Global Journal of Computer Science and Technology
Software & Data Engineering
Volume 13 Issue 6 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Database Autopsy Close Look to Database Auditing for Oracle Database

By Elham Iskandarnia
AMA International university, Bahrain

Abstract - Today, that business has different rules and regulation and supplied threats; organizations must go well beyond securing their data, and managing their database. Essentially, Data have to be perpetually monitored to be aware of who what, to all their data. Database auditing involves monitoring database to be aware of what user of proceedings. In this article we will offer a novel procedure for finding auditing records from different locations that DBMS keeps records, further more we will discuss which user, or system activity to keep records to do auditing efficiently and also avoid over use of system resources which will caused on slow transaction time.

GJCST-C Classification : H.2.m

Strictly as per the compliance and regulations of:

Database Autopsy Close Look to Database Auditing for Oracle Database

Elham Iskandarnia

Abstract - Today, that business has different rules and regulation and supplied threats; organizations must go well beyond securing their data, and managing their database. Essentially, Data have to be perpetually monitored to be aware of who what, to all their data. Database auditing involves monitoring database to be aware of what user of proceedings. In this article we will offer a novel procedure for finding auditing records from different locations that DBMS keeps records, further more we will discuss which user, or system activity to keep records to do auditing efficiently and also avoid over use of system resources which will caused on slow transaction time.

The Problem and Its Background

I. Introduction

Today, that business has different rules and regulation and supplied threats, organizations must go well Beyond securing their data, and managing their database. Essentially, Data have to be perpetually monitored to be aware of who what, to all their data. Database auditing involves monitoring database to be aware of what user of proceedings. Database consultant and DBA often set up auditing policy for security purposes, for example, to ensure that everybody get access to what it has permission . This study looks at auditing as a concept, what are threats and how to diagnose that threat when they are happening.

One of challenge regarding auditing that Organizations today are facing is data security, they have to recognize threats and threat them in a more cost effective way. There are some policies which are force by platform the DBA must understand the cost of this policy of database performance and base of need modify or unable these predefine policies as well as create new policies base of their needs.

By understanding the audit concept companies can decrease the increasing cost of database security.

a) Back Ground of Study

Database security is a very broad area that addresses many issues like legal and ethical, policy issues at governmental, or corporate and system-related issues such as system level.

Threats to database results in the loss or degradation of some or all of following commonly accepted security Goals: integrity, availability, and confidentiality.

Grate amount of different errors can leak into organizational databases; these errors may range from data entry errors to violations of accounting standards. It seems that although database systems have radically changed the file system in terms speed and competence, detecting errors and keeping quality did not cope with speed of events.

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

- Access control
- Authentication
- Authorization
- Auditing

Database auditing is directly related to database security. Auditing is one aspect of database security. In practice, if there is need to secure a particular database system, then auditing is essential. Auditing mechanism implemented on a database system facilitates the security implemented in a system.

Three different strategies for database auditing are introduced and compare in term of efficiently (Data Base Auditing, Levant V. Orman, and Cornell University).

In this paper we will discuss Data base Autopsy, that is when a threat happened you use tools to find out what was type of threat, who attack your data base, when that happened. And from this information you can review and change your Authentication, authorization policies.

Regulatory compliance requirements can be met for your data base by carrying out auditing which enforces internal controls, so that unwanted changes can be prevented.

b) Statement of Problem

i. *General Objective*

The outcomes of database auditing can be used by administrator to watch the activities of Information System Users (ISU). System user can be aware of database and its capabilities (sophistic user) or they can be completely unaware of facilities offered by database (naïve user) .The information that they can access is defined as constrained by the explicit privileges which is defined by the Database

Author : AMA International university-Kingdom of Bahrain School Year 2012-2013. E-mail : mashdyelham@yahoo.com

Management System (DBMS), or any other tier in multi tier architecture like Application Servers (AS) or in any another tier. However if a naughty user (inside organization) or a malicious user (from outside) attempts to access a piece of information for whom he has no privileges, an audit trial must be made. And his activity must be trace and record.

ii. *Specific Objective*

1. What are different types of threats in Database Management system?
2. What is the importance of database auditing?
3. What in formations must be kept in database auditing report?
4. What are locations you can find auditing records?
5. What are the effects of big auditing file on system performance?

c) The Scope and Delimitation

The Information system which are manipulating and storing financial, accounting, or other legally sensitive data can use this study. Legal vulnerabilities can be created by even basic trading operation, in today increasingly litigious world. For example.

The investor who lose large amount in trading may hope to recover his capital, and/or the investor's employee may seek to escape responsibility, by legal action against the broker. If related trade data has been modified by the broker without an acceptable Autopsy, which can be seen as *apparent* indicator from the investor's opposing results which are due to the misconduct of the broker.

Auditing, which means capturing and storing information about what is happening in the system, increase the amount of work the system must do. Auditing must be focused so that only events that are of interest are captured .Well designed auditing policies has minimal impact on system performance .Improperly focused auditing can significantly affect performance.

The scope and depth of the audit should be designed to meet the specific objective of organizations base of its environments and type of threats it is facing.

The coverage of this study is the Oracle database 11g, without SAM, which data renovation period is specified by DBA However, we will discuss FGA auditing in this paper, but will not consider RAID system.

The researcher is limited this research to user of relational database.

d) Importance & Significance of Study

Database auditing and database security are directly related to each other. One aspect of database security is auditing. Auditing is essential tasks for DBA of database management system which need to secure a particular database system, then. Auditing mechanism which is deploying on a database system facilitates the security implemented in a system.

Auditing, which means capturing and storing information about what is happening in the system, increase the amount of work the system must do.

Auditing must be focused so that only events that are of interest are captured .Properly focused auditing has minimal impact on system performance .Improperly focused auditing can significantly affect performance.

The security administration will use guides provided by Database auditing to develop and enforce a well defined set of security policies based on the initial set of business rules. At the beginning of the specific information system project' the DBA will decide the business rules and later on, modify it with the passage of time, based on the behavior of users.

A wide range of events that can be tracked and collected in Auditing of database records. This creates an additional processing and disk I/O load on database server machine and hence degrades its performance. In other word auditing, which means capturing and storing information about what is happening in the system, increase the amount of work the system must do. Auditing must be focused so that only events that are of interest are captured Properly focused auditing has minimal impact on system performance .but with gathering extra and not needed auditing record you will scarified the performance of database.

So we divide the auditing to

- *Mandatory Auditing:* All oracle database audit certain action regardless of other audit option or parameter .The reason for mandatory audit logs is that the database needs to record some database activities, such as connection by privileged users.
- *Standard Database Auditing:* Enabled at the system level by using the audit trail initialization parameter. After you enabled auditing select the object and privileges that you want to audit and set auditing properties with audit command.
- *Value base Auditing:* Extends standards database auditing, capturing not only the audited event that occurred but also the actual values that were inserted, updated or deleted, Values base auditing is implemented through database trigger.
- *Fine-Grained:* Auditing(FGA) Extends standard database auditing, capturing the actual SQL statement that was issued rather than only the fact that the event occurred.
- *SYSDBA Auditing:* separates the auditing duties between the DBA and an auditor or security administrator who monitors the DBA activates in an operating system audit trail.

So, it is not recommended to keep the excessive auditing of so as to avoid demeaning of performance of the database server. For example, in case of auditing DML commands, it is recommended to

keep insert, update and delete statements are recorded in audit logs, not all retrieval statements.

Following statics may show the important of security and auditing in data base (Neon Enterprise Software).

- Percentage of companies suffers from increasing of security budget? 54%
- Number of companies that claim their job will get more strategic in 2013? 69%
- Number of companies that claim their job will get more compliance? 75%
- Number of companies claim that their top priority will be related to network/security integration? 52%
- How many companies will be more interested to buy best security they can with their budject? 80%
- Sensitive data is losing important data? 68%

This study can be used by

i. All organization using database, especially oracle database.
ii. Researchers, who are interested about DBMS and its features.
iii. Database Professionals: Data base administrators, database sysmans who are responsible for database recoveries.
iv. Teachers and students how are working with database in different aspect.

II. Related Studies

A database is considered as a core asset of an organization. Numerous approaches dealing with Data base Auditing Interface for operating systems and networks have been developed .Nevertheless, they are not sufficient for protecting databases. Still there are many discussions about the abstract and high-level architecture of a DBMS including an ID component.

However, this work mainly focuses on debating generic solutions rather than proposing solid algorithmic solutions. There are many researches about auditing in work done by LIU the authors compare strategies adapted by selected set of vendor for auditing database.

In study done by Cornell University the author introduce three major strategies of database auditing to maintain integrity [1]. Then these strategies are compared in term of efficiency and effectiveness in eliminating error, to do so they compute the optimum timing under each strategy.

In studies submitted to IEEE conference they demonstrate a way in which deductive database cart be used to address elusive problems in the establishment and maintenance of a database audit trail. However, they discus situation and examples of issues that arise in many application computing environments. The means deductive approach can be applied to more than database issues. The main features of the relational model, is extended to more wider concerns of application development in Deductive computing which is an example of an emerging paradigm[2].

In study published in ACM proposed an approach for detecting different type of anomalies and anomalous access patterns in DBMS. They have developed three models, of different granularity, to represent the SQL queries appearing in the database log files. We will use their work to find out what information must be extract from log file to show access patterns of the queries[8].

a) Conceptual Frame Work

We fist will discuss the tolls you can use for auditing, then we will look inside the system and search for different location database stores auditing records, then we will consider what is actions that DBMS produces and audit records about it and how we can add actions to keep data about according to our needs and requirements.

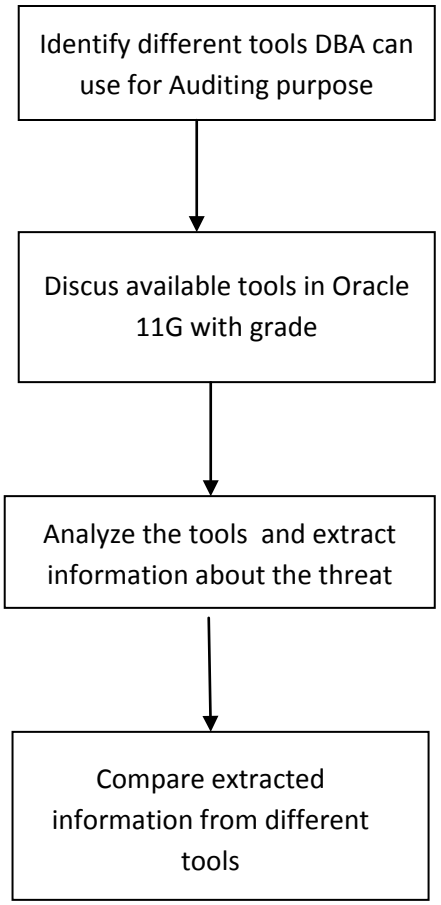


Figure 1 : Conceptual Framework

Research Methodology

III. Specific Research Purpose and Research Questions

The purpose of this study is to help database Administration to identify threats and configure the database to response by predefine procedure to that treads, also it will help oracle DBA to identify the harm the tread will make to system performance or security of data.

The study will address following questions on specific:

- What are the kinds of threats that can affect database performance?
- What are different threats that will attack database security?
- Which location database will store data's about threats?
- How to setup database management system to do predefine actions against each threat?
- What are important information regarding threats. How to extract information from system log?
- Which statement can create audit log?
- How can you add or edit default commends that make audit logs?

a) Research Methodology

Meta Analysis Research methodology is adopted in accomplishing my research goal. The research intends to study the commonly used auditing method and its drawbacks, also the additional factor which solves the problems in widely used methodology. The research analyzed various auditing records and suggested an efficient procedure to abstract information more effectively and efficiently from recourses. Future more, a novel model that avoids extra lose of system resources is proposed.

b) Research Design

i. *Source of Data*

Database audit records for statement, privilege, and object auditing are stored in the table SYS.AUD$. Depending on how extensive you're auditing and retention policies are, you will need to periodically delete old audit records from this table. The database does not provide an interface to assist in deleting rows from the audit table, so you will need to do so yourself.

So we will take a close look at SYS. Audis table and also very important parameter which is audit _trail.

We will look at four level of auditing which oracle 11 G do auditing.

- Statement
- Privilege
- Object
- Fine-grained access

c) Research Plan

A database Administrator knows that when a threat is happened the first priority is backing up and restores the system, but it is also very important to find what the reason for system failure was. To answer this question ,priors to any failure ,you have to analyze your system as database Administrator and decide what are the possible threat for your system, and active or inactive default auditing records ,or modify and extra information to your audit tables.

All DBA know that finding the proper records for your query are one of skills that they will gain it by time and trying, so in this article we will help database administrator to find required information about threat effectively and sufficiently.

Also we will talk about how and when you will purge your unwanted information from Audit table and export them for future used.

Results and Discussions

IV. Location of Audit Records

Oracle 11 record audit records in two locations

- Database
- Operating-system Files

Oracle decided where to keep record by investigating value of initialization parameter **audit trail**. The default is DB, as in AUDIT_TRAIL=DB, you can change this value to DB, EXTENDED to record audit records in the database together with bind variables (SQLBIND) and the SQL.

Statement triggering the audit entry (SQLTEXT). AUDIT_TRAIL=OS tells the database to record audit records in operating-system files.

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

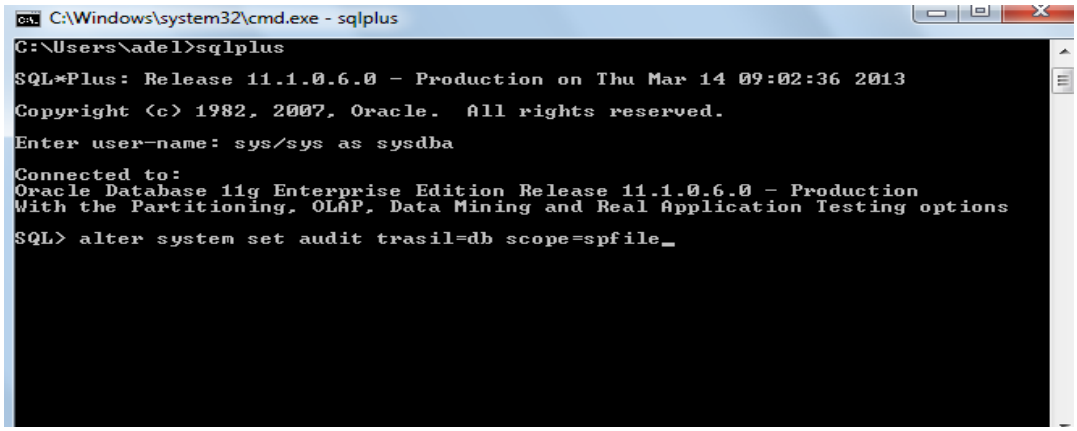


Figure 2 : Set Audit Scope

The audit_ trail parameter can also have values XML and XML, EXTENDED. With these two options, audit records are written to OS files in XML format. The value of NONE disables auditing.

Keep in mind that you should bounce your database instance for change to take effect. When recorded in the database, most audit entries are recorded in the SYS AUD $ table. On UNIX systems, operating-system audit records are written into files in the directory specified by the initialization parameter audit_ file_ dest (which is set to $ORACLE_BASE/ admin/$ORACLE_SID/a dump if the database is created using DBCA). On Windows systems.

These audit records are written to the **Event** Viewer log file. So we can find the locations for gathering information as describe in following chart.

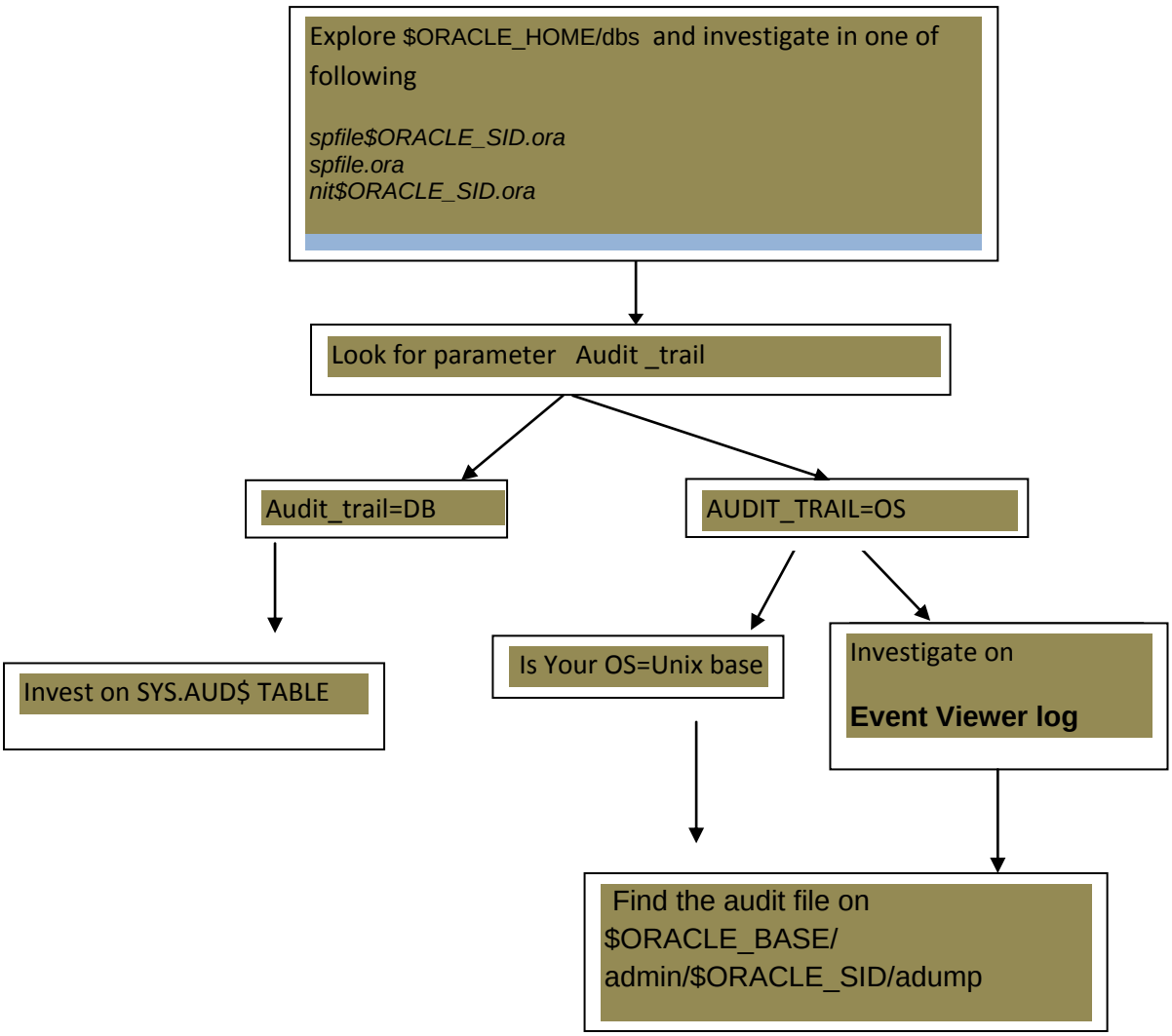


Figure 3 : Procedure for finding audit information

What to audit?

Auditing involves monitoring and recording specific database activity. An Oracle 11*g* database supports four levels of auditing:

- Statement
- Privilege
- Object
- Fine-grained access

We discuss managing each one of this level in following sections.

a) Management Statement Auditing

Statement auditing involves monitoring and recording the execution of specific types of SQL statements. Executions of some statements are enabling by default, but you can modify this list by adding or deleting some statements to this list as explain in code.

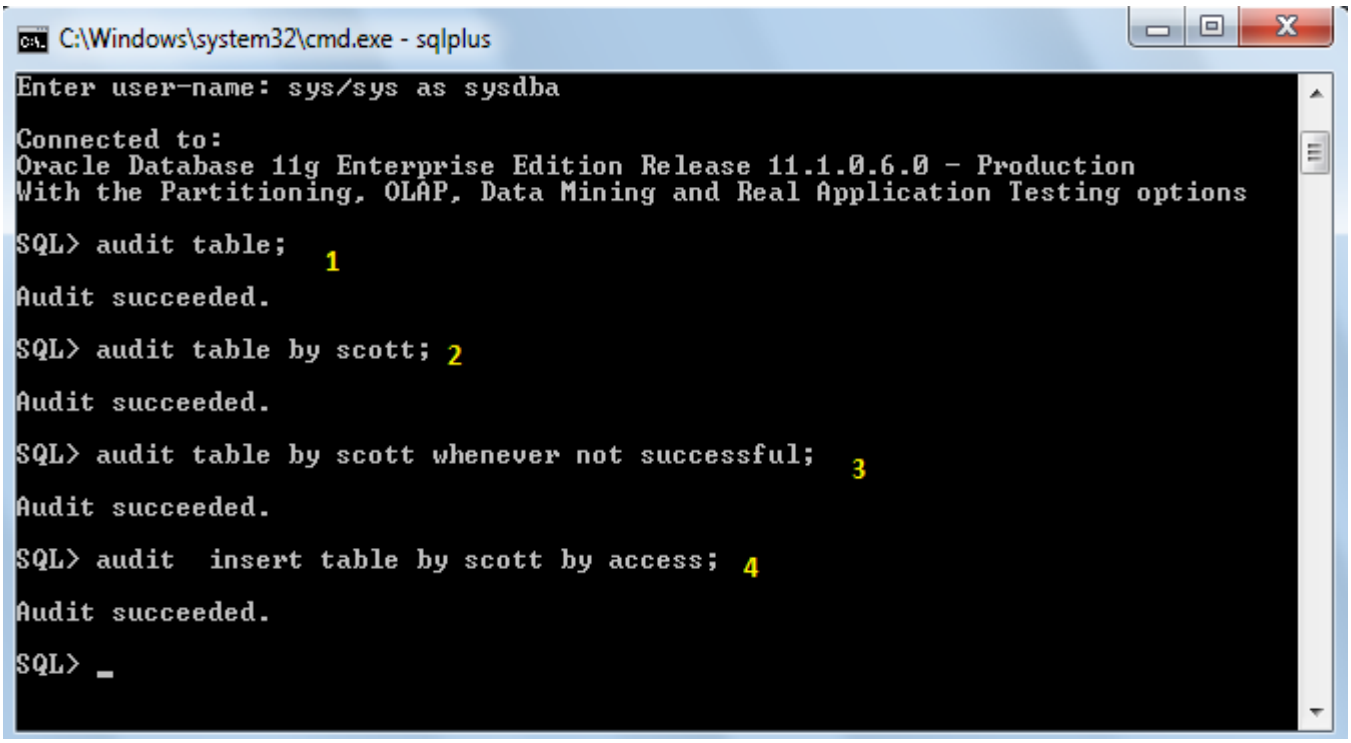


Figure 4 : Modify Audit Record

1. Audit the SQL statements CREATE TABLE, DROP TABLE, and TRUNCATE TABLE, use the TABLE audit option like this. You can add attribute for this command .The attributes are by user, whenever successful by session, whenever not successful and…
2. To record audit entries for specific users only, include a BY USER clause in the AUDIT statement. For example, to audit CREATE, DROP, and TRUNCATE TABLE statements for user scott only …
3. Frequently, you want to record only attempts that fail—perhaps to look for users who are probing the system to see what they can get away with. To further limit auditing to only these unsuccessful executions, use a WHENEVER clause.
4. You can alternately specify WHENEVER SUCCESSFUL to record only successful statements. If you do not include a WHENEVER clause, both successful and unsuccessful statements trigger audit records. You can further configure non-DDL statement to record one audit entry for the triggering session or one entry for each auditable action during the session. Specify BY ACCESS or BY SESSION in the AUDIT statement.

There are many auditing options other than TABLE or INSERT TABLE. Table bellow shows all the statement-auditing options.

Statement-Auditing Option	Triggering SQL Statements
ALTER SEQUENCE	ALTER SEQUENCE
ALTER TABLE	ALTER TABLE
COMMENT TABLE	COMMENT ON TABLE COMMENT ON COLUMN
DATABASE LINK	CREATE DATABASE LINK DROP DATABASE LINK
DELETE TABLE	DELETE
EXECUTE PROCEDURE	Execution of any procedure or function or access to any cur-sor or variable in a package
GRANT PROCEDURE	GRANT on a function, package, or procedure
GRANT SEQUENCE	GRANT on a sequence
GRANT TABLE	GRANT on a table or view
INDEX	CREATEINDEX
INSERT TABLE	INSERT into table or view
LOCK TABLE	LOCK
NOT EXISTS	All SQL statements
PROCEDURE	CREATE FUNCTION DROP FUNCTION CREATE PACKAGE CREATE PACKAGE BODY DROP PACKAGE CREATE PROCEDURE DROP PROCEDURE
PROFILE	CREATE PROFILE ALTER PROFILE DROP PROFILE
ROLE	CREATE ROLE ALTER ROLE DROP ROLE SET ROLE
SELECT SEQUENCE	SELECT on a sequence
SELECT TABLE	SELECT from table or view
SEQUENCE	CREATE SEQUENCE DROP SEQUENCE
SESSION	LOGON
SYNONYM	CREATE SYNONYM DROP SYNONYM
SYSTEM AUDIT	AUDIT NOAUDIT
SYSTEM GRANT	GRANT REVOKE
TABLE	CREATE TABLE DROP TABLE TRUNCATE TABLE
TABLESPACE	CREATE TABLESPACE ALTER TABLESPACE DROP TABLESPACE
TRIGGER	CREATE TRIGGER ALTER TRIGGER (to enable or disable) ALTER TABLE (to enable all or disable all)
UPDATE TABLE	UPDATE on a table or view
USER	CREATE USER ALTER USER DROP USER
VIEW	CREATE VIEW DROP VIEW

Table 4.1 : Auditing Option

All needed information about STAEMENT auditing will exist in the DBA_STMT_AUDIT_OPTS data dictionary view. You can query this view to find needed informations, the recorded in formations are

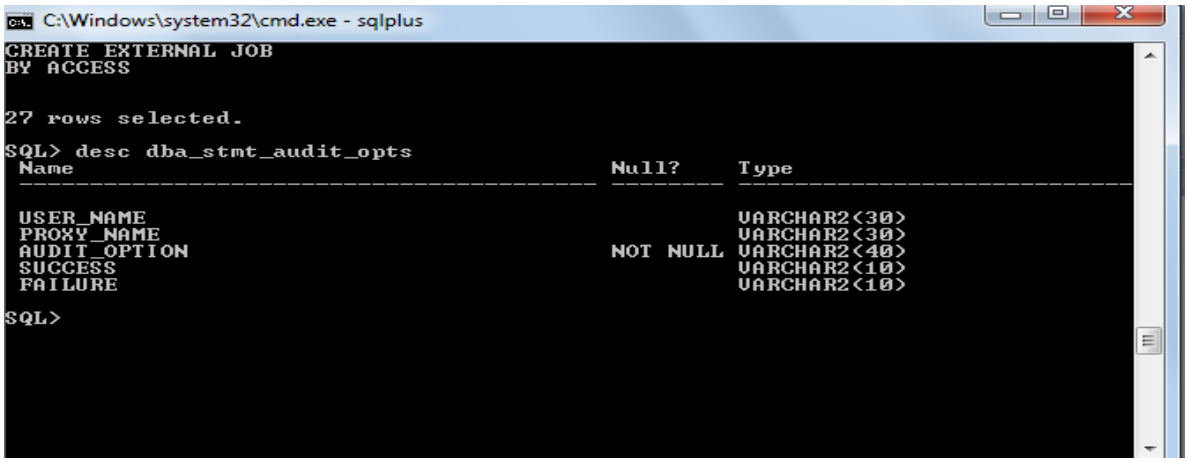


Figure 5 : Structure of Table

You can enable administrator auditing by setting the initialization parameter AUDIT_ SYS_ OPERATIONS=TRUE All the activities performed connected as SYS or SYSDBA/SYSOPER privileges are recorded in the OS audit trail.

If you enable AUDIT SESSION, the database creates one audit record when a user logs on and updates that record when the user logs off successfully.

These session audit records contain some valuable information that can help you narrow the focus of your tuning efforts. Among the information recorded in the audit records are the username, logon time, logoff time, and the number of physical reads and logical reads performed during the session. By looking for sessions with high counts of logical or physical reads, you can identify high-resource-consuming jobs and narrow the focus of your tuning efforts.

The following are statements will create records by default-

ALTER ANY PROCEDURE	CREATE ANY TABLE	DROP USER
ALTER ANY TABLE	CREATE EXTERNAL JOB	EXEMPT ACCESS POLICY
ALTER DATABASE	CREATE PUBLIC DATABASE LINK	GRANT ANY OBJECT PRIVILEGE
ALTER PROFILE	CREATE SESSION	GRANT ANY PRIVILEGE
ALTER SYSTEM	CREATE USER	GRANT ANY ROLE
ALTER USER	DROP ANY PROCEDURE	ROLE
CREATE ANY LIBRARY	DROP ANY TABLE	SYSTEM AUDIT
CREATE ANY PROCEDURE	DROP PROFILE	

You can restricts and limit this by using command “no audit” in order to not decrease your operation time and also avoid overwrite of audit file which cause lose important information so you need .

b) Examining the Audit Trail

Statement, privilege, and object audit records are written to the SYS.AUD$ table and made available via the data dictionary views DBA_AUDIT_TRAIL (displays all standard audit trail entries) and USER_AUDIT_TRAIL (the standard audit trail entries related to the current user. For example, you can view the user, time, and type of statement audited for user Scott by executing the following:

```
SELECT username, timestamp, action name
FROM dba_audit_trail
WHERE username =scott;
```

ORA USER	TIMESTAMP	ACTION_NAME
SCOTT	6/15/2004 18:43	LOGON
SCOTT	6/15/2004 18:44	LOGOFF
SCOTT	6/15/2004 18:46	LOGON
SCOTT	6/15/2004 18:46	CREATE TABLE

Table 4.2

c) Managing of Privilege Auditing

Privilege auditing involves monitoring and recording the execution of SQL statements that require a specific system privilege, such as SELECT ANY TABLE or GRANT ANY PRIVILEGE. You can audit any system privilege. As we discussed before the command that you will use is AUDIT statement, specifying the system

privilege that you want to monitor, or user, or even include DML privilege.

If you want to make report of which privilege is recording in audit records you will query DBA_PRIV_AUDIT_OPTS data dictionary views.

To disable auditing of a system privilege, use a NOAUDIT statement. The NO AUDIT statement.

Allows the same BY options as the AUDIT statement.

d) Managing of Objects Auditing

Object auditing involves monitoring and recording the execution of SQL statements that require a specific object privilege, such as SELECT, INSERT, UPDATE, DELETE, or EXECUTE. Unlike either statement or system privilege auditing, schema object auditing cannot be restrict to specific users, it is enabled for all users or no users.

You enable object auditing with an AUDIT statement, specifying both the object and object privilege that you want to monitor. For example, to audit SELECT statements on the HR.EMPLOYEES TABLE, execute the following:

AUDIT select ON hr. employee:

You can further configure these audit records to record one audit entry for the triggering session or one for each auditable action during the session by specifying BY ACCESS or BY SESSION in the AUDIT statement. This access/session configuration can be defined differently for successful or unsuccessful executions.

The object-auditing options that are enabled in the database are recorded in the DBA_OBJ_AUDIT_OPTS data dictionary view. Unlike the statement and privilege _AUDIT_OPTS views,

The DBA_OBJ_AUDIT_OPTS data dictionary view always has one row for each auditable object in the database. There are columns for each object privilege that auditing can be enabled on, and in each of these columns, a code is reported that shows the auditing options let's see following codes.

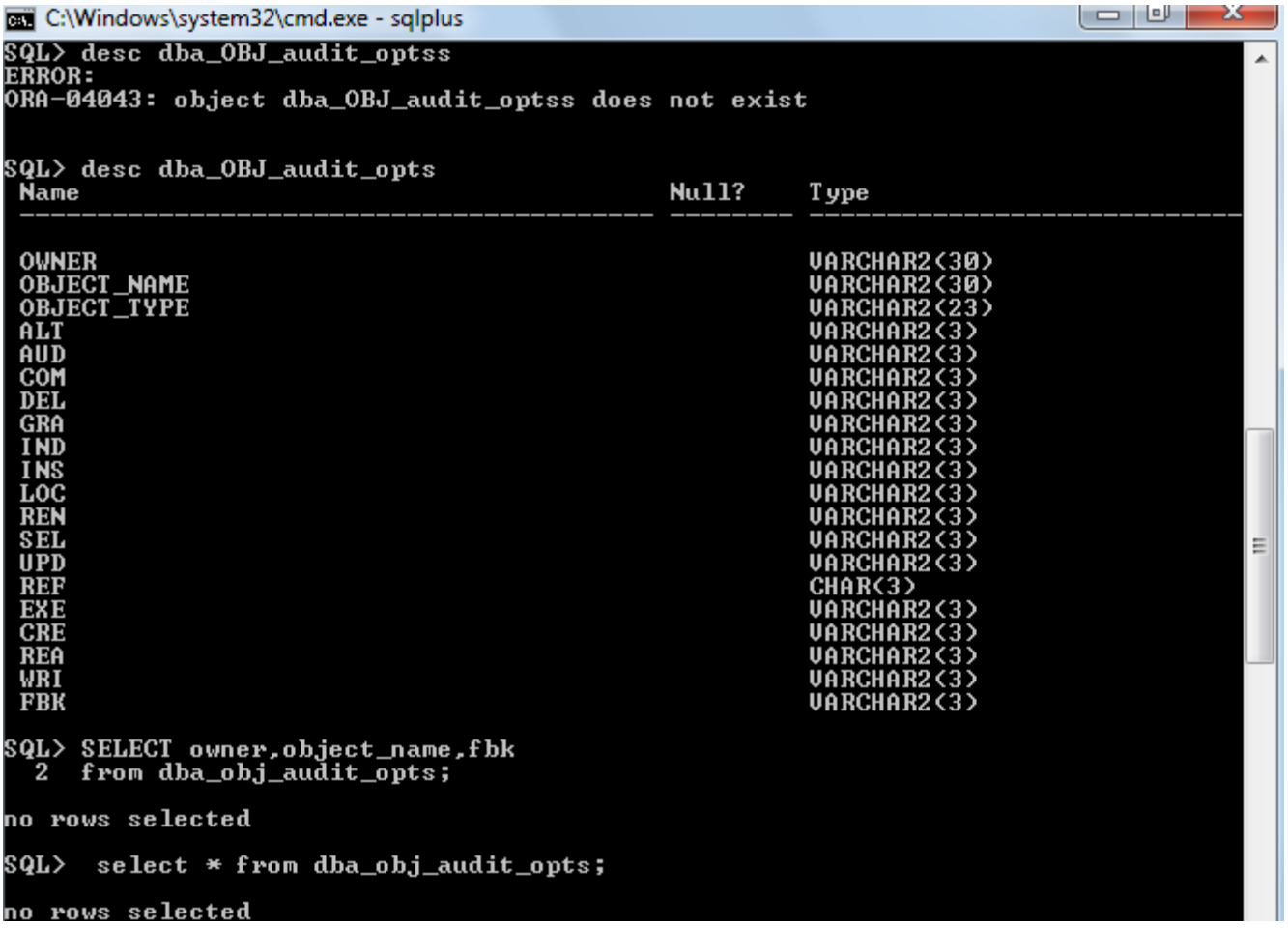
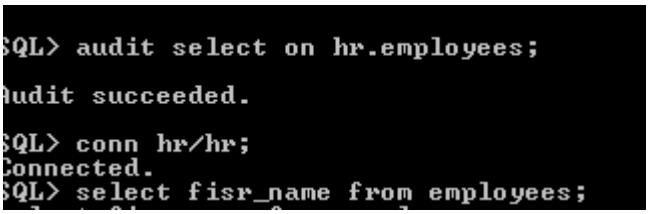


Figure 6 : Empty View

As you can see the view is empty because the audit is not activate ,so we will activate object auditing for employees table of hr schema. And try to access the table.

Figure 7 : Enabling Auditing



No we will look at view again

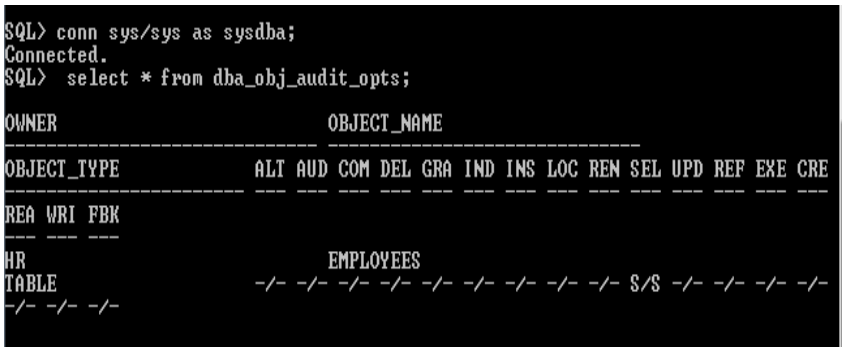


Figure 8 : View with audit record

To disable object auditing, use a NOAUDIT statement, which allows the same WHENEVER options as the AUDIT statement.

e) Purging the Audit Trail

Database audit records for statement, privilege, and object auditing are stored in the table SYS.AUD$. Depending on how extensive your auditing and retention policies are, you will need to periodically delete old audit records from this table. The database does not provide. An interface to assist in deleting rows from the audit table, so you will need to do so yourself.

To purge audit records older than 90 days, execute the following as user SYS:

DELETE FROM sys.aud$ WHERE timestamp# < SYSDATE -90>;

You might want to copy the audit records into a different table for historical retention or export them to an operating-system file before removing them. It is a good practice to audit changes to the AUD$ table so that you can identify when changes were made.

f) Using of DBCA to create base line for Auditing

The Oracle Database Configuration Assistant (DBCA) is a Java-based tool used to create Oracle Databases the DBCA provides a flexible and robust environment in which you not only can create databases but also can generate templates containing the definitions of the databases created. This provides you with the ease of using a GUI-based interface with the flexibility of Oracle-generated XML-based templates that you can use to maintain a library of database definitions.

g) Look at FGA Auditing

Oracle auditing can be divided into two basic categories: standard auditing and FGA. Standard auditing provides the ability to audit based on user, privileges, schemas objects, and statements. For example, it can be based on a specific type of SQL statement (create, alter, update, delete…). FGA provides the ability to audit access to specific application table columns conditionally based on factors such as IP address or the program name used to connect to the database.

Starting with Oracle Database 11g, the Oracle Database Configuration Assistant (DBCA) can automatically configure Oracle recommended minimum audit settings for compliance and internal controls. These audit settings are associated with important security relevant SQL statements and privileges and are listed in the Oracle security documentation. After creating a database with DBCA, the database will audit the following privileges and SQL statements by default:

ALTER ANY PROCEDURE
CREATE ANY TABLE
GRANT ANY OBJECT PRIVILEGE
ALTER ANY TABLE
CREATE EXTERNAL JOB GRANT ANY PRIVILEGE
ALTER DATABASE
CREATE PUBLIC DATABASE LINK
LINK
GRANT ANY ROLE
ALTER PROFILE CREATE SESSION PROFILE
ALTER SYSTEM CREATE USER
PUBLIC SYNONYM
ALTER USER DATABASE LINK
ROLE
AUDIT SYSTEM DROP ANY PROCEDURE SYSTEM AUDIT
CREATE ANY JOB DROP ANY TABLE SYSTEM GRANT
CREATE ANY LIBRARY
DROP PROFILE
CREATE ANY PROCEDURE
DROP USER

h) Managing Fine-Grained Auditing

Fine-grained auditing (FGA) lets you monitor and record data access based on the content of the data. With FGA, you define an audit policy on a table and optionally a column.

When the specified condition evaluates to TRUE, an audit record is created, and an optional event-handler program is called. You use the PL/SQL package DBMS_FGA to configure and manage FGA. The implement of this type of auditing need creating package in Pl/sql which is out of scope of this article.

Conclusions and Recommendations

V. Conclusions

In this study we discussed the important role of auditing not only for detecting mistrustful behavior also providing proof and reasons to auditors, and also it is recommended to use. Oracle database auditing because of it minimal impact for high audit trail load.

We also discussed different methodology in audits which include trigger or Transactional log but you cannot use these methods for some events which go beyond server events.

VI. Recommendations

1. Use oracle database auditing even if you have large amount of audit trail load.
2. Write audit record to Operating system.
3. Set enough size for OS audit file.
4. Set auditing as part of your defense architecture as follow:
   i. Set full audit trail of logon and logoff, and record all failed login attempts, as first category
   ii. Audit Data Control Language (DCL) of the database. For second category.
   iii. The third category is to audit Data Definition Language (DDL) which changes database schema.

References Références Referencias

1. Huang, Liu, "A logging schema for Database Auditing", IEEE conference publication, Computer Science and Engineering, 2009, Huang, liu page 390-393.
2. Qiang, Liu, Lian-zong, "A Framework for database Auditing" IEEE conference publications, Forth conference on Computer Science and Convergence Information 2009, page 902, 910.
3. Oracle White Paper—Oracle Database Auditing: Performance Guidelines.
4. Oracle Database New Features Guide 11g Release 1 (11.1) B28279-02.
5. Oracle Database 11g New Features for DBAs and Developers, by Sam R. Alapati and Charles Kim, Apress, ISBN: 978-1-59059-910.
6. 6. Ramez Elmasri & Shamkant B. Navathe, Fundamentals of Database Systems, Sixth Edition, Addison-Wesley, 2009.
7. LI Yung, ACM publication, Proceedings of the 40th ACM technical symposium on Computer science education page 241-245, ISBN: 978-1-60558-183.
8. Thomas Connolly & Carolyn Begg, Database Systems: A practical approach to Design, Implementation and Management, Fifth Edition, Addison Wesley, 2010.
9. Oracle Database 11g The Complete Reference (Osborne ORACLE Press Series), Kevin Loney, Publisher: McGraw-Hill Osborne Media; 1 edition (December 17, 2010).