Database Security Guide

21 Introduction to Auditing

Auditing tracks changes that users make in the database.

Topics:

> **Note:**
>
> This part describes how to use pure unified auditing, in which all audit records are centralized in one place. If you have not yet migrated to use unified auditing, then see *Oracle Database Upgrade Guide* (../UPGRD/afterup.htm#UPGRD52810). Be aware that the upgrade process itself does not automatically enable unified auditing. You must manually migrate to unified auditing, as described in *Oracle Database Upgrade Guide* (../UPGRD/afterup.htm#UPGRD52810).

> **See Also:**
>
> "Guidelines for Auditing (guidelines.htm#GUID-776AA713-E67B-4DE5-BA51-621AACCFBA37)" for general guidelines to follow for auditing your system

What Is Auditing?

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

"Nondatabase users" refers to application users who are recognized in the database using the `CLIENT_IDENTIFIER` attribute. To audit this type of user, you can use a unified audit policy condition, a fine-grained audit policy, or Oracle Database Real Application Security.

You can base auditing on individual actions, such as the type of SQL statement executed, or on combinations of data that can include the user name, application, time, and so on.

You can configure auditing for both successful and failed activities, and include or exclude specific users from the audit. In a multitenant environment, you can audit individual actions of the pluggable database (PDB) or individual actions in the entire multitenant container database (CDB). In addition to auditing the standard activities the database provides, auditing can include activities from Oracle Database Real Application Security, Oracle Recovery Manager, Oracle Data Pump, Oracle Data Mining, Oracle Database Vault, Oracle Label Security, and Oracle SQL*Loader direct path events.

Auditing is enabled by default. All audit records are written to the unified audit trail in a uniform format and are made available through the `UNIFIED_AUDIT_TRAIL` view. These records reside in the `AUDSYS` schema. The audit records are stored in the `SYSAUX` tablespace by default. Oracle recommends that you configure a different tablespace for the unified audit trail. Be aware that for most Oracle Database editions except for Enterprise Edition, you can only associate the tablespace for unified auditing once. You should perform this association before you generate any audit records for the unified audit trail. After you have associated the tablespace, you cannot modify it because partitioning is only supported on Enterprise Edition.

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 (audit_config.htm#GUID-A215CCAF-4AFF-448A-909C-736EBDED5A8A) 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 (audit_config.htm#GUID-C43651C6-A35C-4EEF-BEA7-EADA408BFF67)

- **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 (audit_config.htm#GUID-B706FF6F-13A6-4944-AFCB-29971F5076FD).

Oracle recommends that you audit your databases. Auditing is an effective method of enforcing strong internal controls so that your site can meet its regulatory compliance requirements, as defined in the Sarbanes-Oxley Act. This enables you to monitor business operations, and find any activities that may deviate from company policy. Doing so translates into tightly controlled access to your database and the application software, ensuring that patches are applied on schedule and preventing ad hoc changes. By creating effective audit policies, you can generate an audit record for audit and compliance personnel. Be selective with auditing and ensure that it meets your business compliance needs.

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.
- **Address auditing requirements for compliance.** Regulations such as the following have common auditing-related requirements:
  - Sarbanes-Oxley Act
  - Health Insurance Portability and Accountability Act (HIPAA)
  - International Convergence of Capital Measurement and Capital Standards: a Revised Framework (Basel II)
  - Japan Privacy Law
  - European Union Directive on Privacy and Electronic Communications

Best Practices for Auditing

You should follow best practices guidelines for auditing.

- **As a general rule, design your auditing strategy to collect the amount of information that you need to meet compliance requirements, but focus on activities that cause the greatest security concerns.** For example, auditing every table in the database is not practical, but auditing tables with columns that contain sensitive data, such as salaries, is. With both unified and fine-grained auditing, there are mechanisms you can use to design audit policies that focus on specific activities to audit.
- **Periodically archive and purge the audit trail data.** See Purging Audit Trail Records (audit_admin.htm#GUID-9B891A44-3DF4-4B52-98D4-A931DBFAEC1D) for more information.

> **See Also:**
>
> Guidelines for Auditing (guidelines.htm#GUID-776AA713-E67B-4DE5-BA51-621AACCFBA37) for general guidelines to follow for auditing your system

What Is Unified Auditing?

In unified auditing, the unified audit trail captures audit information from a variety of sources.

Unified auditing enables you to capture audit records from the following sources:

- Audit records (including `SYS` audit records) from unified audit policies and `AUDIT` settings
- Fine-grained audit records from the `DBMS_FGA` PL/SQL package
- Oracle Database Real Application Security audit records
- Oracle Recovery Manager audit records
- Oracle Database Vault audit records
- Oracle Label Security audit records
- Oracle Data Mining records
- Oracle Data Pump
- Oracle SQL*Loader Direct Load

The unified audit trail, which resides in a read-only table in the `AUDSYS` schema in the `SYSAUX` tablespace, makes this information available in a uniform format in the `UNIFIED_AUDIT_TRAIL` data dictionary view, and is available in both single-instance and Oracle Database Real Application Clusters environments. In addition to the user `SYS`, users who have been granted the `AUDIT_ADMIN` and `AUDIT_VIEWER` roles can query these views. If your users only need to query the views but not create audit policies, then grant them the `AUDIT_VIEWER` role.

When the database is writeable, audit records are written to the unified audit trail. If the database is not writable, then audit records are written to new format operating system files in the `$ORACLE_BASE/audit/$ORACLE_SID` directory.

> **See Also:**
>
> *Oracle Database Reference* (../REFRN/GUID-B7CE1C02-2FD4-47D6-80AA-CF74A60CDD1D.htm#REFRN29162) for detailed information about the `UNIFIED_AUDIT_TRAIL` data dictionary view

Benefits of the Unified Audit Trail

The benefits of a unified audit trail are many.

For example:

- After unified auditing is enabled, it does not depend on the initialization parameters that were used in previous releases. See Table G-1 (audit_changes.htm#GUID-22ED5B2A-13F9-4448-BE3E-578CE3691F3B__CIHDIGAD) for a list of these initialization parameters.

- The audit records, including records from the SYS audit trail, for all the audited components of your Oracle Database installation are placed in one location and in one format, rather than your having to look in different places to find audit trails in varying formats. This consolidated view enables auditors to co-relate audit information from different components. For example, if an error occurred during an INSERT statement, standard auditing can indicate the error number and the SQL that was executed. Oracle Database Vault-specific information can indicate whether this error happened because of a command rule violation or realm violation. Note that there will be two audit records with a distinct AUDIT_TYPE. With this unification in place, SYS audit records appear with AUDIT_TYPE set to Standard Audit.

- The management and security of the audit trail is also improved by having it in single audit trail.

- Overall auditing performance is greatly improved. By default, the audit records are automatically written to an internal relational table in the AUDSYS schema.

- You can create named audit policies that enable you to audit the supported components listed at the beginning of this section, as well as SYS administrative users. Furthermore, you can build conditions and exclusions into your policies.

- If you are using an Oracle Audit Vault and Database Firewall environment, then the unified audit trail greatly facilitates the collection of audit data, because all of this data will come from one location. See *Oracle Audit Vault and Database Firewall Administrator's Guide* (http://www.oracle.com/pls/topic/lookup?ctx=E50529 01&id=SIGAD40485) for more information.

Checking if Your Database Has Migrated to Unified Auditing

The V$OPTION dynamic view indicates if your database has been migrated to unified auditing.

- Query the VALUE column of the V$OPTION dynamic view as follows, entering Unified Auditing in the case shown:

```
SELECT VALUE FROM V$OPTION WHERE PARAMETER = 'Unified Auditing'; PARAMETER VALUE ---
------------ ---------- Unified Auditing TRUE
```

This output shows that unified auditing is enabled. If unified auditing has not been enabled, then the output is FALSE.

> **See Also:**
>
> Disabling Unified Auditing (audit_admin.htm#GUID-80D9305C-29F6-4F3B-BDDB-371F619B08D8) if you must disable unified auditing

Mixed Mode Auditing

Mixed mode auditing is the default auditing in a newly installed database.

Topics:

- About Mixed Mode Auditing (auditing.htm#GUID-E9DB31BB-E90C-4B22-B29D-F9A44B350F9B)
- How Database Creation Determines the Type of Auditing You Have Enabled (auditing.htm#GUID-576F6022-F559-462B-94A4-B4612A7F29AB)
- Capabilities of Mixed Mode Auditing (auditing.htm#GUID-12712083-CA55-400A-93DC-15F97CB83814)

About Mixed Mode Auditing

Mixed mode auditing enables both traditional (that is, the audit facility from releases earlier than Release 12*c*) and the new audit facilities (unified auditing).

You can enable the database in either of these two modes: the mixed mode auditing or pure unified auditing mode. Even though the features of unified auditing are enabled in both these modes, there are differences between them. In mixed mode, you can use the new unified audit facility alongside the traditional auditing facility. In pure unified auditing, you only use the unified audit facility.

Table 21-1 (auditing.htm#GUID-E9DB31BB-E90C-4B22-B29D-F9A44B350F9B__CHDBEGGG) summarizes the features of these two modes and how you enable them.

Table 21-1 Differences Between MIxed Mode Audting and Pure Unified Auditing

Mode	Features	How to Enable
Mixed mode auditing	Has both traditional and unified auditing	Enable any unified audit policy. There is no need to restart the database.
Pure unified auditing	Has only unified auditing	Link the `oracle` binary with `uniaud_on`, and then restart the database.

Mixed mode is intended to introduce unified auditing, so that you can have a feel of how it works and what its nuances and benefits are. Mixed mode enables you to migrate your existing applications and scripts to use unified auditing. Once you have decided to use pure unified auditing, you can relink the `oracle` binary with the unified audit option turned on and thereby enable it as the one and only audit facility the Oracle database runs. If you decide to revert back to mixed mode, you can.

As in previous releases, the traditional audit facility is driven by the `AUDIT_TRAIL` initialization parameter. Only for mixed mode auditing, you should set this parameter to the appropriate traditional audit trail. This traditional audit trail will then be populated with audit records, along with the unified audit trail.

When you upgrade your database to the current release, traditional auditing is preserved, and the new audit records are written to the traditional audit trail. After you complete the migration (as described in *Oracle Database Upgrade Guide* (../UPGRD/afterup.htm#UPGRD52810)), the audit records from the previous release are still available in those audit trails. You then can archive and purge these older audit trails by using the `DBMS_AUDIT_MGMT` PL/SQL procedures, based on your enterprise retention policies.

See Also:

- How the Unified Auditing Migration Affects Individual Audit Features (audit_changes.htm#GUID-22ED5B2A-13F9-4448-BE3E-578CE3691F3B), for a comparison of the features available in the pre-migrated and post-migrated auditing environments

- Checking if Your Database Has Migrated to Unified Auditing (auditing.htm#GUID-57897757-4F56-4E7D-9E81-1372AF3ADF1D)
- *Oracle Database Upgrade Guide* (../UPGRD/afterup.htm#UPGRD52810)for information about migrating your databases to unified auditing, and for references to the documentation you should use if you choose not to migrate

How Database Creation Determines the Type of Auditing You Have Enabled

Unified auditing uses the `$ORACLE_BASE/audit` directory as the location for the new format operating system files.

For newly created databases, mixed mode auditing is enabled by default through the predefined policy `ORA_SECURECONFIG`.

To start using unified auditing, you must enable at least one unified audit policy, and to stop using it, disable all unified audit policies.

See Also:

Secure Options Predefined Unified Audit Policy (audit_config.htm#GUID-C0070008-D2BB-425A-9DC3-153FB1575445for more information about the `ORA_SECURECONFIG` policy

Capabilities of Mixed Mode Auditing

Mixed mode auditing provides the several capabilities.

These capabilities are as follows:

- It enables the use of all existing auditing initialization parameters: `AUDIT_TRAIL`, `AUDIT_FILE_DEST`, `AUDIT_SYS_OPERATIONS`, and `AUDIT_SYSLOG_LEVEL`.
- It writes mandatory audit records only to the traditional audit trails.
- It bases standard audit records on the standard audit configuration, and writes these records to the audit trail designated by the `AUDIT_TRAIL` initialization parameter.

  However, be aware that standard audit trail records are also generated based on unified audit policies and only these audit records are written to the unified audit trail. The standard audit records generated as a result of unified audit policies follow the semantics of unified audit policy enablement.
- Administrative user sessions generate `SYS` audit records. These records are written if the `AUDIT_SYS_OPERATIONS` initialization parameter is set to `TRUE`. This process writes the records only to the traditional audit trails. However, when unified audit policies are enabled for administrative users, these unified audit records are also written to unified audit trail.
- The format of the audit records that are written to traditional audit trails remains the same as in Oracle Database 11*g* Release 2.

- By default, Oracle Database writes unified audit records to system global area (SGA) queues. In other words, it writes the records periodically, not immediately. You can control how often the audit records are written. See Writing the Unified Audit Trail Records to the AUDSYS Schema (audit_admin.htm#GUID-1DD625ED-AC75-47E7-ADF6-1C7C93656F22)for more information.

- The performance cost of writing an audit record is equivalent to the sum of the times required for generating and writing an audit record to the traditional audit trail and the unified audit trail.

- Mixed mode auditing provides a glance of the unified audit mode features. Oracle recommends that you migrate to unified audit mode once you are comfortable with the new style of audit policies and audit trail. To migrate to unified auditing, see *Oracle Database Upgrade Guide* (../UPGRD/afterup.htm#UPGRD52810).

Who Can Perform Auditing?

Oracle provides two roles for users who perform auditing: `AUDIT_ADMIN` and `AUDIT_VIEWER`.

To perform any kind of auditing, you must be granted the `AUDIT_ADMIN` role. An auditor can view audit data after being granted the `AUDIT_VIEWER` role.

The privileges that these roles provide are as follows:

- **AUDIT_ADMIN role.** This role enables you to create unified and fine-grained audit policies, use the `AUDIT` and `NOAUDIT` SQL statements, view audit data, and manage the audit trail administration. Grant this role only to trusted users.

- **AUDIT_VIEWER role.** This role enables users to view and analyze audit data. The kind of user who needs this role is typically an external auditor.

> **Note:**
>
> In previous releases, users were allowed to add and remove audit configuration to objects in their own schemas without any additional privileges. This ability is no longer allowed.

Auditing in a Multitenant Environment

Unified auditing can be used in a multitenant environment.

You can apply audit settings to individual PDBs or to the CDB as a whole, depending on the type of policy. In a multitenant environment, each PDB, including the root, has own unified audit trail.

See the following sections for more information:

- **Unified audit policies created with the CREATE AUDIT POLICY and AUDIT statements:** You can create policies for both the root and individual PDBs. SeeUsing the Unified Audit Policies or AUDIT Settings in a Multitenant Environment (audit_config.htm#GUID-E02D0A5B-6591-4CD1-AF2B-29B0850BB6CB)

- **Fine-grained audit policies:** You can create policies for individual PDBs only, not the root. See Creating a Fine-Grained Audit Policy (audit_config.htm#GUID-374564C6-AF17-44EC-8710-2C8440C5478D)

- **Purging the audit trail:** You can perform purge operations for both the root and individual PDBs. See Purging Audit Trail Records (audit_admin.htm#GUID-9B891A44-3DF4-4B52-98D4-A931DBAEC1D) .

> **See Also:**
>
> *Oracle Database Concepts* (../CNCPT/glossary.htm#CNCPT89367) for information about the common audit configurations in a multitenant environment

Auditing in a Distributed Database

Auditing is site autonomous in that a database instance audits only the statements issued by directly connected users.

A local Oracle Database node cannot audit actions that take place in a remote database.