What Is Auditing?

Auditing is the monitoring and recording of configured database actions, from both database users and nondatabase users.

You can configure auditing by using any of the following methods:

- **Group audit settings into one unified audit policy.** You can create one or more unified audit policies that define all the audit settings that your database needs. Auditing Activities with Unified Audit Policies and the AUDIT Statement describes how to accomplish this.
- **Use one of the default unified audit policies.** Oracle Database provides three default unified audit policies that encompass the standard audit settings that most regulatory agencies require. See Auditing Activities with the Predefined Unified Audit Policies.
- **Create fine-grained audit policies.** You can create fine-grained audit policies that capture data such as the time an action occurred. See Auditing Specific Activities with Fine-Grained Auditing.

Why Is Auditing Used?

You typically use auditing to monitor user activity.

Auditing can be used to accomplish the following:

- **Enable accountability for actions.** These include actions taken in a particular schema, table, or row, or affecting specific content.
- **Deter users (or others, such as intruders) from inappropriate actions based on their accountability.**
- **Investigate suspicious activity.** For example, if a user is deleting data from tables, then a security administrator can audit all

connections to the database and all successful and unsuccessful deletions of rows from all tables in the database.

- **Notify an auditor of the actions of an unauthorized user.** For example, an unauthorized user could be changing or deleting data, or the user has more privileges than expected, which can lead to reassessing user authorizations.
- **Monitor and gather data about specific database activities.** For example, the database administrator can gather statistics about which tables are being updated, how many logical I/Os are performed, or how many concurrent users connect at peak times.
- **Detect problems with an authorization or access control implementation.** For example, you can create audit policies that you expect will never generate an audit record because the data is protected in other ways. However, if these policies generate audit records, then you will know the other security controls are not properly implemented.

Selecting an Auditing Type

You must perform a specific set of steps depending on the type of auditing that you want to perform: general activities (such as SQL statement actions), commonly used auditing activities, or fine-grained auditing.

In addition to these types of auditing, remember that Oracle Database mandatorily audits some activities. See Activities That Are Mandatorily Audited for more information.

Topics:

- Auditing SQL Statements, Privileges, and Other General Activities
- Auditing Commonly Used Security-Relevant Activities
- Auditing Specific, Fine-Grained Activities

Auditing SQL Statements, Privileges, and Other General Activities

You can audit many types of objects, from SQL statements to other Oracle Database components, such as Oracle Database Vault..

In addition, you can create policies that use conditions. However, if you want to audit specific columns or use event handlers, you must use fine-grained auditing.

The general steps for performing this type of auditing are as follows:

1. In most cases, use the CREATE AUDIT POLICY statement to create an audit policy. If you must audit application context values, then use the AUDIT statement.

   See the relevant categories under Auditing Activities with Unified Audit Policies and the AUDIT Statement.

2. If you are creating an audit policy, then use the AUDIT statement to enable it and optionally apply (or exclude) the audit settings to one or more users, including administrative users who log in with the SYSDBA administrative privilege (for example, the SYS user).

   AUDIT also enables you to create an audit record upon an action's success, failure, or both.

   See Enabling Unified Audit Policies to Users.

3. Query the UNIFIED_AUDIT_TRAIL view to find the generated audit records.

   See also Audit Policy Data Dictionary Views for additional views.

4. Periodically archive and purge the contents of the audit trail.

   See Purging Audit Trail Records.

Auditing Commonly Used Security-Relevant Activities

Oracle Database provides a set default unified audit policies that you can choose from for commonly used security-relevant audits.

The general steps for performing this type of auditing are as follows:

1. See Auditing Activities with the Predefined Unified Audit Policies to learn about the default audit policies.
2. Use the AUDIT statement enable the policy and optionally apply (or exclude) the audit settings to one or more users.

   See Enabling Unified Audit Policies to Users.
3. Query the UNIFIED_AUDIT_TRAIL view to find the generated audit records.

   See also Audit Policy Data Dictionary Views for additional views.
4. Periodically archive and purge the contents of the audit trail.

   See Purging Audit Trail Records.

Auditing Specific, Fine-Grained Activities

Use fine-grained auditing if you want to audit individual columns and use event handlers.

This type of auditing provides all the features available in unified audit policies.

The general steps for fine-grained auditing are as follows:

1. See Auditing Specific Activities with Fine-Grained Auditing to understand more about auditing specific activities.

2. Use the DBMS_FGA PL/SQL package to configure fine-grained auditing policies. See Using the DBMS_FGA PL/SQL Package to Manage Fine-Grained Audit Policies.

3. Query the UNIFIED_AUDIT_TRAIL view to find the generated audit records.

   See also Audit Policy Data Dictionary Views for additional views.

4. Periodically archive and purge the contents of the audit trail.

   See Purging Audit Trail Records.

Auditing Activities with Unified Audit Policies and the AUDIT Statement

You can use the CREATE AUDIT POLICY and AUDIT statements to use unified auditing policies.

Topics:

- About Auditing Activities with Unified Audit Policies and AUDIT
- Best Practices for Creating Unified Audit Policies
- Syntax for Creating a Unified Audit Policy
- Auditing Roles
- Auditing System Privileges
- Auditing Administrative Users
- Auditing Object Actions
- Auditing SELECT, READ ANY TABLE, or SELECT ANY TABLE
- Auditing SQL Statements and Privileges in a Multitier Environment
- Creating a Condition for a Unified Audit Policy
- Auditing Application Context Values
- Auditing Oracle Database Real Application Security Events
- Auditing Oracle Database Vault Events

- Auditing Oracle Recovery Manager Events
- Auditing Oracle Label Security Events
- Auditing Oracle Data Mining Events
- Auditing Oracle Data Pump Events
- Auditing Oracle SQL*Loader Direct Load Path Events
- Using the Unified Audit Policies or AUDIT Settings in a Multitenant Environment