AUDIT

Purpose

Use the AUDIT statement to:

- Track the occurrence of SQL statements in subsequent user sessions. You can track the occurrence of a specific SQL statement or of all SQL statements authorized by a particular system privilege. Auditing operations on SQL statements apply only to subsequent sessions, not to current sessions.
- Track operations on a specific schema object. Auditing operations on schema objects apply to current sessions as well as to subsequent sessions.

See Also:

- *Oracle Database Security Guide* for general information about auditing
- *Oracle Database PL/SQL Packages and Types Reference* for information on the DBMS_FGA package, which lets you create and administer value-based auditing policies
- NOAUDIT on page 18-76 for information on disabling auditing

Prerequisites

To audit occurrences of a SQL statement, you must have AUDIT SYSTEM system privilege.

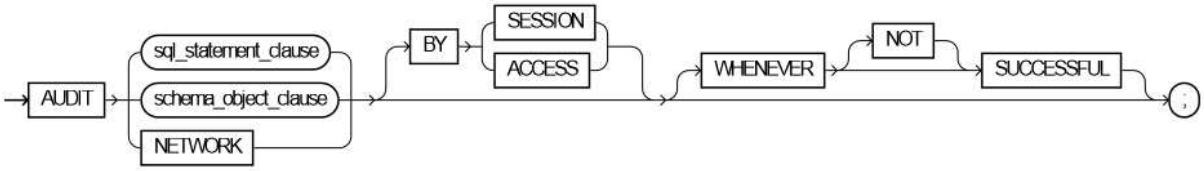
To audit operations on a schema object, the object you choose for auditing must be in your own schema or you must have AUDIT ANY system privilege. In addition, if the object you choose for auditing is a directory object, even if you created it, then you must have AUDIT ANY system privilege.

To collect auditing results, you must set the initialization parameter AUDIT_TRAIL to DB. You can specify auditing options regardless of whether auditing is enabled. However, Oracle Database does not generate audit records until you enable auditing.

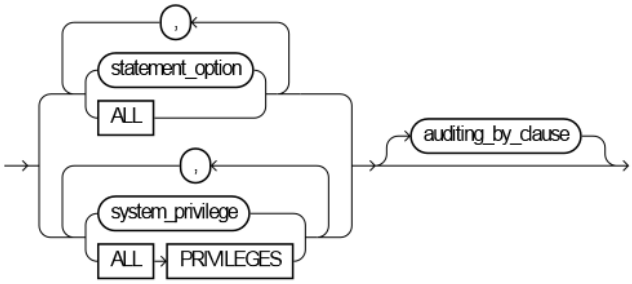
See Also: *Oracle Database Reference* for information on the AUDIT_TRAIL parameter

Syntax

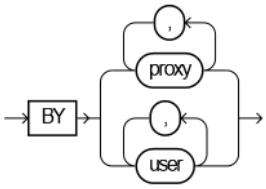
***audit*::=**



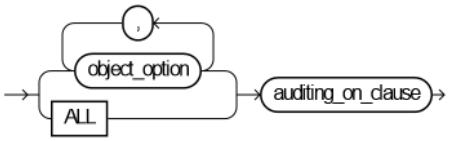
***sql_statement_clause*::=**



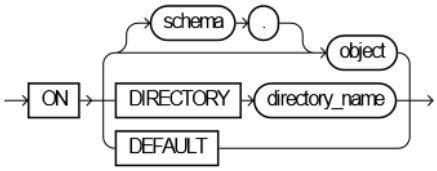
***auditing_by_clause*::=**



***schema_object_clause*::=**



***auditing_on_clause*::=**



Semantics

sql_statement_clause

Use the *sql_statement_clause* to audit SQL statements.

statement_option

Specify a statement option to audit specific SQL statements.

For each audited operation, Oracle Database produces an audit record containing this information:

- The user performing the operation
- The type of operation
- The object involved in the operation
- The date and time of the operation

Oracle Database writes audit records to the audit trail, which is a database table containing audit records. You can review database activity by examining the audit trail through data dictionary views.

See Also:

- Table 13 1 on page 13-46 and Table 13 2 on page 13-48 for a list of statement options and the SQL statements they audit
- *Oracle Database Security Guide* for a listing of the audit trail data dictionary views
- *Oracle Database Reference* for detailed descriptions of the data dictionary views
- "Auditing SQL Statements Relating to Roles: Example" on page 13-50

system_privilege

Specify a system privilege to audit SQL statements that are authorized by the specified system privilege.

Rather than specifying many individual system privileges, you can specify the roles CONNECT, RESOURCE, and DBA. Doing so is equivalent to auditing all of the system privileges granted to those roles.

Oracle Database also provides two shortcuts for specifying groups of system privileges and statement options at once:

ALL Specify ALL to audit all statements options shown in Table 13 1 but not the additional statement options shown in Table 13 2.

ALL PRIVILEGES Specify ALL PRIVILEGES to audit system privileges.

Note: Oracle recommends that you specify individual system privileges and statement options for auditing rather than roles or shortcuts. The specific system privileges and statement options encompassed by roles and shortcuts change from one release to the next and may not be supported in future versions of Oracle Database.

See Also:

- Table 18 1, " System Privileges" on page 18-37 for a list of all system privileges and the SQL statements that they authorize
- GRANT on page 18-32 for more information on the CONNECT, RESOURCE, and DBA roles
- "Auditing Query and Update SQL Statements: Example" on page 13-50, "Auditing Deletions: Example" on page 13-50, and "Auditing Statements Relating to Directories: Examples" on page 13-50

auditing_by_clause

Specify the *auditing_by_clause* to audit only those SQL statements issued by particular users. If you omit this clause, then Oracle Database audits all users statements.

BY user Use this clause to restrict auditing to only SQL statements issued by the specified users.

BY proxy Use this clause to restrict auditing to only SQL statements issued by the specified proxies.

> See Also: *Oracle Database Concepts* for more information on proxies and their use of the database

schema_object_clause

Use the *schema_object_clause* to audit operations on schema objects.

object_option

Specify the particular operation for auditing. Table 13 3 on page 13-49 shows each object option and the types of objects to which it applies. The name of each object option specifies a SQL statement to be audited. For example, if you choose to audit a table with the ALTER option, then Oracle Database audits all ALTER TABLE statements issued against the table. If you choose to audit a sequence with the SELECT option, then the database audits all statements that use any values of the sequence.

ALL

Specify ALL as a shortcut equivalent to specifying all object options applicable for the type of object.

auditing_on_clause

The *auditing_on_clause* lets you specify the particular schema object to be audited.

> See Also: "Auditing Queries on a Table: Example" on page 13-51, "Auditing Inserts and Updates on a Table: Example" on page 13-51, and "Auditing Operations on a Sequence: Example" on page 13-51

schema Specify the schema containing the object chosen for auditing. If you omit *schema*, then Oracle Database assumes the object is in your own schema.

object Specify the name of the object to be audited. The object must be a table, view, sequence, stored procedure, function, package, materialized view, or library.

You can also specify a synonym for a table, view, sequence, procedure, stored function, package, materialized view, or user-defined type.

ON DEFAULT Specify ON DEFAULT to establish the specified object options as default object options for subsequently created objects. After you have established these default auditing options, any subsequently created object is automatically audited with those options. The default auditing options for a view are always the union of the auditing options for the base tables of the view. You can see the current default auditing options by querying the ALL_DEF_AUDIT_OPTS data dictionary view.

When you change the default auditing options, the auditing options for previously created objects remain the same. You can change the auditing options for an existing object only by specifying the object in the ON clause of the AUDIT statement.

> See Also: "Setting Default Auditing Options: Example" on page 13-51

ON DIRECTORY ***directory_name*** The ON DIRECTORY clause lets you specify the name of a directory chosen for auditing.

NETWORK Use this clause to detect internal failures in the network layer.

> See Also: *Oracle Database Security Guide* for information on network auditing

BY SESSION

Specify BY SESSION if you want Oracle Database to write a single record for all SQL statements of the same type issued and operations of the same type executed on the same schema objects in the same session.

Oracle Database can write to an operating system audit file but cannot read it to detect whether an entry has already been written for a particular operation. Therefore, if you are using an operating system file for the audit trail (that is, the AUDIT_FILE_DEST initialization parameter is set to OS), then the database may write multiple records to the audit trail file even if you specify BY SESSION.

BY ACCESS

Specify BY ACCESS if you want Oracle Database to write one record for each audited statement and operation.

If you specify statement options or system privileges that audit data definition language (DDL) statements, then the database automatically audits by access regardless of whether you specify the BY SESSION clause or BY ACCESS clause.

For statement options and system privileges that audit SQL statements other than DDL, you can specify either BY SESSION or BY ACCESS. BY SESSION is the default.

WHENEVER [NOT] SUCCESSFUL

Specify WHENEVER SUCCESSFUL to audit only SQL statements and operations that succeed.

Specify WHENEVER NOT SUCCESSFUL to audit only statements and operations that fail or result in errors.

If you omit this clause, then Oracle Database performs the audit regardless of success or failure.

Tables of Auditing Options

Table 13–1 Statement Auditing Options for Database Objects

Statement Option	SQL Statements and Operations
ALTER SYSTEM	ALTER SYSTEM
CLUSTER	CREATE CLUSTER
	ALTER CLUSTER
	DROP CLUSTER
	TRUNCATE CLUSTER
CONTEXT	CREATE CONTEXT
	DROP CONTEXT
DATABASE LINK	CREATE DATABASE LINK
	DROP DATABASE LINK

Table 13–1 (Cont.) Statement Auditing Options for Database Objects

Statement Option	SQL Statements and Operations
DIMENSION	CREATE DIMENSION ALTER DIMENSION DROP DIMENSION
DIRECTORY	CREATE DIRECTORY DROP DIRECTORY
INDEX	CREATE INDEX ALTER INDEX ANALYZE INDEX DROP INDEX
MATERIALIZED VIEW	CREATE MATERIALIZED VIEW ALTER MATERIALIZED VIEW DROP MATERIALIZED VIEW
NOT EXISTS	All SQL statements that fail because a specified object does not exist.
PROCEDURE (See note at end of table)	CREATE FUNCTION CREATE LIBRARY CREATE PACKAGE CREATE PACKAGE BODY CREATE PROCEDURE DROP FUNCTION DROP LIBRARY DROP PACKAGE DROP PROCEDURE
PROFILE	CREATE PROFILE ALTER PROFILE DROP PROFILE
PUBLIC DATABASE LINK	CREATE PUBLIC DATABASE LINK DROP PUBLIC DATABASE LINK
PUBLIC SYNONYM	CREATE PUBLIC SYNONYM DROP PUBLIC SYNONYM
ROLE	CREATE ROLE ALTER ROLE DROP ROLE SET ROLE
ROLLBACK SEGMENT	CREATE ROLLBACK SEGMENT ALTER ROLLBACK SEGMENT DROP ROLLBACK SEGMENT
SEQUENCE	CREATE SEQUENCE DROP SEQUENCE
SESSION	Logons

Table 13–1 (Cont.) Statement Auditing Options for Database Objects

Statement Option	SQL Statements and Operations
SYNONYM	CREATE SYNONYM
	DROP SYNONYM
SYSTEM AUDIT	AUDIT *sql_statements*
	NOAUDIT *sql_statements*
SYSTEM GRANT	GRANT *system_privileges_and_roles*
	REVOKE *system_privileges_and_roles*
TABLE	CREATE TABLE
	DROP TABLE
	TRUNCATE TABLE
TABLESPACE	CREATE TABLESPACE
	ALTER TABLESPACE
	DROP TABLESPACE
TRIGGER	CREATE TRIGGER
	ALTER TRIGGER
	with ENABLE and DISABLE clauses
	DROP TRIGGER
	ALTER TABLE
	with ENABLE ALL TRIGGERS clause
	and DISABLE ALL TRIGGERS clause
TYPE	CREATE TYPE
	CREATE TYPE BODY
	ALTER TYPE
	DROP TYPE
	DROP TYPE BODY
USER	CREATE USER
	ALTER USER
	DROP USER
VIEW	CREATE VIEW
	DROP VIEW

Note: Java schema objects (sources, classes, and resources) are considered the same as procedures for purposes of auditing SQL statements.

Table 13–2 Additional Statement Auditing Options for SQL Statements

Statement Option	SQL Statements and Operations
ALTER SEQUENCE	ALTER SEQUENCE
ALTER TABLE	ALTER TABLE

Table 13–2 (Cont.) Additional Statement Auditing Options for SQL Statements

Statement Option	SQL Statements and Operations
COMMENT TABLE	COMMENT ON TABLE *table*, *view*, *materialized view* COMMENT ON COLUMN *table.column*, *view.column*, *materialized view.column*
DELETE TABLE	DELETE FROM *table*, *view*
EXECUTE PROCEDURE	CALL Execution of any procedure or function or access to any variable, library, or cursor inside a package.
GRANT DIRECTORY	GRANT privilege ON directory REVOKE privilege ON directory
GRANT PROCEDURE	GRANT privilege ON procedure, function, package REVOKE privilege ON procedure, function, package
GRANT SEQUENCE	GRANT privilege ON sequence REVOKE privilege ON sequence
GRANT TABLE	GRANT privilege ON table, view, materialized view REVOKE privilege ON table, view, materialized view
GRANT TYPE	GRANT privilege ON TYPE REVOKE privilege ON TYPE
INSERT TABLE	INSERT INTO table, view
LOCK TABLE	LOCK TABLE table, view
SELECT SEQUENCE	Any statement containing *sequence*.CURRVAL or *sequence*.NEXTVAL
SELECT TABLE	SELECT FROM table, view, materialized view
UPDATE TABLE	UPDATE table, view

Table 13–3 Object Auditing Options

Object Option	Table	View	Sequence	Procedure, Function, Package (Note 1)	Materialized View (Note 2)	Directory	Library	Object Type	Context
ALTER	X	--	X	--	X	--	--	X	--
AUDIT	X	X	X	X	X	X	--	X	X
COMMENT	X	X	--	--	X	--	--	--	--
DELETE	X	X	--	--	X	--	--	--	--
EXECUTE	--	--	--	X	--	--	X	--	--
FLASHBACK (Note 3)	X	X	--	--	--	--	--	--	--
GRANT	X	X	X	X	--	X	X	X	X
INDEX	X	--	--	--	X	--	--	--	--
INSERT	X	X	--	--	X	--	--	--	--
LOCK	X	X	--	--	X	--	--	--	--

Table 13–3 (Cont.) Object Auditing Options

Object Option	Table	View	Sequence	Procedure, Function, Package (Note 1)	Materialized View (Note 2)	Directory	Library	Object Type	Context
READ	--	--	--	--	--	X	--	--	--
RENAME	X	X	--		--	--	--	--	--
SELECT	X	X	X	--	X	--	--	--	--
UPDATE	X	X	--	--	X	--	--	--	--

Note 1: Java schema objects (sources, classes, and resources) are considered the same as procedures, functions, and packages for purposes of auditing options.

Note 2: You can audit INSERT, UPDATE, and DELETE operations only on updatable materialized views.

Note 3: The FLASHBACK audit object option applies only to flashback queries.

Examples

Auditing SQL Statements Relating to Roles: Example To choose auditing for every SQL statement that creates, alters, drops, or sets a role, regardless of whether the statement completes successfully, issue the following statement:

```
AUDIT ROLE;
```

To choose auditing for every statement that successfully creates, alters, drops, or sets a role, issue the following statement:

```
AUDIT ROLE
    WHENEVER SUCCESSFUL;
```

To choose auditing for every CREATE ROLE, ALTER ROLE, DROP ROLE, or SET ROLE statement that results in an Oracle Database error, issue the following statement:

```
AUDIT ROLE
    WHENEVER NOT SUCCESSFUL;
```

Auditing Query and Update SQL Statements: Example To choose auditing for any statement that queries or updates any table, issue the following statement:

```
AUDIT SELECT TABLE, UPDATE TABLE;
```

To choose auditing for statements issued by the users hr and oe that query or update a table or view, issue the following statement

```
AUDIT SELECT TABLE, UPDATE TABLE
    BY hr, oe;
```

Auditing Deletions: Example To choose auditing for statements issued using the DELETE ANY TABLE system privilege, issue the following statement:

```
AUDIT DELETE ANY TABLE;
```

Auditing Statements Relating to Directories: Examples To choose auditing for statements issued using the CREATE ANY DIRECTORY system privilege, issue the following statement:

```
AUDIT CREATE ANY DIRECTORY;
```

To choose auditing for CREATE DIRECTORY (and DROP DIRECTORY) statements that do not use the CREATE ANY DIRECTORY system privilege, issue the following statement:

```
AUDIT DIRECTORY;
```

To choose auditing for every statement that reads files from the bfile_dir directory, issue the following statement:

```
AUDIT READ ON DIRECTORY bfile_dir;
```

Auditing Queries on a Table: Example To choose auditing for every SQL statement that queries the employees table in the schema hr, issue the following statement:

```
AUDIT SELECT
    ON hr employees;
```

To choose auditing for every statement that successfully queries the employees table in the schema hr, issue the following statement:

```
AUDIT SELECT
    ON hr employees
    WHENEVER SUCCESSFUL;
```

To choose auditing for every statement that queries the employees table in the schema hr and results in an Oracle Database error, issue the following statement:

```
AUDIT SELECT
    ON hr employees
    WHENEVER NOT SUCCESSFUL;
```

Auditing Inserts and Updates on a Table: Example To choose auditing for every statement that inserts or updates a row in the customers table in the schema oe, issue the following statement:

```
AUDIT INSERT, UPDATE
    ON oe customers;
```

Auditing Operations on a Sequence: Example To choose auditing for every statement that performs any operation on the employees_seq sequence in the schema hr, issue the following statement:

```
AUDIT ALL
    ON hr employees_seq;
```

The preceding statement uses the ALL shortcut to choose auditing for the following statements that operate on the sequence:

- ALTER SEQUENCE
- AUDIT
- GRANT
- any statement that accesses the values of the sequence using the pseudocolumns CURRVAL or NEXTVAL

Setting Default Auditing Options: Example The following statement specifies default auditing options for objects created in the future:

```
AUDIT ALTER, GRANT, INSERT, UPDATE, DELETE
```

```
ON DEFAULT;
```

Any objects created later are automatically audited with the specified options that apply to them, if auditing has been enabled:

- If you create a table, then Oracle Database automatically audits any ALTER, GRANT, INSERT, UPDATE, or DELETE statements issued against the table.
- If you create a view, then Oracle Database automatically audits any GRANT, INSERT, UPDATE, or DELETE statements issued against the view.
- If you create a sequence, then Oracle Database automatically audits any ALTER or GRANT statements issued against the sequence.
- If you create a procedure, package, or function, then Oracle Database automatically audits any ALTER or GRANT statements issued against it.