International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 1, December 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Enable Auditing in Oracle database

Amrish Srivastava

United States

How to cite this paper: Amrish Srivastava "Enable Auditing in Oracle database" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-1, December 2019, pp.1214-1215, URL: www.ijtsrd.com/papers/ijtsrd29881.pdf

IJTSRD29881

INRODUCTION

Auditing is the observing and recording of selected user database activities. It can be recorded individual actions, like type of SQL statement executed, action performed in database and can also observe any factors that can include user, application, and time. Based on the company security policies trigger auditing in an Oracle database are accessed.

Configure the auditing on oracle database:

1. Set AUDIT_TRAIL parameter.

AUDIT_TRAIL can be set to one of the following values:

- DB/TRUE: In this auditing mode, audited records will be written to the database audit trail(the SYS.AUD$ table).
- OS: In this auditing mode, audit data is written to text files into the directory specified by the AUDIT_FILE_DEST parameter.
- DB,EXTENDED(DB_EXTENDED): In this auditing mode, auditing as DB/TRUE does. Moreover it generates the SQLTEXT and SQLBIND CLOB columns of the SYS.AUD$ table.
- XML: In this auditing mode, the audit data will be written to XML files in stated directory by the AUDIT_FILE_DEST parameter.
- XML,EXTENDED(XML_EXTENDED): : In this auditing mode.it generates the SQLBIND and SQLTEXT columns.

2. Restart the database instance by below method.

SQL> ALTER SYSTEM SET AUDIT_TRAIL = DB SCOPE=SPFILE;
SQL> SHUTDOWN IMMEDIATE;
SQL> STARTUP

3. Verify name of the audit files

Assume that AUDIT_FILE_DEST is set to $ORACLE_HOME/rdbms/audit. This is how the audit files will look:
$ ls -l $ORACLE_HOME/rdbms/audit
-rw-r----- 1 oracle DBA 777 Oep 20 11:04 g1 p11204 _ora_ 18672_1.aud

$ view g1p11204_ora_18672_1.aud

Audit file /oracle/xxx/xx/g1p11204_ora_18672_1.aud

Oracle Database 11g Enterprise Edition Release 11.2.0.2.0 - 64bit Production

With the Partitioning, OLAP, Data Mining and Oracle Database Vault options

ORACLE_HOME = /oracle/xxx/product/11202
System name: Linux
Node name: XXXXX.
Release: 2.6.18-238.12.1.0.1.el5
Version: #1 SMP Sun Nov 10 14:51:07 EDT 2019
Machine: x86_64
Instance name: XXXX
Redo thread mounted by this instance: 1
Oracle process number: 32
Unix process pid: 14072, image:XXX.(TNS V1-V3)
Fri Nov 08 12:57:43 2019 +03:00
LENGTH : '158'
ACTION :[12] 'CONNECT'
DATABASE USER:[1] '/'
PRIVILEGE :[4] 'SYSDBA'
CLIENT USER:[8] 'oracle'
CLIENT TERMINAL:[5] 'pts/4'
STATUS:[1] '0'
DBID:[9] '55654345'

4. View Audit Trail

The audit trail is stored in the SYS.AUD$ table. Its contents can be viewed directly or via the following views.

DBA_AUDIT_EXISTS
DBA_AUDIT_OBJECT
DBA_AUDIT_SESSION
DBA_AUDIT_STATEMENT
DBA_AUDIT_TRAIL
DBA_OBJ_AUDIT_OPTS
DBA_PRIV_AUDIT_OPTS
DBA_STMT_AUDIT_OPTS

The audit trail contains a lot of data, but the following are most likely to be of interest.

USERNAME: Oracle Username.
TERMINAL: Machine that the user performed the action from.

TIMESTAMP: When the action occured.
OBJECT_OWNER: The owner of the object that was interacted with.
OBJECT_NAME: The name of the object that was interacted with.
ACTION_NAME: The action that occured against the object. (INSERT, UPDATE, DELETE, SELECT, EXECUTE)

Conclusion

Now a days applications have become classier and database auditing plays an important part not only in helping notice doubtful behavior but providing proof of controls to auditors.

It has minimal impact on performance of database even for very high audit trail loads. Auditing inside the database, should be part of your defense-in-depth architecture.