International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org
Volume 4, Issue 7, July 2015 ISSN 2319 - 4847

Overview of Database Auditing for Oracle Database

Miss Reena R. Chaudhari[1], Dr. Jagdish W. Bakal[2]

[1]M.E (Computer) student,ARMIET

[2]Principal of S.S.Jondhale College of Engineering

ABSTRACT

Databases the heart of the data center, contains company's most confidential and organized information. Thus, they are main areas for today's advanced threats. Company must secure their data, and manage their database. Mostly, data have to be regularly examined to be aware of threats and should be protected to prevent the loss of sensitive customer, financial and other commercial data. Database auditing is the process that monitors, captures and stores information about what is happening in the database. Thus, this paper focused on finding auditing records from different locations that DBMS keeps so that only relevant events are seized. Moreover, the evidences are produced in the form of W's for investigator to present them in the court of law.

Keywords: Oracle 10g, dba_audit_trail, threats.

1. INTRODUCTION

Databases are one of the most compromised assets in the organisation. The databases are often targeted [1] as they are at the heart of any company, storing various records and other important and trusted data. When hackers and suspicious users gain access to sensitive data, they can quickly extract value, cause loss or impact business operations. In addition to economic loss or status damage, breaches can result in governing fines and permissible fees. Thus, organizations need to protect their data as well as databases. Database auditing is the process of monitoring and recording selected user database actions, thereby making aware of what users of actions. Auditing is done for security purposes by Database consultant so that everyone can access it [2]. Thus, auditing concept along with preventing and detecting threats is revealed in this paper. Today, regarding auditing, Organizations are facing problem in data security as well as how to recognize threats and threat them in a more cost effective way. The audit concept will help the company to decrease the increasing cost of database security.

1.1 Database security

Database security concerns the use of a broad range of information security controls to protect databases against threats. It involves various types or categories of controls, such as technical, organizational and physical. Database security entails allowing or disallowing user actions on the database and the objects within it. Oracle uses schemas and security domains to control access to data and to restrict the use of various database resources.

Threats and risks to databases have increased and therefore, the need for securing databases has also increased. Database security protects security goals (fig.1) like Confidentiality, Integrity, and Availability of the database. Unauthorized entry or access to a database server signifies a loss of confidentiality, illegal modification to the available data signifies loss of integrity and lack of access to database services signifies loss of availability. Loss of one or more of these basic facets will have a significant impact on the security of the database.

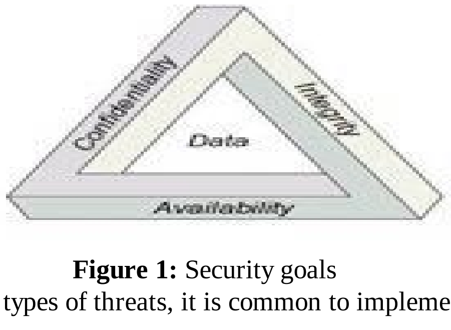


Figure 1: Security goals

Thus, to protect database against various types of threats, it is common to implement four kind of control measurement.

- Access control
- Authentication
- Authorization

- Auditing

1.2 Database auditing [3], [4]

Auditing has become an important tool for forensic analysis of data breaches. Audit records provide an certain record of actions taken whether they are generated by a database, directory, or operating system. Database auditing is a method of monitoring and recording database activity as part of database security. Auditing is essential to secure a particular database system. Thus, auditing tool implemented on a database system enables the security implemented in a system. Information such as the event type (create table, drop table, create procedure, truncate table, select, insert, update, delete) coupled with the context of the event such as the initiating IP address, event time, and actual SQL statement, are just a few examples of audit information that is commonly needed in forensic reports. A database administrator can audit all actions that take place within a database. This is good practice from a security standpoint, as auditing can detect suspicious activity and enable the DBA to take appropriate action.

2. PROMINENCE AND SIGNIFICANCE OF STUDY [2], [7]

Database security and database auditing are linked to each other. Auditing is an important feature of database security. Auditing is crucial tasks for DBA of database management system which need to secure a particular database system. Thus, auditing mechanism which is deploying on a database system facilitates the security implemented in a system.Moreover, Database auditing helps the investigator to collect evidences to present in front of law by asking following questions:
1. Who access the data?
2. At what date and time was the access?
3. What program or client software was used to access the data?
4. From what location was the request issued?
5. was the request successful, and if so how many rows of data were retrieved?
6. If request was modified, then what data was changed?

2.1 Database access auditing techniques [3]

There are several popular techniques that can be deployed to audit database structures.

Trace-based auditing

This technique is usually built directly into the native capabilities of the DBMS. Commands or parameters are set to turn on auditing and the DBMS begins to trace records when activity occurs against audited objects.

Transaction-logs auditing: Every DBMS uses transaction logs to capture every database modification for recovery purposes. Software exists that interprets these logs and identifies what data was changed and by which users.

Fine-grained auditing

Fine-grained auditing allows the monitoring of data access based on content. A built-in audit mechanism in the database prevents users from by-passing the audit. Oracle triggers can potentially monitor DML actions such as `INSERT`, `UPDATE`, and `DELETE`.

Mandatory auditing

Oracle Database always audits certain database-related operations and writes them to the operating system audit files. It includes the actions of any user who is logged in with the **SYSDBA** or **SYSOPER** privilege. This is called Oracle Database always audits certain database-related operations and writes them to the operating system audit files. It includes the actions of any user who is logged in with the SYSDBA or SYSOPER privilege. This is called mandatory auditing.

SYSDBA auditing

SYSDBA auditing splits the auditing duties between the DBA and an auditor or security administrator who examines the DBA activities in an operating system audit trail.

Standard Database Auditing

Audit trail initialization parameter is used to enabled these auditing at the system level. Once enabled auditing, select the object and privileges that we want to audit and set auditing properties with audit command.

3. CONCEPTUAL FRAMEWORK

The tools for auditing is used by DBA and examine the locations where databases stores auditing records, and study the actions produced by DBMS as well as add actions to satisfy the requirements.

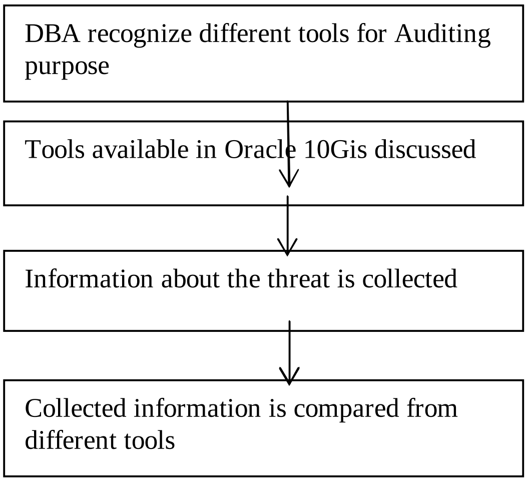

DBA recognize different tools for Auditing purpose
Tools available in Oracle 10Gis discussed
Information about the threat is collected
Collected information is compared from different tools

Figure 2: Conceptual Framework

3.1 Locations of audit records

The audit records provide information on who performed what database operation and when it was performed. It is normally used to investigate suspicious activity. For example, if an unauthorized user is deleting data from tables, the security administrator might decide to audit all connections to the database and all successful and unsuccessful deletions of rows from all tables in the database. Records are written to a SYS-owned table named AUD$. The SYS.AUD$ (dba_audit_trail and dba_fga_audit_trail) are commonly referred to as the audit trail.

3.2 Audit trail

Standard audit sends output to two locations, DB and OS. Standard audit records are written only if two conditions are true:

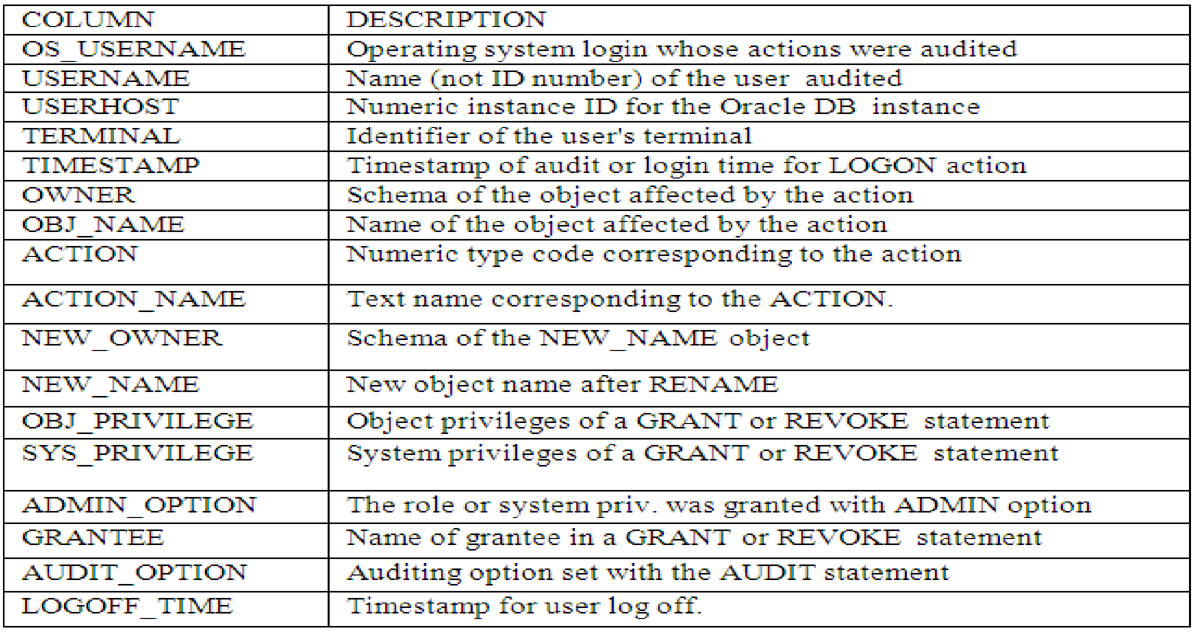
(1) The initialization parameter AUDIT_TRAIL is set to something besides “OFF”.

(2) Audit records is produced for audit events currently enabled via the SQL command AUDIT. Regardless of the AUDIT_TRAIL setting, no actions when connected “AS SYSDBA” are audited by the AUDIT command. AUDIT_TRAIL determines the destination of the audit trail data, and can be set to “DB”, “OS”, or “OFF”. AUDIT_TRAIL is a static parameter, requiring a DB restart to change its value. “OFF “disables standard audit, but does not change the audit settings established by the AUDIT command.

3.2.1 The DB audit trail [4], [5]

The DB audit trail table is normally found in SYS.AUD$. DB audit records are sparse, in that many of the fields are not populated depending upon the audit type. Oracle provides numerous views based on AUD$ which limit the type of records and columns displayed for particular interests. DBA_AUDIT_TRAIL (Table1) is the most comprehensive view and it includes all audit records

Table: 1 DBA_AUDIT_TRAIL table definition



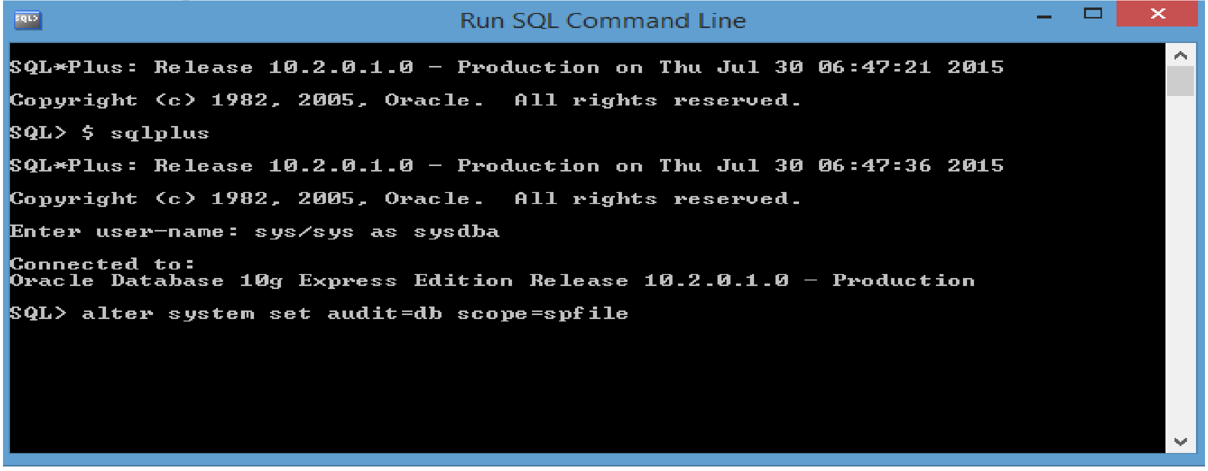
COLUMN	DESCRIPTION
OS_USERNAME	Operating system login whose actions were audited
USERNAME	Name (not ID number) of the user audited
USERHOST	Numeric instance ID for the Oracle DB instance
TERMINAL	Identifier of the user's terminal
TIMESTAMP	Timestamp of audit or login time for LOGON action
OWNER	Schema of the object affected by the action
OBJ_NAME	Name of the object affected by the action
ACTION	Numeric type code corresponding to the action
ACTION_NAME	Text name corresponding to the ACTION.
NEW_OWNER	Schema of the NEW_NAME object
NEW_NAME	New object name after RENAME
OBJ_PRIVILEGE	Object privileges of a GRANT or REVOKE statement
SYS_PRIVILEGE	System privileges of a GRANT or REVOKE statement
ADMIN_OPTION	The role or system priv. was granted with ADMIN option
GRANTEE	Name of grantee in a GRANT or REVOKE statement
AUDIT_OPTION	Auditing option set with the AUDIT statement
LOGOFF_TIME	Timestamp for user log off.

3.2.2 OS audit trail

The OS audit trail location varies by platform. On Solaris, individual files containing one or more audit records are, by default, put in $ORACLE_HOME/rdbms/audit. The optional initialization parameter AUDIT_FILE_DEST can override the default location on some platforms. On Windows, the OS trail goes into the event log which can be accessed by event viewer or dumped to a flat file with dumpel.exe, a free resource kit component from Microsoft.

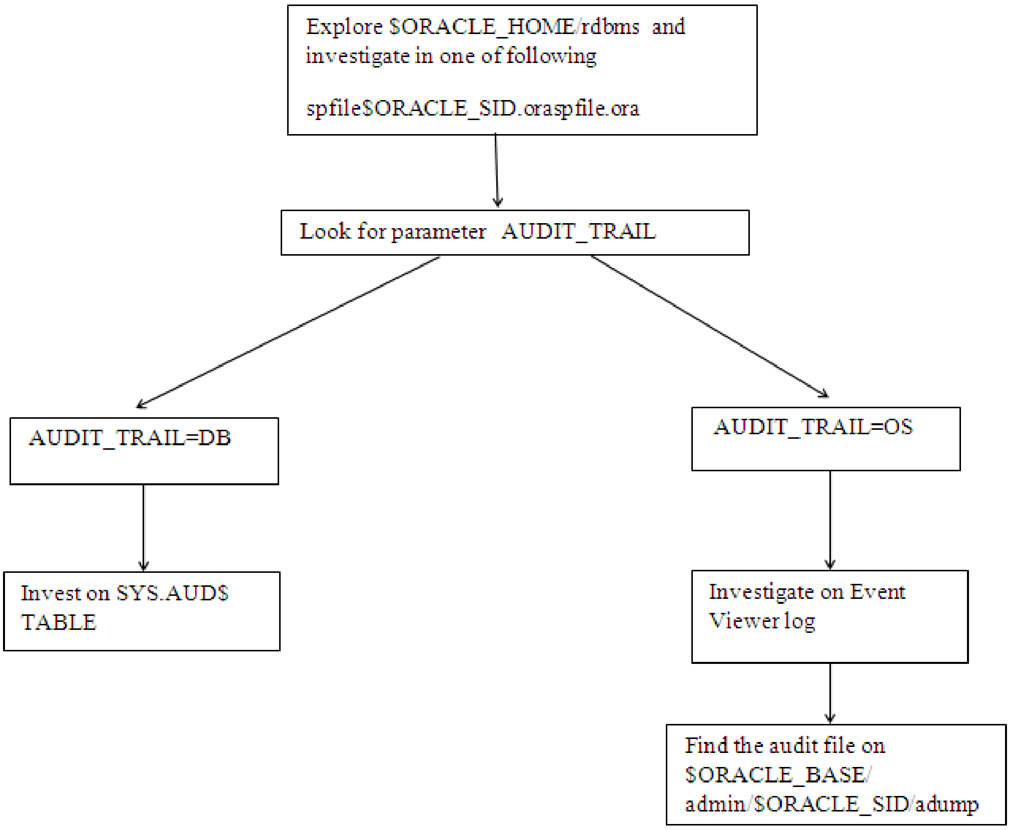
The DB audit trail is the most common choice since it contains more information and is easier to access and analyse. The OS audit trail is more difficult to access and modify from inside the database, which makes it easier to protect from malicious database users or DBAs. In either case, certain audit records always go to the OS audit trail and these should be reviewed regularly.

To change value for audit _trail , edit pile or file. For example, the following statement will change the location of audit records in the spilled.



```
SQL*Plus: Release 10.2.0.1.0 - Production on Thu Jul 30 06:47:21 2015
Copyright (c) 1982, 2005, Oracle.  All rights reserved.
SQL> $ sqlplus
SQL*Plus: Release 10.2.0.1.0 - Production on Thu Jul 30 06:47:36 2015
Copyright (c) 1982, 2005, Oracle.  All rights reserved.
Enter user-name: sys/sys as sysdba
Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production
SQL> alter system set audit=db scope=spfile
```

Figure: 3 Set audit scope



Explore $ORACLE_HOME/rdbms and investigate in one of following
spfile$ORACLE_SID.oraspfile.ora
Look for parameter AUDIT_TRAIL
AUDIT_TRAIL=DB
AUDIT_TRAIL=OS
Invest on SYS.AUD$ TABLE
Investigate on Event Viewer log
Find the audit file on $ORACLE_BASE/ admin/$ORACLE_SID/adump

Figure 4: View for finding audit information

4.1 SQL AUDIT command [8][9]

ORACLE supports three different kinds of audits enabled via various syntax of the SQL command AUDIT:

1. Statement
2. Privilege
3. Object.

Statement and privilege audits share syntax and can be limited by user. Object audits apply to a single object but cannot be restricted by user. All three share certain common options.

4.2 Audit options relevant to all auditing

All Oracle auditing produced by the AUDIT statement goes to the same audit trail. However, the following options are applicable to all forms of the AUDIT statement and modify the details of when auditing is recorded.

4.2.1 AUDIT option BY SESSION

Auditing BY SESSION produces a single audit trail record per audit option regardless of the number of successful or unsuccessful attempts within that session. In most cases, auditing BY ACCESS is used instead of BY SESSION for the increased information.

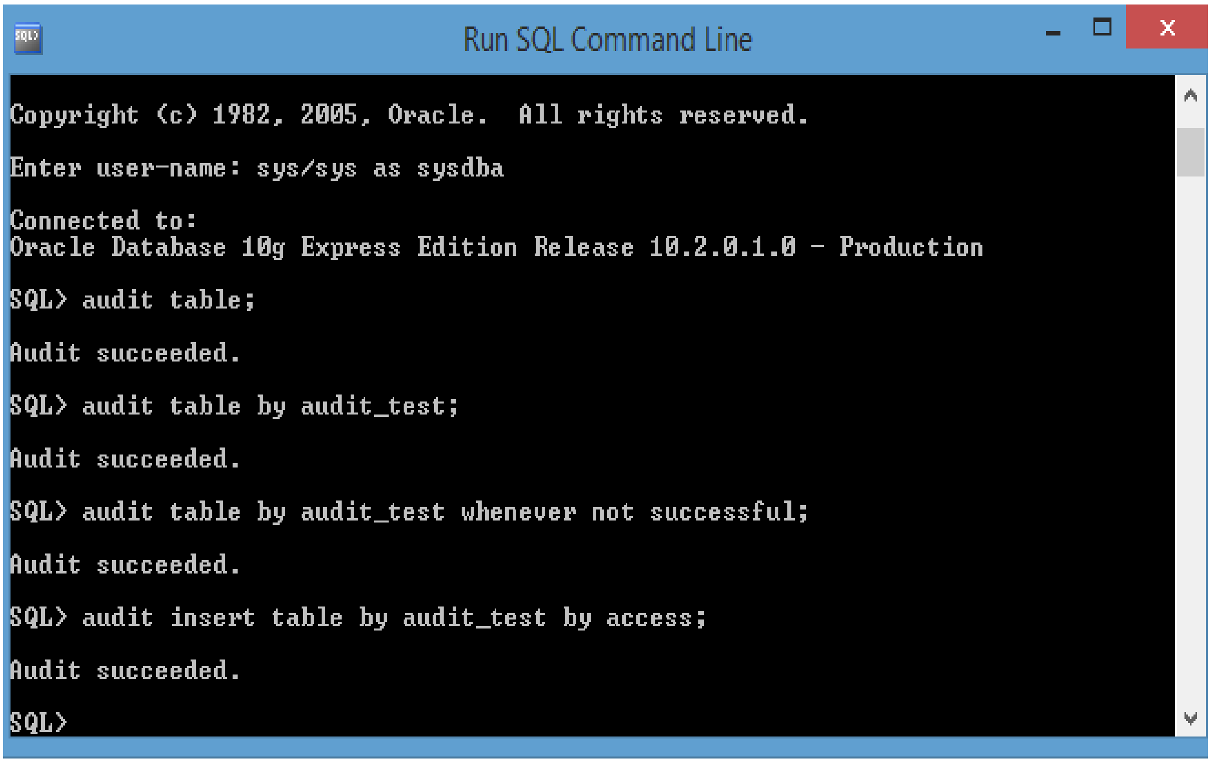
4.2.2 AUDIT option BY ACCESS

Auditing BY ACCESS generates an audit trail record for every user attempt. An ACCESS record with a nonzero DBA_AUDIT_TRAIL.RETURNCODE indicates a failed attempt. The RETURNCODE is simply the Oracle Error code returned due to the failure. The benefit of BY ACCESS is that the audit trail shows the number of times the audited action was attempted, the sequence of audited actions, and the result (either success or the failure code) of each action.

4.2.3 AUDIT WHENEVER SUCCESSFUL or NOT SUCCESSFUL

All AUDIT types can be restricted to audit only when a user action succeeds, only when it fails, or both. The syntax is "WHENEVER [NOT] SUCCESSFUL". If the clause is removed entirely, the audit statement will enable audit independent upon the outcome.

This can be viewed as follow:



```
Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Enter user-name: sys/sys as sysdba

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> audit table;

Audit succeeded.

SQL> audit table by audit_test;

Audit succeeded.

SQL> audit table by audit_test whenever not successful;

Audit succeeded.

SQL> audit insert table by audit_test by access;

Audit succeeded.

SQL>
```

Figure 5: Modify audit records

Table audit option like SQL statements CREATE TABLE, DROP TABLE, and TRUNCATE TABLE can be audited and attribute for this command can be added. For example, by user, whenever successful by session, whenever not successful .

BY USER clause is used to record audit entries for specific users only in the AUDIT statement. For example, to audit CREATE, DROP, and TRUNCATE TABLE statements for user audit_test only.

4.2.4 Statement and Privilege Auditing

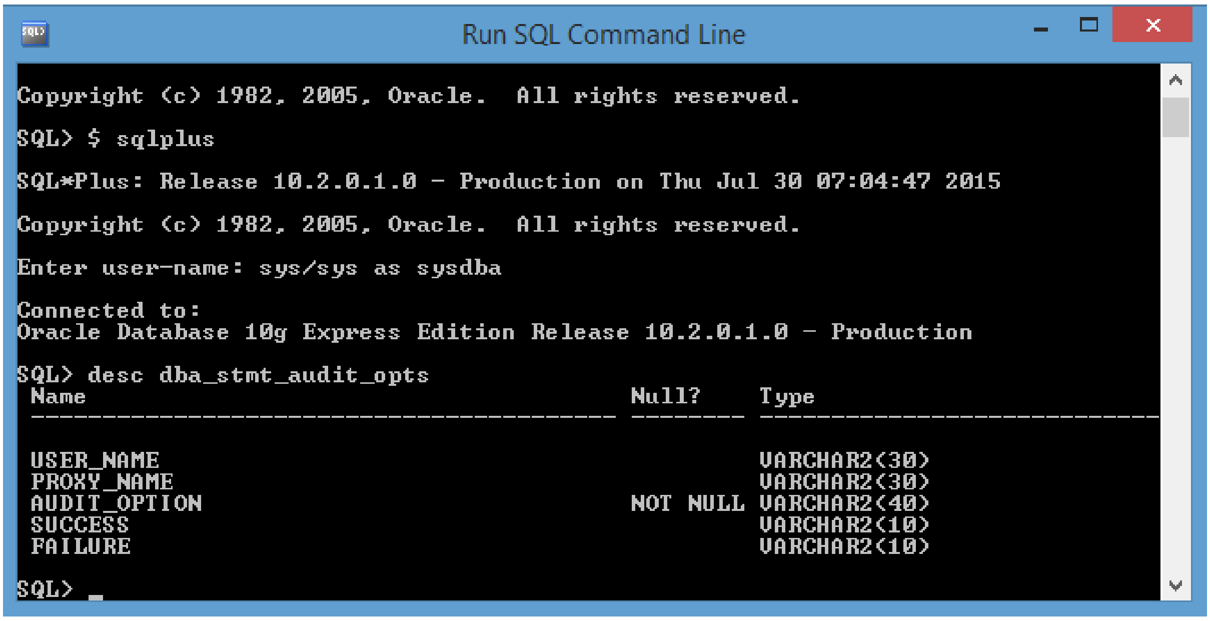
Statement and privilege auditing are separated in the Oracle documentation and data dictionary views. However, they use identical syntax, and considering them as identical will simplify things greatly. A statement audit fires when a user issues the matching SQL statement.

The following queries tells if statement or privilege actions are being audited.

SQL> SELECT * FROM dba_stmt_audit_opts

SQL> SELECT * FROM dba_priv_audit_opts;

Thus, following recorded information shows the view after query for statement audit.



```
Copyright (c) 1982, 2005, Oracle.  All rights reserved.

SQL> $ sqlplus

SQL*Plus: Release 10.2.0.1.0 - Production on Thu Jul 30 07:04:47 2015

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Enter user-name: sys/sys as sysdba

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> desc dba_stmt_audit_opts
 Name                                      Null?    Type
 ----------------------------------------- -------- ----------------------------

 USER_NAME                                          VARCHAR2(30)
 PROXY_NAME                                         VARCHAR2(30)
 AUDIT_OPTION                              NOT NULL VARCHAR2(40)
 SUCCESS                                            VARCHAR2(10)
 FAILURE                                            VARCHAR2(10)

SQL> _
```

Figure 6: Structure of table

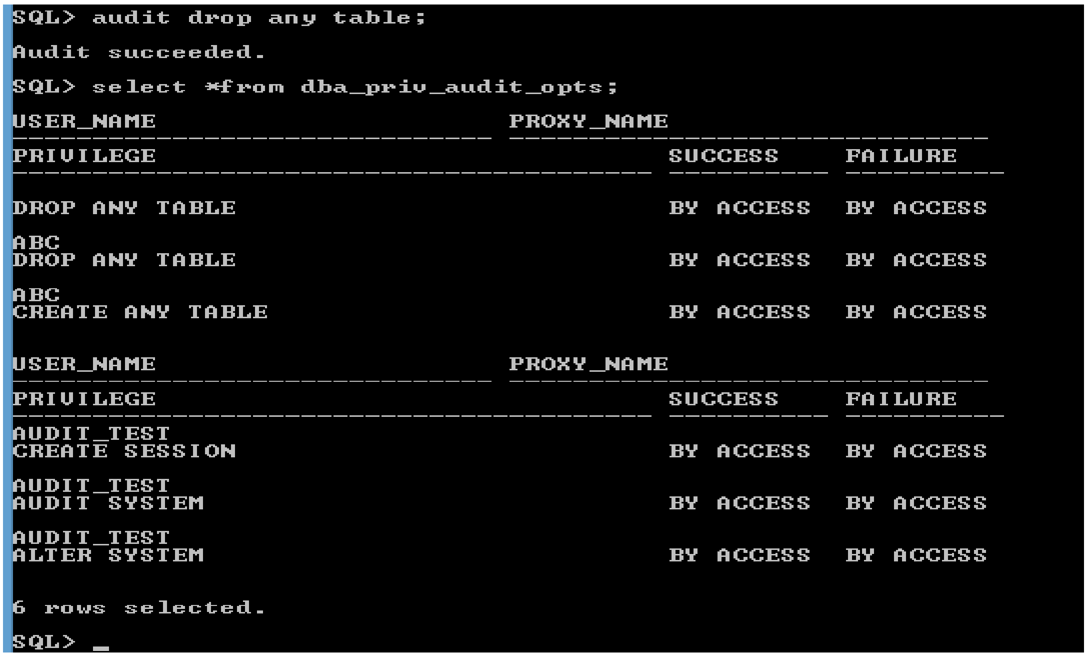
A privilege audit fires when the SQL statement requires that privilege in order to succeed.

As an example, consider if audit_test issues the following two statements:

DROP TABLE audit_test.MYTAB

DROP TABLE HR_APP.PAYROLL

Both of these are drop table statements, but the second one would need the privilege "DROP ANY TABLE" to succeed. If the requirement is to detect drop actions by users against objects which they do not own, auditing the statement would produce many audit records of no consequence. The privilege audit "AUDIT DROP ANY TABLE BY ACCESS", however, fires only on the privilege use, which will detect successful drops as shown below.



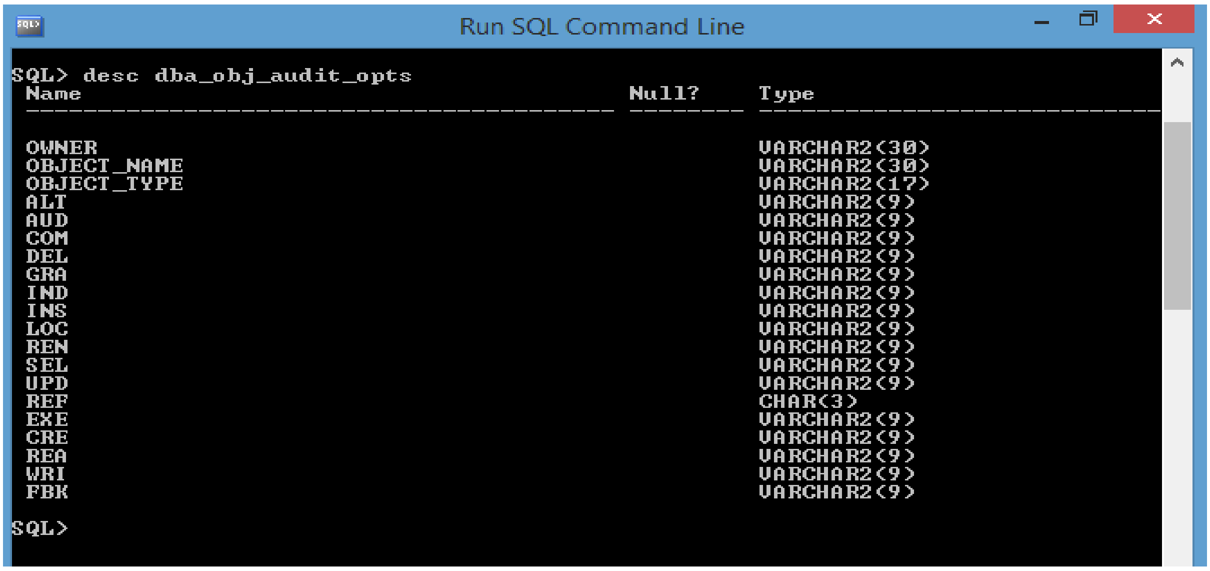
```
SQL> audit drop any table;

Audit succeeded.

SQL> select *from dba_priv_audit_opts;

USER_NAME                      PROXY_NAME
------------------------------ ------------------------------
PRIVILEGE                                SUCCESS    FAILURE
---------------------------------------- ---------- ----------

DROP ANY TABLE                           BY ACCESS  BY ACCESS

ABC
DROP ANY TABLE                           BY ACCESS  BY ACCESS

ABC
CREATE ANY TABLE                         BY ACCESS  BY ACCESS


USER_NAME                      PROXY_NAME
------------------------------ ------------------------------
PRIVILEGE                                SUCCESS    FAILURE
---------------------------------------- ---------- ----------
AUDIT_TEST
CREATE SESSION                           BY ACCESS  BY ACCESS

AUDIT_TEST
AUDIT SYSTEM                             BY ACCESS  BY ACCESS

AUDIT_TEST
ALTER SYSTEM                             BY ACCESS  BY ACCESS


6 rows selected.

SQL> _
```

Figure 7: Privilege auditing

To use the AUDIT statement to set statement and privilege options, there must be AUDIT SYSTEM privilege.

4.2.5 Object Auditing

Object auditing allows the access or usage of specific objects to be audited. Unlike statement/privilege auditing which can be limited to audit only specific users, object auditing is active for all users, but it is limited to one object. The AUDIT ANY privilege is required to be able to set an object audit in general. However, the object owner can enable or disable auditing on owned objects, as well as see which audit options are currently enabled for the object.



```
SQL> desc dba_obj_audit_opts
 Name                                      Null?    Type
 ----------------------------------------- -------- ----------------------------

 OWNER                                              VARCHAR2(30)
 OBJECT_NAME                                        VARCHAR2(30)
 OBJECT_TYPE                                        VARCHAR2(17)
 ALT                                                VARCHAR2(9)
 AUD                                                VARCHAR2(9)
 COM                                                VARCHAR2(9)
 DEL                                                VARCHAR2(9)
 GRA                                                VARCHAR2(9)
 IND                                                VARCHAR2(9)
 INS                                                VARCHAR2(9)
 LOC                                                VARCHAR2(9)
 REN                                                VARCHAR2(9)
 SEL                                                VARCHAR2(9)
 UPD                                                VARCHAR2(9)
 REF                                                CHAR(3)
 EXE                                                VARCHAR2(9)
 CRE                                                VARCHAR2(9)
 REA                                                VARCHAR2(9)
 WRI                                                VARCHAR2(9)
 FBK                                                VARCHAR2(9)

SQL>
```

Figure 8: Object auditing

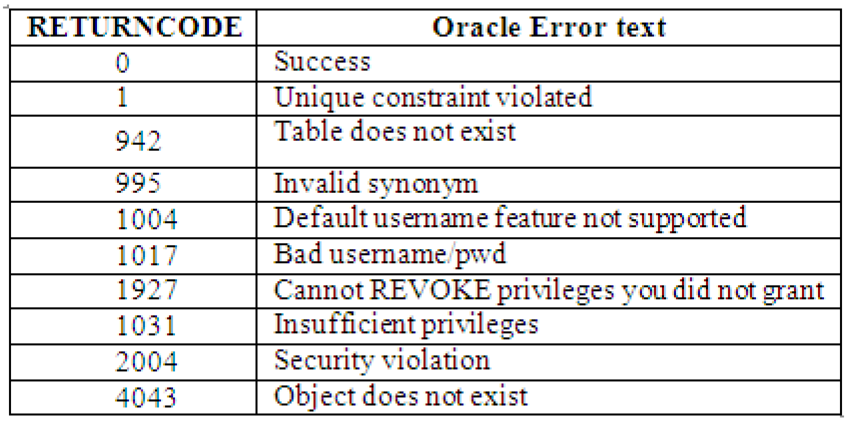
5. PROTECTING THE AUDIT TRAIL

It is important to protect the audit trail from modification. To audit changes made to the database audit trail (the AUD$ table), the following statement: AUDIT, INSERT, UPDATE, DELETE ON AUD$ BY ACCESS is used.
Audit records in the AUD$ table can only be deleted by a SYSDBA or an account with delete on AUD$. The SYSDBA account should be restricted to a highly trusted DBA and all other DBAs should be operating under least privilege. Write a package to automate the process of purging the audit trail so that the direct privilege is not needed by the auditors.

5.1 Audit return codes

The DBA_AUDIT_TRAIL table has a RETURNCODE column which indicates the results of the auditing action. The code is the Oracle error message (ORA-nnnn) that was audited. While a non-zero return code is the Oracle error code, it is not necessarily the error code returned to the user. In some cases, the user gets a generic error while a more specific one is written to the audit trail to avoid giving malicious users unauthorized information. The easiest way to look up the error code is to use the UNIX oerr facility (“oerrorannnn”). Here are some common codes.

Table 2: Audit Return Code



RETURNCODE	Oracle Error text
0	Success
1	Unique constraint violated
942	Table does not exist
995	Invalid synonym
1004	Default username feature not supported
1017	Bad username/pwd
1927	Cannot REVOKE privileges you did not grant
1031	Insufficient privileges
2004	Security violation
4043	Object does not exist

6. CONCLUSION

Thus,discussed the important role of auditing for detecting suspicious behaviour and providing evidences to forensic investigator to present in court of law. The different locations where audit records are stored is studied along with auditing types.Thus, auditing is an important tool for organizations for detecting threats to databases and thereby improving the performance effectively.

REFERENCES

[1] Huang, Liu,“A logging schema for Database Auditing”, IEEE conference publication, Computer Science and Engineering,2009, Huang, liu page 390-393.

[2] ElhamIskandarnia ,” Database Autopsy Close Look to Database Auditing for Oracle Database”,Global journal of Comp[uter science and technology,2013.

[3] Qiang, Liu, Lian-zong, “A Framework for database Auditing” IEEE conference publications, Forth conference on Computer Science and Convergence Information 2009, page 902, 910.

[4] Oracle White Paper—Oracle Database Auditing: Performance Guidelines.

[5] Oracle Database New Features Guide 10g Release 2 ASM.

[6] Auditing in Oracle10g Release 2.

[7] RamezElmasri&Shamkant B. Navathe, Fundamentals of Database Systems, Sixth Edition, Addison-Wesley, 2009.

[8] LI Yung, ACM publication, Proceedings of the 40th ACM technical symposium on Computer science education page 241-245, ISBN: 978-1-60558-183.

[9] Thomas Connolly & Carolyn Begg, Database Systems: A practical approach to Design, Implementation and Management, Fifth Edition, Addison Wesley, 2010.