

Memorandum

To: Bill Cunningham

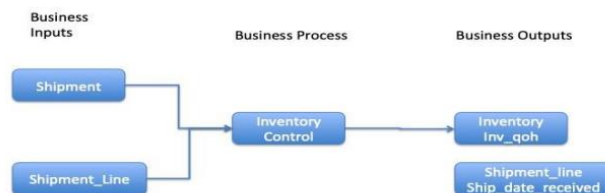
From: Jeong Eun Jang (W0451032)

1. EXSITING SYSTEM

This document contains that important analysis to perform a data security audit for the Clearwater Trader. The Clearwater Trader is an e-business company and has three key business processes: advertising, sales, and inventory control. As a DBA, I will perform a comprehensive data security audit in the aspects of the physical system of a database, logical structure of the memory, and application level for users.

For this project, I have been provided the followings:

- The inventory control business process diagram
- Clearwater Entity Relationship Diagram (ERD)
- Clearwater inventory Control jpg file
- Clearwater-Receiving-Process jpg file



To prepare the environment for this project, I have performed the following steps:

- Install Oracle RDBMS 11g Enterprise Edition on a Windows.
- Creation of a new oracle_home named itdb_home
- Connection to itdb as the sys user
- Create a user named Clearwater and grant a dba role.
- Connect as Clearwater and run the CH4Clearwater.sql.script

After analysis of expected security issues, I will implement applicable testing plan for recommendations. The testing plan will follow:

- Iteration
- Test
- Expected result
- Actual result
- Action required

2. STATEMENT OF REQUIREMENTS

This project will focus on facilitating the inventory control business process in the warehouse business unit and keep database secured by mitigating expected database security issues.

3. ANALYSIS

PHYSICAL SECURITY OF DATA

Issue 1. Tablespace

In Oracle Database, data is stored in tablespaces logically and in datafiles within the corresponding tablespace physically. It means the size of database is the size of the tablespaces associating with the database and the size of a tablespace is the size of the datafiles associating with the tablespace. If the size of database is small, it may need only the SYSTEM tablespace. However, Oracle recommends that at least one additional tablespace for more flexibility in database administration and more security in database.

Multiple tablespaces help to perform control disk space allocation for database data and assign specific space quotas for users. It also provides availability of data by taking each tablespace online or offline and partial database backup or recovery operations.

[Edit] [View] [Delete] [Actions] [Add Datafile] [Go]											
Select	Name	Allocated Size(MB)	Space Used(MB)	Allocated Space Used(%)	Auto Extend	Allocated Free Space(MB)	Status	Datafiles	Type	Extent Management	Segment Management
<input checked="" type="radio"/>	EXAMPLE	100.0	78.4	<div><div></div></div> 78.4	YES	21.6	✓	1	PERMANENT	LOCAL	AUTO
<input type="radio"/>	SYSAUX	520.0	494.5	<div><div></div></div> 95.1	YES	25.5	✓	1	PERMANENT	LOCAL	AUTO
<input type="radio"/>	SYSTEM	690.0	682.8	<div><div></div></div> 98.9	YES	7.2	✓	1	PERMANENT	LOCAL	MANUAL
<input type="radio"/>	TEMP	20.0	0.0	<div><div></div></div> 0.0	YES	20.0	✓	1	TEMPORARY	LOCAL	MANUAL
<input type="radio"/>	UNDOTBS1	55.0	24.5	<div><div></div></div> 44.5	YES	30.5	✓	1	UNDO	LOCAL	MANUAL
<input type="radio"/>	USERS	6.2	5.5	<div><div></div></div> 88.0	YES	0.8	✓	1	PERMANENT	LOCAL	AUTO

Total Allocated Size (GB) 1.36

Total Used (GB) 1.26

Total Allocated Free Space (GB) 0.10

✓ Online

✗ Offline

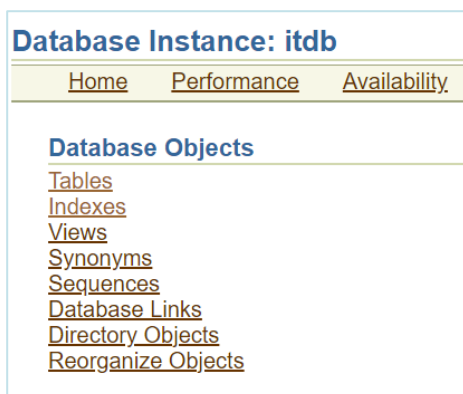
📖 Read Only

This screenshot above shows the tablespaces of the Clearwater database. As you see, the total allocated size is 1.36 GB, and the total used size is 1.26 GB. A database administrator can do the following actions for current tablespaces:

- Create new tablespaces
- Add datafiles to tablespaces
- Increase the size of a datafile

Issue 2. Schemas

A schema consists of database objects. Each database user owns a single schema, and a schema has the same name as its user. Each database username contains schema objects as a schema-a-security domain (Oracle, n.d.). Schema objects include structures like tables, views, and indexes. We can create, access, and manipulate schema objects using Oracle Enterprise Manager.

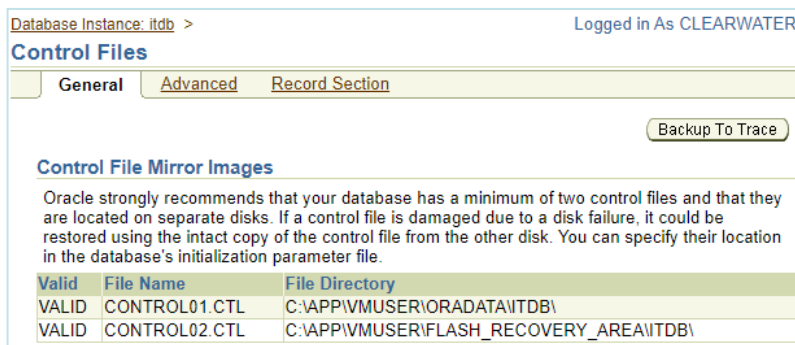


As a DBA, we need to establish a control plan to protect confidential schema objects against malicious access. There are several different privileges involved in the database application, we should keep track of privileges granted and used properly.

Issue 3. Control File & Redo Log File

A **control file** records the physical structure of the database. For example, the database name, locations of related datafiles and redo log files, the timestamp of the database creation, the current sequence number, and checkpoint information are recorded inside the control file. The control file's role is very important. It is difficult to mount and recover the database without the control file. When the database is created, the control file is also created with at least one copy. Even though Oracle recommends storing two or more copies of the control file on a different physical disk.

We can see where the control files are located, as shown below:



Database Instance: itdb > Logged in As CLEARWATER

Control Files

General **Advanced** Record Section

Backup To Trace

Control File Mirror Images

Oracle strongly recommends that your database has a minimum of two control files and that they are located on separate disks. If a control file is damaged due to a disk failure, it could be restored using the intact copy of the control file from the other disk. You can specify their location in the database's initialization parameter file.

Valid	File Name	File Directory
VALID	CONTROL01.CTL	C:\APP\VMUSER\ORADATA\ITDB\
VALID	CONTROL02.CTL	C:\APP\VMUSER\FLASH_RECOVERY_AREA\ITDB\

I will try to back up the control file in the different folder for security in the recommendation section.

Redo Log Files store all changes made to the database and protect the database against an instance failure. Each Oracle database has a set of two or more redo log files as a default. For the better security, log files should be stored on different disks. Even if all copies of the redo log files are on the same disk, some issues could be mitigated from this redundancy.

We can see Redo Log groups inside the Clearwater database as shown below:

Database Instance: itdb > Logged in As CLEARWATER

Redo Log Groups

Object Type: Redo Log Group

Search
Enter an object name to filter the data that is displayed in your results set.
Object Name
By default, the search returns all uppercase matches beginning with the string you entered. To run an exact or case-sensitive match, double quote the search string. You can use the wildcard symbol (%) in a double quoted string.

Selection Mode:

Clear logfile

Select	Group	Status	# of Members	Archived	Size (KB)	Sequence	First Change#
<input checked="" type="radio"/>	1	Inactive	1	No	51200	25	1503028
<input type="radio"/>	2	Inactive	1	No	51200	26	1530345
<input type="radio"/>	3	Current	1	No	51200	27	1559536

I used SQL query to check the group numbers and the locations of the Log files.

Worksheet Query Builder

1 select group#, member from v\$logfile order by group#, member;

Query Result x

All Rows Fetched: 3 in 0.271 seconds

GROUP#	MEMBER
1	C:\APP\VMUSER\ORADATA\ITDB\RED001.LOG
2	C:\APP\VMUSER\ORADATA\ITDB\RED002.LOG
3	C:\APP\VMUSER\ORADATA\ITDB\RED003.LOG

There are 3 groups of log files, and each group has only one log file inside. I will be creating multiplexed copies of redo log in the recommendation section.

Lastly, we can see all Clearwater database files are stored on the same folder.

We need a proper back-up plan for our database.

14
15 SELECT * from dba_data_files;

Query Result x

All Rows Fetched: 8 in 0.071 seconds

FILE_NAME	FILE_ID	TABLESPACE_NAME
C:\APP\VMUSER\ORADATA\ITDB\USERS01.DBF	4	USERS
C:\APP\VMUSER\ORADATA\ITDB\UNDOTBS01.DBF	3	UNDOTBS1
C:\APP\VMUSER\ORADATA\ITDB\SYSAUX01.DBF	2	SYSAUX
C:\APP\VMUSER\ORADATA\ITDB\SYSTEM01.DBF	1	SYSTEM
C:\APP\VMUSER\ORADATA\ITDB\EXAMPLE01.DBF	5	EXAMPLE
C:\APP\VMUSER\ORADATA\ITDB\CLEARWATER01	6	CLEARWATER
C:\APP\VMUSER\ORADATA\ITDB\CLEARWATER02	7	CLEARWATER
C:\APP\VMUSER\ORADATA\ITDB\CLEARWATER03	8	CLEARWATER

DATA APPLICATION SECURITY

Issue 4. Users

There are several ways to authenticate users in the Oracle database: username and password, PKI certificate, Kerberos, and RADIUS. Among them, username and password authentication are the simplest and basic mechanism for security. It is essential to ensure that the users are under the good password discipline. If there is no discipline, a DBA needs to establish standard organizational policies, including password length, lifetime, and complexity. I will be performing to enhance the security using password control using SQL queries as a DBA in the recommend section.

DATA APPLICATION SECURITY & LOGICAL SECURITY OF DATA

Issue 5. System Grants

A system privilege is the right to allow users to deal with managing the database and the server. To grant a system of privilege, the grantor should grant the ADMIN OPTION or GRANT ANY ROLE for users. Here are some examples of Oracle system privileges.

- Create a user: The granted user can create a new user using `CREATE USER` permission.
- Create a table: The user who has the `CREATE TABLE` permission can create a table in her schema.
- Create a session: This `CREATE SESSION` permission allows a user can connect to the database.

This privilege should be granted to a user who absolutely needs the system privilege for a necessary work. If we grant the privilege to users excessively and unnecessarily, it may cause compromised security. The end users usually do not require the server and database related capabilities, so this privilege should be granted to DBA and application developers. I will be performing to create a user Clearwater and grant DBA to Clearwater in recommendation section.

Issue 6. Object Grants

A DBA needs to decide the types of users and the level of access associated with their designated tasks to design the application. Then, the DBA should categorize each user to each role group and grant the privilege. End users are typically granted object privileges and perform database object related actions on a specific table, view, sequence, procedure, function, or package. Assigning the proper roles to each user is an important job for database security. In the recommendation section, I will be creating roles for staff of Clearwater warehouse and implementing the test using scenarios for each role. Through test and fine-grained authorizations, I will coordinate that proper user can access to the database.

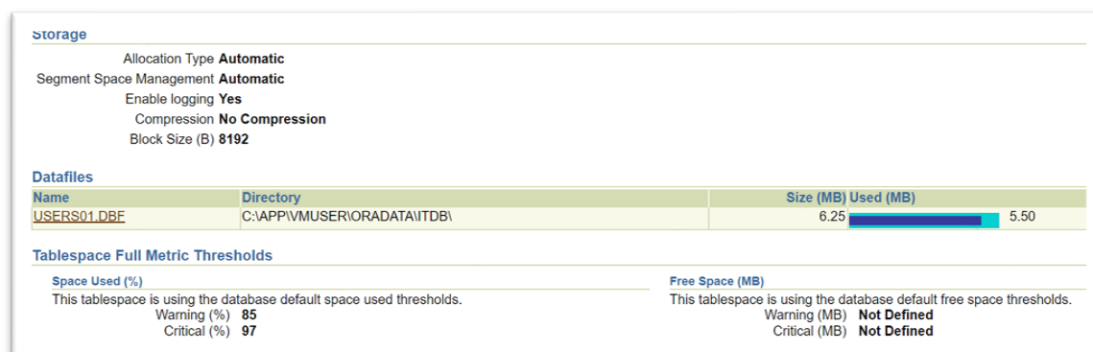
4. RECOMMENDATION

Issue 1. Tablespace - Allocate More Space for a Database

I will try the following actions to allocate more space for current tablespaces:

- Add datafiles to tablespaces for the USERS tablespace
- Increase the size of a datafile for the SYSTEM tablespace
- Create new tablespaces

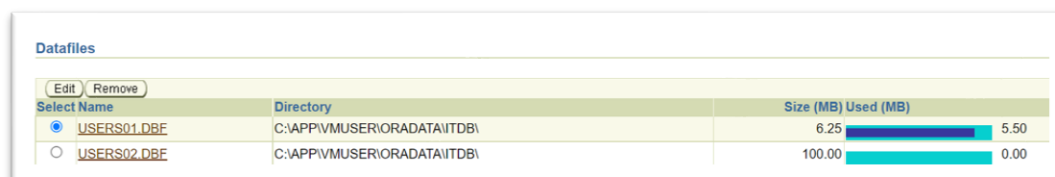
Add datafiles to tablespaces for the USERS tablespace



The USERS tablespace has only one datafile named USERS01.DBF and over 88% of space is already used. I will add one more datafile for this tablespace and increase the disk space for a better flexibility. I will use the pseudo-code below.

```
ALTER TABLESPACE "USERS" ADD DATAFILE 'C:\APP\VMUSER\ORADATA\ITDB\USERS02.DBF' SIZE 100M
```

You can see that USERS tablespace has two datafiles now.



Increase the size of a datafile for the SYSTEM tablespace

Select Name	Allocated Size(MB)	Space Used(MB)	Allocated Space Used(%)	Auto Extend	Allocated Free Space(MB)	Status	Datafiles	Type	Extent Management	Segment Management
<input checked="" type="radio"/> EXAMPLE	100.0	78.4	<div><div></div></div> 78.4	YES	21.6	✓	1	PERMANENT LOCAL	AUTO	
<input type="radio"/> SYSAUX	520.0	494.5	<div><div></div></div> 95.1	YES	25.5	✓	1	PERMANENT LOCAL	AUTO	
<input type="radio"/> SYSTEM	690.0	682.8	<div><div></div></div> 98.9	YES	7.2	✓	1	PERMANENT LOCAL	MANUAL	
<input type="radio"/> TEMP	20.0	0.0	<div><div></div></div> 0.0	YES	20.0	✓	1	TEMPORARY LOCAL	MANUAL	
<input type="radio"/> UNDOTBS1	55.0	24.5	<div><div></div></div> 44.5	YES	30.5	✓	1	UNDO LOCAL	MANUAL	
<input type="radio"/> USERS	6.2	5.5	<div><div></div></div> 88.0	YES	0.8	✓	1	PERMANENT LOCAL	AUTO	

Total Allocated Size (GB) 1.36
 Total Used (GB) 1.26
 Total Allocated Free Space (GB) 0.10

✓ Online ✗ Offline ◻ Read Only

The SYSTEM tablespace has only one datafile named SYSTEM01.DBF. The allocated size is 690 MB, and 682.8 MB is used currently. I will resize the size of datafile for more space and change to extend automatically when datafile is full. I will use the pseudo-code below.

```
ALTER DATABASE DATAFILE 'C:\APP\VMUSER\ORADATA\ITDB\SYSTEM
01.DBF' RESIZE 800M
ALTER DATABASE DATAFILE 'C:\APP\VMUSER\ORADATA\ITDB\SYSTEM
01.DBF' AUTOEXTEND ON NEXT 10M
```

You can see the SYSTEM tablespace has extended to 800MB now.

Select Name	Directory	Size (MB)	Used (MB)
<input checked="" type="radio"/> SYSTEM01.DBF	C:\APP\VMUSER\ORADATA\ITDB\	800.00	<div><div></div></div> 683.81

Moreover, I added one more datafile named SYSTEM02.DBF inside SYSTEM tablespace.

Select Name	Directory	Size (MB)	Used (MB)
<input checked="" type="radio"/> SYSTEM01.DBF	C:\APP\VMUSER\ORADATA\ITDB\	690.00	<div><div></div></div> 683.75
<input type="radio"/> SYSTEM02.DBF	C:\APP\VMUSER\ORADATA\ITDB\	200.00	<div><div></div></div> 0.00

Create new tablespaces

I will create a new tablespace named CLEARWATER with three datafiles inside to increase the size of a database. Each datafiles will have 200MB and be automatically increase 10 KB when it is full. I will use the pseudo-code below.

```
CREATE SMALLFILE TABLESPACE "CLEARWATER" DATAFILE 'C:\APP\
VMUSER\ORADATA\ITDB\clearwater01' SIZE 100M AUTOEXTEND ON
NEXT 10K MAXSIZE UNLIMITED , 'C:\APP\VMUSER\ORADATA\ITDB\c
learwater02' SIZE 100M AUTOEXTEND ON NEXT 10K MAXSIZE UNLI
MITED , 'C:\APP\VMUSER\ORADATA\ITDB\clearwater03' SIZE 100
M AUTOEXTEND ON NEXT 10K MAXSIZE UNLIMITED LOGGING EXTENT
MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO
```

Here is the result.

Information
Modification to the datafile will not take effect until you click "OK" button.

General Storage

Name: CLEARWATER

Extent Management: ☒ Locally Managed, ☐ Dictionary Managed

Type: ☒ Permanent, ☐ Temporary, ☐ Undo

Status: ☒ Read Write, ☐ Read Only, ☐ Offline

Datafiles: ☐ Use bigfile tablespace

Select	Name	Directory	Size (M)
<input checked="" type="radio"/>	clearwater01	C:\APP\VMUSER\ORADATA\ITDB\	100
<input type="radio"/>	clearwater02	C:\APP\VMUSER\ORADATA\ITDB\	100

You can see the CLEARWATER tablespace has been created now.

Confirmation
The object has been created successfully

tablespaces Object Type: Tablespace

Search
Enter an object name to filter the data that is displayed in your results set.
Object Name
By default, the search returns all uppercase matches beginning with the string you entered. To run an exact or case-sensitive match, double quote the search string. You can use the wildcard symbol (%) in a double quoted string.

Selection Mode: Single

Select	Name	Allocated Size(MB)	Space Used(MB)	Allocated Space Used(%)	Auto Extend	Allocated Free Space(MB)	Status	Datafiles	Type	Extent Management	Segment Management
<input checked="" type="radio"/>	CLEARWATER	300.0	3.0	1.0	YES	297.0	✓	3	PERMANENT LOCAL	AUTO	
<input type="radio"/>	EXAMPLE	100.0	78.4	78.4	YES	21.6	✓	1	PERMANENT LOCAL	AUTO	
<input type="radio"/>	SYSAUX	530.0	498.3	94.0	YES	31.7	✓	1	PERMANENT LOCAL	AUTO	
<input type="radio"/>	SYSTEM	690.0	683.8	99.1	YES	6.2	✓	1	PERMANENT LOCAL	MANUAL	
<input type="radio"/>	TEMP	20.0	0.0	0.0	YES	20.0	✓	1	TEMPORARY LOCAL	MANUAL	
<input type="radio"/>	UNDOTBS1	55.0	10.0	18.2	YES	45.0	✓	1	UNDO	LOCAL	MANUAL
<input type="radio"/>	USERS	6.2	5.5	88.0	YES	0.8	✓	1	PERMANENT LOCAL	AUTO	

Total Allocated Size (GB) 1.66
Total Used (GB) 1.25
Total Allocated Free Space (GB) 0.41

✓ Online ✗ Offline 📖 Read Only

It is an important role to plan the tablespaces efficiently as a DBA. The DBA needs to figure out the exact needs for the database's security and create enough tablespaces and can assign tablespace quotas to proper users. I also recommend adding one or two large datafiles or using auto extension enabled instead of creating several small datafiles.

Issue 2. Schemas

A DBA can grant schema object privileges using an ADMIN OPTION:

- Grant the system privilege or role
- Grant system privilege or role
- Alter or drop the role.

Clearwater, the DBA of the database, created three users: Ron, George, Bill.

```

20 CREATE USER Ron IDENTIFIED BY secret1 DEFAULT TABLESPACE users;
21 CREATE USER George IDENTIFIED BY secret2 DEFAULT TABLESPACE users;
22 CREATE USER Bill IDENTIFIED BY secret3 DEFAULT TABLESPACE users;
23
24

```

Query Result x Script Output x

Task completed in 0.247 seconds

User RON created.

User GEORGE created.

User BILL created.

Search And Select: Schema

Search

To filter the list or to search for a specific item in the list, enter text in the text field and click Go and click Go.

Schema

Go

By default, the search returns all uppercase matches beginning with the string you entered. To run an exact or case- You can use the wildcard symbol (% , *) in a double-quoted string.

Select Schema

- ☒ ANONYMOUS
- ☐ APEX_030200
- ☐ APEX_PUBLIC_USER
- ☐ APPQOSSYS
- ☐ BI
- ☐ BILL
- ☐ CLEARWATER
- ☐ CTXSYS
- ☐ DBSNMP
- ☐ DIP
- ☐ EXFSYS
- ☐ FLOWM_FILES
- ☐ GEORGE
- ☐ HR

Connections

Oracle Connections

- ☒ Bill_as_Clearwater
- ☒ George_as_Clearwater
- ☒ itdb_as_Clearwater
- ☒ Ron_as_Clearwater

I created three roles by referring to the table that analyzed each role.

- o Role goon

```

--Warehouse GOONS
CREATE ROLE goon; --create role
GRANT CREATE SESSION TO goon; --connect to DB
GRANT SELECT, UPDATE ON clearwater.shipment_line TO goon; --receive orders
SET ROLE goon;
SELECT * FROM session_roles;

```

Script Output x Query Result x

All Rows Fetched: 1 in 2.621 seconds

ROLE

1	GOON
---	------

We can see the details of each role using Oracle Enterprise Manager.

View Role: GOON

General

Name

GOON

Authentication

None

Roles

Role

Admin Option

No items found

System Privileges

System Privilege

Admin Option

CREATE SESSION

N

Object Privileges

Object Privilege

Schema

Object

SELECT

CLEARWATER

SHIPMENT_LINE

UPDATE

CLEARWATER

SHIPMENT_LINE

Consumer Group Privileges

Consumer Group

No items found

o Role manager

--Warehouse Manager

CREATE ROLE manager; --create role

GRANT CREATE SESSION TO manager; --connect to DB

GRANT goon TO manager; -- inherit

GRANT INSERT, DELETE ON clearwater.shipment_line TO manager

GRANT SELECT, INSERT, UPDATE ON clearwater.shipment TO manager;

GRANT SELECT, INSERT, UPDATE ON clearwater.shipment_line TO manager;

--report shipments of inventory items

GRANT SELECT ON clearwater.inventory TO manager;

GRANT SELECT ON clearwater.item TO manager;

SET ROLE manager;

SELECT * FROM session_roles;

Script Output x

Query Result x

SQL

All Rows Fetched: 2 in 0.003 seconds

ROLE

1 MANAGER

2 GOON

Name

MANAGER

Authentication

None

Roles

Role

Admin Option

GOON

N

System Privileges

System Privilege

Admin Option

CREATE SESSION

N

Object Privileges

Object Privilege

Schema

Object

SELECT

CLEARWATER

INVENTORY

SELECT

CLEARWATER

ITEM

INSERT

CLEARWATER

SHIPMENT

SELECT

CLEARWATER

SHIPMENT

UPDATE

CLEARWATER

SHIPMENT

INSERT

CLEARWATER

SHIPMENT_LINE

SELECT

CLEARWATER

SHIPMENT_LINE

UPDATE

CLEARWATER

SHIPMENT_LINE

○ Role leadership

```
--Company Leadership
CREATE ROLE leadership; --create role
GRANT CREATE SESSION TO leadership; --connect to DB
GRANT manager TO leadership; --inherit
-- manage the daily operation
GRANT SELECT, INSERT, UPDATE, DELETE ON clearwater.inventory TO leadership;
GRANT SELECT, INSERT, UPDATE, DELETE ON clearwater.item TO leadership;
GRANT SELECT, INSERT, UPDATE, DELETE ON clearwater.shipment TO leadership;
GRANT SELECT, INSERT, UPDATE, DELETE ON clearwater.shipment_line TO leadership;
-- report of sales and inventory control
GRANT SELECT, INSERT, UPDATE, DELETE ON clearwater.inventory TO leadership;
GRANT SELECT, INSERT, UPDATE, DELETE ON clearwater.item TO leadership;
GRANT SELECT, INSERT, UPDATE, DELETE ON clearwater.category TO leadership;
GRANT SELECT, INSERT, UPDATE, DELETE ON clearwater.color TO leadership;
-- reports of advertising and sales
GRANT SELECT ON clearwater.Customer TO leadership;
GRANT SELECT ON clearwater.order_line TO leadership;
GRANT SELECT ON clearwater.orders TO leadership;
GRANT SELECT ON clearwater.order_source TO leadership;
SET ROLE leadership;
SELECT * FROM session_roles;
```

Query Result x

SQL | All Rows Fetched: 3 in 0.001 seconds

ROLE
1 LEADERSHIP
2 MANAGER
3 GOON

I granted leadership role to user Bill.

```
GRANT leadership TO Bill;
```

Now, Bill can access and see the customer table to generate reports on the effectiveness of advertising and sales.


Worksheet

Query Builder

1

SELECT* FROM clearwater.customer;

Query Result x

 All Rows Fetched: 6 in 0.122 seconds

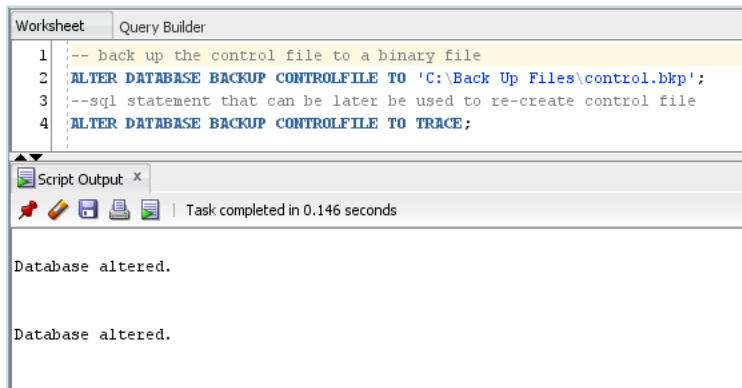
	C_ID	C_LAST	C_FIRST	C_MI	C_BIRTHDATE	C_ADDRESS	C_CITY	C_STATE
1	1	Harris	Paula	E	09-APR-53	1156 Water Street, Apt. #3	Osseo	WI
2	2	Garcia	Maria	H	14-JUL-58	2211 Pine Drive	Radisson	WI
3	3	Miller	Lee	(null)	05-JAN-36	699 Pluto St. NW	Silver Lake	WI
4	4	Chang	Alissa	R	01-OCT-76	987 Durham Rd.	Apple Valley	MN
5	5	Edwards	Mitch	M	20-NOV-86	4204 Garner Street	Washburn	WI
6	6	Nelson	Kyle	E	04-DEC-84	232 Echo Rd.	Minnetonka	MN

Sensitive data, such as customer information, requires more careful authorization.

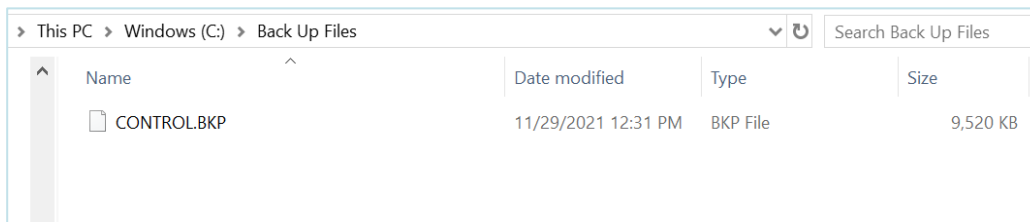
Issue 3. Control File & Redo Log File

Backing up the Control Files

First, I made a new folder named 'Back Up Files' for back up important files. Let's assume this folder was a new physical storage.



I backed up the control files using the syntax above and was able to see the backup files were located inside a new folder.



Multiplexing redo log files

At first, we can identify how many groups and members exist using the query below.

```
select group#, member from v$logfile order by group#, member;
```


Worksheet

Query Builder

1

select group#, member from v\$logfile order by group#, member

Query Result x

All Rows Fetched: 3 in 0.271 seconds

	GROUP#	MEMBER
1	1	C:\APP\VMUSER\ORADATA\ITDB\RED001.LOG
2	2	C:\APP\VMUSER\ORADATA\ITDB\RED002.LOG
3	3	C:\APP\VMUSER\ORADATA\ITDB\RED003.LOG

I created 'redo01a.log', 'redo02a.log', and 'redo03a.log' files in the same folder.

This way can mitigate the issue against a drive failure, but the best plan is storing members on separate disks (Savaram, 2021).

Worksheet

Query Builder

1

--identify how many groups and members exist

2

SELECT group#, member FROM v\$logfile ORDER BY group#, member;

3

--multiplex the redo log

4

ALTER DATABASE ADD logfile member 'C:\APP\VMUSER\ORADATA\ITDB\redo01a.log' TO group 1;

5

ALTER DATABASE ADD logfile member 'C:\APP\VMUSER\ORADATA\ITDB\redo02a.log' TO group 2;

6

ALTER DATABASE ADD logfile member 'C:\APP\VMUSER\ORADATA\ITDB\redo03a.log' TO group 3;

Script Output x

Query Result x

SQL

All Rows Fetched: 6 in 0.021 seconds

	GROUP#	MEMBER
1	1	C:\APP\VMUSER\ORADATA\ITDB\RED001.LOG
2	1	C:\APP\VMUSER\ORADATA\ITDB\RED001A.LOG
3	2	C:\APP\VMUSER\ORADATA\ITDB\RED002.LOG
4	2	C:\APP\VMUSER\ORADATA\ITDB\RED002A.LOG
5	3	C:\APP\VMUSER\ORADATA\ITDB\RED003.LOG
6	3	C:\APP\VMUSER\ORADATA\ITDB\RED003A.LOG

View Redo Log Group: 1

Group # 1

File size **51200 KB**

Status **CURRENT**

Redo Log Members

File Name	File Directory
RED001.LOG	C:\APP\VMUSER\ORADATA\ITDB\
RED001A.LOG	C:\APP\VMUSER\ORADATA\ITDB\

Here is another problem. All Clearwater database files were stored in the same folder. Even though this is a default installation, it may cause serious security problems when a system failure or attack happens on C drive or this computer. We need to prepare a different physical storage or cloud computer service for backing up the database.

This PC > Windows (C:) > app > vmuser > oradata > itdb					Search itdb
Name	Date modified	Type	Size		
CONTROL01.CTL	11/26/2021 8:32 AM	CTL File	9,520 KB		
EXAMPLE01.DBF	11/26/2021 8:32 AM	DBF File	102,408 KB		
REDO01	11/25/2021 3:30 PM	Text Document	51,201 KB		
REDO02	11/26/2021 8:32 AM	Text Document	51,201 KB		
REDO03	11/26/2021 8:32 AM	Text Document	51,201 KB		
SYSAUX01.DBF	11/26/2021 8:32 AM	DBF File	532,488 KB		
SYSTEM01.DBF	11/26/2021 8:32 AM	DBF File	706,568 KB		
TEMP01.DBF	11/26/2021 8:32 AM	DBF File	20,488 KB		
UNDOTBS01.DBF	11/26/2021 8:32 AM	DBF File	56,328 KB		
USERS01.DBF	11/26/2021 8:32 AM	DBF File	6,408 KB		

Not only password or lock for data but also a key or authorization for a facility could be the first line of defense to protect data against malicious intrusions and attacks. We should perform the security evaluation of facilities and staffs regularly. If we improve controlling physical access to data center, it can enhance data security.

Issue 4. Users

If users use weak and short passwords, somebody may guess the passwords and break-in. I recommend creating a common policy of password using user profiles and it will be used as authorization parameters for user security. We can set up each user account associating with a selected user profile, and it will help to manage of company's policies simply.

I created a new user profile called `clearwater_profile`:

The screenshot shows the SQL Developer interface with a worksheet containing the following SQL script:

```

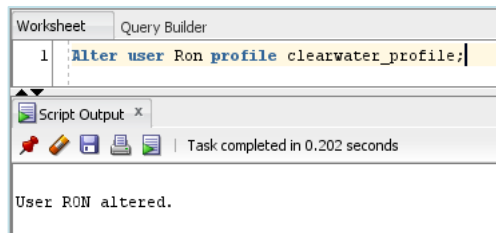
1  --password
2  CREATE PROFILE clearwater_profile LIMIT
3  CONNECT TIME 90 --Limit connection time to 90 min
4  SESSIONS_PER_USER 2 --Allow two sessions for each user
5  IDLE TIME 30 --Automatic logout after 30 min idle
6  FAILED_LOGIN_ATTEMPTS 5 --Lock the account after 5 attempts
7  PASSWORD_LIFE_TIME 180; --Force password change after 180 days
  
```

Below the script, the 'Script Output' pane shows the message: 'Profile CLEARWATER_PROFILE created.' and 'Task completed in 0.285 seconds'.

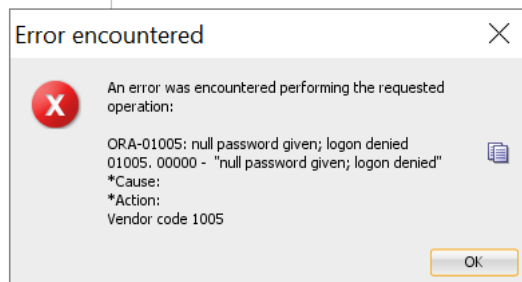
Database Instance: `itdb` > Profiles > View Profile: **CLEARWATER_PROFILE**

Name CLEARWATER_PROFILE	
Details	
CPU/Session (Sec./100)	DEFAULT
CPU/Call (Sec./100)	DEFAULT
Connect Time (Minutes)	90
Idle Time (Minutes)	30
Database Services	
Concurrent Sessions (Per User)	2
Reads/Session (Blocks)	DEFAULT
Reads/Call (Blocks)	DEFAULT
Private SGA (KBytes)	DEFAULT
Composite Limit (Service Units)	DEFAULT
Password	
Expire in (days)	180
Lock (days past expiration)	DEFAULT
History	
Number of passwords to keep	DEFAULT
Number of days to keep for	DEFAULT
Complexity	
Complexity function	DEFAULT
Failed Login	
Number of failed login attempts to lock after	5
Number of days to lock for	DEFAULT

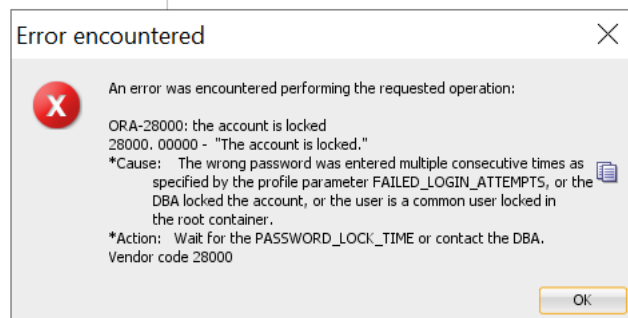
When I create a new user without specific profile, the **Default** profile will be assigned to the user. I assigned `clearwater_profile` to user Ron.



I tried to log in by wrong password.



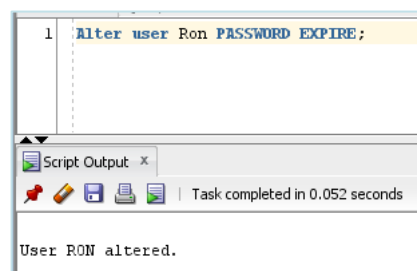
After attempting 5 times, I was able to see the account is locked.

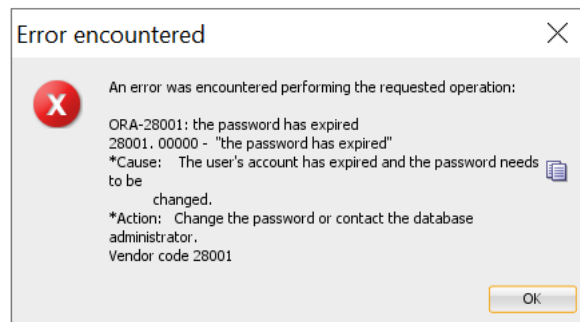


To unlock the user Ron, I used the following statement.

```
ALTER USER Ron ACCOUNT UNLOCK;
```

I tested using the following statement in case Ron's password expired.





I could see a message indicating that the user Ron's password expired. As a DBA, I changed his password.

```
ALTER USER Ron IDENTIFIED BY Secret123;
```

(Result: User Ron altered.)

I can check and control users' account using Oracle Enterprise Manager as shown below.

Users

Search

Enter an object name to filter the data that is displayed in your results set.

Object Name Go

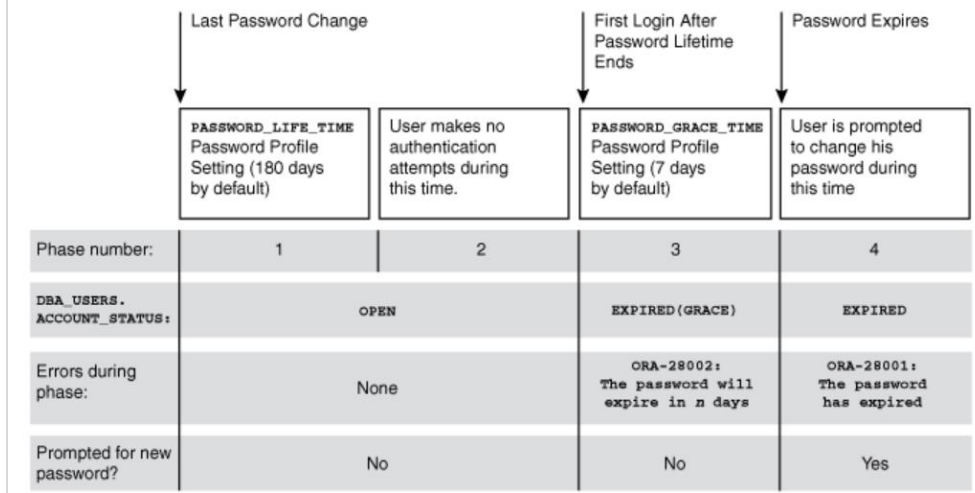
By default, the search returns all uppercase matches beginning with the string you entered. To run an exact or case-sensitive match, double quote the search string. You can use the wildcard sy

Selection Mode ▼

Select	UserName	Account Status	Expiration Date	Default Tablespace
<input checked="" type="radio"/>	ANONYMOUS	EXPIRED & LOCKED	Mar 30, 2010 11:05:19 AM ADT	SYS_AUX
<input type="radio"/>	APEX_030200	EXPIRED & LOCKED	Mar 30, 2010 11:05:19 AM ADT	SYS_AUX
<input type="radio"/>	APEX_PUBLIC_USER	EXPIRED & LOCKED	Mar 30, 2010 11:05:19 AM ADT	USERS
<input type="radio"/>	APPQOSSYS	EXPIRED & LOCKED	Mar 30, 2010 10:16:56 AM ADT	SYS_AUX
<input type="radio"/>	BI	EXPIRED & LOCKED	Nov 10, 2021 4:05:30 PM AST	USERS
<input type="radio"/>	BILL	OPEN	May 26, 2022 9:02:52 PM ADT	USERS
<input type="radio"/>	CLEARWATER	OPEN	May 9, 2022 4:24:55 PM ADT	USERS
<input type="radio"/>	CTXSYS	EXPIRED & LOCKED	Mar 30, 2010 11:05:19 AM ADT	SYS_AUX
<input type="radio"/>	DBSNMP	OPEN	May 9, 2022 4:06:06 PM ADT	SYS_AUX
<input type="radio"/>	DIP	EXPIRED & LOCKED	Mar 30, 2010 10:09:52 AM ADT	USERS
<input type="radio"/>	EXFSYS	EXPIRED & LOCKED	Mar 30, 2010 10:27:00 AM ADT	SYS_AUX
<input type="radio"/>	FLWS_FILES	EXPIRED & LOCKED	Mar 30, 2010 11:05:19 AM ADT	SYS_AUX
<input type="radio"/>	GEORGE	OPEN	May 26, 2022 9:02:44 PM ADT	USERS
<input type="radio"/>	HR	EXPIRED & LOCKED	Nov 10, 2021 4:05:30 PM AST	USERS
<input type="radio"/>	IV	EXPIRED & LOCKED	Nov 10, 2021 4:05:30 PM AST	USERS

We can reference 'password change life cycle' for managing user account after a password is created.

Figure 3-1 Chronology of Password Lifetime and Grace Period

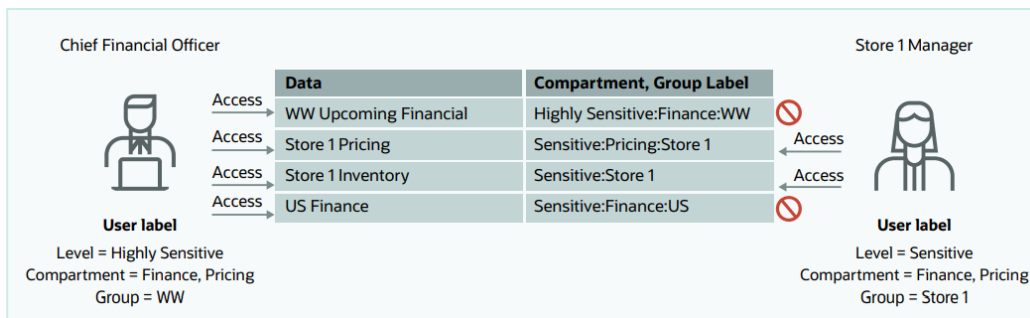


(Oracle, n.d.)

Data labels for users

I also recommend controlling data access using labels, such as level, compartment, and group. I made a leadership Bill's data label referencing from the Oracle example.

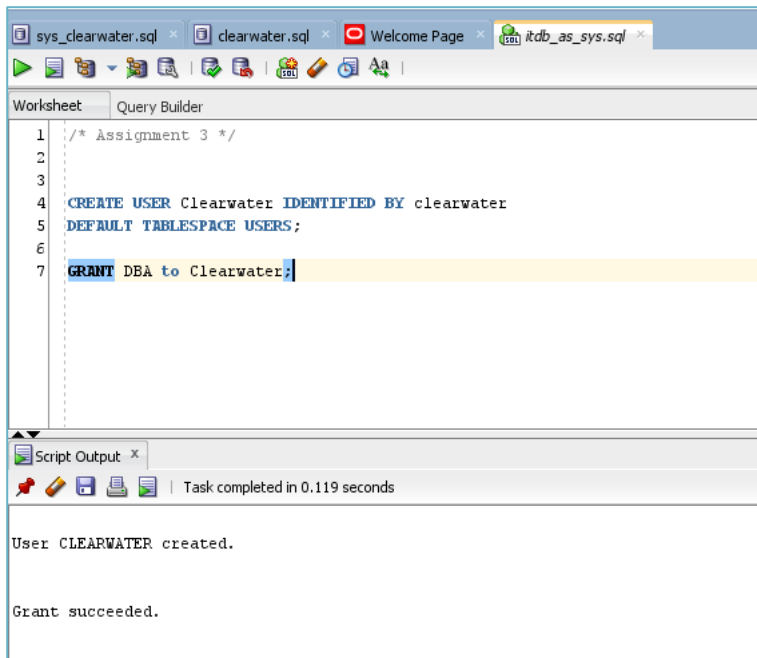
- User Bill has a level of Highly sensitive (The user's level should be the same or higher level than the level of data).
- Bill's compartment in the data label is an inventory.
- Bill's group is Warehouse 1.



(Oracle, 2021)

Issue 5. System Grants

I created Clearwater as a DBA for Clearwater database.



We can know which user has been granted the DBA role using the following query:

```
SELECT * from dba_role_privs WHERE granted_role = 'DBA'; --find the
users having DBA privileges
```

```
desc dba_role_privs --describes the roles granted to all users and
roles in the DB
```

No! ANY TABLE

Select **ANY** table privilege is a system privilege and allows users to access the sensitive data. If we use this system privileges frequently for convenience, it causes malicious SQL injection attacks to access data into the database.

Issue 6. Object Grants

Roles and authorities may be predicted through scenarios. Before assigning roles and authorities to users, it is necessary to subdivide and organize the necessary roles as shown in the table below.

Role	Duties	Authorities
Warehouse Goons	<ul style="list-style-type: none"> ○ Receive shipments of inventory and record them in the database. 	<ul style="list-style-type: none"> ● Connect ● Select, update on clearwater.shipment_line,
Warehouse Manager	<ul style="list-style-type: none"> ○ Manage Warehouse Goons ○ Create new Shipment, Shipment_lines ○ Generate reports on shipments of inventory items 	<ul style="list-style-type: none"> ● Grant role Goons to Manager ● Select, insert, update on clearwater.Shipment & clearwater.Shipment_line ● Select clearwater. inventory & item & color & category for reports on shipments of inventory items
Company Leadership	<ul style="list-style-type: none"> ○ Manage the daily operation of Clearwater Traders ○ Generate reports on the effectiveness of advertising and sales ○ Generate reports on the effectiveness of sales and inventory control 	<ul style="list-style-type: none"> ● Grant Goons, Manager's role to Leadership ● Select, insert, update, delete on shipment and clearwater. shipment_line ● Select, insert, update, delete on clearwater. Inventory & item & category & color ● Select on clearwater. Customer & order_line & orders &

order_source to generate reports on the effectiveness of advertising and sales.

We can see which object privileges are granted to users or roles in each table.

The screenshot shows the SQL Developer interface with the 'SHIPMENT_LINE' table selected. The 'Grants' tab is active, displaying the following SQL code:

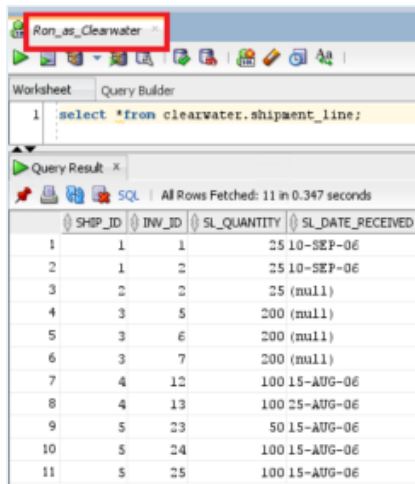
```
1 CREATE TABLE "CLEARWATER"."SHIPMENT_LINE"
2 (
3   "SHIP_ID" NUMBER(10,0),
4   "INV_ID" NUMBER(10,0),
5   "SL_QUANTITY" NUMBER(4,0),
6   "SL_DATE_RECEIVED" DATE,
7   CONSTRAINT "SHIPMENT_LINE_SHIPID_INVID_PK" PRIMARY KEY ("SHIP_ID", "INV_ID")
8 USING INDEX PCTFREE 10 INITRANS 2 MAXTRANS 255 COMPUTE STATISTICS
9 STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
10 PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1 BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
11 TABLESPACE "USERS" ENABLE,
12   CONSTRAINT "SHIPMENT_LINE_SHIP_ID_FK" FOREIGN KEY ("SHIP_ID")
13   REFERENCES "CLEARWATER"."SHIPMENT" ("SHIP_ID") ENABLE,
14   CONSTRAINT "SHIPMENT_LINE_INV_ID_FK" FOREIGN KEY ("INV_ID")
15   REFERENCES "CLEARWATER"."INVENTORY" ("INV_ID") ENABLE
16 ) SEGMENT CREATION IMMEDIATE
17 PCTFREE 10 PCTUSED 40 INITRANS 1 MAXTRANS 255 NOCOMPRESS LOGGING
18 STORAGE(INITIAL 65536 NEXT 1048576 MINEXTENTS 1 MAXEXTENTS 2147483645
19 PCTINCREASE 0 FREELISTS 1 FREELIST GROUPS 1 BUFFER_POOL DEFAULT FLASH_CACHE DEFAULT CELL_FLASH_CACHE DEFAULT)
20 TABLESPACE "USERS" ;
21
22
23
24 GRANT SELECT, UPDATE ON "CLEARWATER"."SHIPMENT_LINE" TO "GOON";
25
26 GRANT INSERT, SELECT, UPDATE ON "CLEARWATER"."SHIPMENT_LINE" TO "MANAGER";
27
28 GRANT DELETE, INSERT, SELECT, UPDATE ON "CLEARWATER"."SHIPMENT_LINE" TO "LEADERSHIP";
29
30
```

The screenshot shows the 'Grants' tab for the 'SHIPMENT_LINE' table. The table below lists the granted privileges, grantees, and grantors.

	PRIVILEGE	GRANTEE	GRANTABLE	GRANTOR	OBJECT_NAME
1	SELECT	GOON	NO	CLEARWATER	SHIPMENT_LINE
2	UPDATE	GOON	NO	CLEARWATER	SHIPMENT_LINE
3	INSERT	MANAGER	NO	CLEARWATER	SHIPMENT_LINE
4	SELECT	MANAGER	NO	CLEARWATER	SHIPMENT_LINE
5	UPDATE	MANAGER	NO	CLEARWATER	SHIPMENT_LINE
6	DELETE	LEADERSHIP	NO	CLEARWATER	SHIPMENT_LINE
7	INSERT	LEADERSHIP	NO	CLEARWATER	SHIPMENT_LINE
8	SELECT	LEADERSHIP	NO	CLEARWATER	SHIPMENT_LINE
9	UPDATE	LEADERSHIP	NO	CLEARWATER	SHIPMENT_LINE

I am going to test if object privileges are granted properly.

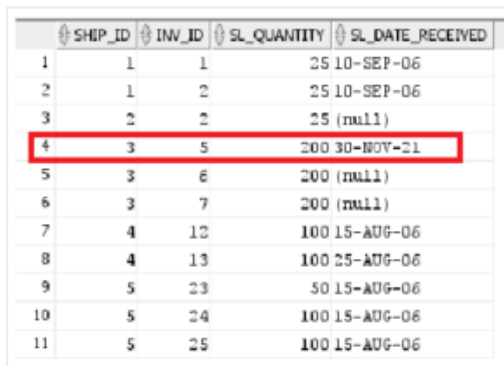
- Warehouse Goons 'Ron' can insert a new shipment of inventory in the database.



The screenshot shows a database query tool interface. At the top, a window titled 'Ron_as_Clearwater' is highlighted with a red box. Below it, the 'Query Builder' tab is active, showing a query: `select * from clearwater.shipment_line;`. The 'Query Result' tab shows the results of the query, with a status bar indicating 'All Rows Fetched: 11 in 0.347 seconds'.

SHIP_ID	INV_ID	SL_QUANTITY	SL_DATE_RECEIVED
1	1	1	25 10-SEP-06
2	1	2	25 10-SEP-06
3	2	2	25 (null)
4	3	5	200 (null)
5	3	6	200 (null)
6	3	7	200 (null)
7	4	12	100 15-AUG-06
8	4	13	100 25-AUG-06
9	5	23	50 15-AUG-06
10	5	24	100 15-AUG-06
11	5	25	100 15-AUG-06

```
UPDATE clearwater.shipment_line
SET sl_date_received = TO_DATE('11/30/2021', 'MM/DD/YYYY')
WHERE ship_id = '3' AND inv_id = '5';
```



The screenshot shows the same database query tool interface as before, but the query results have been updated. The row with SHIP_ID 3 and INV_ID 5 is highlighted with a red box, showing a date of 30-NOV-21.

SHIP_ID	INV_ID	SL_QUANTITY	SL_DATE_RECEIVED
1	1	1	25 10-SEP-06
2	1	2	25 10-SEP-06
3	2	2	25 (null)
4	3	5	200 30-NOV-21
5	3	6	200 (null)
6	3	7	200 (null)
7	4	12	100 15-AUG-06
8	4	13	100 25-AUG-06
9	5	23	50 15-AUG-06
10	5	24	100 15-AUG-06
11	5	25	100 15-AUG-06

- Warehouse Manager 'George' can create a new shipment in the database.

```
INSERT INTO clearwater.shipment_line
VALUES (6, 7, 100, TO_DATE ('11/30/2021', 'MM/DD/YYYY'));
```

```
INSERT INTO clearwater.shipment VALUES
(6, TO_DATE('11/30/2021', 'MM/DD/YYYY'));
```

SHIP_ID	SHIP_DATE_EXPECTED
1	1 15-SEP-06
2	2 15-NOV-06
3	3 25-JUN-06
4	4 25-JUN-06
5	5 15-AUG-06
6	6 30-NOV-21

SHIP_ID	INV_ID	SL_QUANTITY	SL_DATE_RECEIVED
1	1	1	25 10-SEP-06
2	1	2	25 10-SEP-06
3	2	2	25 (null)
4	3	5	200 30-NOV-21
5	3	6	200 (null)
6	3	7	200 (null)
7	4	12	100 15-AUG-06
8	4	13	100 25-AUG-06
9	5	23	50 15-AUG-06
10	5	24	100 15-AUG-06
11	5	25	100 15-AUG-06
12	5	12	300 30-NOV-21
13	6	7	100 30-NOV-21

- Company leadership 'Bill' can check today's shipment records in the database.

```
SELECT * FROM clearwater.shipment_line
WHERE sl_date_received=TO_DATE('11/30/2021','MM/DD/YYYY');
```

SHIP_ID	INV_ID	SL_QUANTITY	SL_DATE_RECEIVED
1	3	5	200 30-NOV-21
2	5	12	300 30-NOV-21
3	6	7	100 30-NOV-21

Through the test, I checked all object privileges are granted properly. I recommend a DBA should perform regular monitoring and ensure all privileges and roles are working correctly.

5. CONCLUSION

I think transparent identification of the Oracle DBA is also a necessary factor to keep data security because the DBA can access to all datafiles within the database. That is also why we learn 'Ethics and Law in Data Analytics' in our program. Before hiring DBAs, not only criminal and credit check but also a moral frame should be figured out. Moreover, I highly recommend a regular monitoring and scheduled security testing for security.

REFERENCES

Oracle. (n.d.). *Database Security Guide*.

https://docs.oracle.com/cd/E11882_01/network.112/e36292/authentication.htm#DBSEG99815

Oracle Application Developer's Guide. (n.d.). Establishing a Security Policy.

https://docs.oracle.com/cd/A58617_01/server.804/a58241/ch13.htm#645

Oracle Database security product management team. (January 2021). *Securing the Oracle Database, A Technical Primer*. Oracle E-books.

download.oracle.com/database/oracle-database-security-primer.pdf

Savaram, R. (February 15, 2021). Managing the Redo Log – Oracle DBA. *MindMajix*.

<https://mindmajix.com/oracle-dba/managing-redo-log>