP` statements for various tablespaces and tables. The results pane shows a table with 11 columns: USERNAME, USER\_ID, PASSWORD, ACCOUNT\_STATUS, LOCK\_DATE, EXPIRY\_DATE, DEFAULT\_TABLESPACE, TEMPORARY\_TABLESPACE, CREATED, PROFILE, and INITIAL. The table contains 28 rows of data, including users like OUTLN, SYS, SYSTEM, and various account rep users.

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_GRO	
20 SYS	0 (null)	OPEN	(null)	(null)	SYSTEM	TEMP	17-JAN-19	RDSADMIN	SYS_GRO	
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;`

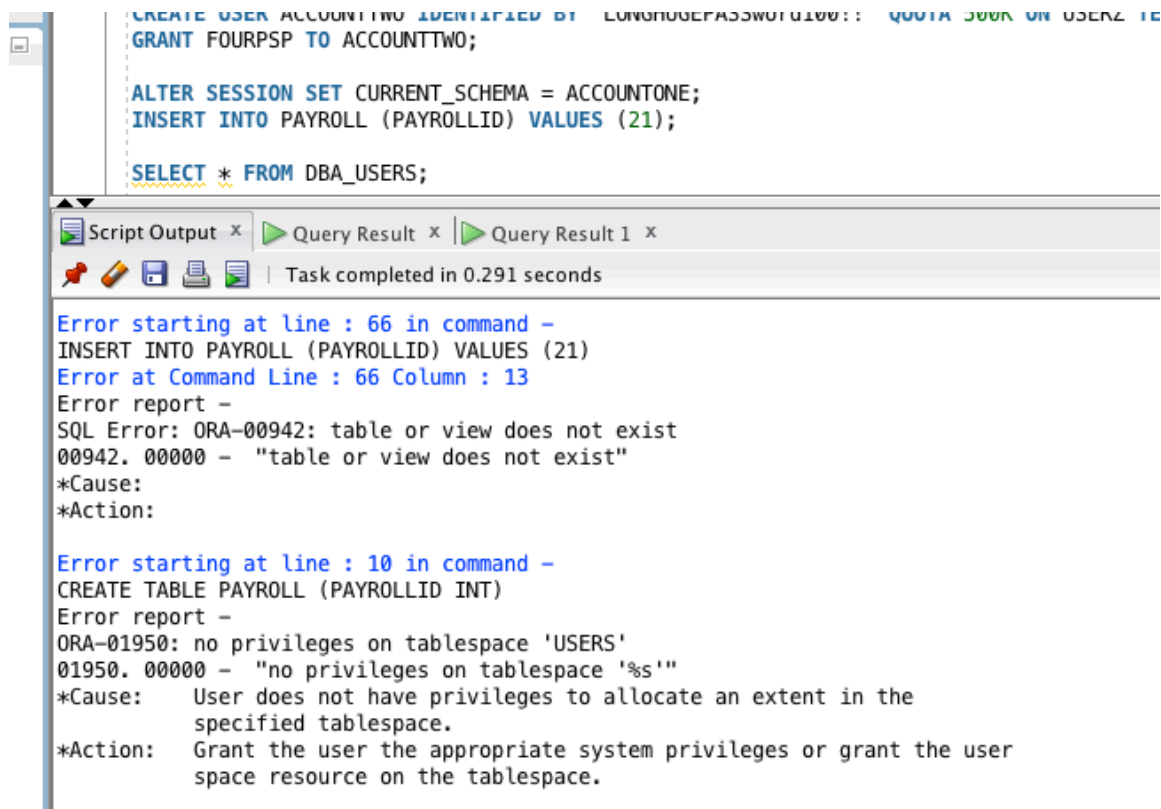


The screenshot shows a SQL Developer window with a script editor containing the command: `ALTER SESSION SET CURRENT_SCHEMA = ACCOUNTONE;` followed by a blank line and then `SELECT * FROM DBA_USERS;`. The results pane shows the message "Session altered." and "Task completed in 0.223 seconds".

Script Output
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.



The screenshot shows the Oracle SQL Developer interface. At the top, a SQL script is visible with the following commands:

```
CREATE USER ACCOUNTTWO IDENTIFIED BY LONGHOUSEPASSW0R0100!! QUOTA 500K ON USERS;
GRANT FOURPSP TO ACCOUNTTWO;

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

SELECT * FROM DBA_USERS;
```

Below the script, the 'Script Output' pane shows the execution results and errors. The status bar indicates 'Task completed in 0.291 seconds'. The output pane displays two error messages:

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 FORTWO;
DROP USER FOURTHREE;
DROP USER FOURFOUR;
DROP USER SELONE;
DROP USER SELTWO;
DROP USER ACCOUNTONE;
```

Script Output x Query Result x Query Result 1 x

Task completed in 14.754 seconds

SP2-0306: Invalid option.  
Usage: CONN[ECT] [{logon|/|proxy}] [AS {SYSDBA|SYSOPER|SYSASM|SYSBACKUP}]  
where <logon> ::= <username>[/<password>] [@<connect\_identifier>]  
      <proxy> ::= <proxyuser>[<username>] [/<password>] [@<connect\_identifier>]  
SP2-0306: Invalid option.  
Usage: CONN[ECT] [{logon|/|proxy}] [AS {SYSDBA|SYSOPER|SYSASM|SYSBACKUP}]  
where <logon> ::= <username>[/<password>] [@<connect\_identifier>]  
      <proxy> ::= <proxyuser>[<username>] [/<password>] [@<connect\_identifier>]  
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;
```

Script Output x Query Result x Query Result 1 x

Task completed in 0.478 seconds

>>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;
```

Script Output x Query Result x Query Result 1 x

Task completed in 13.726 seconds

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](https://vaulted.io/library/disa-stigs-srgs/video_services_policy_stig/V-17689)