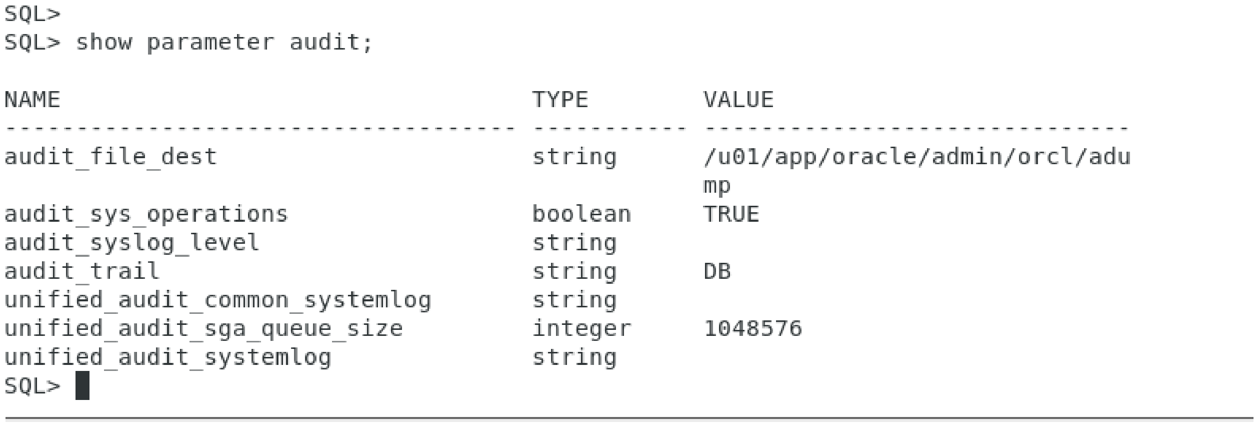
Secure and Monitor Your Database with Oracle Auditing

Oracle database auditing allows you to monitor certain database actions happening inside the database. Auditing also helps in tracking actions performed against a particular table, schema, or specific rows.

Step 1: Check if Database Auditing is Enabled

You can check the database auditing status using the SHOW PARAMETER command:

show parameter audit;



```
SQL>
SQL> show parameter audit;

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
audit_file_dest                      string      /u01/app/oracle/admin/orcl/adu
                                                 mp
audit_sys_operations                 boolean     TRUE
audit_syslog_level                   string
audit_trail                          string      DB
unified_audit_common_systemlog       string
unified_audit_sga_queue_size         integer     1048576
unified_audit_systemlog              string
SQL> █
```

Step 2: Understand the AUDIT_TRAIL Parameter

The AUDIT_TRAIL parameter defines the database auditing status. It can take any of the following values:

none: Database auditing is disabled.

os: Auditing is enabled, and audit logs are stored at the OS level, not inside the database.

db: Auditing is enabled, and audit records are stored inside the database (in the SYS.AUD$ table).

db,extended: Same as db but also populates SQL_BIND and SQL_TEXT columns.

xml: Auditing is enabled, and audit records are stored at the OS level in XML format.

xml,extended: Same as xml but also populates SQL_BIND and SQL_TEXT columns.

Default Behavior:

If the database is created via DBCA, the default value is DB.

Otherwise, the default is NONE.

Step 3: AUDIT_FILE_DEST Parameter

The AUDIT_FILE_DEST parameter defines the OS-level location of the audit trail files. By default, it is set to the adump directory.

Step 4: AUDIT_SYS_OPERATIONS Parameter

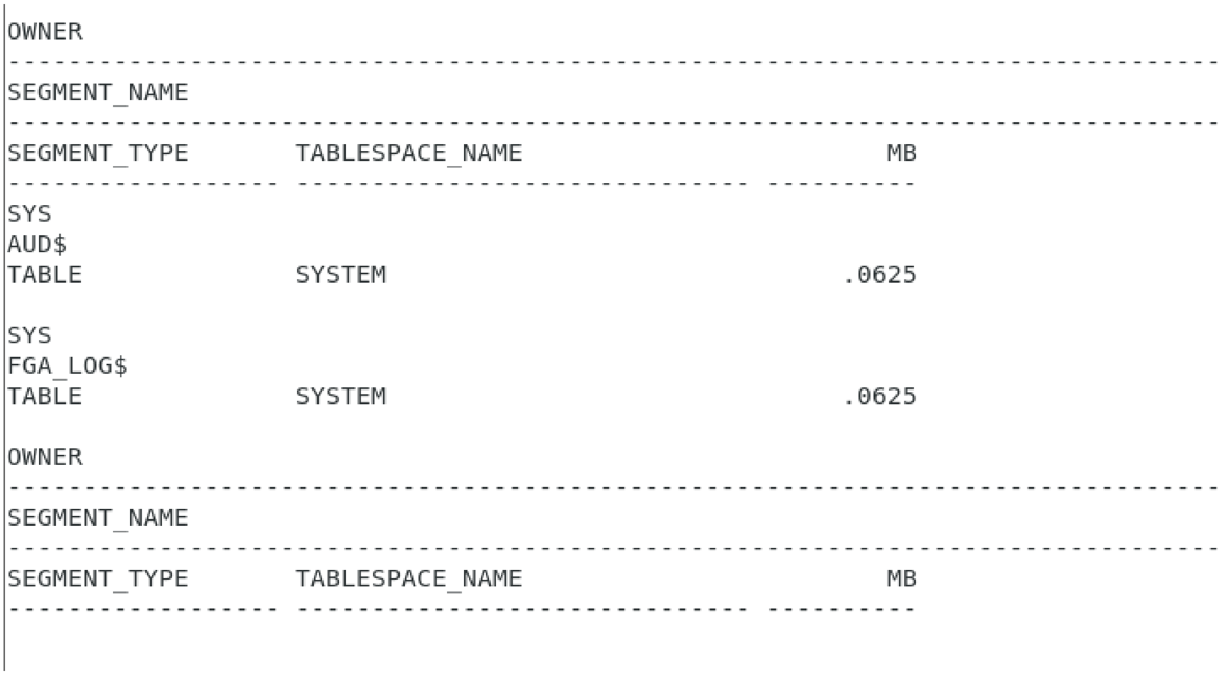
The AUDIT_SYS_OPERATIONS parameter determines whether auditing is enabled for any user connecting to the database as SYSDBA.

This is enabled by default. All SYS operations audit records are stored at the OS level in the AUDIT_FILE_DEST location.

Step 5: Move AUD$ Table to Another Tablespace

By default, the SYS.AUD$ (which stores database audit records) and SYS.FGA_LOG$ (which stores fine-grained audit records) tables reside in the SYSTEM tablespace. You can check their current location using the following query:

```
select owner, segment_name, segment_type, tablespace_name,
bytes / 1024 / 1024 AS MB
from dba_segments
where segment_name IN ('AUD$', 'FGA_LOG$');
```



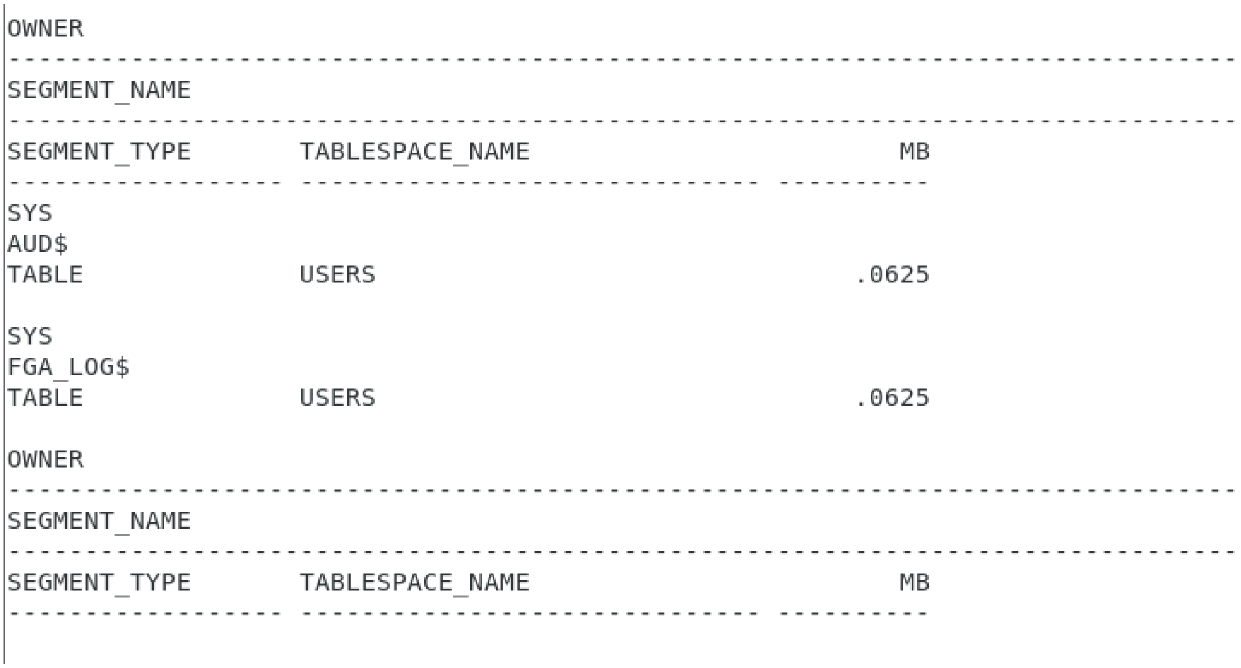
```
OWNER
--------------------------------------------------------------------------------
SEGMENT_NAME
--------------------------------------------------------------------------------
SEGMENT_TYPE       TABLESPACE_NAME                        MB
------------------ ------------------------------ ----------
SYS
AUD$
TABLE              SYSTEM                              .0625

SYS
FGA_LOG$
TABLE              SYSTEM                              .0625

OWNER
--------------------------------------------------------------------------------
SEGMENT_NAME
--------------------------------------------------------------------------------
SEGMENT_TYPE       TABLESPACE_NAME                        MB
------------------ ------------------------------ ----------
```

To move these tables to another tablespace (e.g., USERS), use the DBMS_AUDIT_MGMT package:

```
BEGIN
DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_LOCATION(
audit_trail_type           =>
DBMS_AUDIT_MGMT.AUDIT_TRAIL_DB_STD,
audit_trail_location_value => 'USERS');
END;
/
```

```
PL/SQL procedure successfully completed.
```

```
select owner, segment_name, segment_type, tablespace_name,
bytes / 1024 / 1024 AS MB
from dba_segments
where segment_name IN ('AUD$', 'FGA_LOG$');
```



```
OWNER
--------------------------------------------------------------------------------
SEGMENT_NAME
--------------------------------------------------------------------------------
SEGMENT_TYPE       TABLESPACE_NAME                        MB
------------------ ------------------------------ ----------
SYS
AUD$
TABLE              USERS                               .0625

SYS
FGA_LOG$
TABLE              USERS                               .0625

OWNER
--------------------------------------------------------------------------------
SEGMENT_NAME
--------------------------------------------------------------------------------
SEGMENT_TYPE       TABLESPACE_NAME                        MB
------------------ ------------------------------ ----------
```

Additional Options

To move only the **AUD$** table:

audit_trail_type => DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD

To move only the **FGA_LOG$** table:

audit_trail_type => DBMS_AUDIT_MGMT.AUDIT_TRAIL_FGA_STD

Final Thoughts

By securing and monitoring your database with Oracle auditing, you can enhance security, track database actions, and ensure compliance with organizational policies. Implementing these steps will provide better visibility into database activities and help protect your critical data assets.

==================GOOD LUCK=======================