29

Provisioning Audit Policies

Oracle Database provides a variety of ways for you to audit activities.

- Getting Started with Auditing
  Effective auditing requires that audit policies be selective and focused. This ensures that the audit records generated are what is needed to support forensic analysis, and compliance, without generating unnecessary audit records.
- About Audit Policies
  An audit policy is a named group of audit settings that enable you to audit a particular aspect of user behavior in the database.
- Activities That Are Mandatorily Audited
  Certain security sensitive database activities are always audited and such audit configurations cannot be disabled.
- Auditing Activities with the Predefined Unified Audit Policies
  Oracle Database provides predefined unified audit policies that cover commonly used security-relevant audit settings.
- Steps to Provision Unified Audit Policies
  Apart from mandatorily audited activities and predefined unified audit policies enabled by default in the Oracle database, you may need to provision additional unified audit policies based on your security and compliance needs.
- Common Audit Configurations Across All PDBs
  A common audit configuration is visible and enforced across all PDBs.
- General Audit Data Dictionary Views
  Oracle Database provides different types of data dictionary and dynamic views for use with unified auditing.

29.1 Getting Started with Auditing

Effective auditing requires that audit policies be selective and focused. This ensures that the audit records generated are what is needed to support forensic analysis, and compliance, without generating unnecessary audit records.

The most common activities to audit includes but are not limited to the following

- Failed logins
- Any login from outside of the application or monitoring tools
- Data Definition Language – creating, dropping, or changing database objects
- Data Control Language – especially create user, alter user, privilege and role grants
- Oracle Data Pump import operations
- Any Oracle Database Vault activity or rule violation
- Any `SYSDBA` or database administrator activity

The top three tips to get started on auditing activities with Oracle Database with unified auditing are as follows:

1. Do not duplicate mandatory audit configurations which are always on in the Oracle database.
2. Use the predefined unified audit policies provided in Oracle Database, Oracle Data Safe, or Oracle Audit Vault and Database Firewall (AVDF).
3. Create custom audit policies (unified audit or fine-grained) for specialized needs.

You can fine-tune unified audit policies with conditions and enforced on specific users to reduce audit volume. You may want to use conditional enablement features for use cases, such as the following:

- Monitor access to sensitive data outside the trusted application path to focus only on the activity that matters.
- Monitor any activity from ad-hoc or power users who typically have access to query the data outside the trusted application paths.

Related Topics

- Guidelines for Auditing
  Oracle provides guidelines for auditing.

29.2 About Audit Policies

An audit policy is a named group of audit settings that enable you to audit a particular aspect of user behavior in the database.

You can create audit policies that monitor a wide range of activities, such as the following:

- User accounts (including administrative users who log in with the `SYSDBA` administrative privilege), roles, and privileges
- Object actions, such as dropping a table or a running a procedure
- Application context values
- Activities from other Oracle Database products, such as Oracle Database Real Application Security, Oracle Recovery Manager, or Oracle Data Pump.

Oracle Database provides three ways for you to create audit policies:

- **Use predefined unified audit policies for auditing the most common security relevant activities.** The predefined audit policies enable you to follow certain industry standards, such as the Center for Internet Security Recommendations or the Security Technical Implementation Guide standards. Predefined policies are also available for common audit tasks such as failed logins, and for other Oracle products, such as Oracle Database Real Application Security and Oracle Database Vault. The predefined audit policies should be sufficient for most auditing needs, but if they are not, then you can create custom audit policies or fine-grained audit policies.
- **Create custom unified audit policies for more specific activities.** Custom unified audit policies enable you to audit a wide range of activities, such as auditing the use of roles or actions performed on objects like tables. You use the `CREATE AUDIT POLICY` statement to create the unified audit policy, and the `AUDIT` statement to enable it. The `CREATE AUDIT POLICY` syntax is flexible enough for you to build in conditions, for example, or audit application context values.
- **Create fine-grained audit policies for more granular audit needs.** Fine-grained audit policies are not unified audit policies; you use the `DBMS_FGA` PL/SQL package to create a fine-grained audit policy. Fine-grained audit policies enable you to include conditions and event handlers. For example, you can send alerts to an administrator if a user violates the

audit policy. You can also audit specific rows of a table based on the value in a certain column with fine-grained audit.

29.3 Activities That Are Mandatorily Audited

Certain security sensitive database activities are always audited and such audit configurations cannot be disabled.

Activities that are always audited include but are not limited to the following:

- Activities of administrative users such as `SYSDBA`, `SYSBACKUP`, and `SYSKM` when the database is down is always audited.
- Any DDL or DML attempts on `UNIFIED_AUDIT_TRAIL` or the underlying dictionary tables in `AUDSYS` schema is always audited. These operations are not permitted by design. The unified audit trail resides in a read-only table in the `AUDSYS` schema.

Mandatorily audited activities will have audit policy by name `ORA$MANDATORY` in the `UNIFIED_AUDIT_POLICIES` column of the `UNIFIED_AUDIT_TRAIL` data dictionary view. The `ORA$MANDATORY` is always listed first in this column, if there are other unified audit policies that are tracking mandatorily audited activities. The `SYSTEM_PRIVILEGE_USED` column shows the type of administrative privilege that was used for the activity.

The following activities are mandatorily audited in Oracle Database:

Non-Audit-Related Activities

- SQL Firewall administrative actions
- `ORADEBUG` utility

Audit-Related Activities

- `CREATE AUDIT POLICY`
- `ALTER AUDIT POLICY`
- `DROP AUDIT POLICY`
- `AUDIT`
- `NOAUDIT`
- `EXECUTE` of the `DBMS_FGA` PL/SQL package
- `EXECUTE` of the `DBMS_AUDIT_MGMT` PL/SQL package
- `ALTER TABLE` attempts on the `AUDSYS` audit trail table (remember that this table cannot be altered)
- Top level statements by the administrative users `SYS`, `SYSDBA`, `SYSOPER`, `SYSASM`, `SYSBACKUP`, `SYSDG`, and `SYSKM`, until the database opens.
- All user-issued DML statements on the `SYS.AUD$` and `SYS.FGA_LOG$` dictionary tables
- Any attempts to modify the data or metadata of the unified audit internal table. `SELECT` statements on this table are not audited by default or mandatorily.
- All configuration changes that are made to Oracle Database Vault

Mandatorily Audited Access to Sensitive Columns in the Oracle Optimizer Dictionary Tables

Be aware that internal access to these table columns by the `DBMS_STATS` package does not generate mandatory audit records. You can use the `ORA$DICTIONARY_SENS_COL_ACCESS` predefined audit policy to audit these tables. The optimizer dictionary tables are as follows:

Optimizer Dictionary Table	Columns
SYS.HIST_HEAD$	minimum, maximum, lowval, hival
SYS.HISTGRM$	endpoint, epvalue_raw
SYS.WRI$_OPSTAT_HISTGRM_HISTORY	endpoint, epvalue_raw
SYS.WRI$_OPTSTAT_HISTHEAD_HISTORY	minimum, maximum, lowval, hival

Mandatorily Audited Operations on Blockchain and Immutable Tables

- `CREATE TABLE`
- `DROP TABLE`
- Failed `ALTER TABLE` operations
- Failed `DELETE` operations
- Failed `FLASHBACK TABLE` operations
- Failed `RENAME` operations
- Failed `TRUNCATE TABLE` operations
- Failed `UPDATE` operations

Related Topics

- Auditing Administrative Users
  You can create unified audit policies to capture the actions of administrative user accounts, such as `SYS`.
- ORA_DICTIONARY Sensitive Column Queries Predefined Unified Audit Policy
  The `ORA$DICTIONARY_SENS_COL_ACCESS` predefined audit policy audits the sensitive columns in the Oracle Optimizer dictionary tables.

29.4 Auditing Activities with the Predefined Unified Audit Policies

Oracle Database provides predefined unified audit policies that cover commonly used security-relevant audit settings.

- About Auditing Activities with the Predefined Unified Audit Policies
  Oracle Database has a set of predefined unified audit policies that address most auditing needs.
- Secure Options Predefined Unified Audit Policy
  The `ORA_SECURECONFIG` unified audit policy provides audit options using Oracle Database security best practices.
- Oracle Database Parameter Changes Predefined Unified Audit Policy
  The `ORA_DATABASE_PARAMETER` policy audits commonly used Oracle Database parameter modification commands.

- User Account and Privilege Management Predefined Unified Audit Policy
  The `ORA_ACCOUNT_MGMT` policy audits commonly used user account and privilege settings.
- Center for Internet Security Recommendations Predefined Unified Audit Policy
  The `ORA_CIS_RECOMMENDATIONS` policy performs audits that the Center for Internet Security (CIS) recommends.
- Security Technical Implementation Guide Predefined Unified Audit Policies
  You can use predefined unified audit policies to implement Security Technical Implementation Guide (STIG) audit requirements.
- ORA_DICTIONARY Sensitive Column Queries Predefined Unified Audit Policy
  The `ORA$DICTIONARY_SENS_COL_ACCESS` predefined audit policy audits the sensitive columns in the Oracle Optimizer dictionary tables.
- Oracle Database Real Application Security Predefined Audit Policies
  You can use predefined unified audit policies for Oracle Database Real Application Security events.
- Oracle Database Vault Predefined Unified Audit Policy for DVSYS and LBACSYS Schemas
  The `ORA_DV_SCHEMA_CHANGES` (previously called `ORA_DV_AUDPOL`) predefined unified audit policy audits Oracle Database Vault `DVSYS` and `LBACSYS` schema objects.
- Oracle Database Vault Predefined Unified Audit Policy for Default Realms and Command Rules
  The `ORA_DV_DEFAULT_PROTECTION` (previously called `ORA_DV_AUDPOL2`) predefined unified audit policy audits the Oracle Database Vault default realms and command rules.
- Oracle Label Security Predefined Unified Audit Policy for LBACSYS Objects
  The `ORA_OLS_SCHEMA_CHANGES` predefined unified audit policy audits objects that are owned by the Oracle Label Security `LBACSYS` user.

Related Topics

- Auditing Most Commonly Used Security-Relevant Activities
  Oracle Database provides a set of predefined unified audit policies that you can choose from for the most common security-relevant activities.

29.4.1 About Auditing Activities with the Predefined Unified Audit Policies

Oracle Database has a set of predefined unified audit policies that address most auditing needs.

These audit policies address common scenarios such as capturing login failures and secure options and requirements by the Security Internet Implementation Guide and the Center for Internet Security Recommendations.

You might see certain predefined audit policies that have already been enabled by default in your database. You can see the list of enabled audit policies by querying the `AUDIT_UNIFIED_ENABLED_POLICIES` data dictionary view. You can enable predefined audit policies by using the `AUDIT` PL/SQL statement.

To find the latest list of Oracle-supplied predefined unified audit policies, query the `AUDIT_UNIFIED_POLICIES` data dictionary view as follows:

```
SELECT DISTINCT POLICY_NAME FROM AUDIT_UNIFIED_POLICIES WHERE ORACLE_SUPPLIED
= 'YES';
```

If you are using Oracle Data Safe or Oracle Audit Vault and Database Firewall (AVDF) to monitor the database activity across your enterprise, these products also offer a number of predefined audit policies in addition to the ones provided in the Oracle Database. You can provision these policies with a single click.

Related Topics

- Enabling and Applying Unified Audit Policies to Users and Roles
  You can use the `AUDIT POLICY` statement to enable and apply unified audit policies to users and roles.
- Creating Custom Unified Audit Policies
  Oracle Database provides the flexibility to create and manage custom unified audit policies for your specialized needs.
- Value-Based Auditing with Fine-Grained Audit Policies
  Fine-grained auditing enables you to perform value-based auditing to audit access to certain rows based on values in specific columns.
- Oracle Data Safe
- Oracle Audit Vault and Database Firewall

29.4.2 Secure Options Predefined Unified Audit Policy

The `ORA_SECURECONFIG` unified audit policy provides audit options using Oracle Database security best practices.

For new databases, this policy is enabled by default for both pure unified auditing and mixed-mode auditing environments. This policy is not enabled for databases that were upgraded from earlier versions, except if you have created a new database from the previous release and then upgrade it to the current release.

> **Note:**
>
> Only user `SYS` can alter or drop this predefined policy.

The following statement shows the `ORA_SECURECONFIG` unified audit policy definition.

```
PRIVILEGES ALTER ANY TABLE, CREATE ANY TABLE, DROP ANY TABLE,
           CREATE ANY PROCEDURE, DROP ANY PROCEDURE, ALTER ANY PROCEDURE,
           GRANT ANY PRIVILEGE, GRANT ANY OBJECT PRIVILEGE, GRANT ANY ROLE,
           AUDIT SYSTEM, CREATE EXTERNAL JOB, CREATE ANY JOB,
           CREATE ANY LIBRARY,
           EXEMPT ACCESS POLICY,
           CREATE USER, DROP USER,
           ALTER DATABASE, ALTER SYSTEM,
           CREATE PUBLIC SYNONYM, DROP PUBLIC SYNONYM,
           CREATE SQL TRANSLATION PROFILE, CREATE ANY SQL TRANSLATION
PROFILE,
           DROP ANY SQL TRANSLATION PROFILE, ALTER ANY SQL TRANSLATION
PROFILE,
           TRANSLATE ANY SQL,
           EXEMPT REDACTION POLICY,
           PURGE DBA_RECYCLEBIN, LOGMINING,
           ADMINISTER KEY MANAGEMENT, BECOME USER,
```

```
            ADMINISTER FINE GRAINED AUDIT POLICY,
            ADMINISTER REDACTION POLICY,
            ADMINISTER ROW LEVEL SECURITY POLICY,
            GRANT ANY SCHEMA PRIVILEGE,
            CREATE ANY DOMAIN, ALTER ANY DOMAIN,
            DROP ANY DOMAIN,
            CREATE ANY MLE, ALTER ANY MLE, DROP ANY MLE,
            ADMINISTER SQL FIREWALL
 ACTIONS ALTER USER, CREATE ROLE, ALTER ROLE, DROP ROLE,
            SET ROLE, CREATE PROFILE, ALTER PROFILE,
            DROP PROFILE, CREATE DATABASE LINK,
            ALTER DATABASE LINK, DROP DATABASE LINK,
            CREATE DIRECTORY, DROP DIRECTORY,
            CREATE PLUGGABLE DATABASE,
            DROP PLUGGABLE DATABASE,
            ALTER PLUGGABLE DATABASE,
            ALTER DATABASE DICTIONARY,
            EXECUTE ON REMOTE_SCHEDULER_AGENT.ADD_AGENT_CERTIFICATE;
```

To enable `ORA_SECURECONFIG` audit policy, run the following:

```
AUDIT POLICY ORA_SECURECONFIG;
```

29.4.3 Oracle Database Parameter Changes Predefined Unified Audit Policy

The `ORA_DATABASE_PARAMETER` policy audits commonly used Oracle Database parameter modification commands.

> **Note:**
>
> Only user `SYS` can alter or drop this predefined policy.

The following statement shows the `ORA_DATABASE_PARAMETER` unified audit policy definition. By default, this policy is not enabled.

```
ACTIONS ALTER DATABASE, ALTER SYSTEM, CREATE SPFILE;
```

To enable `ORA_DATABASE_PARAMETER`, run the following command:

```
AUDIT POLICY ORA_DATABASE_PARAMETER;
```

29.4.4 User Account and Privilege Management Predefined Unified Audit Policy

The `ORA_ACCOUNT_MGMT` policy audits commonly used user account and privilege settings.

> **Note:**
>
> Only user SYS can alter or drop this predefined policy.

The following statement shows the ORA_ACCOUNT_MGMT unified audit policy definition. By default, this policy is not enabled.

```
ACTIONS CREATE USER, ALTER USER, DROP USER, CREATE ROLE, DROP ROLE,
  ALTER ROLE, SET ROLE, GRANT, REVOKE;
```

To enable ORA_ACCOUNT_MGMT, run the following command:

```
AUDIT POLICY ORA_ACCOUNT_MGMT;
```

29.4.5 Center for Internet Security Recommendations Predefined Unified Audit Policy

The ORA_CIS_RECOMMENDATIONS policy performs audits that the Center for Internet Security (CIS) recommends.

> **Note:**
>
> Only user SYS can alter or drop this predefined policy.

The following statement shows the ORA_CIS_RECOMMENDATIONS unified audit policy definition. By default, this policy is not enabled.

```
PRIVILEGES SELECT ANY DICTIONARY, ALTER SYSTEM
ACTIONS CREATE USER, ALTER USER, DROP USER,
        CREATE ROLE, DROP ROLE, ALTER ROLE,
        GRANT, REVOKE, CREATE DATABASE LINK,
        ALTER DATABASE LINK, DROP DATABASE LINK,
        CREATE PROFILE, ALTER PROFILE, DROP PROFILE,
        CREATE SYNONYM, DROP SYNONYM,
        CREATE PROCEDURE, DROP PROCEDURE,
        ALTER PROCEDURE, ALTER SYNONYM, CREATE FUNCTION,
        CREATE PACKAGE, CREATE PACKAGE BODY,
        ALTER FUNCTION, ALTER PACKAGE, ALTER SYSTEM,
        ALTER PACKAGE BODY, DROP FUNCTION,
        DROP PACKAGE, DROP PACKAGE BODY,
        CREATE TRIGGER, ALTER TRIGGER,
        DROP TRIGGER;
```

To enable ORA_CIS_RECOMMENDATIONS, run the following command:

```
AUDIT POLICY ORA_CIS_RECOMMENDATIONS;
```

Related Topics

- Logon and Logout Predefined Unified Audit Policy
  The `ORA_LOGIN_LOGOUT` policy (previously called `ORA_LOGON_FAILURES`) tracks logon and logoff operations.

29.4.6 Security Technical Implementation Guide Predefined Unified Audit Policies

You can use predefined unified audit policies to implement Security Technical Implementation Guide (STIG) audit requirements.

- STIG Recommendations Predefined Unified Audit Policy
  The `ORA_STIG_RECOMMENDATIONS` policy performs audits that the Security Technical Implementation Guide (STIG) recommends.
- All Top Level Actions Predefined Unified Audit Policy
  The `ORA_ALL_TOPLEVEL_ACTIONS` policy performs audits of all top level actions of privileged users.
- Logon and Logout Predefined Unified Audit Policy
  The `ORA_LOGIN_LOGOUT` policy (previously called `ORA_LOGON_FAILURES`) tracks logon and logoff operations.

29.4.6.1 STIG Recommendations Predefined Unified Audit Policy

The `ORA_STIG_RECOMMENDATIONS` policy performs audits that the Security Technical Implementation Guide (STIG) recommends.

> **Note:**
>
> Only user `SYS` can alter or drop this predefined policy.

The following statement shows the `ORA_STIG_RECOMMENDATIONS` unified audit policy definition. By default, this policy is not enabled.

```
PRIVILEGES ALTER SESSION
ACTIONS CREATE FUNCTION, ALTER FUNCTION, DROP FUNCTION,
    CREATE PACKAGE, ALTER PACKAGE, DROP PACKAGE,
    CREATE PROCEDURE, ALTER PROCEDURE, DROP PROCEDURE,
    CREATE TRIGGER, ALTER TRIGGER, DROP TRIGGER,
    CREATE PACKAGE BODY, ALTER PACKAGE BODY,
    DROP PACKAGE BODY,
    CREATE TYPE, ALTER TYPE, DROP TYPE,
    CREATE TYPE BODY, ALTER TYPE BODY, DROP TYPE BODY,
    CREATE LIBRARY, ALTER LIBRARY, DROP LIBRARY,
    CREATE JAVA, ALTER JAVA, DROP JAVA,
    CREATE OPERATOR, ALTER OPERATOR, DROP OPERATOR,
    CREATE TABLE, ALTER TABLE, DROP TABLE,
    CREATE VIEW, ALTER VIEW, DROP VIEW,
    CREATE MATERIALIZED VIEW, ALTER MATERIALIZED VIEW,
    DROP MATERIALIZED VIEW,
```

```
    CREATE ASSEMBLY, ALTER ASSEMBLY, DROP ASSEMBLY,
    CREATE SYNONYM, ALTER SYNONYM, DROP SYNONYM,
    CREATE USER, ALTER USER, DROP USER,
    GRANT, REVOKE,
    CREATE ROLE, ALTER ROLE, DROP ROLE, SET ROLE,
    CREATE PROFILE, ALTER PROFILE, DROP PROFILE,
    CREATE LOCKDOWN PROFILE, ALTER LOCKDOWN PROFILE,
    DROP LOCKDOWN PROFILE,
    ALTER SYSTEM, ALTER DATABASE, ALTER PLUGGABLE DATABASE,
    CREATE SPFILE, ALTER DATABASE DICTIONARY,
    ADMINISTER KEY MANAGEMENT,
    EXECUTE ON DBMS_JOB, EXECUTE ON DBMS_RLS,
    EXECUTE ON DBMS_REDACT, EXECUTE ON DBMS_TSDP_MANAGE,
    EXECUTE ON DBMS_TSDP_PROTECT,
    EXECUTE ON DBMS_NETWORK_ACL_ADMIN,
    EXECUTE ON DBMS_SCHEDULER
ACTIONS COMPONENT = OLS ALL';
```

For STIG compliance, enable the `ORA_STIG_RECOMMENDATIONS` unified audit policy for all users.

```
AUDIT POLICY ORA_STIG_RECOMMENDATIONS;
```

29.4.6.2 All Top Level Actions Predefined Unified Audit Policy

The `ORA_ALL_TOPLEVEL_ACTIONS` policy performs audits of all top level actions of privileged users.

> **Note:**
>
> Only user `SYS` can alter or drop this predefined policy.

The following statement shows the `ORA_ALL_TOPLEVEL_ACTIONS` unified audit policy definition. By default, this policy is not enabled.

```
ACTIONS ALL ONLY TOPLEVEL;
```

For STIG compliance, enable the `ORA_ALL_TOPLEVEL_ACTIONS` unified audit policy for all Oracle-defined and site specific privileged users. For example, the following statement audits the Oracle-defined privileged user `SYS` and site defined privileged user `SITEADMIN`:

```
AUDIT POLICY ORA_ALL_TOPLEVEL_ACTIONS BY SYS, SITEADMIN;
```

29.4.6.3 Logon and Logout Predefined Unified Audit Policy

The `ORA_LOGIN_LOGOUT` policy (previously called `ORA_LOGON_FAILURES`) tracks logon and logoff operations.

This policy is required for both the Center for Internet Security (CIS) and Security for Technical Implementation Guides (STIG) requirements. For CIS and STIG compliance, you must ensure that the `ORA_LOGIN_LOGOUT` unified audit policy is enabled for all users.

For new databases, this policy is enabled by default. This policy is not enabled for databases that were upgraded from earlier versions. Note that if you have configured a unified audit policy for `LOGON` statements, then audit records for both direct logins as well as `ALTER SESSION` and `SET CONTAINER` statements are generated.

The following statement shows the `ORA_LOGIN_LOGOUT` unified audit policy definition.

```
ACTIONS LOGON, LOGOFF;
```

> **Note:**
>
> Only user `SYS` can alter or drop this predefined policy.

```
AUDIT POLICY ORA_LOGIN_LOGOUT WHENEVER NOT SUCCESSFUL;
```

29.4.7 ORA_DICTIONARY Sensitive Column Queries Predefined Unified Audit Policy

The `ORA$DICTIONARY_SENS_COL_ACCESS` predefined audit policy audits the sensitive columns in the Oracle Optimizer dictionary tables.

This predefined policy monitors and audits access to sensitive columns in the Oracle Optimizer dictionary tables. When enabled, this policy writes an audit record whenever the sensitive columns in oracle optimizer dictionary tables gets accessed. If disabled, then this policy does not audit access to these tables. If these tables are frequently accessed, then auditing actions can create too many audit records, which causes performance problems.

These tables are as follows:

Optimizer Dictionary Table	Columns
SYS.HIST_HEAD$	minimum, maximum, lowval, hival
SYS.HISTGRM$	endpoint, epvalue_raw
SYS.WRI$_OPTSTAT_HISTHEAD_HISTORY	minimum, maximum, lowval, hival
SYS.WRI$_OPSTAT_HISTGRM_HISTORY	endpoint, epvalue_raw

This policy cannot be dropped; it can only been enabled or disabled. By default, it is enabled.

29.4.8 Oracle Database Real Application Security Predefined Audit Policies

You can use predefined unified audit policies for Oracle Database Real Application Security events.

- System Administrator Operations Predefined Unified Audit Policy
  The `ORA_RAS_POLICY_MGMT` predefined unified audit policy audits policies for all Oracle Real Application Security administrative actions on application users, roles, and policies.
- Session Operations Predefined Unified Audit Policy
  The `ORA_RAS_SESSION_MGMT` predefined unified audit policy audits policies for all run-time Oracle Real Application Security session actions and namespace actions.

Related Topics

- Auditing Oracle Database Real Application Security Events
  You can use `CREATE AUDIT POLICY` statement to audit Oracle Database Real Application Security events.

29.4.8.1 System Administrator Operations Predefined Unified Audit Policy

The `ORA_RAS_POLICY_MGMT` predefined unified audit policy audits policies for all Oracle Real Application Security administrative actions on application users, roles, and policies.

> **Note:**
>
> Only user `SYS` can alter or drop this predefined policy.

The following statement describes the `ORA_RAS_POLICY_MGMT` audit policy. By default, this policy is not enabled.

```
ACTIONS COMPONENT=XS
  CREATE USER, UPDATE USER, DELETE USER,
  CREATE ROLE, UPDATE ROLE, DELETE ROLE, GRANT ROLE, REVOKE ROLE,
  ADD PROXY, REMOVE PROXY,
  SET USER PASSWORD, SET USER VERIFIER, SET USER PROFILE,
  CREATE ROLESET, UPDATE ROLESET, DELETE ROLESET,
  CREATE SECURITY CLASS, UPDATE SECURITY CLASS, DELETE SECURITY CLASS,
  CREATE NAMESPACE TEMPLATE, UPDATE NAMESPACE TEMPLATE, DELETE NAMESPACE
TEMPLATE,
  CREATE ACL, UPDATE ACL, DELETE ACL,
  CREATE DATA SECURITY, UPDATE DATA SECURITY, DELETE DATA SECURITY,
  ENABLE DATA SECURITY, DISABLE DATA SECURITY,
  ADD GLOBAL CALLBACK, DELETE GLOBAL CALLBACK, ENABLE GLOBAL CALLBACK;
```

For STIG compliance, enable the `ORA_RAS_POLICY_MGMT` unified audit policy for all users.

```
AUDIT POLICY ORA_RAS_POLICY_MGMT;
```

29.4.8.2 Session Operations Predefined Unified Audit Policy

The `ORA_RAS_SESSION_MGMT` predefined unified audit policy audits policies for all run-time Oracle Real Application Security session actions and namespace actions.

> **Note:**
>
> Only user `SYS` can alter or drop this predefined policy.

The following statement describes the ORA_RAS_SESSION_MGMT policy. By default, this policy is not enabled.

```
CREATE AUDIT POLICY ORA_RAS_SESSION_MGMT
 ACTIONS COMPONENT=XS
  CREATE SESSION, DESTROY SESSION,
  ENABLE ROLE, DISABLE ROLE,
  SET COOKIE, SET INACTIVE TIMEOUT,
  SWITCH USER, ASSIGN USER,
  CREATE SESSION NAMESPACE, DELETE SESSION NAMESPACE,
  CREATE NAMESPACE ATTRIBUTE, GET NAMESPACE ATTRIBUTE, SET NAMESPACE
ATTRIBUTE,
  DELETE NAMESPACE ATTRIBUTE;
```

For STIG compliance, enable the ORA_RAS_SESSION_MGMT for failed operations.

```
AUDIT POLICY ORA_RAS_SESSION_MGMT WHENEVER NOT SUCCESSFUL;
```

29.4.9 Oracle Database Vault Predefined Unified Audit Policy for DVSYS and LBACSYS Schemas

The ORA_DV_SCHEMA_CHANGES (previously called ORA_DV_AUDPOL) predefined unified audit policy audits Oracle Database Vault DVSYS and LBACSYS schema objects.

The ORA_DV_SCHEMA_CHANGES policy audits all actions that are performed on the Oracle Database Vault DVSYS (including DVF) schema objects and the Oracle Label Security LBACSYS schema objects. It does not capture actions on the F$* factor functions in the DVF schema. By default, this policy is enabled.

> **Note:**
>
> Only user SYS can alter or drop this predefined policy.

To view the complete definition of this policy, query the AUDIT_UNIFIED_POLICIES data dictionary view, where policy_name is ORA_DV_SCHEMA_CHANGES.

Related Topics

- Auditing Oracle Database Vault Events
  In an Oracle Database Vault environment, the CREATE AUDIT POLICY statement can audit Database Vault activities.

29.4.10 Oracle Database Vault Predefined Unified Audit Policy for Default Realms and Command Rules

The ORA_DV_DEFAULT_PROTECTION (previously called ORA_DV_AUDPOL2) predefined unified audit policy audits the Oracle Database Vault default realms and command rules.

The ORA_DV_DEFAULT_PROTECTION policy constitutes the audit settings of the Oracle Database Vault-supplied default realms and command rules. By default, this policy is enabled.

> **Note:**
>
> Only user SYS can alter or drop this predefined policy.

To view the complete definition of this policy, query the AUDIT_UNIFIED_POLICIES data dictionary view, where policy_name is ORA_DV_DEFAULT_PROTECTION.

Related Topics

- Auditing Oracle Database Vault Events
  In an Oracle Database Vault environment, the CREATE AUDIT POLICY statement can audit Database Vault activities.

29.4.11 Oracle Label Security Predefined Unified Audit Policy for LBACSYS Objects

The ORA_OLS_SCHEMA_CHANGES predefined unified audit policy audits objects that are owned by the Oracle Label Security LBACSYS user.

You can use this audit policy if Oracle Database Vault is not in use. You do not need to enable this policy if the ORA_DV_SCHEMA_CHANGES predefined unified audit policy is already enabled. Uninstallation of Oracle Database Vault will drop ORA_DV_SCHEMA_CHANGES. To ensure that the LBACSYS schema objects are still audited, ORA_OLS_SCHEMA_CHANGES will be enabled during uninstallation of Oracle Database Vault if ORA_DV_SCHEMA_CHANGES was enabled.

> **Note:**
>
> Only user SYS can alter or drop this predefined policy.

To view the complete definition of this policy, query the AUDIT_UNIFIED_POLICIES data dictionary view, where policy_name is ORA_OLS_SCHEMA_CHANGES.

Related Topics

- Auditing Oracle Label Security Events
  In an Oracle Label Security environment, the CREATE AUDIT POLICY statement can audit Oracle Label Security activities.

29.5 Steps to Provision Unified Audit Policies

Apart from mandatorily audited activities and predefined unified audit policies enabled by default in the Oracle database, you may need to provision additional unified audit policies based on your security and compliance needs.

- Auditing Most Commonly Used Security-Relevant Activities
  Oracle Database provides a set of predefined unified audit policies that you can choose from for the most common security-relevant activities.

- Auditing SQL Statements, Privileges, and Other Activities of Interest
  You can create custom audit policies to track access to certain objects, actions or use of privileges, or use of Oracle Database components, such as Oracle Label Security. You can conditionally enable them to reduce audit volume.
- Value-Based Fine-Grained Audit Activities
  Use fine-grained auditing if you want to perform value-based auditing to audit access to certain rows based on values in specific columns or if you want to integrate with event handlers within the Oracle database.

29.5.1 Auditing Most Commonly Used Security-Relevant Activities

Oracle Database provides a set of predefined unified audit policies that you can choose from for the most common security-relevant activities.

Follow these steps to enable the predefined unified audit policies:

1. Select from one of the predefined unified audit policies. You can perform the following query to find a list of these policies:

   ```
   SELECT DISTINCT POLICY_NAME FROM AUDIT_UNIFIED_POLICIES WHERE
   ORACLE_SUPPLIED = 'YES';
   ```

2. Use the `AUDIT` statement to enable the policy and optionally apply (or exclude) the audit settings to one or more users.
3. Query the `UNIFIED_AUDIT_TRAIL` data dictionary view to find the generated audit records.
4. Periodically archive and purge the contents of the audit trail.

Related Topics

- Auditing Activities with the Predefined Unified Audit Policies
  Oracle Database provides predefined unified audit policies that cover commonly used security-relevant audit settings.
- Enabling and Applying Unified Audit Policies to Users and Roles
  You can use the `AUDIT POLICY` statement to enable and apply unified audit policies to users and roles.
- Purging Audit Trail Records
  The `DBMS_AUDIT_MGMT` PL/SQL package can schedule automatic purge jobs, manually purge audit records, and perform other audit trail operations.

29.5.2 Auditing SQL Statements, Privileges, and Other Activities of Interest

You can create custom audit policies to track access to certain objects, actions or use of privileges, or use of Oracle Database components, such as Oracle Label Security. You can conditionally enable them to reduce audit volume.

Follow these steps to create and enable the custom unified audit policies:

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.
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.

3. Query the `UNIFIED_AUDIT_TRAIL` view to find the generated audit records.
4. Periodically archive and purge the contents of the audit trail.

Related Topics

- Creating Custom Unified Audit Policies
  Oracle Database provides the flexibility to create and manage custom unified audit policies for your specialized needs.
- Configuring Application Context Audit Settings
  The `AUDIT` statement with the `CONTEXT` keyword configures auditing for application context values.
- Unified Audit Policy Data Dictionary Views
  You can query data dictionary and dynamic views to find detailed auditing information about custom unified audit policies.
- Purging Audit Trail Records
  The `DBMS_AUDIT_MGMT` PL/SQL package can schedule automatic purge jobs, manually purge audit records, and perform other audit trail operations.

29.5.3 Value-Based Fine-Grained Audit Activities

Use fine-grained auditing if you want to perform value-based auditing to audit access to certain rows based on values in specific columns or if you want to integrate with event handlers within the Oracle database.

Follow these steps to create and enable fine-grained audit policies:

1. Create a fine-grained auditing policy.
2. Use the `DBMS_FGA` PL/SQL package to configure fine-grained auditing policies.
3. Query the `UNIFIED_AUDIT_TRAIL` or `ALL_AUDIT_POLICIES` view to find the generated audit records.
4. Periodically archive and purge the contents of the audit trail.

Related Topics

- Value-Based Auditing with Fine-Grained Audit Policies
  Fine-grained auditing enables you to perform value-based auditing to audit access to certain rows based on values in specific columns.
- Purging Audit Trail Records
  The `DBMS_AUDIT_MGMT` PL/SQL package can schedule automatic purge jobs, manually purge audit records, and perform other audit trail operations.

29.6 Common Audit Configurations Across All PDBs

A common audit configuration is visible and enforced across all PDBs.

Audit configurations are either local or common. The scoping rules that apply to other local or common phenomena, such as users and roles, all apply to audit configurations.

> **Note:**
>
> Audit initialization parameters exist at the CDB level and not in each PDB.

PDBs support the following auditing options:

- Object auditing

  Object auditing refers to audit configurations for specific objects. Only common objects can be part of the common audit configuration. A local audit configuration cannot contain common objects.

- Audit policies

  Audit policies can be local or common:

  – Local audit policies

    A local audit policy applies to a single PDB. You can enforce local audit policies for local and common users in this PDB only. Attempts to enforce local audit policies across all containers result in an error.

    In all cases, enforcing of a local audit policy is part of the local auditing framework.

  – Common audit policies

    A common audit policy applies to all containers. When you create a common audit policy, prefix the name with `C##` or `c##` (for example, `c##all_select_pol`). This policy can only contain actions, system privileges, common roles, and common objects. You can apply a common audit policy only to common users. Attempts to enforce a common audit policy for a local user across all containers result in an error.

A common audit configuration is stored in the `SYS` schema of the root. A local audit configuration is stored in the `SYS` schema of the PDB to which it applies.

Audit trails are stored in the `SYS` or `AUDSYS` schemas of the relevant CDB or PDB container. Operating system and XML audit trails for PDBs are stored in subdirectories of the directory specified by the `AUDIT_FILE_DEST` (deprecated) initialization parameter.

29.7 General Audit Data Dictionary Views

Oracle Database provides different types of data dictionary and dynamic views for use with unified auditing.

Table 30-20 lists views that are common to all types of auditing.

> **Tip:**
>
> To find error information about audit policies, check the trace files. The `USER_DUMP_DEST` initialization parameter sets the location of the trace files.

Table 29-1 General Audit Data Dictionary Views

View	Description
`AUDIT_UNIFIED_ENABLED_POLICIES`	Describes the conditions on which an audit policy is enabled, such as audits for the success or failure of a user's action that is being monitored in a policy
`AUDIT_UNIFIED_POLICIES`	Describes the action that was intended to be audited by the audit policy
`CDB_UNIFIED_AUDIT_TRAIL`	Similar to the `UNIFIED_AUDIT_TRAIL` view, displays the audit records but from all PDBs in a multitenant environment. This view is available only in the CDB root and must be queried from there.

Table 29-1 (Cont.) General Audit Data Dictionary Views

View	Description
UNIFIED_AUDIT_TRAIL	Displays all audit records
V$OPTION	The PARAMETER column for this view always returns TRUE, which indicates that unified auditing is enabled.
V$XML_AUDIT_TRAIL	Displays standard, fine-grained, SYS, and mandatory audit records written in XML format files.

Related Topics

- *Oracle Database Reference*