Oracle® Audit Vault

Auditor's Guide

Release 10.2.3

E11058-03

September 2008

Beta Draft

Oracle Audit Vault Auditor’s Guide, Release 10.2.3

E11058-03

Primary Author: Patricia Huey

Contributing Author: Rodney Ward

Contributors: Tammy Bednar, Janet Blowney, Raghavendran Hanumantharau, K. Karun, Donna Keesling, Vipul Shah, Prahlada Varadan Thirumalai, Lok Sheung, Andrew Wang

Contents

3 Using Oracle Audit Vault Reports

4 Oracle Audit Vault Data Warehouse Schema

A Oracle Database Audit Events

B Microsoft SQL Server Audit Events

C Sybase Adaptive Server Enterprise Audit Events

D IBM DB2 Audit Events

Index

List of Figures

List of Tables

Preface

Oracle Audit Vault Auditor's Guide explains how Oracle Audit Vault auditors can use the Audit Vault Console to audit data in Oracle, Microsoft SQL Server, and Sybase Adaptive Server Enterprise databases. This guide accompanies Beta Patch Release 10.2.3.0.1.

Audience

This document is intended for users who have been granted the `AV_AUDITOR` role and who are responsible for performing auditing tasks.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at `http://www.oracle.com/accessibility/`.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, 7 days a week. For TTY support, call 800.446.2398. Outside the United States, call +1.407.458.2479.

Related Documents

For more information about Audit Vault, see the following documents:

- *Oracle Audit Vault Administrator's Guide*
- *Oracle Audit Vault Developer's Guide*
- *Oracle Database Vault Administrator's Guide*
- *Oracle Database Security Guide*
- *Oracle Database Advanced Security Administrator's Guide*
- *Oracle Database Reference*
- *Oracle Streams Concepts and Administration*
- *Oracle Database Data Warehousing Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Introducing Oracle Audit Vault for Auditors

This chapter contains:

- How Do Auditors Use Oracle Audit Vault?
- General Steps for Using Oracle Audit Vault
- Database Requirements for Collecting Audit Data
- Starting the Oracle Audit Vault Console
- Ensuring That the Oracle Audit Vault Collectors Can Collect Data

1.1 How Do Auditors Use Oracle Audit Vault?

Oracle Audit Vault collects audit data from multiple databases and then consolidates this data in a set of audit reports. You can collect audit data from multiple instances of the following database products:

- Oracle Database (including Oracle Real Application Clusters and Oracle Data Guard)
- Microsoft SQL Server
- Sybase Adaptive Server Enterprise (ASE)
- IBM DB2

Before you, as an auditor, can use Oracle Audit Vault, an administrator must configure the Audit Vault Server to connect to your source databases. Oracle Audit Vault then collects the audit data that these databases generate, organizes the data, and provides it to you in a variety of reports. For Oracle databases, you can create policies and collect data from redo log files. For all four database products, you can create alerts. In addition to the Oracle Audit Vault reports, you can design reports using another tool, such as Oracle Business Intelligence, or with third-party products. To manage Oracle Audit Vault policies, alerts, and reports, you use the Audit Vault Console.

The Oracle Audit Vault default reports are designed to satisfy standard compliance regulations, such as those mandated by the Sarbanes-Oxley Act. You can create user-defined versions of these reports for specific needs. For example, you can create reports to track activities that occur outside of normal office hours, or to track the activities of specific users.

The policies and alerts features help you to detect security threats to an Oracle database. For example, an alert can notify you when a system administrator tries to view sensitive application data, such as employee salaries.

Because Oracle Audit Vault centralizes audit settings, your job as an auditor is easier and more efficient. You can create, manage, and monitor audit information from one location. This also makes it easier to demonstrate the compliance policy of your company to outside auditors.

The audit data collected by Oracle Audit Vault is stored in its own secure data warehouse repository, where an administrator can use Oracle Database Vault and Oracle Advanced Security to prevent tampering of the audit data.

1.2 General Steps for Using Oracle Audit Vault

To use Oracle Audit Vault, follow these general steps:

- Step 1: Ensure That the Source Databases Are Collecting Audit Data
- Step 2: Create Audit Policies for Oracle Database Data
- Step 3: Optionally, Create and Monitor Alerts
- Step 4: View and Customize the Oracle Audit Vault Reports

1.2.1 Step 1: Ensure That the Source Databases Are Collecting Audit Data

Check that the databases from which you want to collect audit data have auditing enabled and that the Oracle Audit Vault collectors are working. Because database administrators sometimes disable auditing for performance reasons, you cannot assume that auditing is enabled. For Oracle Database, there are recommended audit settings that your database administrator should consider having in place. Your database administrator also should ensure that these databases are properly configured to send audit data to the Audit Vault Server.

See Section 1.3 and Section 1.5 for more information.

1.2.2 Step 2: Create Audit Policies for Oracle Database Data

You use the Audit Vault Console to manage audit policies for Oracle Database source databases. Section 1.4 explains how to start the Audit Vault Console.

You can create policies for the following kinds of data:

- **SQL statements.** For example, you can audit statements that users use when attempting to query the database or modify data, such as `SELECT` or `UPDATE`.
- **Database Schema Objects.** You can audit actions that users may try to perform on database objects, tables, or views.
- **Database Privileges.** You can audit the use of a system privilege, such as `SELECT ANY TABLE`. In this kind of auditing, SQL statements that require the audited privilege to succeed are recorded.
- **Fine-grained audit conditions.** You can audit specific activities that take place in the database, such as whether an IP address from outside the corporate network is being used, or if specific table columns are being modified.
- **Redo log data.** You can capture data from redo log files. The redo log files store all changes that occur in the database. Every instance of an Oracle database has an associated redo log to protect the database in case of an instance failure. In Oracle Audit Vault, the capture rule specifies DML and DDL changes that should be checked when Oracle Database scans the database redo log.

For SQL statements, objects, privileges, and fine-grained auditing data, you create audit policies. For redo log data, you create a capture rule.

Chapter 2, " Creating Oracle Audit Vault Policies and Alerts" describes how to create audit policies and capture rules.

1.2.3 Step 3: Optionally, Create and Monitor Alerts

Optionally, you can create either warning or critical alerts that are triggered when certain events occur in an Oracle Database, SQL Server, Sybase ASE, or IBM DB2 database. Oracle Audit Vault alerts enable you to detect threats, which helps in keeping systems in compliance with internal and external policies. After you create the alerts, you can monitor them in the Audit Vault Console.

Section 2.12 explains how you can create and monitor alerts.

1.2.4 Step 4: View and Customize the Oracle Audit Vault Reports

Oracle Audit Vault automatically populates its reports with the audit and redo log file data from your source databases. You can view this data by selecting from the reports provided in the Audit Vault Console Default Reports and User-Defined Reports pages. The reports are organized by commonly used categories, including categories for compliance regulations. In the Audit Vault Console, you can create user-defined reports to filter specific data if you want.

Oracle Audit Vault has an open data warehouse schema, which you can use to build custom reports using Oracle Application Express, business intelligence tools such as Oracle Business Intelligence Publisher, or third-party business intelligence tools.

Chapter 3, "Using Oracle Audit Vault Reports" explains how to view and customize Oracle Audit Vault reports.

1.3 Database Requirements for Collecting Audit Data

This section contains:

- Requirements for Oracle Database
- Requirements for SQL Server, Sybase ASE, and IBM DB2 Databases

1.3.1 Requirements for Oracle Database

This section contains:

- Ensuring That Auditing Is Enabled in the Source Database
- Using Recommended Audit Settings in the Source Database

1.3.1.1 Ensuring That Auditing Is Enabled in the Source Database

Before Oracle Audit Vault can collect audit data from the source databases, auditing must be enabled in those databases. In Oracle Database, a database administrator can check if auditing has been enabled by using either of the following methods:

- **Ensuring that standard auditing is enabled.** Log in to SQL*Plus with administrative privileges and then check the value of the AUDIT_TRAIL initialization parameter, which enables or disables auditing.

  For example:

  ```
  sqlplus SYSTEM
  Enter password: password
  Connected.
  ```

```
SQL> SHOW PARAMETER AUDIT_TRAIL

NAME                   TYPE        VALUE
---------------------- ----------- -----------
audit_trail            string      NONE
```

This example shows that the AUDIT_TRAIL parameter has been set to the NONE setting. If the AUDIT_TRAIL parameter has been set to NONE and if the database is not using fine-grained auditing, then auditing cannot occur. A database administrator with the SYSDBA privilege can enable standard auditing, and then an administrator with the SYSOPER privilege can restart the database.

For example, to set AUDIT_TRAIL to DB (which enables auditing and sends audit data to the SYS.AUD$ system table) and then restart the database, log in to SQL*Plus and enter the following:

```
SQL> CONNECT SYS/AS SYSDBA
Enter password: password
Connected.

SQL> ALTER SYSTEM SET AUDIT_TRAIL=DB SCOPE=SPFILE;
System altered.

SQL> CONNECT SYS/AS SYSOPER
Enter password: password
Connected.
SQL> SHUTDOWN
Database closed.
Database dismounted.
SQL> STARTUP
ORACLE instance started.
```

- **Ensuring that fine-grained auditing is enabled.** If the database is using fine-grained auditing, then the AUDIT_TRAIL parameter does not need to be set. In fine-grained auditing, you create the auditing policy in a PL/SQL package. You can ensure that fine-grained auditing is enabled by querying the V$OPTION table in the source database. Remember that the parameter value (in this case, Fine-grained Auditing) that you specify with V$OPTION is case-sensitive.

  For example:

```
SQL> SELECT * FROM V$OPTION WHERE PARAMETER = 'Fine-grained Auditing';

PARAMETER               VALUE
----------------------- ---------
Fine-grained Auditing   TRUE
```

  This example shows that fine-grained auditing is enabled. If the query returns FALSE, then ask the Oracle Database security administrator to enable and configure the necessary fine-grained auditing in this database.

  You can check if any fine-grained audit records have been created by asking an administrator to run the following query:

```
SQL> SELECT COUNT(*) FROM DBA_FGA_AUDIT_TRAIL;

  COUNT(*)
----------
       212
```

  This example shows that 212 fine-grained audit records have been created.

1.3.1.2 Using Recommended Audit Settings in the Source Database

After your database administrator checks that auditing is enabled, Oracle recommends that the following areas of the database have auditing enabled:

- **Database schema or structure changes.** Use the following `AUDIT` SQL statement settings.
  - `AUDIT ALTER ANY TABLE BY ACCESS;`
  - `AUDIT CREATE ANY TABLE BY ACCESS;`
  - `AUDIT DROP ANY TABLE BY ACCESS;`
  - `AUDIT CREATE ANY PROCEDURE BY ACCESS;`
  - `AUDIT DROP ANY PROCEDURE BY ACCESS;`
  - `AUDIT ALTER ANY PROCEDURE BY ACCESS;`
  - `AUDIT CREATE EXTERNAL JOB BY ACCESS;`
  - `AUDIT CREATE ANY JOB BY ACCESS;`
  - `AUDIT CREATE ANY LIBRARY BY ACCESS;`
  - `AUDIT ALTER DATABASE BY ACCESS;`
  - `AUDIT ALTER SYSTEM BY ACCESS;`
- **Database access and privileges.** Use the following `AUDIT` SQL statements:
  - `AUDIT AUDIT SYSTEM BY ACCESS;`
  - `AUDIT CREATE PUBLIC DATABASE LINK BY ACCESS;`
  - `AUDIT EXEMPT ACCESS POLICY BY ACCESS;`
  - `AUDIT ALTER USER BY ACCESS;`
  - `AUDIT CREATE USER BY ACCESS;`
  - `AUDIT ROLE BY ACCESS;`
  - `AUDIT CREATE SESSION BY ACCESS;`
  - `AUDIT DROP USER BY ACCESS;`
  - `AUDIT GRANT ANY PRIVILEGE BY ACCESS;`
  - `AUDIT GRANT ANY OBJECT PRIVILEGE BY ACCESS;`
  - `AUDIT GRANT ANY ROLE BY ACCESS;`
  - `AUDIT ALTER PROFILE BY ACCESS;`
  - `AUDIT DROP PROFILE BY ACCESS;`

1.3.2 Requirements for SQL Server, Sybase ASE, and IBM DB2 Databases

Ensure that auditing is enabled in these databases. You also should ensure that they are correctly configured to send audit data to the Audit Vault Server. For more information, check the documentation for these three products and*Oracle Audit Vault Administrator's Guide*.

1.4 Starting the Oracle Audit Vault Console

To start the Audit Vault Console:

1. From a browser, enter the following URL:

   ```
   http://host:port/av
   ```

   In this specification:

   - *host* is the server where you installed Oracle Audit Vault
   - *port* is the Audit Vault Console HTTP port number

   For example:

   ```
   http://123.456.78.9:5700/av
   ```

   If you are unsure of the URL, from the terminal window that you use for the Audit Vault Server, enter the following command to display the URL you should use to start the Audit Vault Console:

   ```
   avctl show_av_status
   ```

2. In the Login page, enter your user name and password. From the **Connect As** list, select **AV_AUDITOR**. Then click **Login**.

   The Home page appears and displays information about configured alerts and audit trail activity. From here, you can do the following:

   - **Ensure that the Oracle Audit Vault collection agents are working.** Section 1.5 explains how to ensure that these agents are collecting audit data.
   - **Create Oracle Database audit policies and alerts.** Chapter 2, " Creating Oracle Audit Vault Policies and Alerts" explains how to create policies and alerts for an Oracle database.
   - **Access audit reports.** You can view audit information that has been collected in the Oracle Audit Vault reports. Optionally, you can control the display of data and create user-defined reports. See Chapter 3, "Using Oracle Audit Vault Reports" for more information.

1.5 Ensuring That the Oracle Audit Vault Collectors Can Collect Data

The Oracle Audit Vault collection agents are responsible for the connection between the source database and the Audit Vault Server. In the Audit Vault Console, you can check the status of the collection agents. If you cannot access Oracle Database audit policies, or if the Oracle Audit Vault default reports do not show any information, then the collection agents may not be working, or the source database has been shut down.

To check the status of the source database collection agents:

1. Log in to the Audit Vault Console as a user who has been granted the `AV_AUDITOR` role.

   Section 1.4 explains how to log in to the Audit Vault Console.

2. Click the **Audit Status** tab.

The Audit Status page shows the following information

- **Collector**. Name of the collector
- **Agent**. The name of the agent with which this collector is associated

- **Audit Source**. The name of the audit data source where the audit data is being collected
- **Status**. Whether the collector is running or not. When the collector is up, a green up arrow indicator is displayed. When the collector is down, a red down arrow indicator is displayed. When there is a problem, an error is displayed. If the collector is not working, then contact your Oracle Audit Vault administrator.

Table 1–1 summarizes the database collector types.

Table 1–1 Database Collector Types Provided by Oracle Audit Vault

Database	Collectors	Description
Oracle	DBAUD	Collector that performs the following: ■ Extracts audit records from the Oracle Database audit trail, where standard audit events are written to the `SYS.AUD$` dictionary table; and the fine-grained audit trail, where audit events are written to the `SYS.FGA_LOG$` dictionary table ■ Extracts audit records from the Oracle Database Vault audit trail `DVSYS.AUDIT_TRAIL$` table
Oracle	OSAUD	Collector that performs the following: ■ **For Linux and UNIX platforms:** extracts audit records from the operating system files (audit logs) (`SYS$AUD` (`.aud`) and XML (`.xml`) files) ■ **For Linux and UNIX platforms:** SYSLOG Collector to extract audit records from the system audit trail where database audit trail records are written to a syslog file ■ **For Microsoft Windows:** EVTLOG Collector to extract audit records from the system audit trail where database audit trail records are written to the Event Log
Oracle	REDO	Collector using Oracle Streams technology to retrieve logical change records from the redo logs.
SQL Server	MSSQLDB	Collector (for Windows platforms) to extract audit records from Microsoft SQL Server databases from the Windows Event logs, Server-side trace files, and C2 auditing logs.
Sybase ASE	SYBDB	Collector to extract audit records from the Sybase databases audit trail logged in audit tables in the `SYBSECURITY` database.
IBM DB2	DB2DB	Collector to extract records from the ASCII text file in which IBM DB2 generates audit data.

2

Creating Oracle Audit Vault Policies and Alerts

This chapter contains:

2.1 About Oracle Audit Vault Policies and Alerts

In the Audit Vault Console, you can create the following types of audit policies for Oracle databases:

- SQL statements
- Schema objects
- Privileges
- Fine-grained auditing
- Capture rules (for redo log file activities)
- Alerts

2.2 General Steps for Creating Oracle Audit Vault Policies and Alerts

In general, to create Oracle Audit Vault policies and alerts, you follow these steps:

1. Fetch the current policy settings from the source Oracle database.

   See Section 2.3 for more information.

2. Create audit policies.

   See the following sections:

   - Section 2.4 to create SQL statement policies
   - Section 2.5 to create schema object policies
   - Section 2.6 to create privilege policies
   - Section 2.7 to create fine-grained auditing policies
   - Section 2.8 to create capture rules for redo log file auditing
   - Section 2.9 to verify the Oracle Audit Vault policies

3. Save the Oracle Audit Vault policy settings to a `.sql` file or manually provision them to the source database.

   See the following sections:

   - Section 2.10 to export the policies to the source Oracle database
   - Section 2.11 to copy the policy settings to other Oracle databases

4. Optionally, create alerts.

   See Section 2.12 for more information.

2.3 Fetching Audit Policy Settings from the Source Oracle Database

Before you create policies and alerts in the Audit Vault Console, you must fetch the current audit settings that have been created in the source Oracle database. This way, you have a snapshot of the audit settings in the source database from that point in time, before you begin to create policies and alerts.

Follow these steps:

- Step 1: Retrieve the Audit Settings from the Source Oracle Database
- Step 2: Activate (Update) the Fetched Audit Settings State

2.3.1 Step 1: Retrieve the Audit Settings from the Source Oracle Database

To retrieve audit settings from the source Oracle Database:

1. Log in to the Audit Vault Console as a user who has been granted the `AV_AUDITOR` role.

   Section 1.4 explains how to start the Audit Vault Console. The Overview page appears.

2. In the Audit Vault Console, select the **Audit Policy** tab.

   By default, the Audit Settings page appears.

3. From the Audit Source listing, select the source database, and then click the **Retrieve from Source** button.

To filter the list of audit sources, enter text in the **Audit Source** text field or click the flashlight icon to display the Search And Select: Audit Source page. If you make selections on the Search And Select: Audit Source page, when you return, the **Audit Source** column will be populated with your selections.

The Audit Vault Console displays a summary of audit settings for the source database.

At this stage, you are ready to view the audit settings. Table 2–1 shows the fields used in the audit settings list in the Audit Settings page, which indicate the state of the source database. If the **Problem** field contains a value higher than 0, then most likely you need to activate (that is, update for use in Oracle Audit Vault) the audit settings. If the **Problem** field is set to 0, then all the existing audit settings already have been activated.

Table 2–1 Fields Under Apply Audit Settings in the Audit Settings Page

Field	Description
Select	Select which audit source to retrieve
Audit Source	Displays the name of the audit source
In Use	Number of active settings in the source database
Needed	Number of audit settings you (the auditor) have specified to be required
Problem	Number of audit settings that require attention by the auditor
Audit Trail	The location to which database audit records are directed, based on the `AUDIT_TRAIL` initialization parameter. See *Oracle Database Reference* for the `AUDIT_TRAIL` parameter values. If the setting is `NONE`, then ask the database administrator to enable auditing. See Section 1.3.1.1 for more information.
Audit Sys	Indicates that the `SYS` user is being audited
Last Retrieved	The time that the information for the selected audit source was last retrieved
Last Provisioned	The time that the settings were provisioned to the source database

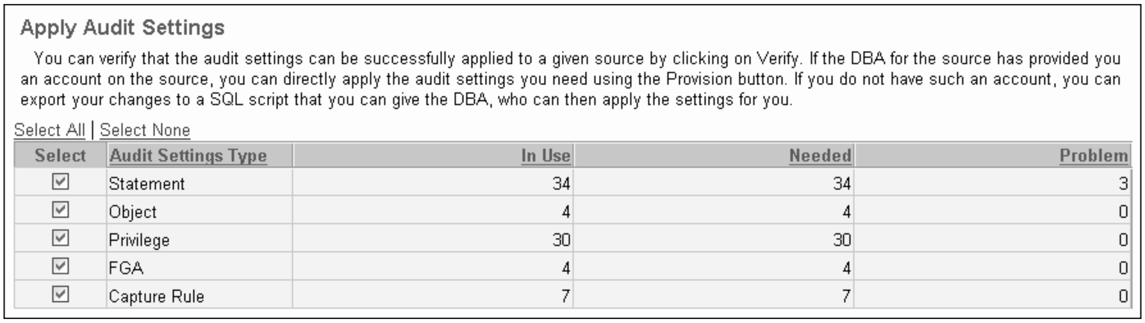
2.3.2 Step 2: Activate (Update) the Fetched Audit Settings State

After you retrieve the source database, you are can view the audit settings so that you can modify them as needed. Remember that you are capturing a snapshot of the audit settings from a particular point in time: if these settings change in the source database, then you must retrieve the audit settings again.

1. In the Audit Settings page, select the name of the source database listed in the Audit Source field.

   The Apply Audit Settings section appears. In the following example, the **Problem** field shows that there are three SQL statement audit settings that may be activated or removed from the source database. None of the other audit settings types need to be activated.

   A nonzero value in the **Problem** field can indicate that an audit policy that was created in the source database has not yet been updated in Oracle Audit Vault. If you do not need the audit policy, then do not activate it. In that case, when you provision the Audit Vault settings back to the source database, this audit policy will be deleted in the source database.



Apply Audit Settings

You can verify that the audit settings can be successfully applied to a given source by clicking on Verify. If the DBA for the source has provided you an account on the source, you can directly apply the audit settings you need using the Provision button. If you do not have such an account, you can export your changes to a SQL script that you can give the DBA, who can then apply the settings for you.

Select	Audit Settings Type	In Use	Needed	Problem
☑	Statement	34	34	3
☑	Object	4	4	0
☑	Privilege	30	30	0
☑	FGA	4	4	0
☑	Capture Rule	7	7	0

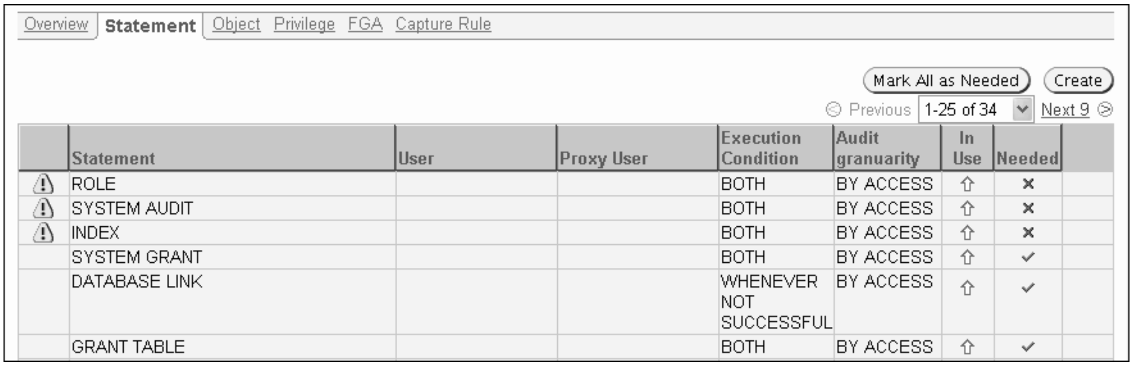
This image shows the Apply Audit Settings region of the Audit Settings page. This region appears only after you select the source database. It shows rows for each of the audit settings types (Statement, Object, Privilege, FGA, and Capture Rule) with these columns:

- In Use: Shows the number of active audit settings in the source database
- Needed: Shows the number of audit settings that an auditor has selected to be activated in Oracle Audit Vault
- Problem: Shows the number audit settings that require attention by the auditor

****

2. To update the statement audit settings, select the **Statement** tab.

   The Statement page appears. The settings that need to be updated are indicated with an **X** in the **Needed** column. As the Audit Vault auditor, you can indicate that the audit policies are required.



	Statement	User	Proxy User	Execution Condition	Audit granuarity	In Use	Needed
⚠	ROLE			BOTH	BY ACCESS	⇧	×
⚠	SYSTEM AUDIT			BOTH	BY ACCESS	⇧	×
⚠	INDEX			BOTH	BY ACCESS	⇧	×
	SYSTEM GRANT			BOTH	BY ACCESS	⇧	✓
	DATABASE LINK			WHENEVER NOT SUCCESSFUL	BY ACCESS	⇧	✓
	GRANT TABLE			BOTH	BY ACCESS	⇧	✓

This image shows the Statement page and table. Table 2–2 describes the fields in the table. Above the table, the window contains buttons to Mark as Needed and Create.

****

3. Select each **X** in the **Needed** column to update the audit settings for SQL statements. Alternatively, click the **Mark All as Needed** button to update the settings for all the SQL statements.

   A check mark indicates that the Oracle Audit Vault auditor has determined that the audit setting is needed. A green up arrow in the **In Use** column indicates that both Oracle Audit Vault and the source database are currently storing consistent definitions of the audit policies. A red X in the **Needed** column indicates that these policy definitions are inconsistent, with Oracle Audit Vault having the outdated version of the policy.

At this stage, the audit settings between the source database and Oracle Audit Vault should be the same, except for any settings that you have omitted in Step 3, or if changes in the audit settings are made independently in the source database.

2.4 Creating Oracle Vault Audit Policies for SQL Statements

This section contains:

- About SQL Statement Auditing
- Defining a SQL Statement Audit Policy

2.4.1 About SQL Statement Auditing

Statement auditing audits SQL statements by type of statement, not by the specific schema objects on which the statement operates. Statement auditing can be broad or focused (or example, by auditing the activities of all database users or of only a select list of users). Typically broad, statement auditing audits the use of several types of related actions for each option. These statements are in the following categories:

- **Data definition statements (DDL).** For example, `AUDIT TABLE` audits all `CREATE TABLE` and `DROP TABLE` statements. `AUDIT TABLE` tracks several DDL statements regardless of the table on which they are issued. You can also set statement auditing to audit selected users or every user in the database.
- **Data manipulation statements (DML).** For example, `AUDIT SELECT TABLE` audits all `SELECT ... FROM TABLE` or `SELECT ... FROM VIEW` statements, regardless of the table or view.

2.4.2 Defining a SQL Statement Audit Policy

To define a SQL statement audit policy:

1. If necessary, retrieve and activate the current statement audit policies.

   See Section 2.3 for more information.

2. In the Audit Settings page, select the **Statement** tab to display the Statement page.

   Table 2–2 on page 2-6 describes the fields used in the Statement page.

3. Click the **Create** button and in the Create Statement Audit page, define the audit policy.

   Table 2–3 on page 2-6 describes the Create Statement Audit fields.

4. Click **OK**.

   The statement audit policy is created. To ensure that the statement audit policy is semantically correct, see Section 2.9.

5. In the Overview page, select **Save All Audit Settings**.

   To display the Overview page, click the **Audit Settings** link, and then in the Audit Settings page, select the name of the source database.

Table 2–2 lists the fields used in the Statement page.

Table 2–2 Fields in the Statement Page

Field	Description
(Leftmost column)	An exclamation mark icon indicates one of the following conditions: - The statement is needed but is not in use. - The statement is in use but is not needed.
Statement	The statement that is audited
User	The user to which this setting applies, if any
Proxy User	The proxy user for the database, if any
Execution Condition	The execution condition audited: `WHENEVER SUCCESSFUL`, `WHENEVER NOT SUCCESSFUL`, or `BOTH`
Audit granularity	The granularity of auditing: `BY ACCESS` or `BY SESSION`
In Use	The arrow points upward if the setting is active in the source database and downward if it has not been provisioned or is not active.
Needed	A check mark indicates that the policy is needed. An **X** indicates that the policy is not needed. If a policy that is not in use is set to needed, the In Use arrow points up after provisioning. If a policy that is in use is set to not needed, the audit policy is no longer displayed after provisioning.
(Rightmost column)	Click the trash can icon to remove the policy. You can use the trash can icon to remove the policy only if you had just created it and decided it was not required in the source database, or if it is not active in the source database.

Table 2–3 lists the fields used in the Create Statement Audit page.

Table 2–3 Fields in the Create Statement Audit Page

Field	Description
Statements	Select the SQL statements to audit. To display a list of SQL statements from which to select, click the flashlight icon. Examples are: - `ALTER TABLE` - `DATABASE LINK` - `DROP DIRECTORY`
Audited By	Choose the category of users to audit: - **All**: Audits all users, including proxy users. - **User**: Audits the user to which this setting applies. When you select this option, the **Users** field appears, in which you must specify at least one user. To display a list of users and their audit sources from which to select, click the flashlight icon. - **Proxy User**: Audits the proxy user for the database. When you select this option, the **Proxy User** field appears, in which you must specify at least one user. To display a list of proxy users and their audit sources from which to select, click the flashlight icon.

Table 2–3 (Cont.) Fields in the Create Statement Audit Page

Field	Description
Statement Execution Condition	Choose the execution condition: ▪ **Both**: Audits both successful and failed statements ▪ **Success**: Audits the statement if it is successful ▪ **Failure**: Audits the statement if it fails
DML Audit Granularity	Choose the level of granularity: ▪ **Access**: Creates an audit record each time the operation occurs ▪ **Session**: Creates an audit record the first time an operation occurs in the current session

2.5 Creating Oracle Audit Vault Policies for Schema Objects

This section contains:

- About Schema Object Auditing
- Defining a Schema Object Audit Policy

2.5.1 About Schema Object Auditing

Schema object auditing is the auditing of specific statements on a particular schema object, such as `AUDIT SELECT ON HR.EMPLOYEES`. Schema object auditing is very focused, auditing only a specific statement on a specific schema object for all users of the database.

For example, object auditing can audit all `SELECT` and DML statements permitted by object privileges, such as `SELECT` or `DELETE` statements on a given table. The `GRANT` and `REVOKE` statements that control those privileges are also audited.

Object auditing lets you audit the use of powerful database commands that enable users to view or delete very sensitive and private data. You can audit statements that reference tables, views, sequences, standalone stored procedures or functions, and packages.

Oracle Database and Oracle Audit Vault always set schema object audit options for all users of the database. You cannot set these options for a specific list of users.

2.5.2 Defining a Schema Object Audit Policy

To define a schema object audit policy:

1. If necessary, retrieve and activate the current object audit policies.

   See Section 2.3 for more information.

2. In the Audit Settings page, select the **Object** tab to display the Object page.

   Table 2–4 on page 2-8 describes the fields used in the Object page.

3. Click the **Create** button and in the Create Object Audit page, define the audit policy.

   Table 2–5 on page 2-9 describes the Create Object Audit fields.

4. Click **OK**.

   The object audit policy is created. To ensure that the object audit policy is semantically correct, see Section 2.9.

5. In the Overview page, select **Save All Audit Settings**.

   To display the Overview page, click the **Audit Settings** link, and then in the Audit Settings page, select the name of the source database.

Table 2–4 lists the fields used in the Object page.

Table 2–4 Fields in the Object Page

Field	Description
(Leftmost column)	An exclamation mark icon indicates one of the following conditions: ■ The statement is needed but is not in use. ■ The statement is in use but is not needed.

Table 2–4 (Cont.) Fields in the Object Page

Field	Description
Statement	The statement that is audited
Schema	The database schema to which this setting applies
Object	The object to which this setting applies
Execution Condition	The execution condition audited: `WHENEVER SUCCESSFUL`, `WHENEVER NOT SUCCESSFUL`, or `BOTH`
Audit granularity	The granularity of auditing: `BY ACCESS` or `BY SESSION`
In Use	The arrow points upward if the setting is active in the source database and downward if it has not been provisioned or is not active.
Needed	A check mark indicates that the policy is needed. An **X** indicates that the policy is not needed. If a policy that is not in use is set to needed, the In Use arrow points up after provisioning. If a policy that is in use is set to not needed, the audit policy is no longer displayed after provisioning.
(Rightmost column)	Click the trash can icon to remove the policy. You can use the trash can icon to remove the policy only if you had just created it and decided it was not required in the source database, or if it is not active in the source database.

Table 2–5 lists the fields used in the Create Object Audit page.

Table 2–5 Fields in the Create Object Audit Page

Field	Description
Statements	Select the SQL statements to audit. To display a list of SQL statements from which to select, click the flashlight icon. Examples are: ■ `ALTER` ■ `AUDIT` ■ `UPDATE`
Object Type	Select the type of object to audit, such as table. To display a list of object types and their audit sources from which to select, click the flashlight icon. Examples are: ■ `LOB` ■ `RULE` ■ `VIEW`
Object	Optional. Select the object to audit. To display a list of objects and their source databases from which to select, and to filter the list by audit source and object owner, click the flashlight icon. For example, if you entered `TABLE` for the **Object Type** field, you could select `EMPLOYEES`, `JOBS`, or any of the other tables in the `HR` schema.
Statement Execution Condition	Choose the execution condition: ■ **Both**: Audits both successful and failed statements ■ **Success**: Audits the statement if it is successful ■ **Failure**: Audits the statement if it fails

Table 2–5 (Cont.) Fields in the Create Object Audit Page

Field	Description
DML Audit Granularity	Choose the level of granularity: ■ **Access**: Creates an audit record each time the operation occurs ■ **Session**: Creates an audit record the first time an operation occurs in the current session

2.6 Creating Oracle Audit Vault Policies for Privileges

This section contains:

- About Privilege Auditing
- Defining a Privilege Audit Policy

2.6.1 About Privilege Auditing

Privilege auditing is the auditing of SQL statements that use a system privilege. You can audit the use of any system privilege. Like statement auditing, privilege auditing can audit the activities of all database users or of only a specified list of users.

For example, if you enable `AUDIT SELECT ANY TABLE`, Oracle Database audits all `SELECT` *`tablename`* statements issued by users who have the `SELECT ANY TABLE` privilege. This type of auditing is very important for the Sarbanes-Oxley (SOX) Act compliance requirements. Sarbanes-Oxley and other compliance regulations require the privileged user be audited for inappropriate data changes or fraudulent changes to records.

Privilege auditing audits the use of powerful system privileges enabling corresponding actions, such as `AUDIT CREATE TABLE`. If you set both similar statement and privilege audit options, then only a single audit record is generated.

For example, if the statement clause `TABLE` and the system privilege `CREATE TABLE` are both audited, then only a single audit record is generated each time a table is created. The statement auditing clause, `TABLE`, audits `CREATE TABLE`, `ALTER TABLE`, and `DROP TABLE` statements. However, the privilege auditing option, `CREATE TABLE`, audits only `CREATE TABLE` statements, because only the `CREATE TABLE` statement requires the `CREATE TABLE` privilege.

Privilege auditing does not occur if the action is already permitted by the existing owner and schema object privileges. Privilege auditing is triggered only if these privileges are insufficient, that is, only if what makes the action possible is a system privilege.

Privilege auditing is more focused than statement auditing for the following reasons:

- It audits only a specific type of SQL statement, not a related list of statements.
- It audits only the use of the target privilege.

2.6.2 Defining a Privilege Audit Policy

To define a privilege audit policy:

1. If necessary, retrieve and activate the current privilege audit policies.

   See Section 2.3 for more information.

2. In the Audit Settings page, select the **Privilege** tab to display the Privilege page.

Table 2–6 on page 2-11 describes the fields used in the Privilege page.

3. Click the **Create** button and in the Create Privilege Audit page, define the privilege audit policy.

   Table 2–7 on page 2-11 describes the Create Privilege Audit fields.

4. Click **OK**.

   The privilege audit policy is created. To ensure that the privilege audit policy is semantically correct, see Section 2.9.

5. In the Overview page, select **Save All Audit Settings**.

   To display the Overview page, click the **Audit Settings** link, and then in the Audit Settings page, select the name of the source database.

Table 2–6 lists the fields used in the Privilege page.

Table 2–6 Fields in the Privilege Page

Field	Description
(Leftmost column)	An exclamation mark icon indicates one of the following conditions: ■ The statement is needed but is not in use. ■ The statement is in use but is not needed.
Privilege	The privilege that is audited
User	The user to which this setting applies
Proxy User	The proxy user for the database, if any
Execution Condition	The execution condition audited: `WHENEVER SUCCESSFUL`, `WHENEVER NOT SUCCESSFUL`, or `BOTH`
Audit granularity	The granularity of auditing: `BY ACCESS` or `BY SESSION`
In Use	The arrow points upward if the setting is active in the source database and downward if it has not been provisioned or is not active.
Needed	A check mark indicates that the policy is needed. An **X** indicates that the policy is not needed. If a policy that is not in use is set to needed, the In Use arrow points up after provisioning. If a policy that is in use is set to not needed, the audit policy is no longer displayed after provisioning.
(Rightmost column)	Click the trash can icon to remove the policy. You can use the trash can icon to remove the policy only if you had just created it and decided it was not required in the source database, or if it is not active in the source database.

Table 2–7 lists the fields used in the Create Privilege Audit page.

Table 2–7 Fields in the Create Privilege Audit Page

Field	Description
Privilege	Select the privilege to audit. To display a list of privileges from which to select, click the flashlight icon. Examples are: ■ `ADMINISTER DATABASE TRIGGER` ■ `CREATE ANY TABLE` ■ `MANAGE TABLESPACE`

Table 2–7 (Cont.) Fields in the Create Privilege Audit Page

Field	Description
Audited By	Choose the category of users to audit: ■ **All**: Audits all users, including proxy users. ■ **User**: Audits the user to which this setting applies. When you select this option, the **Users** field appears, in which you must specify at least one user. To display a list of users and their audit sources from which to select, click the flashlight icon. ■ **Proxy User**: Audits the proxy user for the database. When you select this option, the **Proxy User** field appears, in which you must specify at least one user. To display a list of proxy users and their audit sources from which to select, click the flashlight icon.
Statement Execution Condition	Choose the execution condition: ■ **Both**: Audits both successful and failed statements ■ **Success**: Audits the statement if it is successful ■ **Failure**: Audits the statement if it fails
DML Audit Granularity	Choose the level of granularity: ■ **Access**: Creates an audit record each time the operation occurs ■ **Session**: Creates an audit record the first time an operation occurs in the current session

2.7 Creating Oracle Audit Vault Policies for Fine-Grained Auditing

This section contains:

- About Fine-Grained Auditing
- Defining a Fine-Grained Auditing Policy

2.7.1 About Fine-Grained Auditing

Fine-grained auditing (FGA) enables you to create a policy that defines specific conditions that must exist for the audit to occur. For example, fine-grained auditing lets you audit the following types of activities:

- Accessing a table between 9 p.m. and 6 a.m. or on Saturday and Sunday
- Using an IP address from outside the corporate network
- Selecting or updating a table column
- Modifying a value in a table column

A fine-grained audit policy provides granular auditing of select, insert, update, and delete operations. Furthermore, you reduce the amount of audit information generated by restricting auditing to only the conditions that you want to audit. This creates a more meaningful audit trail that supports compliance requirements. For example, a central tax authority can use fine-grained auditing to track access to tax returns to guard against employee snooping, with enough detail to determine what data was accessed. It is not enough to know that a specific user used the `SELECT` privilege on a particular table. Fine-grained auditing provides a deeper audit, such as when the user queried the table or the computer IP address user who performed the action.

2.7.1.1 Auditing Specific Columns and Rows

When you define the fine-grained audit policy, you can target one or more specific columns, called a relevant column, to be audited if a condition is met. This feature enables you to focus on particularly important, sensitive, or privacy-related data to audit, such as the data in columns that hold credit card numbers, patient diagnoses, U.S. Social Security numbers, and so on. A relevant-column audit helps reduce the instances of false or unnecessary audit records, because the audit is triggered only when a particular column is referenced in the query.

You further can fine-tune the audit to specific columns and rows by adding a condition to the audit policy. For example, suppose you enter the following fields in the Create Fine Grained Audit page:

- **Condition**: `department_id = 50`
- **Columns**: `salary, commission_pct`

This setting audits anyone who tries to select data from the `salary` and `commission_pct` columns of employees in Department 50.

If you do not specify a relevant column, then Oracle Database applies the audit to all the columns in the table; that is, auditing occurs whenever any specified statement type affects any column, whether or not any rows are returned.

2.7.1.2 Using Event Handlers in Fine-Grained Auditing

In a fine-grained audit policy, you can specify an event handler to process an audit event. The event handler provides flexibility in determining how to handle a triggering audit event. For example, it could write the audit event to a special audit table for further analysis, or it could send a pager or an e-mail alert to a security administrator. This feature enables you to fine-tune audit responses to appropriate levels of escalation.

For additional flexibility in implementation, you can employ a user-defined function to determine the policy condition, and identify a relevant column for auditing (audit column). For example, the function could allow unaudited access to any salary as long as the user is accessing data within the company, but specify audited access to executive-level salaries when they are accessed from the outside the company.

2.7.2 Defining a Fine-Grained Auditing Policy

To define a fine-grained auditing policy:

1. If necessary, retrieve and activate the current fine-grained auditing policies.

   See Section 2.3 for more information.

2. In the Audit Settings page, select the **FGA** tab to display the FGA (fine-grained auditing) page.

   Table 2–8 on page 2-14 describes the fields used in the FGA page.

3. Click the **Create** button and in the Create Fine Grained Audit page, define the audit policy.

   Table 2–9 on page 2-14 describes the Create Fine Grained Audit fields.

4. Click **OK**.

   The fine-grained audit policy is created. To ensure that the fine-grained audit policy is semantically correct, see Section 2.9.

5. In the Overview page, select **Save All Audit Settings**.

To display the Overview page, click the **Audit Settings** link, and then in the Audit Settings page, select the name of the source database.

Table 2–8 lists the fields used in the Fine-Grained Audit page.

Table 2–8 Fields in the Fine-Grained Audit Page

Field	Description
(Leftmost column)	An exclamation mark icon indicates one of the following conditions: ■ The statement is needed but is not in use. ■ The statement is in use but is not needed.
Policy Name	The name of this fine-grained audit policy
Schema	The schema to which this policy applies
Object	The object to which this policy applies
Statement	The SQL statement to which this policy applies. Values are: ■ `S`: `SELECT` SQL statement ■ `I`: `INSERT` SQL statement ■ `U`: `UPDATE` SQL statement ■ `D`: `DELETE` SQL statement ■ `M`: `MERGE` SQL statement
Columns	The database columns being audited, also referred to as the relevant columns. If this field is empty, all columns are audited.
In Use	The arrow points upward if the setting is active in the source database and downward if it has not been provisioned or is not active.
Needed	A check mark indicates that the policy is needed. An **X** indicates that the policy is not needed. If a policy that is not in use is set to needed, the In Use arrow points up after provisioning. If a policy that is in use is set to not needed, the audit policy is no longer displayed after provisioning.
(Rightmost column)	Click the trash can icon to remove the policy. You only can use the trash can icon to remove the policy if you had just created it and decided it was not required in the source database, or if it is not active in the source database.

Table 2–9 lists the fields in the Create Fine-Grained Audit page.

Table 2–9 Fields in the Create Fine-Grained Audit Page

Field	Description
Policy Name	Enter a name for this fine-grained audit policy.

Table 2–9 (Cont.) Fields in the Create Fine-Grained Audit Page

Field	Description
Audit Trail	Select from one of the following audit trail types: ■ **Database**: Writes the policy records to the database audit trail `SYS.FGA_LOG$` system table. ■ **Database with SQL Text**: Performs the same function as the Database option, but also populates the SQL bind and SQL text CLOB-type columns of the `SYS.FGA_LOG$` table. ■ **XML**: Writes the policy records to an operating system XML file. To find the location of this file, a database administrator can run the following command in SQL*Plus: `SQL> show parameter audit_file_dest` ■ **XML with SQL Text**: Performs the same function as the XML option, but also includes all columns of the audit trail, including `SQLTEXT` and `SQLBIND` values.
Object	Select an object to audit (for example `OE.CUSTOMERS`). To display a list from which to select and to filter objects by audit source, object owner, and object, click the flashlight icon.
Statements	Select one or more SQL statements to audit. To display a list of statements from which to choose, click the flashlight icon. Select from the following SQL statements: ■ `SELECT` ■ `INSERT` ■ `UPDATE` ■ `DELETE` ■ `MERGE`
Columns	Optional. Enter the names of the database columns (relevant columns) to audit. Separate each column name with a comma. If you enter more than one column, select **All** or **Any** as the condition that triggers this policy. For example, assuming you selected the `OE.CUSTOMERS` table: `CUSTOMER_ID, CREDIT_LIMIT, DATE_OF_BIRTH` See Section 2.7.1.1 for more information about relevant columns.
Condition	Optional. Enter a Boolean condition to filter row data. For example: `department_id = 50` If this field is blank or null, auditing occurs regardless of condition.
Handler Schema	Mandatory if you specify an event handler. Enter the name of the schema account in which the event handler was created. For example: `SEC_MGR` See Section 2.7.1.2 for more information about event handlers.
Handler Package	Mandatory if you specify an event handler. Enter the name of the package in which the event handler was created. For example: `OE_FGA_POLICIES`

Table 2–9 (Cont.) Fields in the Create Fine-Grained Audit Page

Field	Description
Handler	Optional. Enter the name of the event handler. For example: `CHECK_OE_VIOLATIONS` If you specify an event handler, then specify its schema and package as well.

2.8 Creating Capture Rules for Redo Log File Auditing

This section contains:

- About Capture Rules Used for Redo Log File Auditing
- Defining a Capture Rule for Redo Log File Auditing

2.8.1 About Capture Rules Used for Redo Log File Auditing

You can create a capture rule to track changes in the database redo log files. The capture rule specifies DML and DDL changes that should be checked when Oracle Database scans the database redo log. You can apply the capture rule to an individual table, a schema, or globally to the entire database. Unlike statement, object, privilege, and fine-grained audit policies, you do not retrieve and activate capture rule settings from a source database, because you cannot create them there. You only can create the capture rule in the Audit Vault Console.

2.8.2 Defining a Capture Rule for Redo Log File Auditing

To define a capture rule:

1. In the Audit Settings page, select the **Capture Rule** tab to display the Capture Rule page.

   Table 2–10 on page 2-16 describes the fields used in the Capture Rule page.

2. Click the **Create** button and in the Create Capture rule page, define the capture rule.

   Table 2–11 on page 2-17 describes the Create Capture Rule page fields.

3. Click **OK**.

   The capture rule is created. To ensure that the capture rule is semantically correct, see Section 2.9.

4. In the Overview page, select **Save All Audit Settings**.

   To display the Overview page, click the **Audit Settings** link, and then in the Audit Settings page, select the name of the source database.

Table 2–10 lists the fields used in the Capture Rule page.

Table 2–10 Fields in the Capture Rule Page

Field	Description
(Leftmost column)	An exclamation mark icon indicates one of the following conditions: ■ The statement is needed but is not in use. ■ The statement is in use but is not needed.

Table 2–10 (Cont.) Fields in the Capture Rule Page

Field	Description
Rule Type	The types of capture rules are as follows: - **Table**: Captures or discards either row changes resulting from DML changes or DDL changes to a particular table. - **Schema**: Captures or discards either row changes resulting from DML changes or DDL changes to the database objects in a particular schema. - **Global**: Captures or discards either all row changes resulting from DML changes or all DDL changes in the database.
Schema	Indicates the schema to which this rule applies
Table	For table capture rules, this indicates the table to which this rule applies.
DDL	`YES` or `NO` indicates whether data definition language (DDL) statements are audited.
DML	`YES` or `NO` indicates whether data manipulation language (DML) statements are audited.
In Use	The arrow points upward if the setting is active in the source database and downward if it has not been provisioned or is not active.
Needed	A check mark indicates that the policy is needed. An **X** indicates that the policy is not needed. If a policy that is not in use is set to needed, the In Use arrow points up after provisioning. If a policy that is in use is set to not needed, the audit policy is no longer displayed after provisioning.
(Rightmost column)	Click the trash can icon to remove the policy. You can use the trash can icon to remove the policy only if you had just created it and decided it was not required in the source database, or if it is not active in the source database.

Table 2–11 lists the fields used in the Create Capture Rule page.

Table 2–11 Fields in the Create Capture Rule Page

Field	Description
Capture Rule	Select from the following capture rule types: - **Table**: Captures either row changes resulting from DML changes or DDL changes to a particular table. The **Table** field appears; enter the name of the table to which the capture rule applies. To display a list of tables and their audit sources, and to filter by object owner and object, click the flashlight icon. - **Schema**: Captures either row changes resulting from DML changes or DDL changes to the database objects in a particular schema. The **Schema** field appears; enter the name of the schema, or click the flashlight icon to select from a list. - **Global**: Captures either all row changes resulting from DML changes or all DDL changes in the database.

Table 2–11 (Cont.) Fields in the Create Capture Rule Page

Field	Description
Capture	Select from the following: ■ **DDL** (data definition language) ■ **DML** (data manipulation language) ■ **Both**

2.9 Verifying Oracle Audit Vault Policy Settings

After you have created an audit policy or capture rule, you can verify its semantic correctness.

1. In the Overview page, click the **Audit Policy** tab.

   From within the Audit Vault Console, click the **Database Instance** link to display the Overview page.

2. Select the name of the source database.

   The Apply Audit Settings section appears.

3. Select the audit settings types that you want to verify: **Statement**, **Object**, **Privilege**, **FGA**, or **Capture Rule**.

   By default, all audit types are selected.

4. Click the **Verify** button.

   The Audit Vault Console displays a message letting you know that the settings have been verified.

2.10 Exporting Oracle Audit Vault Policies to the Source Oracle Database

After you have created, verified, and saved the audit policies and capture rules, you need to export them to the source database. This ensures that the audit settings in the source database and Oracle Audit Vault are the same.

You can export the settings in the following ways:

- **Save the settings to a SQL script.** Afterwards, give this script to your database administrator, who can apply the policies to the source database.
- **Provision the audit settings to the source database yourself.** You can provision the settings if you have been granted `EXECUTE` privileges for the `AUDIT` SQL statement, the `NOAUDIT` SQL statement, and the `DBMS_FGA` PL/SQL package.

After you export the audit settings to the source database, a database administrator can modify or delete audit policies. For this reason, you should periodically fetch the settings to ensure that you have the latest audit settings. Section 2.3 describes how to fetch audit settings.

To export the audit settings:

1. In the Overview page, click the **Audit Policy** tab.

   From within the Audit Vault Console, click the **Database Instance** link to display the Overview page.

2. Select the name of the source database.

   The Apply Audit Settings section appears.

3. Select from the audit settings types the audit settings that you want to export: **Statement**, **Object**, **Privilege**, **FGA**, or **Capture Rule**.

   By default, all the audit settings types are selected.

4. Use one of the following methods to export the audit settings:

   - **Exporting to a SQL file:** Click **Export as SQL** to save the settings to a SQL script. In the **Browse** dialog field, select a location for the SQL file.
   - **Provisioning to the source database:** In the **Audit Source User Name** and **Audit Source Password** fields, enter the name and password of a user who has been granted `EXECUTE` privileges for the `AUDIT` SQL statement, the `NOAUDIT` SQL statement, and the `DBMS_FGA` PL/SQL package. Then click **Provision**.

2.11 Copying Oracle Audit Vault Policies to Other Oracle Databases

You can copy audit policies from one Oracle database to another Oracle database that has been added to Oracle Audit Vault. You can copy policies that are already in use in the database or copy policies that you have created in Oracle Audit Vault but not yet applied to that database.

1. In the Overview page, click the **Audit Policy** tab.

   From within the Audit Vault Console, click the **Database Instance** link to display the Overview page.

2. Select the name of the source database.

   The Apply Audit Settings section appears.

3. Select from the audit settings types whose audit settings you want to copy: **Statement**, **Object**, **Privilege**, **FGA**, or **Capture Rule**.

   By default, all the audit settings types are selected.

4. In the **From** field under Copy Audit Settings from Another Source, enter the name of a source database that is different from the currently used source database, or use the flashlight icon to select it from a list.

5. After **Copy**, select either of the following options:

   - **Actual (In Use):** Copies the settings listed in the **In Use** field under Apply Audit Settings.
   - **Needed (Not Yet In Use):** Copies the settings listed in the **Needed** field under Apply Audit Settings.

6. In the **From** field, enter the full name of the source database from which you want to copy, or use the flashlight icon to select its name from a list.

   You can filter the source databases by source name, host name, and host IP address.

7. Click the **Load** button.

8. Click the **Save All Audit Settings** button.

9. Export the settings to a SQL file or provision the settings to the source database, using the procedure described in Section 2.10.

2.12 Creating and Configuring Alerts

This section contains:

- About Alerts
- Creating an Alert
- Monitoring Alerts

2.12.1 About Alerts

You can create and configure alerts for Oracle Database, Microsoft SQL Server, Sybase ASE, and IBM DB2 source databases. The alert is raised when the incoming audit data violates specific audit policies. You can specify an alert level, and associate the alert with the events described in Appendix A through Appendix D.

When an incoming audit record meets the specified condition, an alert is raised and placed in the alert store, where you can review it. Oracle Audit Vault updates the Overview page to reflect the alert data, and places the alert in an output queue within the Oracle Audit Vault database. An Oracle Audit Vault administrator can install software to read this queue and process the alert appropriately. Appropriate actions can include sending a page to a security officer or filing a trouble ticket within the appropriate tracking system. Oracle Audit Vault provides an example of an alert handler, which demonstrates actions taken as a result of alerts. The source files for this handler are in the `$ORACLE_HOME/av/demo/alert` directory. For more information, see the `README.txt` file in the `alert` directory.

Remember that alerts are raised when the audit data reaches the Oracle Audit Vault database, not when the actual action occurs. The time lag between when the action occurs and when the alert is raised depends on several factors, including how frequently the audit data collectors collect the audit records. An Oracle Audit Vault administrator can configure this frequency.

Alerts are independent of audit policies. That is, you do not need to perform the tasks described under Section 2.3 before you create an alert.

> **Note:** An Oracle Audit Vault administrator can disable alerts. If the alerts are not firing, then check with your administrator.

2.12.2 Creating an Alert

When you create an alert, you categorize it as either a basic alert or an advanced alert.

This section contains:

- Creating an Alert Rule
- Configuring the Basic Alert Condition
- Configuring the Advanced Alert Condition

2.12.2.1 Creating an Alert Rule

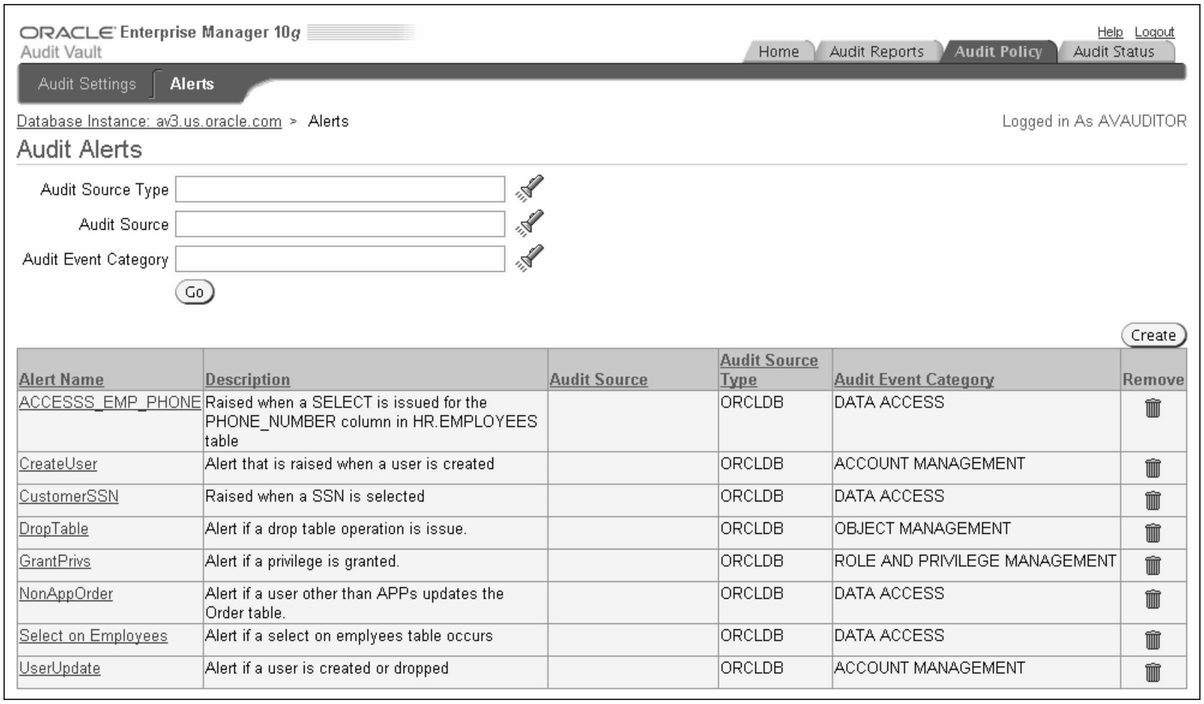
To create an alert rule:

1. Log in to the Audit Vault Console as a user who has been granted the `AV_AUDITOR` role.

   Section 1.4 explains how to start the Audit Vault Console.

2. In the Audit Vault Console, select the **Audit Policy** tab, then select the **Alerts** tab.

The Audit Alerts page appears, which lists the existing alerts. You can use the **Audit Source Type**, **Audit Source**, and **Audit Event Category** fields or their flashlight icons to filter the list of existing alerts. To view the definition for an existing alert, select its name in the **Alert Name** field.



Database Instance: av3.us.oracle.com > Alerts

Logged in As AVAUDITOR

Audit Alerts

Audit Source Type

Audit Source

Audit Event Category

Alert Name	Description	Audit Source	Audit Source Type	Audit Event Category	Remove
ACCESSS_EMP_PHONE	Raised when a SELECT is issued for the PHONE_NUMBER column in HR.EMPLOYEES table		ORCLDB	DATA ACCESS	🗑
CreateUser	Alert that is raised when a user is created		ORCLDB	ACCOUNT MANAGEMENT	🗑
CustomerSSN	Raised when a SSN is selected		ORCLDB	DATA ACCESS	🗑
DropTable	Alert if a drop table operation is issue.		ORCLDB	OBJECT MANAGEMENT	🗑
GrantPrivs	Alert if a privilege is granted.		ORCLDB	ROLE AND PRIVILEGE MANAGEMENT	🗑
NonAppOrder	Alert if a user other than APPs updates the Order table.		ORCLDB	DATA ACCESS	🗑
Select on Employees	Alert if a select on emplyees table occurs		ORCLDB	DATA ACCESS	🗑
UserUpdate	Alert if a user is created or dropped		ORCLDB	ACCOUNT MANAGEMENT	🗑

This is a screen shot of the Audit Alerts page. It contains these fields, ordered from top to bottom:

- Audit Source Type
- Audit Source
- Audit Event Category

To the right of each of these fields is a flashlight icon. Clicking icon display a search field for the item. Below this are buttons to Go and Create.

Beneath these buttons is a grid with information about the alert. From left to right are these columns:

- Alert Name
- Description
- Audit Source
- Audit Source Type
- Audit Event Category
- Remove (a Trash can icon)

****

3. Click **Create**.

   The Create Alert Rule page appears.

4. In the **Alert** field, enter the alert name and then in the **Description** field, enter a brief description of the alert.

5. Specify the following information: level of severity, source type, source, and event category for the alert.
   - **Alert Severity**: Select **Warning** or **Critical**.
   - **Audit Source Type**: Select one of the following audit source types:
     - **SYBDB** (for Sybase Adaptive Server Enterprise)
     - **MSSQLDB** (for Microsoft SQL Server)
     - **ORCLDB** (for Oracle Database)
     - **DB2DB** (for IBM DB2)
   - **Audit Source**: Select from the list of source databases based on the audit source type that you selected.
   - **Audit Event Category**: Select from the list of available categories based on the audit source type that you selected. For detailed information about the audit events for these categories, see the following appendixes:
     - Appendix A, "Oracle Database Audit Events"
     - Appendix B, "Microsoft SQL Server Audit Events"
     - Appendix C, "Sybase Adaptive Server Enterprise Audit Events"
     - Appendix D, "IBM DB2 Audit Events"
6. For the alert conditions, select either **Basic** or **Advanced**. Then go to the following sections:
   - Section 2.12.2.2 to configure a basic alert condition
   - Section 2.12.2.3 configure an advanced alert condition
7. Click **OK**.

After you create alert rules, you can monitor the alert activity from the Overview page. See Section 2.12.3 for more information.

2.12.2.2 Configuring the Basic Alert Condition

Table 2–12 lists the basic alert condition fields in the Basic Alert Condition section of the Create Alert Rule page.

Table 2–12 Fields in the Basic Alert Condition Section

Field	Description
User	Specify the name of one or more users or click the flashlight icon to search for and select user names.
Table	Specify the name of one or more tables or click the flashlight icon to search for and select table names.
Audit Event	Select the name of an audit event from the list. The audit events that appear are based on the audit event category that you selected. See the following appendixes for more information about audit events: ■ Appendix A, "Oracle Database Audit Events" ■ Appendix B, "Microsoft SQL Server Audit Events" ■ Appendix C, "Sybase Adaptive Server Enterprise Audit Events" ■ Appendix D, "IBM DB2 Audit Events"

Table 2–12 (Cont.) Fields in the Basic Alert Condition Section

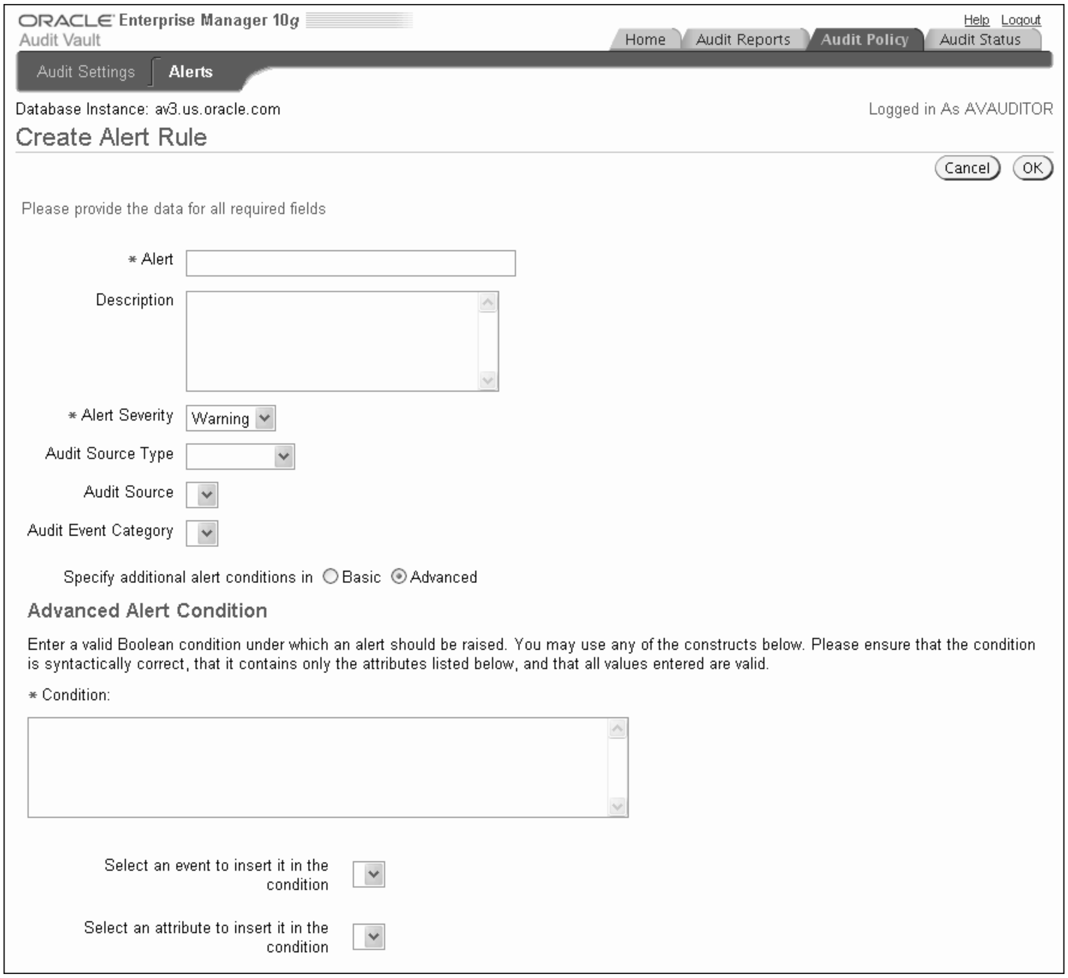
Field	Description
Audit Event Status	Select an option to represent whether the event has a status of **Success**, **Failure**, or **Both**.

2.12.2.3 Configuring the Advanced Alert Condition

In the Advanced Alert Condition section of the Create Alert Rule page, you construct the Boolean condition for when this alert should be evaluated. When audit data violates the Boolean condition, Oracle Audit Vault raises the alert.

Figure 2–1 shows the Advanced Alert Condition section.

Figure 2–1 Create Alert Rule Page, Advanced Alert Condition



Database Instance: av3.us.oracle.com

Logged in As AVAUDITOR

Create Alert Rule

Please provide the data for all required fields

* Alert

Description

* Alert Severity: Warning

Audit Source Type

Audit Source

Audit Event Category

Specify additional alert conditions in ○ Basic ● Advanced

Advanced Alert Condition

Enter a valid Boolean condition under which an alert should be raised. You may use any of the constructs below. Please ensure that the condition is syntactically correct, that it contains only the attributes listed below, and that all values entered are valid.

* Condition:

Select an event to insert it in the condition

Select an attribute to insert it in the condition

This is a screen shot of the Create Alert Rule page. There are four tabs, Home, Audit Reports, Audit Policy, and Audit Status. Audit Policy is selected. There is text Database Instance, with this example ads.us.oracle.com. Below that is text Create Alert Rule, and buttons Cancel and OK.

Below this are fields in this order, Alert*, Description, Alert Severity* with Warning showing, Audit Source Type, and Audit Event Category. The asterik (*) indicates Condition. Then there are options to Specify additional alert conditions in Basic or Advanced, with Advanced selected.

Next, there is the a field to enter the Advanced Alert Condition with this instruction. "Enter a valid Boolean condition under which an alert should be raised. You may use any of the constructs below. Please ensure that the condition is syntactically correct, that it contains only the attributes listed below, and that all values entered are valid."

After this entry field, appear the lists to Select an event to insert it in the condition and Select an attribute to insert it in the condition.

****

To construct a Boolean condition:

1. From the **Select an event to insert in the condition** list, select an event.

   The event appears in the **Condition** field with its associated event ID. For example, if the source database is an Oracle database and you selected **INSERT** from the list, Oracle Audit Vaults adds the following event code to the Condition field:

   ```
   SOURCE_EVENTID = '2'
   ```

   (Appendix A through Appendix D describe the event codes in detail.)

2. From the **Select an attribute to insert in the condition** list, select an attribute.

   For example, if you select **EVENT_STATUS**, it is added to the **Condition** field. At this stage, the **Condition** field appears as follows:

   ```
   SOURCE_EVENTID = '2' EVENT_STATUS
   ```

3. Edit the event and attribute to create a Boolean condition. In this example, you must insert the `AND` condition after `'2'` to create a valid expression.

   For example:

   ```
   SOURCE_EVENTID = '2' AND EVENT_STATUS !=0
   ```

   An event status of '0' specifies success in an Oracle database. A nonzero status specifies the `ORA` error number returned by the database in response to the event.

4. Click **OK**.

2.12.3 Monitoring Alerts

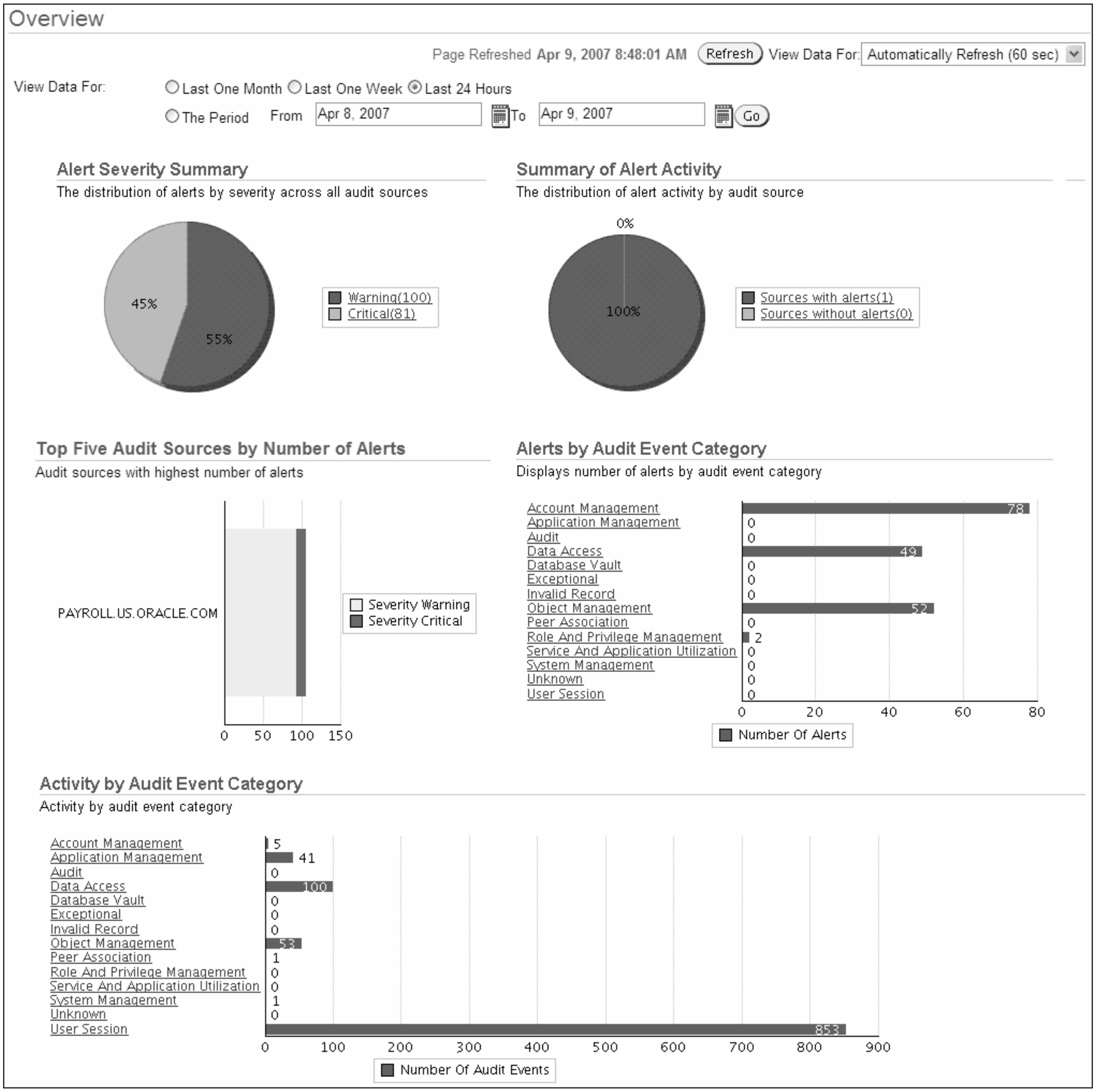
The **Overview** page is the homepage for auditors to view alert summaries, drill down to reports, and view agent and collector status. To display the Overview page, select the **Audit Reports** tab, and then select the **Home** tab.

When an audit record is generated, Oracle Audit Vault classifies it into the event category that you specified when you created the alert. Audit event activity is monitored by the event category to which the audit record belongs. For example, a Logon event belongs to the User Session event category.

Oracle Audit Vault raises an alert when data in a single audit record matches an alert rule condition. Alerts are grouped by the sources with which they are associated, by the event category to which the event belongs, and by the severity level of the alert (warning or critical).

Figure 2–2 shows the Overview page.

Figure 2–2 Overview Page



Overview

Page Refreshed Apr 9, 2007 8:48:01 AM (Refresh) View Data For: Automatically Refresh (60 sec)

View Data For: ○ Last One Month ○ Last One Week ● Last 24 Hours

○ The Period From Apr 8, 2007 To Apr 9, 2007 (Go)

This is a screen shot of the Overview page. At the top center of the page, the last refresh date appears. To the right of the refresh date is a the Refresh button, for viewing data. To right of this Refresh button is the View Data For list, with options Automatically Refresh (60 sec) or Manually.

Beneath the Refresh button is the View Data For area, with these options, from left to right:

- Last One Month
- Last One Week
- Last 24 Hours

And then alternative viewing options, listed from left to right:

- The Period

- From (enter a date or select a date by clicking the calendar icon to the right)
- To (enter a date or select a date by clicking the calendar icon to the right)

To the right of the To calendar icon is the Go button.

This produces various pie charts and bar charts as described in the text.

****

From the Overview page, you can:

- Select an event start time and end time in which to view Audit Vault event data. You can specify a time period by month, week, or day time span or the period between a specified begin and end date.
- View five types of graphical summaries (pie charts and bar graphs) of alert activity and event activity over the specified time period. These graphical summaries include:
  - **Alert Severity Summary** (pie chart)

    Click a section in this pie chart to drill down to a more detailed critical or warning alert report to see what sources are showing a particular severity level. See Section 3.7 for more information about critical and warning alert reports.
  - **Summary of Alert Activity** (pie chart)

    Click a section in this pie chart to find critical and warning alerts to see the affected sources for all alert activity.
  - **Top Five Audit Sources by Number of Alerts** (bar graph)

    Click a bar in this bar graph to find more detailed critical and warning alert information that shows a severity level for a particular source.
  - **Alerts by Audit Event Category** frequency (number of alerts) (bar graph)

    Click an event category link in this bar graph to drill down to see more detailed critical and warning alert information that shows all alerts for that event category.
  - **Activity by Audit Event Category** frequency (number of events) (bar graph)

    Click an event category link in this bar graph to find events for that event category. You can generate default reports for these event categories. See Chapter 3, "Using Oracle Audit Vault Reports" for more information.
- Click a pie section or bar chart y-axis event category label to drill down to a more detailed report level.

3 Using Oracle Audit Vault Reports

This chapter contains:

3.1 What Are Oracle Audit Vault Reports?

The Oracle Audit Vault reports are automatically generated reports that describe the state of audited activities. They reflect audited data collected from the Oracle Database, Microsoft SQL Server, Sybase ASE, and IBM DB2 source databases that connect to the Audit Vault Server. For all three of these products, they track the audit events described in Appendix A through Appendix D.

The default reports are organized into various categories, such as access reports and management reports. You can create user-defined reports that focus on specific areas or audited events.

Any user who has been granted the `AV_AUDITOR` role can view and modify the reports.

3.2 Accessing the Oracle Audit Vault Audit Reports

To access the Oracle Audit Vault audit reports:

1. Log in to the Oracle Audit Vault Console and log in as a user who has been granted the `AV_AUDITOR` role, as explained in Section 1.4.

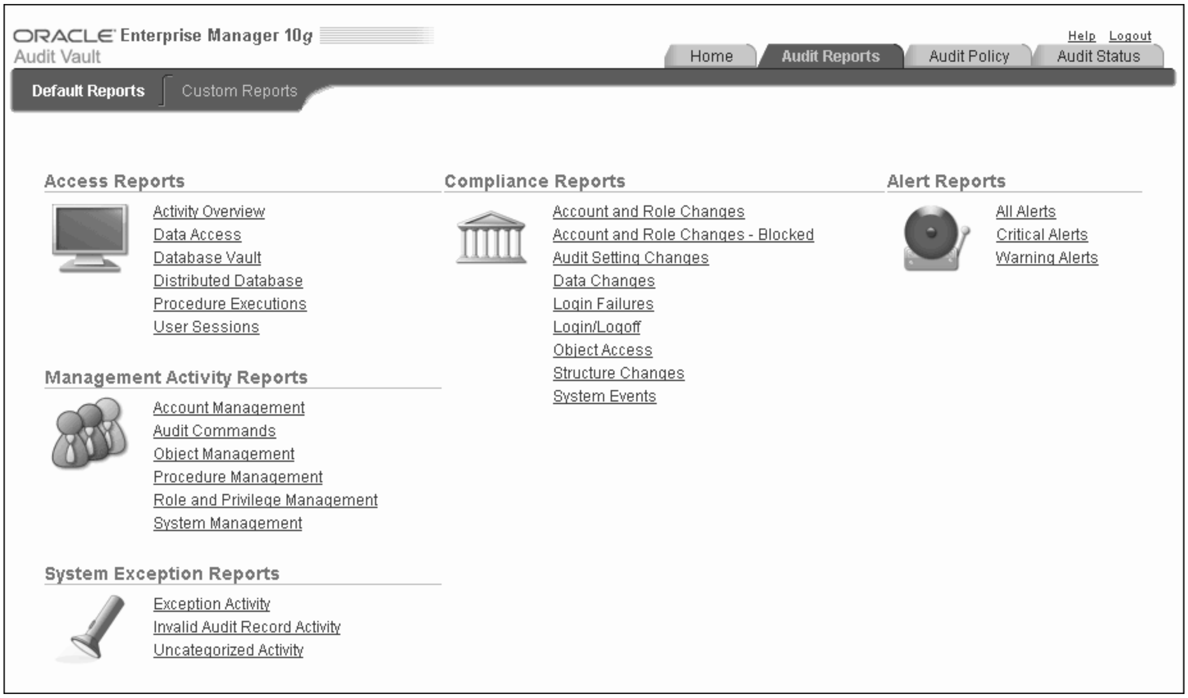
   The Home page appears.

2. Click the **Audit Reports** tab in the upper-right corner of the window.

3. Do one of the following:
   - **To use the default reports:** Click the **Default Reports** secondary tab. Figure 3–1 shows the Default Reports page. To view a report (for example, Data Access under the Access Reports category), click its link.
   - **To use user-defined reports:** Click the **Custom Reports** secondary tab. If you have created any user-defined reports, click the name of the report in the Report Name column to access the report.

Figure 3–1 shows the Default Reports page.

Figure 3–1 Default Reports Page



This is a screen shot of the Activity Reports page which is described in the surrounding text.

- **Access.** These reports are: Activity Overview, Data Access, Database Vault, Peer Association, Service and Application Access, and User Sessions
- **Management Activity**. These reports are: Audit Commands, Account Management, Application Management, Object Management, Role and Privilege Management, and System Management
- **Exception Activity**. These reports are: Exception Activity, Invalid Audit Record Activity, and Uncategorized Activity
- **Compliance Activity**. These reports are: Changes to Audit, DDL Report, Object Access, Logon Failure, Security Admin, Security Admin - Failed Attempts, System Events, and User Logon or Logoff
- **Alert Activity**. These reports are: Critical Alerts and Warning Alerts

****

3.3 Using the Default Access Reports

The default access reports track general database access activities such as audited SQL statements, Oracle Database Vault activities, application access activities, and user login activities. You can create user-defined reports from these reports; see Section 3.8 and Section 3.10.

The access reports are as follows:

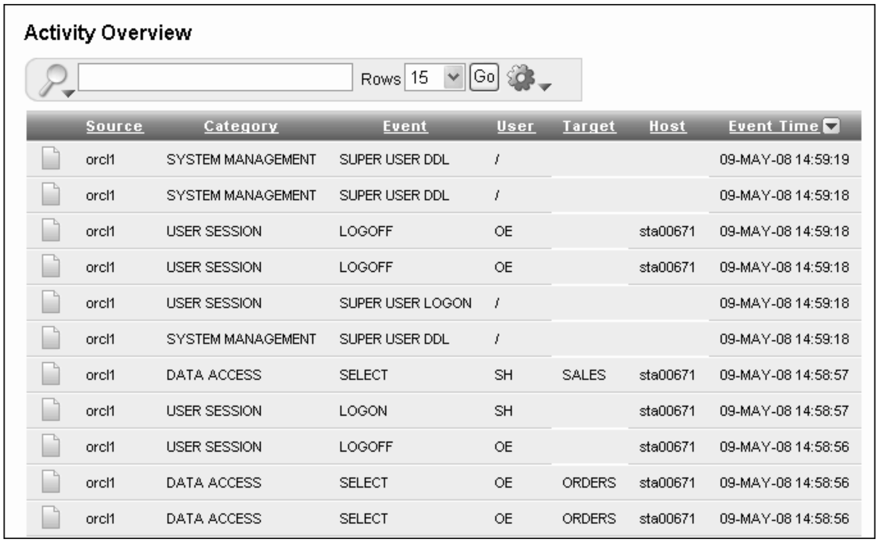
- Activity Overview Report
- Data Access Report
- Database Vault Report
- Distributed Database Report
- Procedure Executions Report
- User Sessions Report

3.3.1 Activity Overview Report

The **Activity Overview** report page displays all audit trail records. Audit records display based on their audit event time in descending order (newest record first). This report can be very large, but you can create a user-defined version that filters specific audit data. By default, 15 audit records are displayed on each page.

Figure 3–2 shows the Activity Overview page.

Figure 3–2 Activity Overview Report Page



Activity Overview

Rows 15

	Source	Category	Event	User	Target	Host	Event Time
	orcl1	SYSTEM MANAGEMENT	SUPER USER DDL	/			09-MAY-08 14:59:19
	orcl1	SYSTEM MANAGEMENT	SUPER USER DDL	/			09-MAY-08 14:59:18
	orcl1	USER SESSION	LOGOFF	OE		sta00671	09-MAY-08 14:59:18
	orcl1	USER SESSION	LOGOFF	OE		sta00671	09-MAY-08 14:59:18
	orcl1	USER SESSION	SUPER USER LOGON	/			09-MAY-08 14:59:18
	orcl1	SYSTEM MANAGEMENT	SUPER USER DDL	/			09-MAY-08 14:59:18
	orcl1	DATA ACCESS	SELECT	SH	SALES	sta00671	09-MAY-08 14:58:57
	orcl1	USER SESSION	LOGON	SH		sta00671	09-MAY-08 14:58:57
	orcl1	USER SESSION	LOGOFF	OE		sta00671	09-MAY-08 14:58:56
	orcl1	DATA ACCESS	SELECT	OE	ORDERS	sta00671	09-MAY-08 14:58:56
	orcl1	DATA ACCESS	SELECT	OE	ORDERS	sta00671	09-MAY-08 14:58:56

This screen shows the Activity Overview Reports page. A description of this figure is in the surrounding text. The page starts with a look-up filter field and a field to enter the number of rows for display. After that is a Go button.

In addition to the standard columns that appear in the activity report, the Activity Overview Reports page includes the Category column for the report, for example, User Session for all User Session reports.

****

3.3.2 Data Access Report

The Data Access Report displays audited SQL statements, such as Oracle Database data manipulation language (DML) activities (for example, all SELECT, INSERT, UPDATE, or DROP SQL statements).

See Also:

- Section A.5 for Oracle Database audit events
- Section B.5 for SQL Server audit events
- Section C.5 for Sybase Adaptive Server Enterprise audit events
- Section D.5 for IBM DB2 audit events
- Section 3.6.4 if you want to use the Data Change Report to track changes to row data from INSERT or UPDATE statements

3.3.3 Database Vault Report

The Database Vault Report displays audited Oracle Database Vault activity. These audit records are collected from the Oracle Database Vault audit trail.

If the Database Vault Report does not show data, then Oracle Database Vault may not be enabled. To check that Oracle Database Vault is enabled, log in to SQL*Plus and then query the V$OPTION table. Any user can query this table. If Oracle Database Vault is enabled, the query returns TRUE; otherwise it returns FALSE. Remember that you must enter the parameter value, Oracle Database Vault, using case-sensitive letters, as in the following example:

```
SQL> SELECT * FROM V$OPTION WHERE PARAMETER = 'Oracle Database Vault';

PARAMETER                    VALUE
---------------------------- -----------------------
Oracle Database Vault        TRUE
```

See also Section A.6 for a listing of the Oracle Database Vault audit events.

3.3.4 Distributed Database Report

The Distributed Database Report displays audited distributed database activity, such as Oracle Database CREATE DATABASE LINK or DROP DATABASE LINK statements. (Note that the associated audit events are called *peer association events*.)

See Also:

- Section A.10 for Oracle Database audit events
- Section B.9 for SQL Server audit events
- Section C.9 for Sybase Adaptive Server Enterprise audit events
- Section D.9 for IBM DB2 audit events

3.3.5 Procedure Executions Report

The Procedure Executions Report displays audited application access activity, such as the execution of SQL procedures or functions. (Note that the associated audit events are called *service and application utilization events*.)

See Also:

- Section A.12 for Oracle Database audit events
- Section B.11 for SQL Server audit events
- Section C.11 for Sybase Adaptive Server Enterprise audit events
- Section D.11 for IBM DB2 audit events
- Section 3.4.4 for information about the Procedure Management Report

3.3.6 User Sessions Report

The User Sessions Report displays audited authentication events for users who log in to the database. This includes the time the user logged in, the login event, and how the user was authenticated.

See Also:

- Section A.15 for Oracle Database audit events
- Section B.14 for SQL Server audit events
- Section C.14 for Sybase Adaptive Server Enterprise audit events
- Section D.14 for IBM DB2 audit events

3.4 Using the Default Management Activity Reports

The default management activity reports track the use of `AUDIT` SQL statements, changes to user accounts, actions performed on the underlying packages for applications, actions performed on database objects, roles and privileges, and system management activities such as database shutdowns and startups. You can create user-defined reports from these reports; see Section 3.8 and Section 3.10.

The management activity reports are as follows:

- Account Management Report
- Audit Commands Report
- Object Management Report
- Procedure Management Report
- Role and Privilege Management Report
- System Management Report

3.4.1 Account Management Report

The Account Management Report displays account management activity of the user's audited SQL statements. This includes audited changes to user accounts and profiles (setting limits on database resources), for example, when user accounts are created, altered, or deleted, and when database schemas are created.

See Also:

- Section A.2 for Oracle Database audit events
- Section B.2 for SQL Server audit events
- Section C.2 for Sybase Adaptive Server Enterprise audit events
- Section D.2 for IBM DB2 audit events

3.4.2 Audit Commands Report

The Audit Commands Report displays the use of audit commands, such as Oracle Database `AUDIT` SQL statements for other SQL statements and database objects. For example, for Oracle Database, this page tracks `AUDIT ALL`, `AUDIT SELECT ON` *`table_name`* statements, `NOAUDIT` statements, and so on.

See Also:

- Section A.4 for Oracle Database audit events
- Section B.4 for SQL Server audit events
- Section C.4 for Sybase Adaptive Server Enterprise audit events
- Section D.4 for IBM DB2 audit events

3.4.3 Object Management Report

The Object Management Report displays audited actions performed on database objects. For example, these audit records are created for create, alter, or drop operations on database objects that are performed on a database table.

See Also:

- Section A.9 for Oracle Database audit events
- Section B.8 for SQL Server audit events
- Section C.8 for Sybase Adaptive Server Enterprise audit events
- Section D.8 for IBM DB2 audit events

3.4.4 Procedure Management Report

The Procedure Management Report displays audited actions that were performed on the underlying procedures or functions of system services and applications. For example, it lists the audit records that were created for Oracle Database `ALTER FUNCTION`, `ALTER JAVA`, or `ALTER PACKAGE` statements. (Note that the associated audit events are called *application management events*.)

See Also:

- Section A.3 for Oracle Database audit events
- Section B.3 for SQL Server audit events
- Section C.3 for Sybase Adaptive Server Enterprise audit events
- Section D.3 for IBM DB2 audit events
- Section 3.3.5 for information about the Procedure Executions Report

3.4.5 Role and Privilege Management Report

The Role and Privilege Management Report lists audited role and privilege management activity, such as the creating, granting, revoking, and dropping of roles and privileges. It lists the name of the user performing the action, and the user to whom the action applies.

See Also:

- Section A.11 for Oracle Database audit events
- Section B.10 for SQL Server audit events
- Section C.10 for Sybase Adaptive Server Enterprise audit events
- Section D.10 for IBM DB2 audit events

3.4.6 System Management Report

The System Management Report displays audited system management activity. For example, it lists activities such as startup and shutdown operations on a database, enable and disable operations on all triggers, and rollback operations. It also lists user-related operations, such as unlocking a user account.

See Also:

- Section A.13 for Oracle Database audit events
- Section B.12 for SQL Server audit events
- Section C.12 for Sybase Adaptive Server Enterprise audit events
- Section D.12 for IBM DB2 audit events

3.5 Using the Default System Exception Reports

The default system exception reports track audit events, such as exceptions that occur and audit activities that Oracle Audit Vault cannot recognize or place into a category. You can create user-defined reports from these reports; see Section 3.8 and Section 3.10.

The system exception reports are as follows:

- Exception Activity Report
- Invalid Audit Record Report
- Uncategorized Activity Report

3.5.1 Exception Activity Report

The Exception Activity Report displays audited error and exception activity, such as network errors.

See Also:

- Section A.7 for Oracle Database audit events
- Section B.6 for SQL Server audit events
- Section C.6 for Sybase Adaptive Server Enterprise audit events
- Section D.6 for IBM DB2 audit events

3.5.2 Invalid Audit Record Report

The Invalid Audit Record Report displays audited activity that Oracle Audit Vault cannot recognize, possibly due to a corrupted audit record.

See Also:

- Section A.8 for Oracle Database audit events
- Section B.7 for SQL Server audit events
- Section C.7 for Sybase Adaptive Server Enterprise audit events
- Section D.7 for IBM DB2 audit events

3.5.3 Uncategorized Activity Report

The Uncategorized Activity Report displays audited activity that cannot be categorized. For example, it lists events such as Oracle Database `COMMENT`, `CREATE SUMMARY`, or `NO-OP` events.

See Also:

- Section A.14 for Oracle Database audit events
- Section B.13 for SQL Server audit events
- Section C.13 for Sybase Adaptive Server Enterprise audit events
- Section D.13 for IBM DB2 audit events

3.6 Using the Default Compliance Reports

The default compliance reports show compliance-related information that may appear in other Oracle Audit Vault reports. They track activities that are typically required to meet standard compliance regulations, such as changes to the database structure or its objects, failed logins, administrator activities, system events, and user logins or logoffs. You can create user-defined reports from these reports; see Section 3.8 and Section 3.10.

The compliance reports are as follows:

- Account and Role Changes - Blocked Report
- Account and Role Changes Report
- Changes to Audit Report
- Data Change Report
- DDL Report
- Login Failures Report
- Login/Logoff Report
- Object Access Report
- System Events Report

3.6.1 Account and Role Changes - Blocked Report

The Account and Role Changes - Blocked Report displays audited activity that identifies all failed attempts to perform security administration changes in the database. For example, these audit records are generated when you enable privilege auditing to audit failed attempts to grant system and table privileges.

3.6.2 Account and Role Changes Report

The Account and Role Changes Report displays audited activity that identifies all successful attempts to perform security administration changes in the database. For example, these audit records are generated when you use statement or object auditing to audit changes to users that were successfully added, dropped, or altered in the database.

3.6.3 Changes to Audit Report

The Changes to Audit Report displays audited activity of audit setting changes (for example, changes to the `AUDIT ALL` SQL statement).

3.6.4 Data Change Report

The Data Change Report displays changes to row data when an insert or update operation occurs in Oracle Database. This report is especially useful if you are using the redo collector to extract the before and after values of data updates.

3.6.5 DDL Report

The DDL Report displays audited data definition language (DDL) activities (for example, changes to the database structure that result from SQL `ALTER`, `CREATE`, or `DROP` statements).

3.6.6 Login Failures Report

The Login Failures Report displays audited failed login attempts. These audit records are generated for failed login, proxy authentication only, and super user login attempts.

3.6.7 Login/Logoff Report

The Login/Logoff Report displays audited login and logoff operations of users. For example, these audit records are generated when you audit events, such as login, logoff, super user login, logoff by cleanup, and proxy authentication only.

3.6.8 Object Access Report

The Object Access Report displays audited SQL statements that have been performed on database objects, such as insert or update operations on a specific table.

3.6.9 System Events Report

The System Events Report displays audited system event activities. These audit records are generated when you audit local system processes. Examples of a local system process are starting and shutting down a database or changing database parameters.

3.7 Using the Critical and Warning Alert Reports

The critical and warning alert reports track critical and warning alerts. An alert is raised when data in a single audit record matches a predefined alert rule condition. Alerts are grouped by associated source, by event category, and by the severity level of the alert (either warning or critical). You can create user-defined reports from these alerts; see Section 3.8.

The alert reports are as follows:

- All Alerts Report
- Critical Alerts Report
- Warning Alerts Report

3.7.1 All Alerts Report

This report tracks all alerts, both critical and warning alerts.

3.7.2 Critical Alerts Report

This report tracks critical alerts.

3.7.3 Warning Alerts Report

This report tracks warning alerts.

3.8 Controlling the Display of Data in a Report

This section contains:

- About Controlling the Display of Report Data
- Hiding or Showing Columns in a Report
- Filtering Data in a Report
- Sorting Data in a Report
- Highlighting Rows in a Report
- Charting Data in a Report
- Adding a Control Break to a Column in a Report
- Resetting the Report Display Values to Their Default Settings

3.8.1 About Controlling the Display of Report Data

You can control the display of data in a default or user-defined report to focus on a particular set of data. Oracle Audit Vault automatically saves the report settings so that if you leave the page, the report settings are still in place when you return. Optionally, you can save the report to a user-defined report.

3.8.2 Hiding or Showing Columns in a Report

When you hide or show columns in a report, you still can perform operations on hidden columns, such as filtering data based on a column that you have hidden.

This section contains:

- Hiding the Currently Selected Column
- Hiding or Showing Any Column

3.8.2.1 Hiding the Currently Selected Column

To hide the currently selected column:

1. In the report, select the column that you want to hide.

2. In the **Column Heading** menu, click the **Hide Column** button.

3.8.2.2 Hiding or Showing Any Column

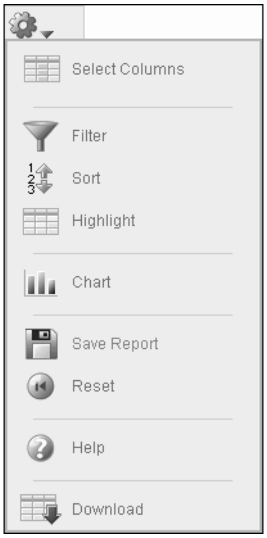
To hide or show columns in a report:

1. Access the report that you want.

   Section 3.2 explains how to access a report.

2. Select the **Actions** menu (gear) icon on the Search bar.

   The Actions menu appears.



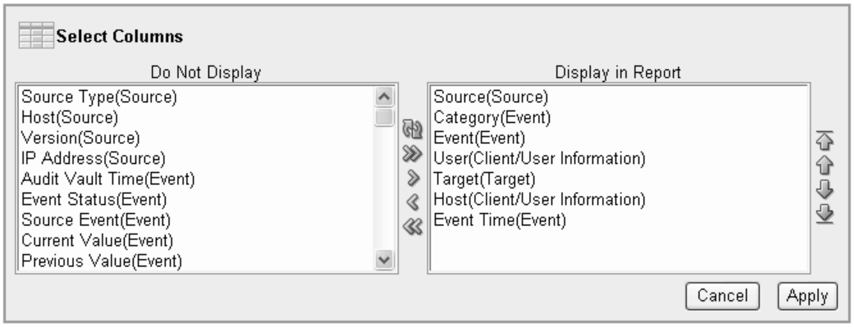
This screen shows the Actions menu, under the Actions Menu (gear) icon. This menu lists the following items:

- Select Columns
- Filter
- Sort
- Highlight
- Chart
- Save Report
- Reset
- Help
- Download

****

3. From the Actions menu, select **Select Columns**.

   The Select Columns dialog field appears under the Search bar.



This screen shows the Select Columns dialog box. It contains the Do Not Display box on the left, and the Display in Report box on the right. In between the two boxes are right and left arrows that enable you to move items from one box to the other. On the right side of the Display in Report box are up and down arrows that let you arrange the order in which the displayed columns appear in the report. After these two boxes, there are Cancel and Apply buttons.

****

4. To move column names between the **Do Not Display** and **Display in Report** boxes:

   - Select the column names to move and then click the move to the left symbol (<) or the move to the right symbol (>) between the column name boxes.
   - Move all columns left or right by using the >> and << buttons.
   - Use the top button (the arrows in a circle) to reset the columns to their original locations in the two boxes.

5. To set the order of appearance in the report for displayed columns, in the **Display in Report** box, select the column name, then click the up arrow or down arrow on the right side of the box to reorder its position in the list.

   Report columns names are arranged in a report from left to right by their top-to-bottom order in the **Display in Report** box.

6. Click **Apply**.

3.8.3 Filtering Data in a Report

You can filter the report to show all rows based on a particular column, or a subset of of rows, using an expression.

If you need to perform subquery, join, and AND SQL operations, you can create multiple filters as needed. For example, if you want to filter all SYS users who are being audited for the SUPER USER LOGON event, you would create one filter to catch all SYS users, and then a second filter to catch all SUPER USER LOGON events. If two or more of the filters for a report are enabled, then Oracle Audit Vault uses both or all of them (as in an AND operation). You can toggle specific filters on or off, depending on the results that you want.

This section contains:

- Filtering All Rows Based on Data from the Currently Selected Column
- Filtering Column and Row Data
- Filtering Row Data Using an Expression

3.8.3.1 Filtering All Rows Based on Data from the Currently Selected Column

This filtering method lets you filter data in all rows based on the currently selected column (for example, all rows that only contain SYS in the **User** column).

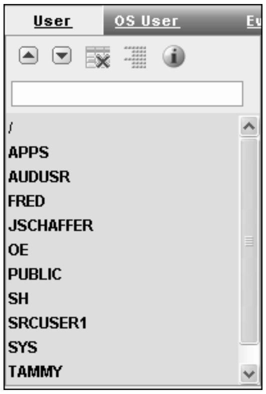
To filter all rows based on data from the current column:

1. Access the report that you want.

   Section 3.2 explains how to access a report.

2. Under the report name, select the column that you want to use as a basis for the filter.

   The Column Heading menu appears. This menu shows the row data used in the column that you selected. For example, if you select the **User** column, it will list user names found in the source database for this column, such as users APPS, OE, and SH.

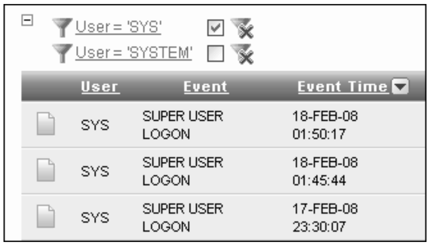


This screen shows the contents of a Column Heading menu for the User event. This example shows a list of users found in the currently used activity report. The Column Heading menu also includes icons for sorting the column data in ascending or descending order, hiding the display of a column, adding a control break, and finding information about the selected column.

****

3. In the Column Heading menu, select the row data on which you want to base the filter, or enter the row data item in the text area field.

   For example, to only show rows for users SYS and SYSTEM, select **SYS** and **SYSTEM** from the Column Heading menu. Oracle Audit Vault filters the display to only show the data in the filter you created. The filter definitions for the current user session are added above the report columns.



User = 'SYS' ☑

User = 'SYSTEM' □

User	Event	Event Time
SYS	SUPER USER LOGON	18-FEB-08 01:50:17
SYS	SUPER USER LOGON	18-FEB-08 01:45:44
SYS	SUPER USER LOGON	17-FEB-08 23:30:07

This screen shows filtered data for the User column showing only rows for the SYS and SYSTEM users. The filter definition, for example User = 'SYS', appears before the column data. The data displayed include User, Event, and Event Time.

****

4. To enable or disable the display of the filtered data, select its corresponding check box. To remove a filter, click its **Remove Filter** icon.

3.8.3.2 Filtering Column and Row Data

You can use the Search bar to search for row data in one or all columns in the report (for example, all rows that contain the letters `SYS`, such as `SYS` and `SYSTEM`, in the **User** column).

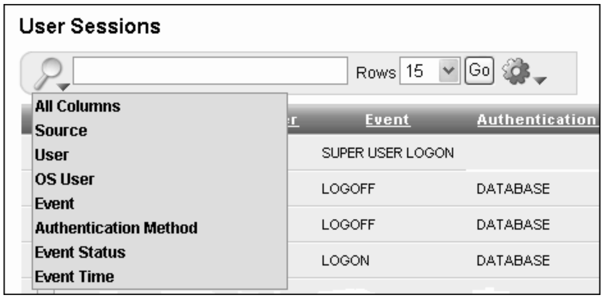
To search for row data in one or all columns:

1. Access the report that you want.

   Section 3.2 explains how to access a report.

2. If you want to focus the search on a specific column, in the Search bar, use the Search icon to select from the list of available columns.

   By default, Oracle Audit Vault searches all columns.



Event	Authentication
SUPER USER LOGON	
LOGOFF	DATABASE
LOGOFF	DATABASE
LOGON	DATABASE

This screen shows the Search Bar with the Search icon selected to display the columns in this report. The Search icon is to the left of the text area. This is a entry field for the number of rows to display and a Go button.

****

3. In the Search bar text area, enter all or part of the text in the column row that you want.

   For example, enter `SYS` to find all user names that contain the letters `SYS`.

   The search is not case-sensitive.

4. In the **Rows** list, select the number of rows that you want to appear on each page.

   The default is 15 rows.

5. Click **Go**.

3.8.3.3 Filtering Row Data Using an Expression

This method lets you select all rows that meet a `WHERE` condition, such as all users who are *not* user `SYS`. You can create the expression for all columns in the source database table, even those that are not shown in the current report.

To filter row data using an expression:

1. Access the report that you want.

   Section 3.2 explains how to access a report.

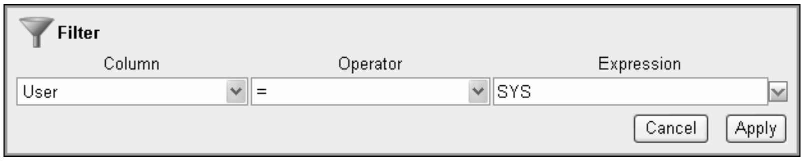
2. Select the **Actions** menu (gear) icon on the Search bar.

3. Select **Filter**.

   The Filter dialog box appears under the Search bar.

4. Enter the following information:

   - **Column**: Select the name of the column from the list. Note that you can select all columns, including hidden columns.
   - **Operator**: Select a SQL operator from the list, for example, > for "greater than" or = for "equals."
   - **Expression**: Select an expression from the list. The expression lists the row data (for example, names of users found in the **User** column). If you type the expression in the **Expression** field, remember that the expression is case-sensitive. In most cases, use uppercase letters.



Filter

Column	Operator	Expression
User	=	SYS

This screen shows the Filter dialog box, which contains the following fields, which are described in this step:

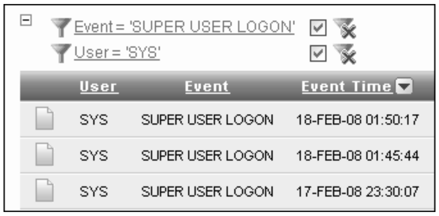
- Column. For this example, the Column value is set to User.
- Operator. For this example, the Operator value is set to =.
- Expression. For this example, the Expression value is set to SYS.

At the bottom, are Cancel and Apply buttons.

****

5. Click **Apply**.

   Oracle Audit Vault filters the display of row data based on the expression you created, and then adds the filter definition before the report columns. From here, you can disable or enable the display of the filtered data, or remove the filter, if you want.



Event = 'SUPER USER LOGON' ☑

User = 'SYS' ☑

User	Event	Event Time
SYS	SUPER USER LOGON	18-FEB-08 01:50:17
SYS	SUPER USER LOGON	18-FEB-08 01:45:44
SYS	SUPER USER LOGON	17-FEB-08 23:30:07

This screen shows two filters, which appear after the Search Bar. To the right of each filter is a check box, which enables you to disable or re-enable the filter, and the Remove Filter icon. The data displayed include User, Event, and Event Time for the SYS user.

****

3.8.4 Sorting Data in a Report

You can sort data in ascending or descending order for all columns at once, or sort data on a selected column.

This section contains:

- Sorting Row Data for the Currently Selected Column
- Sorting Row Data for All Columns

3.8.4.1 Sorting Row Data for the Currently Selected Column

To sort row data for the current column:

1. Select the column on which you want to base the sort.
2. In the Column Heading menu, select either the **Sort Ascending** or **Sort Descending** icon.

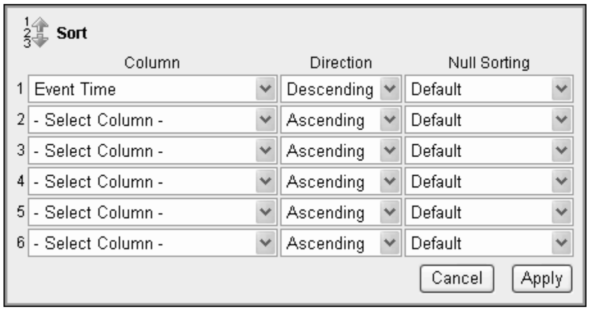
3.8.4.2 Sorting Row Data for All Columns

To sort row data for all columns:

1. Access the report that you want.

   Section 3.2 explains how to access a report.
2. Select the **Actions** menu (gear) icon on the Search bar.
3. In the Actions Menu, select **Sort**.

   The Sort dialog box appears under the Search bar.



	Column	Direction	Null Sorting
1	Event Time	Descending	Default
2	- Select Column -	Ascending	Default
3	- Select Column -	Ascending	Default
4	- Select Column -	Ascending	Default
5	- Select Column -	Ascending	Default
6	- Select Column -	Ascending	Default

This screen shows the Sort dialog box. It has six rows under the three columns Column, Direction, and Null Sorting. Row 1 by default is always the column named Event Time and is sorted in descending order. Column 1 of Rows 2 through 6 are blank, to be selected, from the drop down list. Column 2 for these rows show the defaults, Ascending and Descending, and column 3 shows default. Following the rows are the Cancel and Apply buttons.

****

4. Enter the following information:
   - **Column**: For up to six columns, select the columns to sort. By default, the first sort column is Event Time, which is sorted in descending order.
   - **Direction**: Select either **Ascending** or **Descending**.
   - **Null Sorting**: Select the Null sorting rule for each column (Default, Nulls Always Last, or Nulls Always First). The default is to not sort nulls.
5. Click **Apply**.

3.8.5 Highlighting Rows in a Report

You can highlight specific rows in a report by assigning them colors. This enables anyone viewing the report to quickly find areas that are of particular interest.

To highlight rows in the report:

1. Access the report that you want.

   Section 3.2 explains how to access a report.

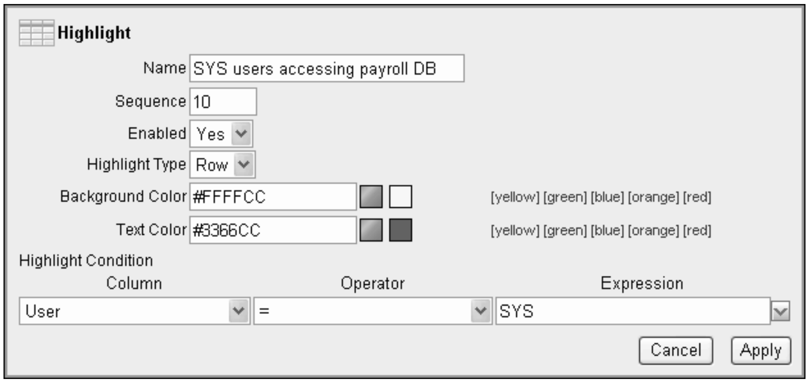
2. Select the **Actions** menu (gear) icon on the Search bar.

3. In the Actions menu, select **Highlight**.

   The Highlight dialog box appears under the Search bar.

4. Enter the following information:

   - **Name**: Enter a name for this highlight instance. (Optional)
   - **Sequence**: Enter a sequence number to determine the order in which the highlight filter rules are to be applied when two or more highlight filter rules are in effect. The default value is 10.
   - **Enabled**: Select **Yes** to enable the highlight or select **No** to disable it.
   - **Highlight Type**: Select **Row** to highlight a row or select **Cell** to highlight a cell.
   - **Background Color**: Select a background color for the row or cell. Click a color to display color options, or click the colored icon to the right of the color selection field to display a color selection box from which to choose a different color. Alternatively, you can manually enter the HTML code for a color.
   - **Text Color**: Select a text color for the row or cell using the same method you used for the background color. (Optional)
   - **Highlight Condition**: Edit the highlight filter rule expression by identifying the column, the operator, and the expression for each of the three fields in the highlight condition.
     - **Column**: Select any column name, including hidden columns.
     - **Operator**: Select an operator from a list of standard Oracle Database operators, such as `=`, `!=`, `NOT IN`, and `BETWEEN`.
     - **Expression**: Enter the comparison expression (without quotation marks) based on a known value for that column name to complete the filter expression. For example, entering the filter expression `EVENT=SUPER USER LOGON` filters for all values in the **Event** column that contain the value `SUPER USER LOGON`.



Highlight

Name: SYS users accessing payroll DB

Sequence: 10

Enabled: Yes

Highlight Type: Row

Background Color: #FFFFCC

Text Color: #3366CC

Highlight Condition

Column	Operator	Expression
User	=	SYS

[yellow] [green] [blue] [orange] [red]
[yellow] [green] [blue] [orange] [red]
Cancel
Apply

This screen shows the highlight dialog box. A description of this figure is in the surrounding text.

****

5. Click **Apply**.

3.8.6 Charting Data in a Report

You can select from four chart styles to chart data in a report. After you create the chart, you can access it whenever you access the report.

To chart data in a report:

1. Access the report that you want.

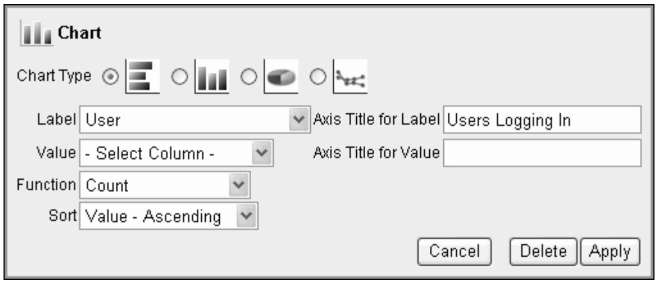
   Section 3.2 explains how to access a report.

2. Select the **Actions** menu (gear) icon on the Search bar, and then select **Chart**.

   The Chart dialog box appears under the Search bar.

3. Enter the following information:

   - **Chart style**: Select from one of the four chart styles: **Horizontal Column**, **Vertical Column**, **Pie**, and **Line**.
   - **Label**: Select from the list of columns for this report. You can include hidden columns as well as displayed columns.
   - **Value**: Select from the list of columns for this report, including hidden columns. If the function you select from the **Function** list is **Count**, then you do not need to select a value from the **Value** column.
   - **Function**: Select an aggregate function (Sum, Average, Minimum, Maximum, or Count) on which to aggregate the data values.
   - **Sort**: Select ascending or descending sorting for values and labels.
   - **Axis Title for Label**: Enter a name for the axis title.
   - **Axis Title for Value**: Enter a name for the axis value.



Chart

Chart Type ● ○ ○ ○

Label: User

Axis Title for Label: Users Logging In

Value: - Select Column -

Axis Title for Value:

Function: Count

Sort: Value - Ascending

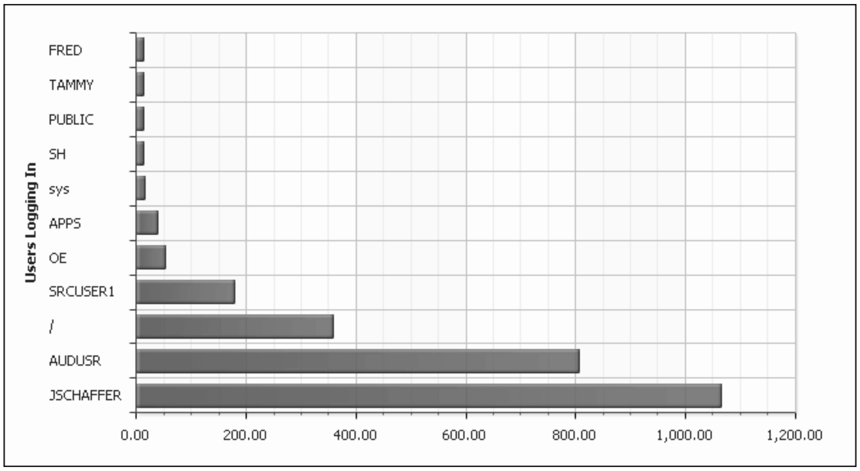
This screen shows the Chart dialog box. It contains the icons for Chart Type, left to right: Horizontal Column, Vertical Column, Pie, and Line. It also shows the following fields, top to bottom: Label, Value, Function, Sort; then Axis Title for Label and Axis Title for Value. This example shows a count of users logging in.

At the bottom, are buttons to Cancel, Delete, and Apply.

****

4. Click **Apply**.

The chart appears, with the **Edit Chart** and **View Report** links under the Search bar. The following example displays a count of users who have logged in, clearly showing that user JSCHAFFER has been very, very busy.



This screen shows a bar chart with a count of user activity. The left side has the X axis label Users Logging In, with a list of users who have logged in to the database. The Y axis has lists the values 0.00, 200.00, 400.00, 600.00, 800.00, 1,000.00, and 1,200.00 in increments of no label because this is a count.

****

3.8.7 Adding a Control Break to a Column in a Report

You can create a break group on the selected column. This pulls the column out of the report as a master record. A break group is a way of grouping all rows with the same value under a master record, thus creating groups of master records, withone master record for each column value. This is useful for filtering by multiple column values.

To add a control break in a column:

1. Access the report that you want.

   Section 3.2 explains how to access a report.

2. Select the column to which you want to add a control break.

3. In the Column Heading menu, select the **Control Break** icon.

   The control break is added to the column, and icons for enabling, disabling, and removing the control break are added before the column headings.

3.8.8 Resetting the Report Display Values to Their Default Settings

You can reset the report display values to their original default settings.

To reset the display settings to their defaults:

1. Access the report that you want.

   Section 3.2 explains how to access a report.

2. Select the **Actions** menu (gear) icon on the Search bar, then select **Reset**.
3. In the Reset confirmation dialog box, select **Apply**.

3.9 Finding Information About Report Data

This section contains:

- Finding Detailed Information About an Audit Record
- Finding Information About the Purpose of a Column

3.9.1 Finding Detailed Information About an Audit Record

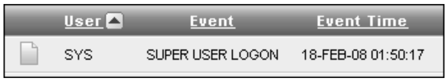
You can find the following detailed information about an individual audit record: information about the source database, audited event, audited objects (such as tables or views), client/user information, the host computer on which the user is logged, audited SQL statements, the user session information, and miscellaneous information such as the audit record ID, instance number, and fine-grained audit policy name.

To find detailed information about an audit record:

1. Access the report that you want.

   Section 3.2 explains how to access a report.

2. Use the methods described in Section 3.8 to find the audit record.
3. Select the Audit Record Details icon, which appears to the left of the first column in the report.



	User ▲	Event	Event Time
🗋	SYS	SUPER USER LOGON	18-FEB-08 01:50:17

This screen shows the Single Row View icon. In this screen, the User column is the left-most column and lists SYS as the column row data. The next column is Event, showing SUPER.USER LOGON. The last column is Event time, showing 18-FEB-08 01:50:17.

The Single Row View column appears to the left of SYS.

****

A detailed report for the audit record appears.

3.9.2 Finding Information About the Purpose of a Column

To find information about the purpose of a column:

1. Access the report that you want.

   Section 3.2 explains how to access a report.

2. Select the column on which you want information.

3. In the Column Heading menu, select the **Column Information** icon.

3.10 Working with User-Defined Reports

This section contains:

- About User-Defined Reports
- Creating a Category for User-Defined Reports
- Creating a User-Defined Report
- Accessing a User-Defined Report

3.10.1 About User-Defined Reports

You can create user-defined reports based on the default reports or other user-defined reports. You can create a category for the report independently or when you create the user-defined report.

3.10.2 Creating a Category for User-Defined Reports

Before you create a user-defined report, you may want to create a category in which to assign it. You can create and manage category names on the **User-Defined Reports** page.

This section contains:

- Creating a Category Name
- Alphabetizing the Category Name List
- Editing a Category Name

3.10.2.1 Creating a Category Name

To create a category name for user-defined reports:

1. Under **Tasks**, click **Manage Categories**.
2. On the **Categories** page, click **Create Category**.
3. In the **Category Name** field, enter the name of the new category.
4. Click **Create**.

3.10.2.2 Alphabetizing the Category Name List

To alphabetize the category name list:

1. Click the **Category Name** column label name once.

   This positions the direction pointer to point upward (category names appear in ascending order).
2. Click the **Category Name** column label name once again to position the direction pointer to point downward (category names appear in descending order).

3.10.2.3 Editing a Category Name

To edit a category name:

1. To edit a category name, click the **Edit** icon (pencil) to the left of the category name.

   The **Category** page appears for the selected category name.

2. On the **Category** page, revise the category name by editing the text in the **Category Name** field.
3. Click **Apply**.

3.10.3 Creating a User-Defined Report

You can save the display settings that you have created to a user-defined report. User-defined reports are listed in the **Custom Reports** secondary tab of the Audit Reports tab. Oracle Audit Vault saves the report settings and makes the user-defined report available the next time you log in to Oracle Audit Vault.

When you save a user-defined report, you can save the report under a specific category that you select or create as you save the report. You can also make the user-defined report private or share it among other Oracle Audit Vault users as a public report.

To create a user-defined report:

1. Access the report that you want.

   Section 3.2 explains how to access a report.
2. Use the methods described in Section 3.8 to design the display of data as needed.
3. Select the **Actions** menu (gear) icon on the Search bar, and then select **Save Report**.

   The Save Report dialog box appears, under the Search bar.
4. Enter the following information:
   - **Name**: Enter a name for the report.
   - **Category**: Select from the list of available categories. If you select **New Category**, then enter a name for the new category.

     If you need to create a new category, see Section 3.10.2.
   - **Description**: Enter a brief description of the report.
   - **Public**: Select this check box to enable the report to be accessible to all Oracle Audit Vault users.
5. Click **Apply**.

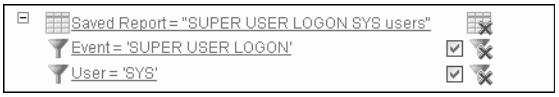
3.10.4 Accessing a User-Defined Report

To access a user-defined report:

1. Log in to the Oracle Audit Vault Console and log in as a user who has been granted the `AV_AUDITOR` role, as explained in Section 1.4.

   The Home page appears.
2. Select the **Audit Reports** tab, and then select the **Custom Reports** secondary tab.
3. In the **Report Name** column, select the link for the report that you want to access.

   The report appears. Its report details icon and filter definitions appear after the Search bar. From here, you can click the **Saved Report** link to change the report settings, delete the report, or disable and enable the report filters.



Saved Report = "SUPER USER LOGON SYS users"

Event = 'SUPER USER LOGON' ☑

User = 'SYS' ☑

This screen shows the Saved Report link and the two filters for a user-defined report. To the right of the Saved Report link is the Delete Report icon. Following the Saved Report link are the filters, which have check boxes for enabling and disabling, and delete icons.

****

3.11 Downloading a Report to a CSV File

You can download reports to a file that is in a comma-separated values (CSV) format. The CSV file format is a delimited data format with fields separated by the comma character and records separated by newline characters.

To download a report to a CSV file:

1. Access the report that you want.

   Section 3.2 explains how to access a report.

2. Select the **Actions** menu (gear) icon on the Search bar, and then select.
3. In the Download dialog box, select **CSV**.
4. In the File Download dialog box, enter a name for the file.
5. Click **Save** to save the file to a location in your file system.

4

Oracle Audit Vault Data Warehouse Schema

This chapter contains:

- About the Oracle Audit Vault Data Warehouse Schema
- Oracle Audit Vault Audit Data Warehouse Architecture
- Design of the Audit Data Warehouse Schema
- How the Fact Table and Dimension Tables Work
- Relationships Between the Fact and Dimension Tables

4.1 About the Oracle Audit Vault Data Warehouse Schema

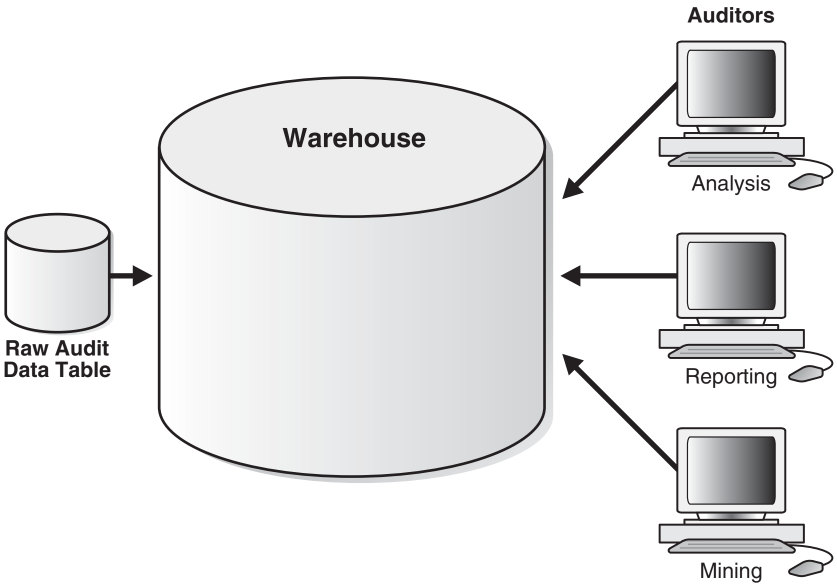
Oracle Audit Vault has an internal data warehouse schema that manages the audit data collected from the source databases. The data warehouse collects the data from the Oracle Audit Vault collection agents, organizes it, and then provides it in report format for the reports described in Chapter 3, "Using Oracle Audit Vault Reports."

If you plan to design custom reports using tools such as Oracle Business Intelligence Publisher and the Oracle Business Intelligence Suite, you must understand the structure of the Oracle Audit Vault data warehouse schema. This appendix describes the schema in detail. You must also understand the structure of the audit events provided by the source database products; Oracle Database, Microsoft SQL Server, Sybase Adaptive Server Enterprise, and IBM DB2. Appendix A through Appendix D describe the structure of these audit events.

4.2 Oracle Audit Vault Audit Data Warehouse Architecture

Figure 4–1 illustrates the Oracle Audit Vault audit data warehouse architecture. Audit Vault stores the audit records in the raw audit data table, which is typical of a traditional online transaction processing (OLTP) system that is optimized for insert performance for the records arriving from their audit sources.

Figure 4–1 Architecture of the Oracle Audit Vault Audit Data Warehouse



This graphic shows the architecture of the Audit Vault Audit data warehouse. The Raw Audit Data Table on the left points to the Warehouse in the middle. On the far right, computers representing the analysis, reporting, and mining auditors all have input arrows pointing to the warehouse.

****

Audit records, stored in the raw audit data table go through an extraction and transformation process before the data loading process (ETL). The ETL operation takes place in the staging area. Oracle Audit Vault optimizes data in the data warehouse for data analysis, and includes the metadata and summaries that aid in these data analysis.

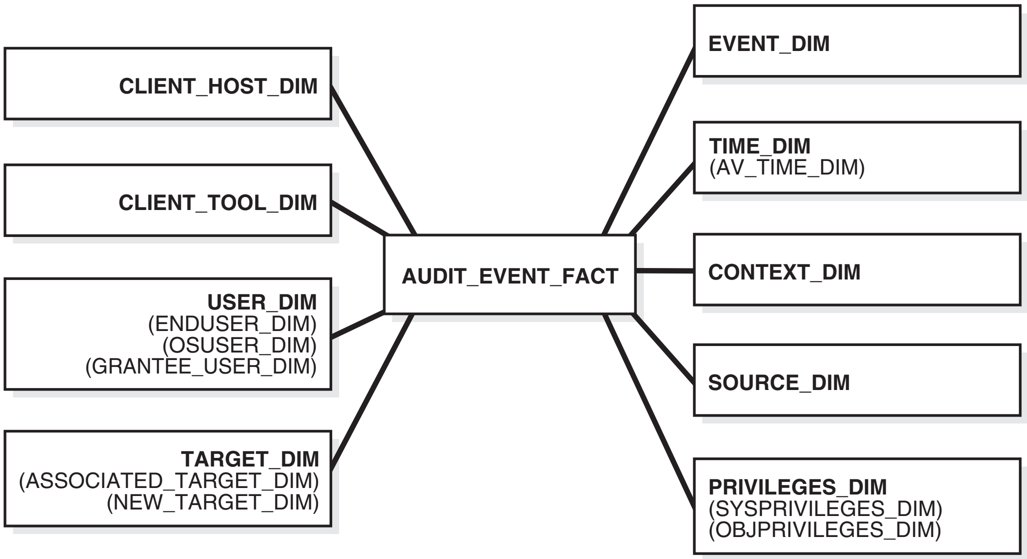
If you have been granted the `AV_AUDITOR` role, then you can directly access audit data in the audit data warehouse to analyze data, generate reports, and perform data mining. See *Oracle Database Data Warehousing Guide* for more information about Oracle data warehouses.

4.3 Design of the Audit Data Warehouse Schema

The audit data warehouse uses a logical design to model the logical relationships among the entities (tables) and their attributes (columns) as entity-relationship modeling. The audit record is the most important information, and it contains attributes or columns that describe it. Other information about the audit record is linked by foreign key to other tables that store this related information. This related information includes items such as its source information, its event information, its description of the objects in the source on which users performed actions, the client computer information from which these events originated, and the time when these events occurred. In data warehouse terminology, the audit record forms the *fact table* and its most important attributes form the *dimension tables*.

Oracle Audit Vault uses a star schema to model the audit data warehouse, as shown in Figure 4–2. The audit record is an entity (the fact table, `AUDIT_EVENT_FACT`) in the center of the star that is further described by its attributes (the dimensions) that form its points. A star schema optimizes performance by keeping queries simple and providing fast response time. All the information about each level is stored in one row.

Figure 4–2 Structure of the Oracle Audit Data Warehouse



This is a description of the audit data warehouse structure.

The AUDIT_EVENT_FACT is the center of this star-shaped configuration. From there, spokes go out to these attributes or dimension tables: CLIENT_HOST_DIM, CLIENT_TOOL_DIM, USER_DIM, TARGET_DIM, EVENT_DIM, TIME_DIM, CONTEXT_DIM, SOURCE_DIM, and PRIVILEGES_DIM.

Included in some of these are the names of dimension tables that reference the attribute. For example, the ENDUSER_DIM, OSUSER_DIM, and GRANTEE_USER_DIM dimension tables reference the USER_DIM dimension table. The ASSOC_TARGET_DIM and NEW_TARGET_DIM dimension tables reference the TARGET_DIM dimension table. The AV_TIME_DIM dimension table references the TIME_DIM dimension table. The SYSPRIVILEGES_DIM and OBJPRIVILEGES_DIM dimension tables reference the PRIVILEGES_DIM dimension table

****

The audit data warehouse involves a fact (the entity), which is an action, and dimensions (the attributes), which are details about the action. For example, a login attempt is a fact (an audit record). Who logged on, onto what system, at what time, using what authentication system, using what user name and password, and from what system are all dimensions (the attributes) about this fact. In the audit data warehouse, each fact represents an audit record and each dimension represents unique information about that audit record that further describes the audit record.

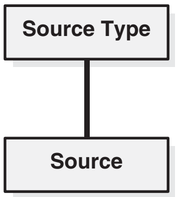
4.4 How the Fact Table and Dimension Tables Work

The **fact table**, `AUDIT_EVENT_FACT`, is linked to each dimension table by its foreign key. The fact table in the audit data warehouse contains the audit record ID, some attributes of the audit record for report generation, and the foreign keys to these dimensions. The main measure of the fact table is the result, whether a particular event was a success or failure.

A **dimension** is a structure, often composed of one or more hierarchies, that categorizes data to enable proper analysis of the data. Dimensions represent natural 1:*n* relationships between columns or column groups (the levels of a hierarchy) that cannot be represented with constraint conditions. Going up a level in the hierarchy is called rolling up the data, and going down a level in the hierarchy is called drilling down the data.

Level relationships specify top-to-bottom ordering of levels from most general (the root) to most specific information. They define the parent-child relationship between the levels in a hierarchy. A dimension hierarchy shows these level relationships. For example, the source dimension consists of two levels, source type and source, with the source being the child of its parent source type, as shown in Figure 4–3.

Figure 4–3 Source Dimension Hierarchy



This is a description of the source dimension hierarchy, which consists of two levels, source type and source, with the source being the child of its parent source type.

****

The primary key in the dimension tables is a unique identifier. Primary keys are represented with the characters PK. Foreign keys are represented by the characters FK.

The audit data warehouse includes the following dimensions:

- **Client Host**. This dimension consists of various systems that are used by clients to perform the operation. The basic hierarchy is IP address, subnet, and domain. The `CLIENT_HOST_DIM` dimension table, described in Section 4.6.2, stores this information. Oracle Audit Vault populates this table dynamically, as the audit records are entered into the raw audit data table.
- **Client Tools**. This dimension represents the information about the tools used to connect to the audit source database. The `CLIENT_TOOL_DIM` dimension table, described in Section 4.6.3, stores this information.
- **User**. This dimension tracks the user information that is associated with the events occurring at the source database. There is no hierarchy associated with the user information. The `USER_DIM` dimension table, described in Section 4.6.10, stores this information.
- **Target**. This dimension contains the information about the object on which the event is performed. The target is the object of the event. For example, if a user is granted a privilege, then the user becomes the target. If there is a query on the table, then the table is a target. The hierarchy is based on ownership of the target objects.

  The `TARGET_DIM` dimension table, described in Section 4.6.8, stores this information. Oracle Audit Vault updates the `TARGET_DIM` table is dynamically as audit records are entered into the raw audit data table. The target name is stored with the owner name appended to the target name (for example, `SCOTT.EMP` to represent the `EMP` table in the `SCOTT` schema).
- **Event**. This dimension is built on the various events that can be performed in any of the source databases. Oracle Audit Vault uses a category of events to group events, and this forms the hierarchy used by this dimension. The `EVENT_DIM` dimension table, described in Section 4.6.5, stores this information.

- **Time**. This dimension tracks actions over time. It is the most common use of the Oracle Audit Vault data warehouse. The hierarchy for time is based on calendar year.

  The TIME_DIM dimension table, described in Section 4.6.9, stores this information. The time dimension tracks event time as well as for the time when the record was received into the raw audit data table. The granularity of the time dimension is one day, and the actual time of the event and recording of the event are stored as measures in the fact table. Oracle Audit Vault uses this time measurement to filter events to granularity smaller than a day.
- **Context**. This dimension is used to represent the context information related to the audit event. This dimension has three levels: sub_context, context, and parent_context. You can use these levels to group events based on the context during analysis. The CONTEXT_DIM dimension table, described in Section 4.6.4, stores this information.
- **Source**. This dimension consists of the list of source databases that send audit data to the data warehouse. The SOURCE_DIM dimension table, described in Section 4.6.7, stores this information.
- **Privileges**. This dimension represents the information about the privileges used during the event. There is no hierarchy for this dimension. The PRIVILEGES_DIM dimension table, described in Section 4.6.6, stores this information.

4.5 Fact Table Constraints and Indexes

Table 4–1 lists the constraints in the AUDIT_EVENT_FACT table. Each constraint references the primary key of a dimension. All constraints are in RELY DISABLE NOVALIDATE mode. The constraints are guaranteed to be validated by the extract, transform, load (ETL) process. RELY is specified to take advantage of query rewrites based on the constraint even though they are disabled.

Table 4–1 Fact Table Constraints and Indexes

Constraint Name	Column Name	Reference Table
AV$FACT_ASSOC_TARGET_DIM_FK	ASSOC_TARGET_DIM	TARGET_DIM (DIMENSION_KEY)
AV$FACT_AV_TIME_DIM_FK	AV_TIME_DIM	TIME_DIM (DIMENSION_KEY)
AV$FACT_CLIENT_HOST_DIM_FK	CLIENT_HOST_DIM	CLIENT_HOST_DIM (DIMENSION_KEY)
AV$FACT_CLIENT_TOOL_DIM_FK	CLIENT_TOOL_DIM	CLIENT_TOOL_DIM (DIMENSION_KEY)
AV$FACT_CONTEXT_DIM_FK	CONTEXT_DIM	CONTEXT_DIM (DIMENSION_KEY)
AV$FACT_ENDUSER_DIM_FK	ENDUSER_DIM	USER_DIM (DIMENSION_KEY)
AV$FACT_EVENT_DIM_FK	EVENT_DIM	EVENT_DIM (DIMENSION_KEY)
AV$FACT_GRANTEE_USER_DIM_FK	GRANTEE_USER_DIM	USER_DIM (DIMENSION_KEY)
AV$FACT_NEW_TARGET_DIM_FK	NEW_TARGET_DIM	TARGET_DIM (DIMENSION_KEY)
AV$FACT_OBJPRIVILEGES_DIM_FK	OBJPRIVILEGES_DIM	PRIVILEGES_DIM (DIMENSION_KEY)
AV$FACT_OSUSER_DIM_FK	OSUSER_DIM	USER_DIM (DIMENSION_KEY)
AV$FACT_PRIVILEGES_DIM_FK	PRIVILEGES_DIM	PRIVILEGES_DIM (DIMENSION_KEY)
AV$FACT_SOURCE_DIM_FK	SOURCE_DIM	SOURCE_DIM (DIMENSION_KEY)
AV$FACT_SYSPRIVILEGES_DIM_FK	SYSPRIVILEGES_DIM	PRIVILEGES_DIM (DIMENSION_KEY)
AV$FACT_TARGET_DIM_FK	TARGET_DIM	TARGET_DIM (DIMENSION_KEY)
AV$FACT_TIME_DIM_FK	TIME_DIM	TIME_DIM (DIMENSION_KEY)
AV$FACT_USER_DIM_FK	USER_DIM	USER_DIM (DIMENSION_KEY)

Table 4–2 lists the local bitmap indexes in the AUDIT_EVENT_FACT table.

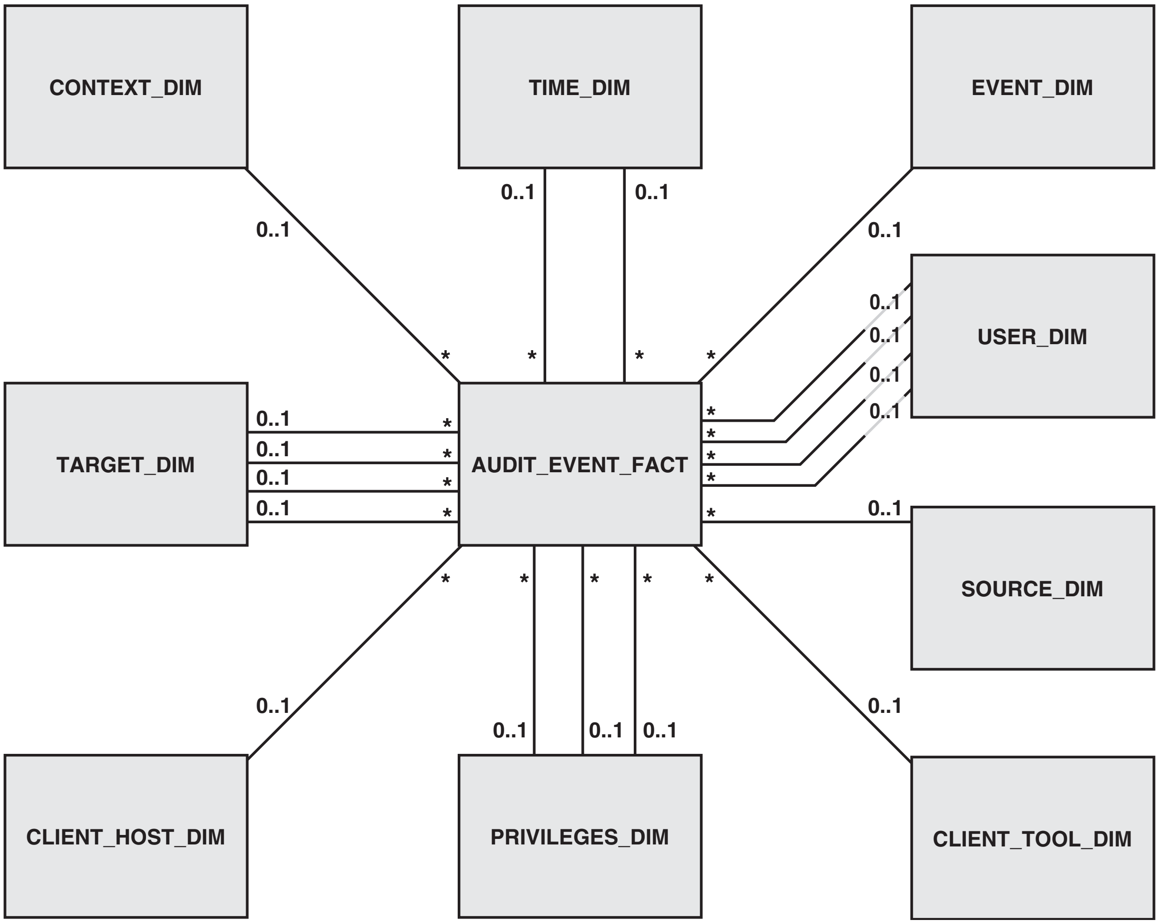
Table 4–2 Local Bitmap Indexes Defined on the AUDIT_EVENT_FACT Table

Index Name	Column Name
ASSOC_TARGET_DIM_IDX	ASSOC_TARGET_DIM
AV_TIME_DIM_IDX	AV_TIME_DIM
CLIENT_HOST_DIM_IDX	CLIENT_HOST_DIM
CLIENT_TOOL_DIM_IDX	CLIENT_TOOL_DIM
CONTEXT_DIM_IDX	CONTEXT_DIM
ENDUSER_DIM_IDX	ENDUSER_DIM
EVENT_DIM_IDX	EVENT_DIM
GRANTEE_USER_DIM_IDX	GRANTEE_USER_DIM
NEW_TARGET_DIM_IDX	NEW_TARGET_DIM
OBJPRIVILEGES_DIM_IDX	OBJPRIVILEGES_DIM
OSUSER_DIM_IDX	OSUSER_DIM
PRIVILEGES_DIM_IDX	PRIVILEGES_DIM
SOURCE_DIM_IDX	SOURCE_DIM
SYSPRIVILEGES_DIM_IDX	SYSPRIVILEGES_DIM
TARGET_DIM_IDX	TARGET_DIM
TIME_DIM_IDX	TIME_DIM
USER_DIM_IDX	USER_DIM

4.6 Relationships Between the Fact and Dimension Tables

Figure 4–4 shows the relationships between the tables of the Oracle Audit Vault data warehouse.

Figure 4–4 Tables in the Oracle Audit Vault Data Warehouse



This is a description of the diagram of ***tables in the Oracle Audit Vault Data Warehouse***. The AUDIT_EVENT_FACT table is in the center and the dimension tables radiate out from it. The dimension tables are CLIENT_HOST_DIM, CONTEXT_DIM, EVENT_DIM, PRIVILEGES_DIM, SOURCE_DIM, TARGET_DIM, TIME_DIM, and USER_DIM. The spokes include all include asterisks and 0...1 indicating a one-to-many relationship that exists between the fact table and the dimension table.

****

Table 4–3 through Table 4–12 contain information about the individual tables, including their columns, the data types for those columns, and whether the columns are allowed to be null. When the column is actually a reference to a dimension table, the referenced table is also listed. The asterisk and 0...1 show a one-to-many relationship that exists between the fact table and the dimension table.

4.6.1 AUDIT_EVENT_FACT Fact Table

Table 4–3 lists the contents of the `AUDIT_EVENT_FACT` table. This table stores audit data that the collectors have retrieved from the raw audit data store of the source databases.

Table 4–3 AUDIT_EVENT_FACT Fact Table

Column	Data Type	References	Description
ACTION_COMMAND_STR	VARCHAR2(4000)	None	The SQL text of the command procedure that was executed that resulted in the audit event being triggered
ACTION_NAME_STR	VARCHAR2(4000)	None	The name of audit event
ACTION_OBJECT_ID_NUM	NUMBER	None	Object identifier affected by the triggered audit action
ACTION_OBJECT_NAME_STR	VARCHAR2(4000)	None	Name of the object affected by the action; also the object name corresponding to the ACTION_OBJECT_ID_NUM identifier
ADMIN_OPTION_NUM	NUMBER	None	When an event includes grants, this field shows if the admin option was included
ASSOC_TARGET_DIM	NUMBER	TARGET_DIM	Dimension key value to the TARGET_DIM table, which contains information about the schema object on which an audit event is performed
AUDIT_OPTION_ID	NUMBER	None	ID links to the AUDIT_OPTION_TAB table, which indicates how the audit record was created; for example, the audit record was created when the event failed
AUTHENTICATION_METHOD_ID	NUMBER	None	ID links to the AUTHENTICATION_METHOD_TAB table, which indicates how the database connection was authenticated
AV_TIME	TIMESTAMP WITH LOCAL TIME ZONE	None	The time in which Oracle Audit Vault receives the audit trail record into the repository
AV_TIME_DIM	NUMBER	TIME_DIM	Dimension key value to the TIME_DIM table, which tracks actions over time
CLIENT_APPINFO_STR	VARCHAR2(4000)	None	Deprecated; will be removed in a future release
CLIENT_HOST_DIM	NUMBER	CLIENT_HOST_DIM	Dimension key value to the CLIENT_HOST_DIM table, which contains information about various systems that are used by clients to perform an operation
CLIENT_ID_ID	NUMBER	None	ID links to the CLIENT_ID_TAB table, which displays the client identifier value in an Oracle database updated by an application

Table 4–3 (Cont.) AUDIT_EVENT_FACT Fact Table

Column	Data Type	References	Description
CLIENT_TOOL_DIM	NUMBER	CLIENT_TOOL_DIM	Dimension key value to the CLIENT_TOOL_DIM table, which contains information about the tools and programs used to connect to an audit source database
COMMENT_TEXT_ID	NUMBER	None	ID that links to the COMMENT_TEXT_TAB table, which contains additional information about the audit event
CONTEXT_DIM	NUMBER	CONTEXT_DIM	Dimension key to the CONTEXT_DIM table, which contains context information related to an audit event such as transaction ID
CREATE_DATE_TS	TIMESTAMP(6) WITH LOCAL TIME ZONE	None	Date the audit trail record was created in the Oracle Database Vault audit trail
CREATED_BY_STR	VARCHAR2(4000)	None	Database login user name of the user who created the Oracle Database Vault rule
CURRENT_VALUE_STR	VARCHAR2(4000)	None	If the event resulted in the update of a value, this item contains the value after the update. This may include changes in a target name or audit option.
DATA_VALUES_CNT	NUMBER	None	Number of columns that have changed due to an insert or update
DATABASE_ID_NUM	NUMBER	None	ID of the database specified by the USE database statement, or the default database if no USE database statement is issued for a given connection
DATABASE_NAME_STR	VARCHAR2(4000)	None	Name of the database specified in the USE database statement
DOMAIN_NAME_STR	VARCHAR2(4000)	None	Domain name of the host system
DURATION_NUM	NUMBER	None	Amount of elapsed time (in milliseconds) taken by the event
ENDUSER_DIM	NUMBER	USER_DIM	Dimension key to the USER_DIM table, which tracks information about the user who is associated with the events that occur in the source database
END_TIME_TS	TIMESTAMP(6) WITH LOCAL TIME ZONE	None	Time at which the event ended. This column is not populated for starting event classes, such as SQL:BatchStarting or SP:Starting.

Table 4–3 (Cont.) AUDIT_EVENT_FACT Fact Table

Column	Data Type	References	Description
ERROR_ID_NUM	NUMBER	None	Error message number
ERROR_MESSAGE_STR	VARCHAR2(4000)	None	Error message text
EVENT_DIM	NUMBER	EVENT_DIM	Dimension key to the EVENT_DIM table, which contains information about various events that can be performed in the source databases
EVENT_STATUS_ID	NUMBER	None	ID of the EVENT_STATUS_TAB table, which contains the status of the audit action. If the action was successful, it shows a status of 0 - Action. If the action was unsuccessful, it shows the error code that the action generates, such as 2004 - Security violation for an Oracle Database security violation.
EVENT_SUB_CLASS_NUM	NUMBER	None	Type of event subclass. This data column is not populated for all event classes.
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE	None	Date and time of the creation of the audit trail entry (date and time of the user login for entries created by AUDIT SESSION) in the local database session time zone
FACTOR_CONTEXT_STR	VARCHAR2(4000)	None	The Oracle Database Vault factor identifiers for the current session at the point when the audit event was triggered
FGA_POLICYNAME_ID	NUMBER	None	Fine-grained audit policy name; only applies to Oracle Database
GRANTEE_USER_DIM	NUMBER	USER_DIM	Dimension key to the USER_DIM table, which tracks information about the user who is associated with the events that occur in the source database
GUID_NUM	NUMBER	None	Global user identifier value, which is dependent on the event class captured in the trace
INDEX_ID_NUM	NUMBER	None	Index ID associated with an audit event
INSTANCE_NUMBER_NUM	NUMBER	None	The database instance number in an Oracle Real Applications Cluster

Table 4–3 (Cont.) AUDIT_EVENT_FACT Fact Table

Column	Data Type	References	Description
IS_SYSTEM_NUM	NUMBER	None	Indicates whether the event occurred on a system process or a user process: ■ 1: system ■ 0: user
LOGOFF_DLOCK_NUM	NUMBER	None	Deadlocks detected during the session
LOGOFF_LREAD_NUM	NUMBER	None	Logical reads for the session
LOGOFF_LWRITE_NUM	NUMBER	None	Logical writes for the session
LOGOFF_PREAD_NUM	NUMBER	None	Logical reads for the session
MODULE_NAME_STR	VARCHAR2(4000)	None	Program that generated the audit trail record
NEW_TARGET_DIM	NUMBER	TARGET_DIM	Dimension key to the TARGET_DIM table, which contains information about the schema object on which an audit event is performed
OBJECT_ID_NUM	NUMBER	None	Object identifier affected by the triggered audit action
OBJPRIVILEGES_DIM	NUMBER	PRIVILEGES_DIM	Dimension key to the PRIVILEGES_DIM table, which contains information about the privileges used during an audit event
ORIGINAL_CONTENT1_STR	VARCHAR2(4000)	None	Original content of an invalid record
ORIGINAL_CONTENT2_STR	VARCHAR2(4000)	None	Original content of an invalid record
ORIGINAL_CONTENT3_STR	VARCHAR2(4000)	None	Original content of an invalid record
OSUSER_DIM	NUMBER	USER_DIM	Dimension key to the USER_DIM table, which tracks information about the user who is associated with the events that occur in the source database
OWNER_ID_NUM	NUMBER	None	Type of the object that owns the lock; for lock events only
PREVIOUS_VALUE_STR	VARCHAR2(4000)	None	If the event resulted in the update of a value, this column contains the value prior to the update. This value can include changes in a target name or audit option. (Non-Oracle databases only)
PRIVILEGES_DIM	NUMBER	PRIVILEGES_DIM	Dimension key to the PRIVILEGES_DIM table, which contains information about the privileges used during an audit event

Table 4–3 (Cont.) AUDIT_EVENT_FACT Fact Table

Column	Data Type	References	Description
PRIV_ID_NUM	NUMBER	None	ID of the privilege used to execute a transaction
PROCESS#	NUMBER	None	Unique process identifier that generated the audit action
PROXY_INFORMATION_STR	VARCHAR2(4000)	None	The original login name if the event occurred while a set proxy was in effect
PROXY_SESSIONID_NUM	NUMBER	None	Session ID of the proxy user
RECORD_ID	NUMBER	None	Unique identifier of the audit record created when the audit trail is inserted into the Oracle Audit Vault repository
ROW_ID_STR	VARCHAR2(4000)	None	Row identifier; for example, for the Oracle Database table row that was accessed or modified
RULE_ID_NUM	NUMBER	None	The unique identifier of the rule that was executing and caused the audit event to trigger in Oracle Database Vault
RULE_NAME_STR	VARCHAR2(4000)	None	The unique name of the rule that was executing and triggered the audit event in Oracle Database Vault
RULE_SET_ID_NUM	NUMBER	None	The unique identifier of the rule set that was executing and triggered the audit event in Oracle Database Vault
RULE_SET_NAME_STR	VARCHAR2(4000)	None	The unique name of the rule set that was executing and triggered the audit event in Oracle Database Vault
SCN_NUM	NUMBER	None	Oracle system change number at the time of query submission when the audit action was recorded
SERVER_NAME_STR	VARCHAR2(4000)	None	Name of the instance of SQL Server, either server name or server name and instance name, being traced
SESSION_ACTIONS_ID	NUMBER	None	ID to the SESSION_ACTIONS_TAB table, which contains session information of transactions
SESSION_CPU_NUM	NUMBER	None	Amount of CPU time used by each session
SESSION_LOGIN_NAME_STR	VARCHAR2(4000)	None	The login name of the user who originated the session
SEVERITY_NUM	NUMBER	None	Error severity
SOURCE_DATABASE_ID_NUM	NUMBER	None	ID of the database in which the source of the object exists

Table 4–3 (Cont.) AUDIT_EVENT_FACT Fact Table

Column	Data Type	References	Description
SOURCE_DIM	NUMBER	SOURCE_DIM	Dimension key to the SOURCE_DIM table, which contains information about the source databases that send audit data to the data warehouse
SOURCE_EVENTID	VARCHAR2(4000)	None	Audit event identifier from the source database
SQL_BIND_STR	VARCHAR2(4000)	None	Bind variable data used by the SQL query statement, if any
SQL_TEXT_STR	VARCHAR2(4000)	None	SQL statement issued by the user that triggered the audit action
STATEMENTID_NUM	NUMBER	None	Numeric identifier for each SQL statement executed
SYSPRIVILEGES_DIM	NUMBER	PRIVILEGES_DIM	Dimension key to the PRIVILEGES_DIM table, which contains information about the privileges used during an audit event
TARGET_DIM	NUMBER	TARGET_DIM	Dimension key to the TARGET_DIM table, which contains information about the schema object on which an audit event is performed
TARGET_LOGIN_SID_STR	VARCHAR2(4000)	None	SID of the login that is the target of some action
TARGET_OBJECT_TYPE_STR	VARCHAR2(4000)	None	Type of object, such as table, function, or stored procedure
THREAD#	NUMBER	None	Unique thread identifier that generated the audit action
TIME_DIM	NUMBER	TIME_DIM	Dimension key to the TIME_DIM table, which tracks actions over time
TRANSACTION_NAME_ID	NUMBER	None	ID to the TRANSACTION_NAME_TAB table, which contains the name of the transaction in which the object is accessed or modified
UNDO_SQL_TEXT_STR	VARCHAR2(4000)	None	Not used
UPDATE_DATE_TS	TIMESTAMP(6) WITH LOCAL TIME ZONE	None	For Oracle Database Vault, the date on which the command rule or realm information was updated

Table 4–3 (Cont.) AUDIT_EVENT_FACT Fact Table

Column	Data Type	References	Description
UPDATED_BY_STR	VARCHAR2(4000)	None	For Oracle Database Vault, the user who updated the command rule or realm
USER_DIM	NUMBER	USER_DIM	Dimension key to the USER_DIM table, which tracks information about the user who is associated with the events that occur in the source database
USER_GUID_ID	NUMBER	None	Global user identifier for the user, if the user has logged in as an enterprise user; also the global user identifier of Oracle Internet Direcgtory (OID) user

4.6.2 CLIENT_HOST_DIM Dimension Table

The CLIENT_HOST_DIM table contains information about various systems that are used by clients to perform an operation.

Table 4–4 lists the contents of the CLIENT_HOST_DIM table.

Table 4–4 CLIENT_HOST_DIM Dimension Table

Column	Data Type	Description
DIMENSION_KEY	NUMBER	Dimension key to the AUDIT_EVENT_FACT fact table
DOMAIN_ID	NUMBER	ID of the domain
DOMAIN_NAME	VARCHAR2(255)	Domain name of the host system
HOST_ID	NUMBER	ID of the host computer
HOST_IP	VARCHAR2(255)	Host IP address
HOST_NAME	VARCHAR2(255)	Name of the host
TERMINAL_ID	NUMBER	Identifier for the user's terminal
TERMINAL_NAME	VARCHAR2(255)	Name of the user’s terminal

4.6.3 CLIENT_TOOL_DIM Dimension Table

The CLIENT_TOOL_DIM table contains information about the tools used to connect to an audit source database.

Table 4–5 lists the contents of the CLIENT_TOOL_DIM table.

Table 4–5 CLIENT_TOOL_DIM Dimension Table

Column	Data Type	Description
DIMENSION_KEY	NUMBER	Dimension key to the AUDIT_EVENT_FACT fact table
TOOL_ID	NUMBER	ID of the tools and programs used to connect to an audit source database
TOOL_NAME	VARCHAR2(4000)	The tools and programs used to connect to an audit source database

4.6.4 CONTEXT_DIM Dimension Table

The CONTEXT_DIM table contains context information related to an audit event.

Table 4–6 lists the contents of the CONTEXT_DIM table.

REVIEWERS: The CONTEXT and CONTEXT_ID columns both have identical descriptions. Same goes for the SUB_CONTEXT and SUB_CONTEXT_ID descriptions. What are their real descriptions?

Table 4–6 CONTEXT_DIM Dimension Table

Column	Data Type	Description
CONTEXT	VARCHAR2(4000)	Session ID of the audit event
CONTEXT_ID	NUMBER	Session ID of the audit event
DIMENSION_KEY	NUMBER	Dimension key to the AUDIT_EVENT_FACT fact table
PARENT_CONTEXT	VARCHAR2(4000)	Sequence number or identifier of a transaction
PARENT_CONTEXT_ID	NUMBER	Sequence number or identifier of a transaction
SUB_CONTEXT	VARCHAR2(4000)	Transaction ID
SUB_CONTEXT_ID	NUMBER	Transaction ID

4.6.5 EVENT_DIM Dimension Table

The EVENT_DIM table contains information about various events that can be performed in the source databases.

Table 4–7 lists the contents of the EVENT_DIM table.

Table 4–7 EVENT_DIM Dimension Table

Column	Data Type	Description
AVEVENT_ID	NUMBER	Oracle Audit Vault audit event identifier
CATEGORY_ID	NUMBER	Oracle Audit Vault category identifier
CATEGORY_NAME	VARCHAR2(255)	Oracle Audit Vault category name
DIMENSION_KEY	NUMBER	Dimension key to the AUDIT_EVENT_FACT fact table
EVENT_DESCRIPTION	VARCHAR2(255)	Description of the event
EVENT_ID	NUMBER	Source audit event ID
EVENT_NAME	VARCHAR2(255)	Source audit event name

4.6.6 PRIVILEGES_DIM Dimension Table

The PRIVILEGES_DIM table contains information about the privileges used during an audit event.

Table 4–8 lists the contents of the PRIVILEGES_DIM table.

Table 4–8 PRIVILEGES_DIM Dimension Table

Column	Data Type	Description
DIMENSION_KEY	NUMBER	Dimension key to the AUDIT_EVENT_FACT fact table
PRIV_ID	NUMBER	ID of the privilege used to execute a transaction
PRIV_NAME	VARCHAR2(4000)	Name of the privilege used to execute a transaction

4.6.7 SOURCE_DIM Dimension Table

The SOURCE_DIM table contains information about the source databases that send audit data to the data warehouse.

Table 4–9 lists the contents of the SOURCE_DIM table.

Table 4–9 SOURCE_DIM Dimension Table

Column	Data Type	Description
DIMENSION_KEY	NUMBER	Dimension key to the AUDIT_EVENT_FACT fact table
SOURCE_DESCRIPTION	VARCHAR2(255)	Description of the source that is defined when the source is added to Oracle Audit Vault
SOURCE_HOST	VARCHAR2(255)	Name of the host computer on which the audit source database resides
SOURCE_HOSTIP	VARCHAR2(255)	IP of the host computer on which the audit source database resides
SOURCE_ID	NUMBER	ID of the audit source database assigned to Oracle Audit Vault
SOURCE_NAME	VARCHAR2(255)	Name of the source database that is defined when the source is added to Oracle Audit Vault
SOURCE_POLICY	NUMBER	Deprecated; will be removed in a future release
SOURCE_STATUS	NUMBER	Indicates if the source database is currently active in Oracle Audit Vault
SOURCE_VERSION	VARCHAR2(30)	Version number of the source database
SOURCETYPE_DESCRIPTION	VARCHAR2(30)	Description of the type of source database in which audit trail records are being extracted
SOURCETYPE_ID	NUMBER	ID of the type of source database in which audit trail records are being extracted
SOURCETYPE_NAME	SOURCETYPE_NAME	Name of the type of source database in which audit trail records are being extracted

4.6.8 TARGET_DIM Dimension Table

The TARGET_DIM table contains information about the schema object on which an audit event is performed.

Table 4–10 lists the contents of the TARGET_DIM table.

Table 4–10 TARGET_DIM Dimension Table

Column	Data Type	Description
DIMENSION_KEY	NUMBER	Dimension key to the AUDIT_EVENT_FACT fact table
OWNER_ID	NUMBER	ID of the owner of the target object
OWNER_NAME	VARCHAR2(4000)	Name of the owner of the target object
TARGET_ID	NUMBER	ID of the target object that is being audited
TARGET_NAME	VARCHAR2(4000)	Name of the target object that is being audited

4.6.9 TIME_DIM Dimension Table

The TIME_DIM table tracks actions over time. This table is the most commonly used by the data warehouse. It implements four levels in the dimension hierarchy (DAY, MONTH, QUARTER, YEAR). The CALENDAR prefix distinguishes between a fiscal quarter and a fiscal year.

Table 4–11 lists the contents of the TIME_DIM table.

Table 4–11 TIME_DIM Dimension Table

Column	Data Type	Description
CALENDAR_MONTH_CODE	NUMBER	Numeric representation for the MONTH level (for example, 200802 for February, 2008)
CALENDAR_MONTH_DESCRIPTION	VARCHAR2(255)	Text description for level for the MONTH level (for example, Feb 2008)
CALENDAR_MONTH_END_DATE	DATE	End date for the MONTH level (for example, 29-feb-08)
CALENDAR_MONTH_ID	NUMBER	ID for the MONTH level
CALENDAR_MONTH_NAME	VARCHAR2(255)	Same as CALENDAR_MONTH_DESCRIPTION
CALENDAR_MONTH_OF_QUARTER	NUMBER	Numeric representation for the month in this quarter (for example, 2 for February, assuming the quarter begins in January)
CALENDAR_MONTH_OF_YEAR	NUMBER	Numeric representation for the month in the year (for example, 2 for February)
CALENDAR_MONTH_START_DATE	DATE	Start date of the MONTH level (for example, 1-feb-08)
CALENDAR_MONTH_TIME_SPAN	NUMBER	Duration of the MONTH level (for example, 29)
CALENDAR_QUART_CODE	NUMBER	Numeric representation for the QUARTER level (for example, 2 for the second quarter)

Table 4–11 (Cont.) TIME_DIM Dimension Table

Column	Data Type	Description
CALENDAR_QUART_DESCRIPTION	VARCHAR2(255)	Text description for the QUARTER level (for example, 2 for the second quarter)
CALENDAR_QUART_END_DATE	DATE	End date for the QUARTER level (for example, 29-feb-08)
CALENDAR_QUART_ID	NUMBER	ID for the QUARTER level
CALENDAR_QUART_NAME	VARCHAR2(255)	Same as CALENDAR_QUART_DESCRIPTION
CALENDAR_QUART_OF_YEAR	NUMBER	Numeric representation of the calendar quarter (for example, 2 for the second quarter of the year)
CALENDAR_QUART_START_DATE	DATE	Start date of the MONTH level (for example, 1-feb-08)
CALENDAR_QUART_TIME_SPAN	NUMBER	Duration of the QUARTER level (for example, 90)
CALENDAR_YEAR_CODE	NUMBER	Numeric representation for the YEAR level (for example, 2008 for the year 2008)
CALENDAR_YEAR_DESCRIPTION	VARCHAR2(255)	Text description for the YEAR level (for example, 2008)
CALENDAR_YEAR_END_DATE	DATE	End date for the YEAR level (for example, 31-dec-08)
CALENDAR_YEAR_ID	NUMBER	ID of the YEAR level
CALENDAR_YEAR_NAME	VARCHAR2(255)	Same as CALENDAR_YEAR_DESCRIPTION
CALENDAR_YEAR_START_DATE	DATE	Start date of the YEAR level (for example, 1-jan-08)
CALENDAR_YEAR_TIME_SPAN	NUMBER	Duration of the YEAR level (for example, 360)
DAY	DATE	Numeric representation of the day (for example, 14 for the 14th day)
DAY_CODE	NUMBER	Numeric representation for the DAY level (for example, 20080214 for February 12, 2008)
DAY_DESCRIPTION	VARCHAR2(255)	Text description of for the DAY level (for example, 14 for the 14th day of the month)
DAY_END_DATE	DATE	End date for the DAY level (for example, 29-feb-08)
DAY_ID	NUMBER	ID for the DAY level
DAY_NAME	VARCHAR2(255)	Same as DAY_DESCRIPTION
DAY_OF_CAL_MONTH	NUMBER	Numeric representation of the day of the calendar month (for example, 14)
DAY_OF_CAL_QUARTER	NUMBER	Numeric representation of the day of the calendar quarter (for example, 14)

Table 4–11 (Cont.) TIME_DIM Dimension Table

Column	Data Type	Description
DAY_OF_CAL_WEEK	NUMBER	Numeric representation of the day of the calendar week (for example, 7)
DAY_OF_CAL_YEAR	NUMBER	Numeric representation of the day of the calendar year (for example, 14)
DAY_START_DATE	DATE	Start date of the DAY level (for example, 1-feb-08)
DAY_TIME_SPAN	NUMBER	Duration of the DAY level (for example, 1)
DIMENSION_KEY	NUMBER	Unique key across all levels

4.6.10 USER_DIM Dimension Table

The USER_DIM table tracks information about the user who is associated with the events that occur in the source database.

Table 4–12 lists the contents of the USER_DIM table.

Table 4–12 USER_DIM Dimension Table

Column	Data Type	Description
DIMENSION_KEY	NUMBER	Dimension key to the AUDIT_EVENT_FACT fact table
USER_ID	NUMBER	ID of the user assigned by Oracle Audit Vault
USER_NAME	VARCHAR2(255)	Name of the user that is associated with an audit trail record

A

Oracle Database Audit Events

This appendix contains:

A.1 About the Oracle Database Audit Events

This appendix lists the audit event names and IDs, and the attribute names and data types for Oracle Database. The audit events are organized by their respective categories; for example, Account Management. You can use these audit events as follows:

- **For alerts.** When you create an alert, you can specify an audit event, based on its category, that can trigger the alert. See Section 2.12.2 for more information.
- **For custom reports using third-party tools.** If you want to create custom reports using other Oracle Database reporting products or third-party tools, refer to the tables in this appendix when you design the reports. See Chapter 4, "Oracle Audit Vault Data Warehouse Schema" for more information about custom reports created with third-party tools.

A.2 Account Management Events

Account management events track SQL statements that affect user accounts, such as creating users or altering their profiles. The Account Management Report, described in Section 3.4.1, uses these events.

Table A–1 lists the Oracle Database account management events and event IDs.

Table A–1 Oracle Database Account Management Events and Event IDs

Event Name	Event ID
ALTER PROFILE	67
ALTER USER	43
CREATE PROFILE	65
CREATE USER	51
DROP PROFILE	66
DROP USER	53

Table A–2 lists the Oracle Database account management event attributes.

Table A–2 Oracle Database Account Management Event Attributes

Attribute Name	Data Type
CLIENT_APPINFO	VARCHAR2(4000)
CLIENT_ID	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INSTANCE_NUMBER	NUMBER
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_SESSIONID	NUMBER
SCN	NUMBER
SESSION_ACTIONS	VARCHAR2(255)
SOURCE_EVENTID	VARCHAR2(255)
SQL_BIND[1]	VARCHAR2(4000)
SQL_TEXT[2]	VARCHAR2(4000)

Table A–2 (Cont.) Oracle Database Account Management Event Attributes

Attribute Name	Data Type
STATEMENTID	NUMBER
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
UNDO_SQL_TEXT	VARCHAR2(4000)
USER_GUID	VARCHAR2(32)
USERNAME	VARCHAR2(4000)

[1] SQL_BIND variable could be truncated to 4000 characters.

[2] SQL_TEXT variable could be truncated to 4000 characters.

A.3 Application Management Events

Application management events track actions that were performed on the underlying PL/SQL procedures or functions of system services and applications, such as ALTER FUNCTION statements. The Procedure Management Report, described in Section 3.4.4, uses these events.

Table A–3 lists the Oracle Database application management events and event IDs.

Table A–3 Oracle Database Application Management Events and Event IDs

Event Name	Event ID
ALTER FUNCTION	92
ALTER JAVA	161
ALTER PACKAGE	95
ALTER PACKAGE BODY	98
ALTER PROCEDURE	25
ALTER RESOURCE COST	70
ALTER REWRITE EQUIVALENCE	210
ALTER TRIGGER	60
ALTER TYPE	80
ALTER TYPE BODY	82
ANALYZE INDEX	63
ANALYZE TABLE	62
ASSOCIATE STATISTICS	168
CREATE CONTEXT	177
CREATE FUNCTION	91
CREATE INDEXTYPE	164
CREATE JAVA	160
CREATE LIBRARY	159

Table A–3 (Cont.) Oracle Database Application Management Events and Event IDs

Event Name	Event ID
CREATE OPERATOR	163
CREATE PACKAGE	94
CREATE PACKAGE BODY	97
CREATE PROCEDURE	24
CREATE TRIGGER	59
CREATE TYPE	77
CREATE TYPE BODY	81
DECLARE REWRITE EQUIVALENCE	209
DISABLE TRIGGER	119
DISASSOCIATE STATISTICS	169
DROP CONTEXT	178
DROP FUNCTION	93
DROP INDEXTYPE	165
DROP JAVA	162
DROP LIBRARY	84
DROP OPERATOR	167
DROP PACKAGE	96
DROP PACKAGE BODY	99
DROP PROCEDURE	68
DROP REWRITE EQUIVALENCE	211
DROP TRIGGER	61
DROP TYPE	78
DROP TYPE BODY	83
ENABLE TRIGGER	118
EXECUTE TYPE	123
EXPLAIN	50

Table A–4 lists the Oracle Database application management event attributes.

Table A–4 Oracle Database Application Management Event Attributes

Attribute Name	Data Type
ASSOCIATED_OBJECT_NAME	VARCHAR2(4000)
ASSOCIATED_OBJECT_OWNER	VARCHAR2(4000)
CLIENT_APPINFO	VARCHAR2(4000)
CLIENT_ID	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)

Table A–4 (Cont.) Oracle Database Application Management Event Attributes

Attribute Name	Data Type
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INSTANCE_NUMBER	NUMBER
NEW_OBJECT_NAME	VARCHAR2(4000)
NEW_OBJECT_OWNER	VARCHAR2(4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_SESSIONID	NUMBER
SCN	NUMBER
SESSION_ACTIONS	VARCHAR2(255)
SOURCE_EVENTID	VARCHAR2(255)
SQL_BIND[1]	VARCHAR2(4000)
SQL_TEXT[2]	VARCHAR2(4000)
STATEMENTID	NUMBER
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
UNDO_SQL_TEXT	VARCHAR2(4000)
USER_GUID	VARCHAR2(32)
USERNAME	VARCHAR2(4000)

[1] SQL_BIND variable could be truncated to 4000 characters.

[2] SQL_TEXT variable could be truncated to 4000 characters.

A.4 Audit Command Events

Audit command events track the use of AUDIT SQL statements on other SQL statements and on database objects. The Audit Command Report, described in Section 3.4.2, uses these events.

Table A–5 lists the Oracle Database audit command events and event IDs.

Table A–5 Oracle Database Audit Command Events and Event IDs

Event Name	Event ID
AUDIT DEFAULT	106
AUDIT OBJECT	30
NOAUDIT DEFAULT	107
NOAUDIT OBJECT	31
SYSTEM AUDIT	104
SYSTEM NOAUDIT	105

Table A–6 lists the Oracle Database audit command event attributes.

Table A–6 Oracle Database Audit Command Event Attributes

Attribute Name	Data Type
AUDIT_OPTION	VARCHAR2(4000)
CLIENT_APPINFO	VARCHAR2(4000)
CLIENT_ID	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INSTANCE_NUMBER	NUMBER
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_SESSIONID	NUMBER
SCN	NUMBER
SESSION_ACTIONS	VARCHAR2(255)
SOURCE_EVENTID	VARCHAR2(255)
SQL_BIND[1]	VARCHAR2(4000)
SQL_TEXT[2]	VARCHAR2(4000)
STATEMENTID	NUMBER
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)

Table A–6 (Cont.) Oracle Database Audit Command Event Attributes

Attribute Name	Data Type
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
UNDO_SQL_TEXT	VARCHAR2(4000)
USER_GUID	VARCHAR2(32)
USERNAME	VARCHAR2(4000)

[1] SQL_BIND variable could be truncated to 4000 characters.

[2] SQL_TEXT variable could be truncated to 4000 characters.

A.5 Data Access Events

Data access events track audited data manipulation language (DML) activities, for example, all SELECT, INSERT, UPDATE, or DROP SQL statements. The Data Access Report, described in Section 3.3.2, uses these events.

Table A–7 lists the Oracle Database data access events and event IDs.

Table A–7 Oracle Database Data Access Events and Event IDs

Event Name	Event ID
DELETE	7
INSERT	2
SELECT	3
TRUNCATE TABLE	85
UPDATE	6

Table A–8 lists the Oracle Database data access event attributes.

Table A–8 Oracle Database Data Access Event Attributes

Attribute Name	Data Type
CLIENT_APPINFO	VARCHAR2(4000)
CLIENT_ID	VARCHAR2(4000)
COL_NAMELIST	VARCHAR2(4000)
COL_NEWVAL1	VARCHAR2(4000)
COL_NEWVAL2	VARCHAR2(4000)
COL_NEWVAL3	VARCHAR2(4000)
COL_NEWVAL4	VARCHAR2(4000)
COL_NEWVAL5	VARCHAR2(4000)
COL_NEWVAL6	VARCHAR2(4000)
COL_NEWVAL7	VARCHAR2(4000)
COL_NEWVAL8	VARCHAR2(4000)
COL_NEWVAL9	VARCHAR2(4000)

Table A–8 (Cont.) Oracle Database Data Access Event Attributes

Attribute Name	Data Type
COL_NEWVAL10	VARCHAR2(4000)
COL_NEWVAL11	VARCHAR2(4000)
COL_OLDVAL1	VARCHAR2(4000)
COL_OLDVAL2	VARCHAR2(4000)
COL_OLDVAL3	VARCHAR2(4000)
COL_OLDVAL4	VARCHAR2(4000)
COL_OLDVAL5	VARCHAR2(4000)
COL_OLDVAL6	VARCHAR2(4000)
COL_OLDVAL7	VARCHAR2(4000)
COL_OLDVAL8	VARCHAR2(4000)
COL_OLDVAL9	VARCHAR2(4000)
COL_OLDVAL10	VARCHAR2(4000)
COL_OLDVAL11	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
DATA_VALUES	AV_DATAVALUES_LIST
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
FGA_POLICYNAME	VARCHAR2(30)
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INSTANCE_NUMBER	NUMBER
NUM_INLINECOL	NUMBER
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_SESSIONID	NUMBER
ROW_ID	VARCHAR2(18)
SCN	NUMBER
SESSION_ACTIONS	VARCHAR2(255)
SOURCE_EVENTID	VARCHAR2(255)
SQL_BIND[1]	VARCHAR2(4000)
SQL_TEXT[2]	VARCHAR2(4000)

Table A–8 (Cont.) Oracle Database Data Access Event Attributes

Attribute Name	Data Type
STATEMENTID	NUMBER
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
TRANSACTION_NAME	VARCHAR2(256)
UNDO_SQL_TEXT	VARCHAR2(4000)
USER_GUID	VARCHAR2(32)
USERNAME	VARCHAR2(4000)

[1] SQL_BIND variable could be truncated to 4000 characters.

[2] SQL_TEXT variable could be truncated to 4000 characters.

A.6 Oracle Database Vault Events

Oracle Database Vault events track audited Oracle Database Vault activity. The Oracle Database Vault Report, described in Section 3.3.3, uses these events.

Table A–9 lists the Oracle Database Vault events and event IDs.

Table A–9 Oracle Database Vault Events and Event IDs

Event Name	Event ID
ACCESS CTRL COMMAND AUTH	1008
ACCESS CTRL SESSION INIT	1009
COMMAND AUTHORIZATION	1005
FACTOR ASSIGNMENT	1001
FACTOR EVALUATION	1000
FACTOR EXPRESSION	1002
LBL SEC ATTEMPT TO UPGRADE	1010
LBL SEC SESSION INIT	1007
REALM AUTHORIZATION	1004
REALM VIOLATION	1003
SECURE ROLE	1006

Table A–10 lists the Oracle Database Vault event attributes.

Table A–10 Oracle Database Vault Event Attributes

Attribute Name	Data Type
ACTION_COMMAND	VARCHAR2(4000)
ACTION_NAME	VARCHAR2(128)
ACTION_OBJECT_ID	NUMBER

Table A–10 (Cont.) Oracle Database Vault Event Attributes

Attribute Name	Data Type
ACTION_OBJECT_NAME	VARCHAR2(128)
AUDIT_OPTION	VARCHAR2(4000)
CREATE_DATE	TIMESTAMP WITH LOCAL TIME ZONE
CREATED_BY	VARCHAR2(30)
FACTOR_CONTEXT	VARCHAR2(4000)
RULE_ID	NUMBER
RULE_NAME	VARCHAR2(90)
RULE_SET_ID	NUMBER
RULE_SET_NAME	VARCHAR2(90)
UPDATE_DATE	TIMESTAMP WITH LOCAL TIME ZONE
UPDATED_BY	VARCHAR2(30)

A.7 Exception Events

Exception events track audited error and exception activity, such as network errors. The Exception Activity Report, described in Section 3.5.1, uses these events.

Table A–11 lists the Oracle Database exception events and event IDs.

Table A–11 Oracle Database Exception Events and Event IDs

Event Name	Event ID
NETWORK ERROR	122

Table A–12 lists the Oracle Database exception event attributes.

Table A–12 Oracle Database Exception Event Attributes

Attribute Name	Data Type
CLIENT_APPINFO	VARCHAR2(4000)
CLIENT_ID	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INSTANCE_NUMBER	NUMBER
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)

Table A–12 (Cont.) Oracle Database Exception Event Attributes

Attribute Name	Data Type
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_SESSIONID	NUMBER
SCN	NUMBER
SESSION_ACTIONS	VARCHAR2(255)
SOURCE_EVENTID	VARCHAR2(255)
SQL_BIND[1]	VARCHAR2(4000)
SQL_TEXT[2]	VARCHAR2(4000)
STATEMENTID	NUMBER
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
UNDO_SQL_TEXT	VARCHAR2(4000)
USER_GUID	VARCHAR2(32)
USERNAME	VARCHAR2(4000)

[1] SQL_BIND variable could be truncated to 4000 characters.

[2] SQL_TEXT variable could be truncated to 4000 characters.

A.8 Invalid Record Events

Invalid record events track audited activity that Oracle Audit Vault cannot recognize, possibly due to a corrupted audit record. The Invalid Audit Record Report, described in Section 3.5.2, uses these events.

Table A–13 lists the Oracle Database invalid record events and event IDs.

Table A–13 Oracle Database Invalid Record Events and Event IDs

Event Name	Event ID
INVALID RECORD	30000

Table A–14 lists the Oracle Database invalid record event attributes.

Table A–14 Oracle Database Invalid Record Event Attributes

Attribute Name	Data Type
CLIENT_APPINFO	VARCHAR2(4000)
CLIENT_ID	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)

Table A–14 (Cont.) Oracle Database Invalid Record Event Attributes

Attribute Name	Data Type
ENDUSER	NUMBER
ERROR_MESSAGE	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INSTANCE_NUMBER	NUMBER
MODULE_NAME	VARCHAR2(100)
OBJECT_ID	NUMBER
ORIGINAL_CONTENT1	VARCHAR2(4000)
ORIGINAL_CONTENT2	VARCHAR2(4000)
ORIGINAL_CONTENT3	VARCHAR2(4000)
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_SESSIONID	NUMBER
SCN	NUMBER
SESSION_ACTIONS	VARCHAR2(255)
SEVERITY	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SQL_BIND[1]	VARCHAR2(4000)
SQL_TEXT[2]	VARCHAR2(4000)
STATEMENTID	NUMBER
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
UNDO_SQL_TEXT	VARCHAR2(4000)
USER_GUID	VARCHAR2(32)
USERNAME	VARCHAR2(4000)

[1] SQL_BIND variable could be truncated to 4000 characters.

[2] SQL_TEXT variable could be truncated to 4000 characters.

A.9 Object Management Events

Object management events track audited actions performed on database objects, such as CREATE TABLE statements. The Object Management Report, described in Section 3.4.3, uses these events.

Table A–15 lists the Oracle Database object management events and event IDs.

Table A–15 Oracle Database Object Management Events and Event IDs

Event Name	Event ID
ALTER DIMENSION	175
ALTER INDEX	11
ALTER MATERIALIZED VIEW	75
ALTER MATERIALIZED VIEW LOG	72
ALTER OPERATOR	183
ALTER OUTLINE	179
ALTER SEQUENCE	14
ALTER TABLE	15
CREATE DIMENSION	174
CREATE DIRECTORY	157
CREATE INDEX	9
CREATE MATERIALIZED VIEW	74
CREATE MATERIALIZED VIEW LOG	71
CREATE OUTLINE	180
CREATE PUBLIC DATABASE LINK	112
CREATE PUBLIC SYNONYM	110
CREATE SCHEMA	56
CREATE SEQUENCE	13
CREATE SYNONYM	19
CREATE TABLE	1
CREATE VIEW	21
DROP DIMENSION	176
DROP DIRECTORY	158
DROP INDEX	10
DROP MATERIALIZED VIEW	76
DROP MATERIALIZED VIEW LOG	73
DROP OUTLINE	181
DROP PUBLIC DATABASE LINK	113
DROP PUBLIC SYNONYM	111
DROP SEQUENCE	16
DROP SYNONYM	20
DROP TABLE	12

Table A–15 (Cont.) Oracle Database Object Management Events and Event IDs

Event Name	Event ID
DROP VIEW	22
FLASHBACK TABLE	205
LOCK	26
PURGE INDEX	201
PURGE TABLE	200
RENAME	28
UNDROP OBJECT	202
UPDATE INDEXES	182
VALIDATE INDEX	23

Table A–16 lists the Oracle Database object management event attributes.

Table A–16 Oracle Database Object Management Event Attributes

Attribute Name	Data Type
ASSOCIATED_OBJECT_NAME	VARCHAR2(4000)
ASSOCIATED_OBJECT_OWNER	VARCHAR2(4000)
CLIENT_APPINFO	VARCHAR2(4000)
CLIENT_ID	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
NEW_OBJECT_NAME	VARCHAR2(4000)
NEW_OBJECT_OWNER	VARCHAR2(4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_SESSIONID	NUMBER
SCN	NUMBER
SESSION_ACTIONS	VARCHAR2(255)
SOURCE_EVENTID	VARCHAR2(255)
SQL_BIND[1]	VARCHAR2(4000)

Table A–16 (Cont.) Oracle Database Object Management Event Attributes

Attribute Name	Data Type
SQL_TEXT[2]	VARCHAR2(4000)
STATEMENTID	NUMBER
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
UNDO_SQL_TEXT	VARCHAR2(4000)
USER_GUID	VARCHAR2(32)
USERNAME	VARCHAR2(4000)

[1] SQL_BIND variable could be truncated to 4000 characters.

[2] SQL_TEXT variable could be truncated to 4000 characters.

A.10 Peer Association Events

Peer association events track database link statements. The Distributed Database Report, described in Section 3.3.4, uses these events.

Table A–17 lists the Oracle Database peer association events and event IDs.

Table A–17 Oracle Database Peer Association Events and Event IDs

Event Name	Event ID
CREATE DATABASE LINK	32
DROP DATABASE LINK	33

Table A–18 lists the Oracle Database peer association event attributes.

Table A–18 Oracle Database Peer Association Event Attributes

Attribute Name	Data Type
CLIENT_APPINFO	VARCHAR2(4000)
CLIENT_ID	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INSTANCE_NUMBER	NUMBER
OBJECT_ID	NUMBER

Table A–18 (Cont.) Oracle Database Peer Association Event Attributes

Attribute Name	Data Type
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_SESSIONID	NUMBER
SCN	NUMBER
SESSION_ACTIONS	VARCHAR2(255)
SOURCE_EVENTID	VARCHAR2(255)
SQL_BIND[1]	VARCHAR2(4000)
SQL_TEXT[2]	VARCHAR2(4000)
STATEMENTID	NUMBER
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
UNDO_SQL_TEXT	VARCHAR2(4000)
USER_GUID	VARCHAR2(32)
USERNAME	VARCHAR2(4000)

[1] SQL_BIND variable could be truncated to 4000 characters.

[2] SQL_TEXT variable could be truncated to 4000 characters.

A.11 Role and Privilege Management Events

Role and privilege management events track audited role and privilege management activity, such as granting object permissions to a user. The Role and Privilege Management Report, described in Section 3.4.5, uses these events.

Table A–19 lists the Oracle Database role and privilege management events and event IDs.

Table A–19 Oracle Database Role and Privilege Management Events and Event IDs

Event Name	Event ID
ALTER ROLE	79
CREATE ROLE	52
DROP ROLE	54
GRANT OBJECT	17
GRANT ROLE	114
REVOKE OBJECT	18
REVOKE ROLE	115

Table A–20 lists the Oracle Database role and privilege management event attributes.

Table A–20 Oracle Database Role and Privilege Management Event Attributes

Attribute Name	Data Type
ADMIN_OPTION	NUMBER
CLIENT_APPINFO	VARCHAR2(4000)
CLIENT_ID	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME
GRANTEE	VARCHAR2(4000)
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INSTANCE_NUMBER	NUMBER
OBJECT_ID	NUMBER
OBJECT_PRIVILEGE	VARCHAR2(255)
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_SESSIONID	NUMBER
ROLE_NAME	VARCHAR2(4000)
SCN	NUMBER
SESSION_ACTIONS	VARCHAR2(255)
SOURCE_EVENTID	VARCHAR2(255)
SQL_BIND[1]	VARCHAR2(4000)
SQL_TEXT[2]	VARCHAR2(4000)
STATEMENTID	NUMBER
SUB_CONTEXTID	VARCHAR2(4000)
SYSTEM_PRIVILEGE	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
UNDO_SQL_TEXT	VARCHAR2(4000)
USER_GUID	VARCHAR2(32)

Table A–20 (Cont.) Oracle Database Role and Privilege Management Event Attributes

Attribute Name	Data Type
USERNAME	VARCHAR2(4000)

[1] SQL_BIND variable could be truncated to 4000 characters.

[2] SQL_TEXT variable could be truncated to 4000 characters.

A.12 Service and Application Utilization Events

Service and application utilization events track audited application access activity, such as the execution of PL/SQL procedures or functions. The Procedure Executions Report, described in Section 3.3.5, uses these events.

Table A–21 lists the Oracle Database service and application utilization events and event IDs.

Table A–21 Oracle Database Service and Application Utilization Events and Event IDs

Event Name	Event ID
CALL METHOD	170
EXECUTE PROCEDURE	116
PL/SQL EXECUTE	47

Table A–22 lists the Oracle Database service and application utilization event attributes.

Table A–22 Oracle Database Service and Application Utilization Event Attributes

Attribute Name	Data Type
CLIENT_APPINFO	VARCHAR2(4000)
CLIENT_ID	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INSTANCE_NUMBER	NUMBER
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_SESSIONID	NUMBER
SCN	NUMBER

Table A–22 (Cont.) Oracle Database Service and Application Utilization Event Attributes

Attribute Name	Data Type
SESSION_ACTIONS	VARCHAR2(255)
SOURCE_EVENTID	VARCHAR2(255)
SQL_BIND[1]	VARCHAR2(4000)
SQL_TEXT[2]	VARCHAR2(4000)
STATEMENTID	NUMBER
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
UNDO_SQL_TEXT	VARCHAR2(4000)
USER_GUID	VARCHAR2(32)
USERNAME	VARCHAR2(4000)

[1] SQL_BIND variable could be truncated to 4000 characters.

[2] SQL_TEXT variable could be truncated to 4000 characters.

A.13 System Management Events

System management events track audited system management activity, such as STARTUP and SHUTDOWN operations. The System Management Report, described in Section 3.4.6, uses these events.

Table A–23 lists the Oracle Database system management events and event IDs.

Table A–23 Oracle Database System Management Events and Event IDs

Event Name	Event ID
ALTER CLUSTER	5
ALTER DATABASE	35
ALTER ROLLBACK SEG	37
ALTER SYSTEM	49
ALTER TABLESPACE	40
ANALYZE CLUSTER	64
CREATE CLUSTER	4
CREATE CONTROL FILE	57
CREATE DATABASE	34
CREATE ROLLBACK SEG	36
CREATE TABLESPACE	39
DISABLE ALL TRIGGERS	121
DROP CLUSTER	8
DROP ROLLBACK SEG	38

Table A–23 (Cont.) Oracle Database System Management Events and Event IDs

Event Name	Event ID
DROP TABLESPACE	41
ENABLE ALL TRIGGERS	120
FLASHBACK	128
FLASHBACK DATABASE	204
PURGE DBA_RECYCLEBIN	198
PURGE TABLESPACE	199
SHUTDOWN	216
STARTUP	215
SUPER USER DDL	213
SUPER USER DML	214
SYSTEM GRANT	108
SYSTEM REVOKE	109
TRUNCATE CLUSTER	86

Table A–24 lists the Oracle Database system management event attributes.

Table A–24 Oracle Database System Management Event Attributes

Attribute Name	Data Type
CLIENT_APPINFO	VARCHAR2(4000)
CLIENT_ID	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INSTANCE_NUMBER	NUMBER
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_SESSIONID	NUMBER
SCN	NUMBER
SESSION_ACTIONS	VARCHAR2(255)
SOURCE_EVENTID	VARCHAR2(255)

Table A–24 (Cont.) Oracle Database System Management Event Attributes

Attribute Name	Data Type
SQL_BIND[1]	VARCHAR2(4000)
SQL_TEXT[2]	VARCHAR2(4000)
STATEMENTID	NUMBER
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
UNDO_SQL_TEXT	VARCHAR2(4000)
USER_GUID	VARCHAR2(32)
USERNAME	VARCHAR2(4000)

[1] SQL_BIND variable could be truncated to 4000 characters.

[2] SQL_TEXT variable could be truncated to 4000 characters.

A.14 Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized, such as ALTER SUMMARY statements. The Uncategorized Activity Report, described in Section 3.5.3, uses these events.

Table A–25 lists the Oracle Database unknown or uncategorized events and event IDs.

Table A–25 Oracle Database Unknown or Uncategorized Events and Event IDs

Event Name	Event ID
ALTER SUMMARY	172
COMMENT	29
CREATE SUMMARY	171
DROP SUMMARY	173
NO-OP	27
SUPER USER UNKNOWN	217
UNKNOWN	0
USER COMMENT	117

Table A–26 lists the Oracle Database unknown or uncategorized event attributes.

Table A–26 Unknown or Uncategorized Event Attributes

Attribute Name	Data Type
CLIENT_APPINFO	VARCHAR2(4000)
CLIENT_ID	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)

Table A–26 (Cont.) Unknown or Uncategorized Event Attributes

Attribute Name	Data Type
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INSTANCE_NUMBER	NUMBER
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_SESSIONID	NUMBER
SCN	NUMBER
SESSION_ACTIONS	VARCHAR2(255)
SOURCE_EVENTID	VARCHAR2(255)
SQL_BIND[1]	VARCHAR2(4000)
SQL_TEXT[2]	VARCHAR2(4000)
STATEMENTID	NUMBER
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
UNDO_SQL_TEXT	VARCHAR2(4000)
USER_GUID	VARCHAR2(32)
USERNAME	VARCHAR2(4000)

[1] SQL_BIND variable could be truncated to 4000 characters.

[2] SQL_TEXT variable could be truncated to 4000 characters.

A.15 User Session Events

User session events track audited authentication events for users who log in to the database. The User Sessions Report, described in Section 3.3.6, uses these events.

Table A–27 lists the Oracle Database user session events and event IDs.

Table A–27 Oracle Database User Session Events and Event IDs

Event Name	Event ID
ALTER SESSION	42

Table A–27 (Cont.) Oracle Database User Session Events and Event IDs

Event Name	Event ID
COMMIT	44
CREATE RESTORE POINT	206
CREATE SESSION	129
DROP RESTORE POINT	207
LOGOFF	101
LOGOFF BY CLEANUP	102
LOGON	100
PROXY AUTHENTICATION ONLY	208
PURGE USER_RECYCLEBIN	197
ROLLBACK	45
SAVEPOINT	46
SESSION REC	103
SET ROLE	55
SET TRANSACTION	48
SUPER USER LOGON	212

Table A–28 lists the Oracle Database user session event attributes.

Table A–28 Oracle Database User Session Event Attributes

Attribute Name	Data Type
AUTHENTICATION_METHOD	VARCHAR2(255)
CLIENT_APPINFO	VARCHAR2(4000)
CLIENT_ID	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INSTANCE_NUMBER	NUMBER
LOGOFF_DLOCK	NUMBER
LOGOFF_LREAD	NUMBER
LOGOFF_LWRITE	NUMBER
LOGOFF_PREAD	NUMBER
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)

Table A–28 (Cont.) Oracle Database User Session Event Attributes

Attribute Name	Data Type
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_SESSIONID	NUMBER
SCN	NUMBER
SESSION_ACTIONS	VARCHAR2(255)
SOURCE_EVENTID	VARCHAR2(255)
SQL_BIND[1]	VARCHAR2(4000)
SQL_TEXT[2]	VARCHAR2(4000)
STATEMENTID	NUMBER
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
UNDO_SQL_TEXT	VARCHAR2(4000)
USER_GUID	VARCHAR2(32)
USERNAME	VARCHAR2(4000)

[1] SQL_BIND variable could be truncated to 4000 characters.

[2] SQL_TEXT variable could be truncated to 4000 characters.

B

Microsoft SQL Server Audit Events

This appendix contains:

- About the Microsoft SQL Server Audit Events
- Account Management Events
- Application Management Events
- Audit Command Events
- Data Access Events
- Exception Events
- Invalid Record Events
- Object Management Events
- Peer Association Events
- Role and Privilege Management Events
- Service and Application Utilization Events
- System Management Events
- Unknown or Uncategorized Events
- User Session Events

B.1 About the Microsoft SQL Server Audit Events

This appendix lists the audit event names and IDs, and the attribute names and data types for Microsoft SQL Server. The audit events are organized by their respective categories; for example, Account Management. You can use these audit events as follows:

- **For alerts.** When you create an alert, you can specify an audit event, based on its category, that can trigger the alert. See "Creating an Alert" on page 2-20 for more information.
- **For custom reports using third-party tools.** If you want to create custom reports using other Oracle Database reporting products or third-party tools,, refer to the tables in this appendix when you design the reports. See Chapter 4, "Oracle Audit Vault Data Warehouse Schema" for more information about custom reports created with other tools.

B.2 Account Management Events

Account management events track SQL statements that affect user accounts, such as adding logins or changing login passwords. The Account Management Report, described in Section 3.4.1, uses these events.

Table B–1 lists the Microsoft SQL Server account management events and event IDs.

Table B–1 SQL Server Account Management Events and Event IDs

Event Name	Event ID:Subclass
Audit AddLogin Event	ADDLOGIN:ADD ADDLOGIN:DROP
Audit Database Principal Management Event	DATABASE PRINCIPAL MANAGEMENT:ALTER: USER DATABASE PRINCIPAL MANAGEMENT:CREATE: USER DATABASE PRINCIPAL MANAGEMENT:DROP: USER
Audit Login Change Password Event	LOGIN CHANGE PASSWORD:PASSWORD CHANGED LOGIN CHANGE PASSWORD:PASSWORD MUST CHANGE LOGIN CHANGE PASSWORD:PASSWORD RESET LOGIN CHANGE PASSWORD:PASSWORD SELF CHANGED LOGIN CHANGE PASSWORD:PASSWORD SELF RESET LOGIN CHANGE PASSWORD:PASSWORD UNLOCKED
Audit Login Change Property Event	LOGIN CHANGE PROPERTY:CREDENTIAL CHANGED LOGIN CHANGE PROPERTY:DEFAULT DATABASE LOGIN CHANGE PROPERTY:DEFAULT DATABASE CHANGED LOGIN CHANGE PROPERTY:DEFAULT LANGUAGE LOGIN CHANGE PROPERTY:DEFAULT LANGUAGE CHANGED LOGIN CHANGE PROPERTY:EXPIRATION CHANGED LOGIN CHANGE PROPERTY:NAME CHANGED LOGIN CHANGE PROPERTY:POLICY CHANGED
Audit Server Object Management Event	SERVER OBJECT MANAGEMENT:CREDENTIAL MAP DROPPED SERVER OBJECT MANAGEMENT:CREDENTIAL MAPPED TO LOGIN
Audit Server Principal Management Event	SERVER PRINCIPAL MANAGEMENT:ALTER: USER SERVER PRINCIPAL MANAGEMENT:CREATE: USER SERVER PRINCIPAL MANAGEMENT:DISABLE: USER SERVER PRINCIPAL MANAGEMENT:DROP: USER SERVER PRINCIPAL MANAGEMENT:ENABLE: USER

Table B–2 lists the Microsoft SQL Server account management event attributes.

Table B–2 SQL Server Account Management Event Attributes

Attribute Name	Data Type
ADDL_INFO	VARCHAR2(4000)
COLUMN_PERMISSIONS	NUMBER
CONTEXTID	VARCHAR2(4000)

Table B–2 (Cont.) SQL Server Account Management Event Attributes

Attribute Name	Data Type
CPU	NUMBER
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
DBUSER_NAME	VARCHAR2(4000)
DURATION	NUMBER
END_TIME	TIMESTAMP
ENDUSER	VARCHAR2(4000)
EVENT_SEQUENCE	NUMBER
EVENT_STATUS	VARCHAR2(30)
EVENT_SUB_CLASS	NUMBER
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GUID	NUMBER
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INDEX_ID	NUMBER
IS_SYSTEM	NUMBER
LINKED_SERVER_NAME	VARCHAR2(4000)
LOGIN_SID	VARCHAR2(4000)
OBJECT_ID	NUMBER
OBJECT_ID2	NUMBER
OSUSER_NAME	VARCHAR2(4000)
OWNER_ID	NUMBER
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SERVER_NAME	VARCHAR2(4000)
SESSION_LOGIN_NAME	VARCHAR2(4000)
SOURCE_DATABASE_ID	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_LOGIN_NAME	VARCHAR2(4000)
TARGET_LOGIN_SID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OBJECT_TYPE	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
TEXT_DATA	VARCHAR2(4000)

Table B–2 (Cont.) SQL Server Account Management Event Attributes

Attribute Name	Data Type
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

B.3 Application Management Events

Application management events track actions that were performed on the underlying SQL statements, such as creating objects. The Procedure Management Report, described in Section 3.4.4, uses these events.

Table B–3 lists the Microsoft SQL Server application management events and event IDs.

Table B–3 SQL Server Application Management Events and Event IDs

Event Name	Event ID:Subclass
Audit Database Object Take Ownership Event	DATABASE OBJECT TAKE OWNERSHIP: TRIGGER
Audit Schema Object Take Ownership Event	SCHEMA OBJECT TAKE OWNERSHIP: PROCEDURE SCHEMA OBJECT TAKE OWNERSHIP: TYPE SCHEMA OBJECT TAKE OWNERSHIP: TRIGGER
Audit Server Object Take Ownership Event	TRIGGER
Object:Created	OBJECT:CREATED:PROCEDURE OBJECT:CREATED:TRIGGER OBJECT:CREATED:TYPE
Object:Deleted	OBJECT:DELETED:PROCEDURE OBJECT:DELETED:TRIGGER

Table B–4 lists the Microsoft SQL Server application management event attributes.

Table B–4 SQL Server Application Management Event Attributes

Attribute Name	Data Type
ADDL_INFO	VARCHAR2(4000)
ASSOCIATED_OBJECT_NAME	VARCHAR2(4000)
ASSOCIATED_OBJECT_OWNER	VARCHAR2(4000)
COLUMN_PERMISSIONS	NUMBER
CONTEXTID	VARCHAR2(4000)
CPU	NUMBER
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
DBUSER_NAME	VARCHAR2(4000)
DURATION	NUMBER
END_TIME	TIMESTAMP

Table B–4 (Cont.) SQL Server Application Management Event Attributes

Attribute Name	Data Type
ENDUSER	VARCHAR2(4000)
EVENT_SEQUENCE	NUMBER
EVENT_STATUS	VARCHAR2(30)
EVENT_SUB_CLASS	NUMBER
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GUID	NUMBER
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INDEX_ID	NUMBER
IS_SYSTEM	NUMBER
LINKED_SERVER_NAME	VARCHAR2(4000)
LOGIN_SID	VARCHAR2(4000)
NEW_OBJECT_NAME	VARCHAR2(4000)
NEW_OBJECT_OWNER	VARCHAR2(4000)
OBJECT_ID	NUMBER
OBJECT_ID2	NUMBER
OSUSER_NAME	VARCHAR2(4000)
OWNER_ID	NUMBER
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SERVER_NAME	VARCHAR2(4000)
SESSION_LOGIN_NAME	VARCHAR2(4000)
SOURCE_DATABASE_ID	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_LOGIN_NAME	VARCHAR2(4000)
TARGET_LOGIN_SID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OBJECT_TYPE	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
TEXT_DATA	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

B.4 Audit Command Events

Audit command events track the use of audit events, such as altering trace events. The Audit Command Report, described in Section 3.4.2, uses these events.

Table B–5 lists the Microsoft SQL Server audit command events and event IDs.

Table B–5 SQL Server Audit Command Events and Event IDs

Event Name	Event ID:Subclass
Audit Change Audit Event	CHANGE AUDIT:AUDIT STARTED CHANGE AUDIT:AUDIT STOPPED CHANGE AUDIT:C2 MODE OFF CHANGE AUDIT:C2 MODE ON CHANGE:AUDIT STOPPED CHANGE:NEW AUDIT STARTED
Audit Server Alter Trace Event	SERVER ALTER TRACE
ExistingConnection	EXISTINGCONNECTION

Table B–6 lists the Microsoft SQL Server audit command events that are logged in the Windows Event Viewer.

Table B–6 SQL Server Audit Command Events Logged in Windows Event Viewer

Event ID:Subclass	Severity
OP ALTER TRACE: START	10
OP ALTER TRACE: STOP	10

Table B–7 lists the Microsoft SQL Server audit command event attributes.

Table B–7 SQL Server Audit Command Event Attributes

Attribute Name	Data Type
ADDL_INFO	VARCHAR2(4000)
AUDIT_OPTION	VARCHAR2(4000)
COLUMN_PERMISSIONS	NUMBER
CONTEXTID	VARCHAR2(4000)
CPU	NUMBER
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
DBUSER_NAME	VARCHAR2(4000)
DURATION	NUMBER
END_TIME	TIMESTAMP
ENDUSER	VARCHAR2(4000)
EVENT_SEQUENCE	NUMBER
EVENT_STATUS	VARCHAR2(30)
EVENT_SUB_CLASS	NUMBER

Table B–7 (Cont.) SQL Server Audit Command Event Attributes

Attribute Name	Data Type
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GUID	NUMBER
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INDEX_ID	NUMBER
IS_SYSTEM	NUMBER
LINKED_SERVER_NAME	VARCHAR2(4000)
LOGIN_SID	VARCHAR2(4000)
OBJECT_ID	NUMBER
OBJECT_ID2	NUMBER
OSUSER_NAME	VARCHAR2(4000)
OWNER_ID	NUMBER
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SERVER_NAME	VARCHAR2(4000)
SESSION_LOGIN_NAME	VARCHAR2(4000)
SOURCE_DATABASE_ID	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_LOGIN_NAME	VARCHAR2(4000)
TARGET_LOGIN_SID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OBJECT_TYPE	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
TEXT_DATA	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

B.5 Data Access Events

The data access event tracks SQL transactions. The Data Access Report, described in Section 3.3.2, uses these events.

Table B–8 shows the Microsoft SQL Server data access event and event ID.

Table B–8 SQL Server Data Access Event and Event ID

Event Name	Event ID:Subclass
SQL Transaction	TRANSACTION:BEGIN

Table B–9 lists the Microsoft SQL Server data access event attributes.

Table B–9 SQL Server Data Access Event Attributes

Attribute Name	Data Type
ADDL_INFO	VARCHAR2(4000)
COLUMN_PERMISSIONS	NUMBER
CONTEXTID	VARCHAR2(4000)
CPU	NUMBER
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
DBUSER_NAME	VARCHAR2(4000)
DURATION	NUMBER
END_TIME	TIMESTAMP
ENDUSER	VARCHAR2(4000)
EVENT_SEQUENCE	NUMBER
EVENT_STATUS	VARCHAR2(30)
EVENT_SUB_CLASS	NUMBER
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GUID	NUMBER
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INDEX_ID	NUMBER
IS_SYSTEM	NUMBER
LINKED_SERVER_NAME	VARCHAR2(4000)
LOGIN_SID	VARCHAR2(4000)
OBJECT_ID	NUMBER
OBJECT_ID2	NUMBER
OSUSER_NAME	VARCHAR2(4000)
OWNER_ID	NUMBER
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SERVER_NAME	VARCHAR2(4000)
SESSION_LOGIN_NAME	VARCHAR2(4000)
SOURCE_DATABASE_ID	NUMBER

Table B–9 (Cont.) SQL Server Data Access Event Attributes

Attribute Name	Data Type
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_LOGIN_NAME	VARCHAR2(4000)
TARGET_LOGIN_SID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OBJECT_TYPE	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
TEXT_DATA	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

B.6 Exception Events

Exception events track audited error and exception activity, such as background job errors. The Exception Activity Report, described in Section 3.5.1, uses these events.

Table B–10 lists the Microsoft SQL Server exception events and event IDs.

Table B–10 SQL Server Exception Events and Event IDs

Event Name	Event ID:Subclass
Background Job Error	BACKGROUND JOB ERROR:ERROR RETURN BACKGROUND JOB ERROR:FAILURE BACKGROUND JOB ERROR:QUEUE IS FULL
Blocked Process Report	BLOCKED PROCESS REPORT

Table B–11 lists the Microsoft SQL Server exception events that are logged in the Windows Event Viewer.

Table B–11 SQL Server Exception Events Logged in the Windows Event Viewer

Event ID:Subclass	Severity
OP ERROR: COMMIT	10
OP ERROR: DB OFFLINE	10
OP ERROR: MIRRORING ERROR	16
OP ERROR: .NET FATAL ERROR	16
OP ERROR: .NET USER CODE	16
OP ERROR: PROCESS VIOLATION	16
OP ERROR: RECOVER	21
OP ERROR: RESTORE FAILED	21
OP ERROR: ROLLBACK	10
OP ERROR: SERVER SHUT DOWN	21

Table B–11 (Cont.) SQL Server Exception Events Logged in the Windows Event Viewer

Event ID:Subclass	Severity
OP ERROR: STACK OVER FLOW	16

Table B–12 lists the Microsoft SQL Server exception event attributes.

Table B–12 SQL Server Exception Event Attributes

Attribute Name	Data Type
ADDL_INFO	VARCHAR2(4000)
COLUMN_PERMISSIONS	NUMBER
CONTEXTID	VARCHAR2(4000)
CPU	NUMBER
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
DBUSER_NAME	VARCHAR2(4000)
DURATION	NUMBER
END_TIME	TIMESTAMP
ENDUSER	VARCHAR2(4000)
EVENT_SEQUENCE	NUMBER
EVENT_STATUS	VARCHAR2(30)
EVENT_SUB_CLASS	NUMBER
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GUID	NUMBER
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INDEX_ID	NUMBER
IS_SYSTEM	NUMBER
LINKED_SERVER_NAME	VARCHAR2(4000)
LOGIN_SID	VARCHAR2(4000)
OBJECT_ID	NUMBER
OBJECT_ID2	NUMBER
OSUSER_NAME	VARCHAR2(4000)
OWNER_ID	NUMBER
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SERVER_NAME	VARCHAR2(4000)
SESSION_LOGIN_NAME	VARCHAR2(4000)
SOURCE_DATABASE_ID	NUMBER

Table B–12 (Cont.) SQL Server Exception Event Attributes

Attribute Name	Data Type
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_LOGIN_NAME	VARCHAR2(4000)
TARGET_LOGIN_SID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OBJECT_TYPE	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
TEXT_DATA	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

B.7 Invalid Record Events

Invalid record events track audited activity that Oracle Audit Vault cannot recognize, possibly due to a corrupted audit record. The Invalid Audit Record Report, described in Section 3.5.2, uses the invalid record event attributes. (These events do not have any event names or event IDs; they only contain event attributes.)

Table B–13 lists the Microsoft SQL Server invalid record event attributes.

Table B–13 SQL Server Invalid Record Event Attributes

Attribute Name	Data Type
ADDL_INFO	VARCHAR2(4000)
COLUMN_PERMISSIONS	NUMBER
CONTEXTID	VARCHAR2(4000)
CPU	NUMBER
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
DBUSER_NAME	VARCHAR2(4000)
DURATION	NUMBER
END_TIME	TIMESTAMP
ENDUSER	VARCHAR2(4000)
ERROR_ID	NUMBER
ERROR_MESSAGE	VARCHAR2(30)
EVENT_SEQUENCE	NUMBER
EVENT_STATUS	VARCHAR2(30)
EVENT_SUB_CLASS	NUMBER
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GUID	NUMBER

Table B–13 (Cont.) SQL Server Invalid Record Event Attributes

Attribute Name	Data Type
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INDEX_ID	NUMBER
IS_SYSTEM	NUMBER
LINKED_SERVER_NAME	VARCHAR2(4000)
LOGIN_SID	VARCHAR2(4000)
MODULE_NAME	VARCHAR2(100)
OBJECT_ID	NUMBER
OBJECT_ID2	NUMBER
ORIGINAL_CONTENT1	VARCHAR2(4000)
ORIGINAL_CONTENT2	VARCHAR2(4000)
ORIGINAL_CONTENT3	VARCHAR2(4000)
OSUSER_NAME	VARCHAR2(4000)
OWNER_ID	NUMBER
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SERVER_NAME	VARCHAR2(4000)
SESSION_LOGIN_NAME	VARCHAR2(4000)
SEVERITY	NUMBER
SOURCE_DATABASE_ID	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_LOGIN_NAME	VARCHAR2(4000)
TARGET_LOGIN_SID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OBJECT_TYPE	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
TEXT_DATA	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

B.8 Object Management Events

Object management events track audited actions performed on database objects, such as altering an object. The Object Management Report, described in Section 3.4.3, uses these events.

Table B–14 lists the Microsoft SQL Server object management events and event IDs.

Table B–14 SQL Server Object Management Events and Event IDs

Event Name	Event ID:Subclass
Audit Database Object Access Event	DATABASE OBJECT ACCESS
Audit Database Object Management Event	DATABASE OBJECT MANAGEMENT:ACCESS
Audit Database Object Take Ownership Event	DATABASE OBJECT TAKE OWNERSHIP: OBJECT DATABASE OBJECT TAKE OWNERSHIP: SCHEMA
Audit Database Principal Management Event	DATABASE PRINCIPAL MANAGEMENT:ALTER: OBJECT DATABASE PRINCIPAL MANAGEMENT:CREATE: OBJECT DATABASE PRINCIPAL MANAGEMENT:DROP: OBJECT
Audit Schema Object Access Event	SCHEMA OBJECT ACCESS
Audit Schema Object Management Event	SCHEMA OBJECT MANAGEMENT:ALTER SCHEMA OBJECT MANAGEMENT:CREATE SCHEMA OBJECT MANAGEMENT:DROP SCHEMA OBJECT MANAGEMENT:TRANSFER
Audit Schema Object Take Ownership Event	SCHEMA OBJECT TAKE OWNERSHIP: INDEX SCHEMA OBJECT TAKE OWNERSHIP: OBJECT SCHEMA OBJECT TAKE OWNERSHIP: TABLE
Audit Server Object Take Ownership Event	SERVER OBJECT TAKE OWNERSHIP: OBJECT
Lock:Deadlock	LOCK:DEADLOCK
Lock:Deadlock Chain	LOCK:DEADLOCK CHAIN LOCK:DEADLOCK CHAIN:RESOURCE TYPE LOCK
Object:Altered	OBJECT:ALTERED OBJECT:ALTERED:COMMIT OBJECT:ALTERED:INDEX OBJECT:ALTERED:PROCEDURE OBJECT:ALTERED:ROLLBACK OBJECT:ALTERED:TABLE OBJECT:ALTERED:TRIGGER OBJECT:ALTERED:TYPE

Table B–14 (Cont.) SQL Server Object Management Events and Event IDs

Event Name	Event ID:Subclass
Object:Closed	OBJECT:CLOSED
Object:Created	OBJECT:CREATED OBJECT:CREATED:COMMIT OBJECT:CREATED:INDEX OBJECT:CREATED:PROCEDURE OBJECT:CREATED:ROLLBACK OBJECT:CREATED:SCHEMA OBJECT:CREATED:SYNONYM OBJECT:CREATED:TABLE OBJECT:CREATED:TRIGGER OBJECT:CREATED:TYPE OBJECT:CREATED:VIEW
Object:Deleted	OBJECT:DELETED OBJECT:DELETED:COMMIT OBJECT:DELETED:INDEX OBJECT:DELETED:PROCEDURE OBJECT:DELETED:ROLLBACK OBJECT:DELETED:SYNONYM OBJECT:DELETED:TABLE OBJECT:DELETED:TRIGGER OBJECT:DELETED:TYPE OBJECT:DELETED:VIEW

Table B–15 lists the Microsoft SQL Server object management event attributes.

Table B–15 SQL Server Object Management Event Attributes

Attribute Name	Data Type
ADDL_INFO	VARCHAR2(4000)
ASSOCIATED_OBJECT_NAME	VARCHAR2(4000)
ASSOCIATED_OBJECT_OWNER	VARCHAR2(4000)
COLUMN_PERMISSIONS	NUMBER
CONTEXTID	VARCHAR2(4000)
CPU	NUMBER
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
DBUSER_NAME	VARCHAR2(4000)
DURATION	NUMBER
END_TIME	TIMESTAMP
ENDUSER	VARCHAR2(4000)
EVENT_SEQUENCE	NUMBER

Table B–15 (Cont.) SQL Server Object Management Event Attributes

Attribute Name	Data Type
EVENT_STATUS	VARCHAR2(30)
EVENT_SUB_CLASS	NUMBER
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GUID	NUMBER
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INDEX_ID	NUMBER
IS_SYSTEM	NUMBER
LINKED_SERVER_NAME	VARCHAR2(4000)
LOGIN_SID	VARCHAR2(4000)
NEW_OBJECT_NAME	VARCHAR2(4000)
NEW_OBJECT_OWNER	VARCHAR2(4000)
OBJECT_ID	NUMBER
OBJECT_ID2	NUMBER
OSUSER_NAME	VARCHAR2(4000)
OWNER_ID	NUMBER
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SERVER_NAME	VARCHAR2(4000)
SESSION_LOGIN_NAME	VARCHAR2(4000)
SOURCE_DATABASE_ID	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_LOGIN_NAME	VARCHAR2(4000)
TARGET_LOGIN_SID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OBJECT_TYPE	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
TEXT_DATA	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

B.9 Peer Association Events

Peer association events track database link statements. The Distributed Database Report, described in Section 3.3.4, uses these events. (These events do not have any event names or event IDs; they only contain event attributes.)

Table B–16 lists the Microsoft SQL Server peer association event attributes.

Table B–16 SQL Server Peer Association Event Attributes

Attribute Name	Data Type
ADDL_INFO	VARCHAR2(4000)
COLUMN_PERMISSIONS	NUMBER
CONTEXTID	VARCHAR2(4000)
CPU	NUMBER
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
DBUSER_NAME	VARCHAR2(4000)
DURATION	NUMBER
END_TIME	TIMESTAMP
ENDUSER	VARCHAR2(4000)
EVENT_SEQUENCE	NUMBER
EVENT_STATUS	VARCHAR2(30)
EVENT_SUB_CLASS	NUMBER
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GUID	NUMBER
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INDEX_ID	NUMBER
IS_SYSTEM	NUMBER
LINKED_SERVER_NAME	VARCHAR2(4000)
LOGIN_SID	VARCHAR2(4000)
OBJECT_ID	NUMBER
OBJECT_ID2	NUMBER
OSUSER_NAME	VARCHAR2(4000)
OWNER_ID	NUMBER
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SERVER_NAME	VARCHAR2(4000)
SESSION_LOGIN_NAME	VARCHAR2(4000)
SOURCE_DATABASE_ID	NUMBER

Table B–16 (Cont.) SQL Server Peer Association Event Attributes

Attribute Name	Data Type
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_LOGIN_NAME	VARCHAR2(4000)
TARGET_LOGIN_SID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OBJECT_TYPE	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
TEXT_DATA	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

B.10 Role and Privilege Management Events

Role and privilege management events track audited role and privilege management activity, such as granting a user access permission. The Role and Privilege Management Report, described in Section 3.4.5, uses these events.

Table B–17 lists the Microsoft SQL Server role and privilege management events and event IDs.

Table B–17 SQL Server Role and Privilege Management Events and Event IDs

Event Name	Event ID:Subclass
Audit Add DB User Event	ADD DB USER:GRANT DATABASE ACCESS ADD DB USER:GRANTDBACCESS ADD DB USER:REVOKE DATABASE ACCESS ADD DB USER:REVOKEDBACCESS
Audit Add Login to Server Role Event	ADD LOGIN TO SERVER ROLE:ADD ADD LOGIN TO SERVER ROLE:DROP
Audit Add Member to DB Role Event	ADD MEMBER TO DB ROLE:ADD ADD MEMBER TO DB ROLE:CHANGE GROUP ADD MEMBER TO DB ROLE:DROP
Audit Add Role Event	ADD ROLE:ADD ADD ROLE:DROP
Audit App Role Change Password Event	APP ROLE CHANGE PASSWORD
Audit Database Object GDR Event	DATABASE OBJECT GDR:DENY DATABASE OBJECT GDR:GRANT DATABASE OBJECT GDR:REVOKE
Audit Database Principal Management Event	DATABASE PRINCIPAL MANAGEMENT:ALTER: ROLE DATABASE PRINCIPAL MANAGEMENT:CREATE: ROLE DATABASE PRINCIPAL MANAGEMENT:DROP: ROLE

Table B–17 (Cont.) SQL Server Role and Privilege Management Events and Event IDs

Event Name	Event ID:Subclass
Audit Login GDR Event	LOGIN GDR:DENY LOGIN GDR:GRANT LOGIN GDR:GRANT LOGIN GDR:REVOKE
Audit Object Derived Permission Event	OBJECT DERIVED PERMISSION:ALTER OBJECT DERIVED PERMISSION:CREATE OBJECT DERIVED PERMISSION:DROP OBJECT DERIVED PERMISSION:DUMP OBJECT DERIVED PERMISSION:LOAD
Audit Object GDR Event	OBJECT GDR:DENY OBJECT GDR:GRANT OBJECT GDR:REVOKE
Audit Object Permission Event	OBJECT PERMISSION
Audit Server Object GDR Event	SERVER OBJECT GDR:DENY SERVER OBJECT GDR:GRANT SERVER OBJECT GDR:REVOKE
Audit Server Scope GDR Event	SERVER SCOPE GDR:DENY SERVER SCOPE GDR:GRANT SERVER SCOPE GDR:REVOKE
Audit Statement GDR Event	STATEMENT GDR:DENY STATEMENT GDR:GRANT STATEMENT GDR:REVOKE
Audit Statement Permission Event	STATEMENT PERMISSION

Table B–18 lists the Microsoft SQL Server role and privilege management event attributes.

Table B–18 SQL Server Role and Privilege Management Event Attributes

Attribute Name	Data Type
ADDL_INFO	VARCHAR2(4000)
ADMIN_OPTION	NUMBER
COLUMN_PERMISSIONS	NUMBER
CONTEXTID	VARCHAR2(4000)
CPU	NUMBER
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
DBUSER_NAME	VARCHAR2(4000)
DURATION	NUMBER
END_TIME	TIMESTAMP
ENDUSER	VARCHAR2(4000)

Table B–18 (Cont.) SQL Server Role and Privilege Management Event Attributes

Attribute Name	Data Type
EVENT_SEQUENCE	NUMBER
EVENT_STATUS	VARCHAR2(30)
EVENT_SUB_CLASS	NUMBER
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GRANTEE	VARCHAR2(4000)
GUID	NUMBER
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INDEX_ID	NUMBER
IS_SYSTEM	NUMBER
LINKED_SERVER_NAME	VARCHAR2(4000)
LOGIN_SID	VARCHAR2(4000)
OBJECT_ID	NUMBER
OBJECT_ID2	NUMBER
OSUSER_NAME	VARCHAR2(4000)
OWNER_ID	NUMBER
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
ROLE_NAME	VARCHAR2(4000)
SERVER_NAME	VARCHAR2(4000)
SESSION_LOGIN_NAME	VARCHAR2(4000)
SOURCE_DATABASE_ID	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
SYSTEM_PRIVILEGE	VARCHAR2(4000)
TARGET_LOGIN_NAME	VARCHAR2(4000)
TARGET_LOGIN_SID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OBJECT_TYPE	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
TEXT_DATA	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

B.11 Service and Application Utilization Events

Service and application utilization events track audited application access activity. The Procedure Executions Report, described in Section 3.3.5, uses these events.

Table B–19 lists the Microsoft SQL Server service and application utilization events and event IDs.

Table B–19 SQL Server Service and Application Utilization Events and Event IDs

Event Name	Event ID
Audit Broker Conversation	BROKER CONVERSATION:INVALID SIGNATURE BROKER CONVERSATION:NO CERTIFICATE BROKER CONVERSATION:NO SECURITY HEADER BROKER CONVERSATION:RUN AS TARGET FAILURE
Broker:Activation	BROKER:ACTIVATION:ABORTED
Broker:Queue Disabled	BROKER:QUEUE DISABLED

Table B–20 lists the Microsoft SQL Server service and application utilization event attributes.

Table B–20 SQL Server Service and Application Utilization Event Attributes

Attribute Name	Data Type
ADDL_INFO	VARCHAR2(4000)
COLUMN_PERMISSIONS	NUMBER
CONTEXTID	VARCHAR2(4000)
CPU	NUMBER
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
DBUSER_NAME	VARCHAR2(4000)
DURATION	NUMBER
END_TIME	TIMESTAMP
ENDUSER	VARCHAR2(4000)
EVENT_SEQUENCE	NUMBER
EVENT_STATUS	VARCHAR2(30)
EVENT_SUB_CLASS	NUMBER
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GUID	NUMBER
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INDEX_ID	NUMBER
IS_SYSTEM	NUMBER
LINKED_SERVER_NAME	VARCHAR2(4000)

Table B–20 (Cont.) SQL Server Service and Application Utilization Event Attributes

Attribute Name	Data Type
LOGIN_SID	VARCHAR2(4000)
OBJECT_ID	NUMBER
OBJECT_ID2	NUMBER
OSUSER_NAME	VARCHAR2(4000)
OWNER_ID	NUMBER
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SERVER_NAME	VARCHAR2(4000)
SESSION_LOGIN_NAME	VARCHAR2(4000)
SOURCE_DATABASE_ID	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_LOGIN_NAME	VARCHAR2(4000)
TARGET_LOGIN_SID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OBJECT_TYPE	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
TEXT_DATA	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

B.12 System Management Events

System management events track audited system management activity, such as backup and restore operations. The System Management Report, described in Section 3.4.6, uses these events.

Table B–21 lists the Microsoft SQL Server system management events and event IDs.

Table B–21 SQL Server System Management Events and Event IDs

Event Name	Event ID:Subclass
Audit Add DB User Event	ADD DB USER:ADD ADD DB USER:DROP ADD DB USER:SP_ADDUSER ADD DB USER:SP_DROPUSER
Audit Backup/Restore Event	BACKUP/RESTORE:BACKUP BACKUP/RESTORE:BACKUPLOG BACKUP/RESTORE:RESTORE
Audit Change Database Owner	CHANGE DATABASE OWNER

Table B–21 (Cont.) SQL Server System Management Events and Event IDs

Event Name	Event ID:Subclass
Audit Database Management Event	DATABASE MANAGEMENT:ALTER
	DATABASE MANAGEMENT:CREATE
	DATABASE MANAGEMENT:DROP
	DATABASE MANAGEMENT:DUMP
	DATABASE MANAGEMENT:LOAD
Audit Database Object Management Event	DATABASE OBJECT MANAGEMENT:ALTER
	DATABASE OBJECT MANAGEMENT:CREATE
	DATABASE OBJECT MANAGEMENT:DROP
	DATABASE OBJECT MANAGEMENT:DUMP
	DATABASE OBJECT MANAGEMENT:LOAD
	DATABASE OBJECT MANAGEMENT:OPEN
Audit Database Operation Event	DATABASE OPERATION:SUBSCRIBE TO QUERY NOTIFICATION
Audit Database Principal Management Event	DATABASE PRINCIPAL MANAGEMENT:DUMP
	DATABASE PRINCIPAL MANAGEMENT:LOAD
Audit DBCC Event	DB CONSISTENCY CHECK
Audit Schema Object Management Event	SCHEMA OBJECT MANAGEMENT:DUMP
	SCHEMA OBJECT MANAGEMENT:LOAD
Audit Server Object Management Event	SERVER OBJECT MANAGEMENT:ALTER
	SERVER OBJECT MANAGEMENT:CREATE
	SERVER OBJECT MANAGEMENT:DROP
	SERVER OBJECT MANAGEMENT:DUMP
	SERVER OBJECT MANAGEMENT:LOAD
Audit Server Operation Event	SERVER OPERATION:ADMINISTER BULK OPERATIONS
	SERVER OPERATION:ALTER RESOURCES
	SERVER OPERATION:ALTER SERVER STATE
	SERVER OPERATION:ALTER SETTINGS
	SERVER OPERATION:AUTHENTICATE
	SERVER OPERATION:EXTERNAL ACCESS
Audit Server Principal Management Event	SERVER PRINCIPAL MANAGEMENT:DUMP: USER
	SERVER PRINCIPAL MANAGEMENT:LOAD: USER
Audit Server Starts and Stops	SERVER STARTS AND STOPS:SHUTDOWN
	SERVER STARTS AND STOPS:STARTED
	SERVER STARTS AND STOPS:PAUSED
	SERVER STARTS AND STOPS:CONTINUE

Table B–21 (Cont.) SQL Server System Management Events and Event IDs

Event Name	Event ID:Subclass
Audit Server Starts and Stops Event	SERVER STARTS AND STOPS:INSTANCE CONTINUED SERVER STARTS AND STOPS:INSTANCE PAUSE SERVER STARTS AND STOPS:INSTANCE SHUTDOWN SERVER STARTS AND STOPS:INSTANCE STARTED
Database Mirroring State Change	DATABASE MIRRORING STATE CHANGE
Mount Tape	MOUNT TAPE:TAPE MOUNT CANCELLED MOUNT TAPE:TAPE MOUNT COMPLETE MOUNT TAPE:TAPE MOUNT REQUEST

Table B–22 lists the Microsoft SQL Server system management event attributes.

Table B–22 SQL Server System Management Event Attributes

Attribute Name	Data Type
ADDL_INFO	VARCHAR2(4000)
COLUMN_PERMISSIONS	NUMBER
CONTEXTID	VARCHAR2(4000)
CPU	NUMBER
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
DBUSER_NAME	VARCHAR2(4000)
DURATION	NUMBER
END_TIME	TIMESTAMP
ENDUSER	VARCHAR2(4000)
EVENT_SEQUENCE	NUMBER
EVENT_STATUS	VARCHAR2(30)
EVENT_SUB_CLASS	NUMBER
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GUID	NUMBER
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INDEX_ID	NUMBER
IS_SYSTEM	NUMBER
LINKED_SERVER_NAME	VARCHAR2(4000)
LOGIN_SID	VARCHAR2(4000)
OBJECT_ID	NUMBER
OBJECT_ID2	NUMBER
OSUSER_NAME	VARCHAR2(4000)

Table B–22 (Cont.) SQL Server System Management Event Attributes

Attribute Name	Data Type
OWNER_ID	NUMBER
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SERVER_NAME	VARCHAR2(4000)
SESSION_LOGIN_NAME	VARCHAR2(4000)
SOURCE_DATABASE_ID	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_LOGIN_NAME	VARCHAR2(4000)
TARGET_LOGIN_SID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OBJECT_TYPE	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
TEXT_DATA	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

B.13 Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized, such as user-created configurations. The Uncategorized Activity Report, described in Section 3.5.3, uses these events.

Table B–23 shows the Microsoft SQL Server unknown or uncategorized event and event ID.

Table B–23 SQL Server Unknown or Uncategorized Event and Event ID

Event Name	Event ID:Subclass
User Configurable (0-9)	USER CONFIGURABLE

Table B–24 lists the Microsoft SQL Server unknown or uncategorized event attributes.

Table B–24 SQL Server Unknown or Uncategorized Event Attributes

Attribute Name	Data Type
ADDL_INFO	VARCHAR2(4000)
COLUMN_PERMISSIONS	NUMBER
CONTEXTID	VARCHAR2(4000)
CPU	NUMBER
DATABASE_ID	NUMBER

Table B–24 (Cont.) SQL Server Unknown or Uncategorized Event Attributes

Attribute Name	Data Type
DATABASE_NAME	VARCHAR2(4000)
DBUSER_NAME	VARCHAR2(4000)
DURATION	NUMBER
END_TIME	TIMESTAMP
ENDUSER	VARCHAR2(4000)
EVENT_SEQUENCE	NUMBER
EVENT_STATUS	VARCHAR2(30)
EVENT_SUB_CLASS	NUMBER
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GUID	NUMBER
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INDEX_ID	NUMBER
IS_SYSTEM	NUMBER
LINKED_SERVER_NAME	VARCHAR2(4000)
LOGIN_SID	VARCHAR2(4000)
OBJECT_ID	NUMBER
OBJECT_ID2	NUMBER
OSUSER_NAME	VARCHAR2(4000)
OWNER_ID	NUMBER
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SERVER_NAME	VARCHAR2(4000)
SESSION_LOGIN_NAME	VARCHAR2(4000)
SOURCE_DATABASE_ID	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_LOGIN_NAME	VARCHAR2(4000)
TARGET_LOGIN_SID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OBJECT_TYPE	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
TEXT_DATA	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)

Table B–24 (Cont.) SQL Server Unknown or Uncategorized Event Attributes

Attribute Name	Data Type
USERNAME	VARCHAR2(4000)

B.14 User Session Events

User session events track audited authentication events for users who log in to the database. The User Sessions Report, described in Section 3.3.6, uses these events.

Table B–25 lists the Microsoft SQL Server user session events and event IDs.

Table B–25 SQL Server User Session Events and Event IDs

Event Name	Event ID:Subclass
Audit Broker Login	BROKER LOGIN:AUTHENTICATION FAILURE BROKER LOGIN:LOGIN SUCCESS BROKER LOGIN:LOGIN PROTOCOL ERROR BROKER LOGIN:MESSAGE FORMAT ERROR BROKER LOGIN:NEGOTIATE FAILURE
Audit Database Operation Event	DATABASE OPERATION:CHECKPOINT
Audit Database Principal Impersonation Event	DATABASE PRINCIPAL IMPERSONATION
Audit Login	AUDIT LOGIN:LOGIN
Audit Login Event	AUDIT LOGIN EVENT:LOGIN
Audit Login Failed	AUDIT LOGIN FAILED:LOGIN FAILED
Audit Login Failed Event	AUDIT LOGIN FAILED EVENT:LOGIN FAILED
Audit Logout	AUDIT LOGOUT:LOGOUT
Audit Logout Event	AUDIT LOGOUT EVENT:LOGOUT
Audit Server Principal Impersonation Event	SERVER PRINCIPAL IMPERSONATION
SQL Transaction	SQL TRANSACTION:COMMIT SQL TRANSACTION:ROLLBACK SQL TRANSACTION:SAVEPOINT

Table B–26 lists the Microsoft SQL Server user session event attributes.

Table B–26 SQL Server User Session Event Attributes

Attribute Name	Data Type
ADDL_INFO	VARCHAR2(4000)
AUTHENTICATION_METHOD	VARCHAR2(255)
COLUMN_PERMISSIONS	NUMBER
CONTEXTID	VARCHAR2(4000)
CPU	NUMBER
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)

Table B–26 (Cont.) SQL Server User Session Event Attributes

Attribute Name	Data Type
DBUSER_NAME	VARCHAR2(4000)
DURATION	NUMBER
END_TIME	TIMESTAMP
ENDUSER	VARCHAR2(4000)
EVENT_SEQUENCE	NUMBER
EVENT_STATUS	VARCHAR2(30)
EVENT_SUB_CLASS	NUMBER
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GUID	NUMBER
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
INDEX_ID	NUMBER
IS_SYSTEM	NUMBER
LINKED_SERVER_NAME	VARCHAR2(4000)
LOGIN_SID	VARCHAR2(4000)
OBJECT_ID	NUMBER
OBJECT_ID2	NUMBER
OSUSER_NAME	VARCHAR2(4000)
OWNER_ID	NUMBER
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SERVER_NAME	VARCHAR2(4000)
SESSION_LOGIN_NAME	VARCHAR2(4000)
SOURCE_DATABASE_ID	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_LOGIN_NAME	VARCHAR2(4000)
TARGET_LOGIN_SID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OBJECT_TYPE	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
TEXT_DATA	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

C

Sybase Adaptive Server Enterprise Audit Events

This appendix contains:

- About the Sybase Adaptive Server Enterprise Audit Events
- Account Management Events
- Application Management Events
- Audit Command Events
- Data Access Events
- Exception Events
- Invalid Record Events
- Object Management Events
- Peer Association Events
- Role and Privilege Management Events
- Service and Application Utilization Events
- System Management Events
- Unknown or Uncategorized Events
- User Session Events

C.1 About the Sybase Adaptive Server Enterprise Audit Events

This appendix lists the audit event names and IDs, and the attribute names and data types for Sybase Adaptive Server Enterprise (ASE). The audit events are organized by their respective categories; for example, Account Management. You can use these audit events as follows:

- **For alerts.** When you create an alert, you can specify an audit event, based on its category, that can trigger the alert. See "Creating an Alert" on page 2-20 for more information.
- **For custom reports using third-party tools.** If you want to create custom reports using other Oracle Database reporting products or third-party tools, refer to the tables in this appendix when you design the reports. See Chapter 4, "Oracle Audit Vault Data Warehouse Schema" for more information about custom reports created with third-party tools.

C.2 Account Management Events

Account management events track Transact-SQL commands that affect user accounts, such as the UNLOCK ADMIN ACCOUNT command. The Account Management Report, described in Section 3.4.1, uses these events.

Table C–1 lists the Sybase ASE account management events and event IDs.

Table C–1 Sybase ASE Account Management Events and Event IDs

Event Name	Event ID
Login Command	CREATE LOGIN COMMAND DROP LOGIN COMMAND
Set SSA Command	SET SSA COMMAND
SSO Changed Password	SSO CHANGED PASSWORD
Unlock Admin Account	UNLOCK ADMIN ACCOUNT

Table C–2 lists the Sybase ASE account management event attributes.

Table C–2 Sybase ASE Account Management Event Attributes

Attribute Name	Data Type
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
CURRENT_VALUE	VARCHAR2(4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_MOD	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_ID	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
KEYWORD	VARCHAR2(4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PREVIOUS_VALUE	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2(4000)
SEQUENCE	VARCHAR2(4000)
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)

Table C–2 (Cont.) Sybase ASE Account Management Event Attributes

Attribute Name	Data Type
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USER_GUID	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

C.3 Application Management Events

Application management events track actions that were performed on the underlying Transact-SQL commands of system services and applications, such as the CREATE RULE command. The Procedure Management Report, described in Section 3.4.4, uses these events.

Table C–3 lists the Sybase ASE application management events and event IDs.

Table C–3 Sybase ASE Application Management Events and Event IDs

Event Name	Event ID
Create Default	CREATE DEFAULT
Create Message	CREATE MESSAGE
Create Procedure	CREATE PROCEDURE
Create Rule	CREATE RULE
Create SQLJ Function	CREATE SQLJ FUNCTION
Create Trigger	CREATE TRIGGER
Drop Default	DROP DEFAULT
Drop Message	DROP MESSAGE
Drop Procedure	DROP PROCEDURE
Drop Rule	DROP RULE
Drop SQLJ Function	DROP SQLJ FUNCTION
Drop Trigger	DROP TRIGGER

Table C–4 lists the Sybase ASE application management event attributes.

Table C–4 Sybase ASE Application Management Event Attributes

Attribute Name	Data Type
ASSOCIATED_OBJECT_NAME	VARCHAR2(4000)
ASSOCIATED_OBJECT_OWNER	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
CURRENT_VALUE	VARCHAR2(4000)
DATABASE_ID	NUMBER

Table C–4 (Cont.) Sybase ASE Application Management Event Attributes

Attribute Name	Data Type
DATABASE_NAME	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_MOD	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
KEYWORD	VARCHAR2(4000)
NEW_OBJECT_NAME	VARCHAR2(4000)
NEW_OBJECT_OWNER	VARCHAR2(4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PREVIOUS_VALUE	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2(4000)
SEQUENCE	VARCHAR2(4000)
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USER_GUID	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

C.4 Audit Command Events

Audit command events track the use of auditing Transact-SQL commands on other Transact-SQL commands and on database objects. The Audit Command Report, described in Section 3.4.2, uses these events.

Table C–5 lists the Sybase ASE audit command events and event IDs.

Table C–5 Sybase ASE Audit Command Events and Event IDs

Event Name	Event ID
Auditing Disabled	AUDITING DISABLED
Auditing Enabled	AUDITING ENABLED

Table C–6 lists the Sybase ASE audit command event attributes.

Table C–6 Sybase ASE Audit Command Event Attributes

Attribute Name	Data Type
AUDIT_OPTION	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
CURRENT_VALUE	VARCHAR2(4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_MOD	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
KEYWORD	VARCHAR2(4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PREVIOUS_VALUE	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2(4000)
SEQUENCE	VARCHAR2(4000)
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USER_GUID	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

C.5 Data Access Events

Data access events track audited Transact-SQL commands, such as all SELECT TABLE, INSERT TABLE, or UPDATE TABLE commands. The Data Access Report, described in Section 3.3.2, uses these events.

Table C–7 lists the Sybase ASE data access events and event IDs.

Table C–7 Sybase ASE Data Access Events and Event IDs

Event Name	Event ID
Access To Audit Table	ACCESS TO AUDIT TABLE
BCP In	BCP IN
Delete Table	DELETE TABLE
Delete View	DELETE VIEW
Insert Table	INSERT TABLE
Insert View	INSERT VIEW
Select Table	SELECT TABLE
Select View	SELECT VIEW
Truncate Table	TRUNCATE TABLE
Truncation of audit table	TRUNCATION OF AUDIT TABLE
Update Table	UPDATE TABLE
Update View	UPDATE VIEW

Table C–8 lists the Sybase ASE data access event attributes.

Table C–8 Sybase ASE Data Access Event Attributes

Attribute Name	Data Type
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
CURRENT_VALUE	VARCHAR2(4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_MOD	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
KEYWORD	VARCHAR2(4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PREVIOUS_VALUE	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2(4000)
SEQUENCE	VARCHAR2(4000)

Table C–8 (Cont.) Sybase ASE Data Access Event Attributes

Attribute Name	Data Type
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USER_GUID	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

C.6 Exception Events

Exception events track audited error and exception activity, such as network errors. The Exception Activity Report, described in Section 3.5.1, uses these events.

Table C–9 lists Sybase ASE exception events and event IDs.

Table C–9 Sybase ASE Exception Events and Event IDs

Event Name	Event ID
Fatal Error	FATAL ERROR
Nonfatal Error	NONFATAL ERROR

Table C–10 lists the Sybase ASE exception event attributes.

Table C–10 Sybase ASE Exception Event Attributes

Attribute Name	Data Type
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
CURRENT_VALUE	VARCHAR2(4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_MOD	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
KEYWORD	VARCHAR2(4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)

Table C–10 (Cont.) Sybase ASE Exception Event Attributes

Attribute Name	Data Type
PREVIOUS_VALUE	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2(4000)
SEQUENCE	VARCHAR2(4000)
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USER_GUID	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

C.7 Invalid Record Events

Invalid record events track audited activity that Oracle Audit Vault cannot recognize, possibly due to a corrupted audit record. The Invalid Audit Record Report, described in Section 3.5.2, uses these events.

Table C–11 lists Sybase ASE invalid record event attributes.

Table C–11 Sybase ASE Invalid Record Event Attributes

Attribute Name	Data Type
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
CURRENT_VALUE	VARCHAR2(4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
ERROR_ID	NUMBER
ERROR_MESSAGE	VARCHAR2(30)
EVENT_MOD	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
KEYWORD	VARCHAR2(4000)
MODULE_NAME	VARCHAR2(100)

Table C–11 (Cont.) Sybase ASE Invalid Record Event Attributes

Attribute Name	Data Type
OBJECT_ID	NUMBER
ORIGINAL_CONTENT2	VARCHAR2(4000)
ORIGINAL_CONTENT3	VARCHAR2(4000)
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PREVIOUS_VALUE	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2(4000)
SEQUENCE	VARCHAR2(4000)
SEVERITY	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USER_GUID	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

C.8 Object Management Events

Object management events track audited actions performed on database objects, such as CREATE TABLE commands. The Object Management Report, described in Section 3.4.3, uses these events.

Table C–12 lists the Sybase ASE object management events and event IDs.

Table C–12 Sybase ASE Object Management Events and Event IDs

Event Name	Event ID
Access To Database	ACCESS TO DATABASE
Alter Table	ALTER TABLE
Bind Default	BIND DEFAULT
Bind Message	BIND MESSAGE
Bind Rule	BIND RULE
Create Index	CREATE INDEX
Create Table	CREATE TABLE
Create View	CREATE VIEW
Drop Index	DROP INDEX
Drop Table	DROP TABLE

Table C–12 (Cont.) Sybase ASE Object Management Events and Event IDs

Event Name	Event ID
Drop View	DROP VIEW
Unbind Default	UNBIND DEFAULT
Unbind Message	UNBIND MESSAGE
Unbind Rule	UNBIND RULE

Table C–13 lists the Sybase ASE object management event attributes.

Table C–13 Sybase ASE Object Management Event Attributes

Attribute Name	Data Type
ASSOCIATED_OBJECT_NAME	VARCHAR2(4000)
ASSOCIATED_OBJECT_OWNER	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
CURRENT_VALUE	VARCHAR2(4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_MOD	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
KEYWORD	VARCHAR2(4000)
NEW_OBJECT_NAME	VARCHAR2(4000)
NEW_OBJECT_OWNER	VARCHAR2(4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PREVIOUS_VALUE	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2(4000)
SEQUENCE	VARCHAR2(4000)
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)

Table C–13 (Cont.) Sybase ASE Object Management Event Attributes

Attribute Name	Data Type
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USER_GUID	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

C.9 Peer Association Events

Peer association events track database link commands. The Distributed Database Report, described in Section 3.3.4, uses these events. (These events do not have any event names or event IDs; they only contain event attributes.)

Table C–14 lists the Sybase ASE peer association event attributes.

Table C–14 Sybase ASE Peer Association Event Attributes

Attribute Name	Data Type
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
CURRENT_VALUE	VARCHAR2(4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_MOD	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
KEYWORD	VARCHAR2(4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PREVIOUS_VALUE	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2(4000)
SEQUENCE	VARCHAR2(4000)
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)

Table C–14 (Cont.) Sybase ASE Peer Association Event Attributes

Attribute Name	Data Type
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USER_GUID	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

C.10 Role and Privilege Management Events

Role and privilege management events track audited role and privilege management activity, such as revoking permissions from a user to use a specified command. The Role and Privilege Management Report, described in Section 3.4.5, uses these events.

Table C–15 lists the Sybase ASE role and privilege management events and event IDs.

Table C–15 Sybase ASE Role and Privilege Management Events and Event IDs

Event Name	Event ID
Grant Command	GRANT COMMAND
Revoke Command	REVOKE COMMAND
Role Check Performed	ROLE CHECK PERFORMED
Role Toggling	ROLE TOGGLING
User-defined Function Command	ALTER ROLE FUNCTION EXECUTED CREATE ROLE FUNCTION EXECUTED DROP ROLE FUNCTION EXECUTED GRANT ROLE FUNCTION EXECUTED REVOKE ROLE FUNCTION EXECUTED

Table C–16 lists the Sybase ASE role and privilege management event attributes.

Table C–16 Sybase ASE Role and Privilege Management Event Attributes

Attribute Name	Data Type
ADMIN_OPTION	NUMBER
CONTEXTID	VARCHAR2(4000)
COMMENT_TEXT	VARCHAR2(4000)
CURRENT_VALUE	VARCHAR2(4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_MOD	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GRANTEE	VARCHAR2(4000)
HOST_IP	VARCHAR2(255)

Table C–16 (Cont.) Sybase ASE Role and Privilege Management Event Attributes

Attribute Name	Data Type
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
KEYWORD	VARCHAR2(4000)
OBJECT_ID	NUMBER
OBJECT_PRIVILEGE	VARCHAR2(255)
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PREVIOUS_VALUE	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2(4000)
ROLE_NAME	VARCHAR2(4000)
SEQUENCE	VARCHAR2(4000)
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
SYSTEM_PRIVILEGE	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USER_GUID	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

C.11 Service and Application Utilization Events

Service and application utilization events track audited application access activity, such as the execution of Transact-SQL commands. The Procedure Executions Report, described in Section 3.3.5, uses these events.

Table C–17 lists the Sybase ASE service and application utilization events and event IDs.

Table C–17 Sybase ASE Service and Application Utilization Events and Event IDs

Event Name	Event ID
Execution Of Stored Procedure	STORED PROCEDURE EXECUTION
Execution Of Trigger	TRIGGER EXECUTION
RPC In	RPC IN
RPC Out	RPC OUT
Trusted procedure execution	TRUSTED PROCEDURE EXECUTION
Trusted trigger execution	TRUSTED TRIGGER EXECUTION

Table C–18 lists the Sybase ASE service and application utilization event attributes.

Table C–18 Sybase ASE Service and Application Utilization Event Attributes

Attribute Name	Data Type
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
CURRENT_VALUE	VARCHAR2(4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_MOD	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
KEYWORD	VARCHAR2(4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PREVIOUS_VALUE	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2(4000)
SEQUENCE	VARCHAR2(4000)
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USER_GUID	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

C.12 System Management Events

System management events track audited system management activity, such as the `CREATE DATABASE` and `DISK INIT` commands. The System Management Report, described in Section 3.4.6, uses these events.

Table C–19 lists the Sybase ASE system management events and event IDs.

Table C–19 Sybase ASE System Management Events and Event IDs

Event Name	Event ID
AEK Add Encryption	AEK ADD ENCRYPTION
AEK Drop Encryption	AEK DROP ENCRYPTION
AEK Key Recovery	AEK KEY RECOVERY
AEK Modify Encryption	AEK MODIFY ENCRYPTION
AEK Modify Owner	AEK MODIFY OWNER
Alter Database	ALTER DATABASE
Alter Encryption Key	ALTER ENCRYPTION KEY
Audit Option Change	AUDIT OPTION CHANGE
Config	CONFIG
Create Database	CREATE DATABASE
Create Encryption Key	CREATE ENCRYPTION KEY
DBCC Command	DB CONSISTENCY CHECK
Deploy UDWS	DEPLOY UDWS
Disk Init	DISK INIT
Disk Mirror	DISK MIRROR
Disk Refit	DISK REFIT
Disk Reinit	DISK REINIT
Disk Release	DISK RELEASE
Disk Remirror	DISK REMIRROR
Disk Resize	DISK RESIZE
Disk Unmirror	DISK UNMIRROR
Drop Database	DROP DATABASE
Drop Encryption Key	DROP ENCRYPTION KEY
Dump Database	DUMP DATABASE
Dump Transaction	DUMP TRANSACTION
Encrypted Column Administration	ENCRYPTED COLUMN ADMINISTRATION
kill/terminate Command	KILL/TERMINATE COMMAND
Load Database	LOAD DATABASE
Load Transaction	LOAD TRANSACTION
Mount Database	MOUNT DATABASE
Online Database	ONLINE DATABASE
Quiesce Database Command	QUIESCE DATABASE COMMAND
Server Boot	SERVER BOOT
Server Shutdown	SERVER SHUTDOWN
SSL Administration	SSL ADMINISTRATION
Undeploy UDWS	UNDEPLOY UDWS
Unmount Database	UNMOUNT DATABASE

Table C–20 lists the Sybase ASE system management event attributes.

Table C–20 Sybase ASE System Management Event Attributes

Attribute Name	Data Type
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
CURRENT_VALUE	VARCHAR2(4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_MOD	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
KEYWORD	VARCHAR2(4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PREVIOUS_VALUE	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2(4000)
SEQUENCE	VARCHAR2(4000)
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USER_GUID	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

C.13 Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized. The Uncategorized Activity Report, described in Section 3.5.3, uses these events.

Table C–21 shows the Sybase ASE unknown or uncategorized event and event ID.

Table C–21 Sybase ASE Unknown or Uncategorized Events and Event IDs

Event Name	Event ID
Ad Hoc Audit record	AD HOC AUDIT RECORD

Table C–22 lists the Sybase ASE unknown or uncategorized event attributes.

Table C–22 Sybase ASE Unknown or Uncategorized Event Attributes

Attribute Name	Data Type
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
CURRENT_VALUE	VARCHAR2(4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_MOD	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
KEYWORD	VARCHAR2(4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PREVIOUS_VALUE	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2(4000)
SEQUENCE	VARCHAR2(4000)
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USER_GUID	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

C.14 User Session Events

User session events track audited authentication events for users who log in to the database. The User Sessions Report, described in Section 3.3.6, uses these events.

Table C–23 lists the Sybase ASE user session events and event IDs.

Table C–23 Sybase ASE User Session Events and Event IDs

Event Name	Event ID
Connect to command	CONNECT TO COMMAND
Log In	LOG IN
Log Out	LOG OUT
Setuser Command	SETUSER COMMAND

Table C–24 lists the Sybase ASE user session event attributes.

Table C–24 Sybase ASE User Session Event Attributes

Attribute Name	Data Type
AUTHENTICATION_METHOD	VARCHAR2(255)
COMMENT_TEXT	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
CURRENT_VALUE	VARCHAR2(4000)
DATABASE_ID	NUMBER
DATABASE_NAME	VARCHAR2(4000)
ENDUSER	VARCHAR2(4000)
EVENT_MOD	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
KEYWORD	VARCHAR2(4000)
OBJECT_ID	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PARENT_CONTEXTID	VARCHAR2(4000)
PREVIOUS_VALUE	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
PROXY_INFORMATION	VARCHAR2(4000)
SEQUENCE	VARCHAR2(4000)
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)

Table C–24 (Cont.) Sybase ASE User Session Event Attributes

Attribute Name	Data Type
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
USER_GUID	VARCHAR2(4000)
USERNAME	VARCHAR2(4000)

D

IBM DB2 Audit Events

This appendix contains:

- About the IBM DB2 Audit Events
- Account Management Events
- Application Management Events
- Audit Command Events
- Data Access Events
- Exception Events
- Invalid Record Events
- Object Management Events
- Peer Association Events
- Role and Privilege Management Events
- Service and Application Utilization Events
- System Management Events
- Unknown or Uncategorized Events
- User Session Events

D.1 About the IBM DB2 Audit Events

This appendix lists the audit event names and IDs, and the attribute names and data types for IBM DB2. The audit events are organized by their respective categories (for example, Account Management). You can use these audit events as follows:

- **For alerts.** When you create an alert, you can specify an audit event, based on its category, that can trigger the alert. See "Creating an Alert" on page 2-20 for more information.
- **For custom reports using third-party tools.** If you want to create custom reports using other Oracle Database reporting products or third-party tools, refer to the tables in this appendix when you design the reports. See Chapter 4, "Oracle Audit Vault Data Warehouse Schema" for more information about custom reports created with third-party tools.

D.2 Account Management Events

Account management events track SQL commands that affect user accounts, such as the UNLOCK ADMIN ACCOUNT command. The Account Management Report, described in Section 3.4.1, uses these events.

Table D–1 lists the IBM DB2 account management events and event IDs.

Table D–1 IBM DB2 Account Management Events and Event IDs

Event Name	Event ID
ADD_USER	ADD_USER
ALTER_USER_ADD_ROLE	ALTER_USER_ADD_ROLE
ALTER_USER_AUTHENTICATION	ALTER_USER_AUTHENTICATION
ALTER_USER_DROP_ROLE	ALTER_USER_DROP_ROLE
DROP_USER	DROP_USER
SET_SESSION_USER	SET_SESSION_USER

Table D–2 lists the IBM DB2 account management event attributes.

Table D–2 IBM DB2 Account Management Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2(4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2(4000)

D.3 Application Management Events

Application management events track actions that were performed on the underlying SQL commands of system services and applications, such as the CREATE RULE command. The Procedure Management Report, described in Section 3.4.4, uses these events.

Table D–3 lists the IBM DB2 application management events and event IDs.

Table D–3 IBM DB2 Application Management Events and Event IDs

Event Name	Event ID	Comments
ALTER_OBJECT	ALTER_OBJEC	This event covers the following object types: ▪ CONTEXT ▪ FUNCTION ▪ JAVA ▪ PACKAGE ▪ TRIGGER ▪ TRUSTED CONTEXT
CREATE_OBJECT	CREATE_OBJECT	This event covers the following object types: ▪ CONTEXT ▪ FUNCTION ▪ JAVA ▪ PACKAGE ▪ TRIGGER ▪ TRUSTED CONTEXT
DROP_OBJECT	DROP_OBJECT	This event covers the following object types: ▪ CONTEXT ▪ FUNCTION ▪ JAVA ▪ PACKAGE ▪ TRIGGER ▪ TRUSTED CONTEXT

Table D–4 lists the IBM DB2 application management event attributes.

Table D–4 IBM DB2 Application Management Event Attributes

Attribute Name	Data Type
ASSOCIATED_OBJECT_NAME	VARCHAR2(4000)
ASSOCIATED_OBJECT_OWNER	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)

Table D–4 (Cont.) IBM DB2 Application Management Event Attributes

Attribute Name	Data Type
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
ORIGIN_NODE_NUM	NUMBER
NEW_OJBECT_NAME	VARCHAR2(4000)
NEW_OBJECT_OWNER	VARCHAR2(4000)
OSUSER_NAME	VARCHAR2(4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2(4000)

D.4 Audit Command Events

Audit command events track the use of auditing SQL commands on other SQL commands and on database objects. The Audit Command Report, described in Section 3.4.2, uses these events.

Table D–5 lists the IBM DB2 audit command events and event IDs.

Table D–5 IBM DB2 Audit Command Events and Event IDs

Event Name	Event ID
AUDIT_REMOVE	AUDIT_REMOVE
AUDIT_REPLACE	AUDIT_REPLACE
AUDIT_USING	AUDIT_USING
START	START
STOP	STOP

Table D–6 lists the IBM DB2 audit command event attributes.

Table D–6 IBM DB2 Audit Command Event Attributes

Attribute Name	Data Type
AUDIT_OPTION	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)

Table D–6 (Cont.) IBM DB2 Audit Command Event Attributes

Attribute Name	Data Type
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2(4000)

D.5 Data Access Events

Data access events track audited SQL commands, such as all SELECT TABLE, INSERT TABLE, or UPDATE TABLE commands. The Data Access Report, described in Section 3.3.2, uses these events.

Table D–7 lists the IBM DB2 data access events and event IDs.

Table D–7 IBM DB2 Data Access Events and Event IDs

Event Name	Event ID	Comments
EXECUTE	EXECUTE	This event covers the following object types: ■ INSERT ■ UPDATE
STATEMENT	STATEMENT	

Table D–8 lists the IBM DB2 data access event attributes.

Table D–8 IBM DB2 Data Access Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2(4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2(4000)

D.6 Exception Events

Exception events track audited error and exception activity, such as network errors. The Exception Activity Report, described in Section 3.5.1, uses these events. These events do not have any event names or event IDs; they only contain event attributes.

Table D–9 lists the IBM DB2 exception event attributes.

Table D–9 IBM DB2 Exception Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2(4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)

Table D–9 (Cont.) IBM DB2 Exception Event Attributes

Attribute Name	Data Type
HOST_TERMINAL	VARCHAR2(255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2(4000)

D.7 Invalid Record Events

Invalid record events track audited activity that Oracle Audit Vault cannot recognize, possibly due to a corrupted audit record. The Invalid Audit Record Report, described in Section 3.5.2, uses these events.

Table D–10 lists IBM DB2 invalid record event attributes.

Table D–10 IBM DB2 Invalid Record Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2(4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2(4000)
ERROR_ID	NUMBER
ERROR_MESSAGE	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
MODULE_NAME	VARCHAR2(4000)
ORIGIN_NODE_NUM	NUMBER
ORIGINAL_CONTEXT1	VARCHAR2(4000)
ORIGINAL_CONTEXT2	VARCHAR2(4000)

Table D–10 (Cont.) IBM DB2 Invalid Record Event Attributes

Attribute Name	Data Type
ORIGINAL_CONTEXT3	VARCHAR2(4000)
OSUSER_NAME	VARCHAR2(4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SEVERITY	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2(4000)

D.8 Object Management Events

Object management events track audited actions performed on database objects, such as CREATE TABLE commands. The Object Management Report, described in Section 3.4.3, uses these events.

Table D–11 lists the IBM DB2 object management events and event IDs.

Table D–11 IBM DB2 Object Management Events and Event IDs

Event Name	Event ID	Comments
ALTER_OJBECT	ALTER_OJBECT	This event covers the following object types: ■ INDEX ■ SEQUENCE ■ STORED_PROCEDURE ■ TABLE ■ VIEW
CREATE_OBJECT	CREATE_OBJECT	This event covers the following object types: ■ INDEX ■ SEQUENCE ■ STORED_PROCEDURE ■ TABLE ■ VIEW

Table D–11 (Cont.) IBM DB2 Object Management Events and Event IDs

Event Name	Event ID	Comments
DROP_OBJECT	DROP_OBJECT	This event covers the following object types: ■ INDEX ■ SEQUENCE ■ STORED_PROCEDURE ■ TABLE ■ VIEW
RENAME_OBJECT	RENAME_OBJECT	

Table D–12 lists the IBM DB2 object management event attributes.

Table D–12 IBM DB2 Object Management Event Attributes

Attribute Name	Data Type
ASSOCIATED_OBJECT_NAME	VARCHAR2(4000)
ASSOCIATED_OBJECT_OWNER	VARCHAR2(4000)
CONTEXTID	VARCHAR2(4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
NEW_OBJECT_NAME	VARCHAR2(4000)
NEW_OBJECT_OWNER	VARCHAR2(4000)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2(4000)

D.9 Peer Association Events

Peer association events track database link commands. The Distributed Database Report, described in Section 3.3.4, uses these events. These events do not have any event names or event IDs; they only contain event attributes.

Table D–13 lists the IBM DB2 peer association event attributes.

Table D–13 IBM DB2 Peer Association Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2(4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2(4000)

D.10 Role and Privilege Management Events

Role and privilege management events track audited role and privilege management activity, such as granting a user permissions to alter an object. The Role and Privilege Management Report, described in Section 3.4.5, uses these events.

Table D–14 lists the IBM DB2 role and privilege management events and event IDs.

Table D–14 IBM DB2 Role and Privilege Management Events and Event IDs

Event Name	Event ID	Comments
ALTER_OBJECT	ALTER_OBJECT	
CHECKING_FUNCTION	CHECKING_FUNCTION	

Table D–14 (Cont.) IBM DB2 Role and Privilege Management Events and Event IDs

Event Name	Event ID	Comments
CHECKING_OBJECT	CHECKING_OBJECT	
CREATE_OBJECT	CREATE_OBJECT	
DROP_OBJECT	DROP_OBJECT	
GRANT	GRANT	This event covers the ROLE object type
GRANT_DB_AUTHORITIES	GRANT_DB_AUTHORITIES	
GRANT_DBADM	GRANT_DBADM	
IMPLICIT_GRANT	IMPLICIT_GRANT	
IMPLICIT_REVOKE	IMPLICIT_REVOKE	
REVOKE	REVOKE	This event covers the ROLE object type
REVOKE_DB_AUTHORITIES	REVOKE_DB_AUTHORITIES	
REVOKE_DBADM	REVOKE_DBADM	
TRANSFER_OWNERSHIP	TRANSFER_OWNERSHIP	

Table D–15 lists the IBM DB2 role and privilege management event attributes.

Table D–15 IBM DB2 Role and Privilege Management Event Attributes

Attribute Name	Data Type
ADMIN_OPTION	NUMBER
CONTEXTID	VARCHAR2(4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
GRANTEE	VARCHAR2(4000)
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
OBJECT_PRIVILEGE	VARCHAR2(4000)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
ROLE_NAME	VARCHAR2(4000)
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)

Table D–15 (Cont.) IBM DB2 Role and Privilege Management Event Attributes

Attribute Name	Data Type
SYSTEM_PRIVILEGE	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2(4000)

D.11 Service and Application Utilization Events

Service and application utilization events track audited application access activity, such as the execution of SQL commands. The Procedure Executions Report, described in Section 3.3.5, uses these events.

Table D–16 lists the IBM DB2 service and application utilization events and event IDs.

Table D–16 IBM DB2 Service and Application Utilization Events and Event IDs

Event Name	Event ID
EXECUTE	EXECUTE
EXECUTE_IMMEDIATE	EXECUTE_IMMEDIATE

Table D–17 lists the IBM DB2 service and application utilization event attributes.

Table D–17 IBM DB2 Service and Application Utilization Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2(4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)

Table D–17 (Cont.) IBM DB2 Service and Application Utilization Event Attributes

Attribute Name	Data Type
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2(4000)

D.12 System Management Events

System management events track audited system management activity, such as the `CREATE DATABASE` and `DISK INIT` commands. The System Management Report, described in Section 3.4.6, uses these events.

Table D–18 lists the IBM DB2 system management events and event IDs.

Table D–18 IBM System Management Events and Event IDs

Event Name	Event ID
ACTIVATE_DB	ACTIVATE_DB
ADD_NODE	ADD_NODE
ALTER_BUFFERPOOL	ALTER_BUFFERPOOL
ALTER_DATABASE	ALTER_DATABASE
ALTER_NODEGROUP	ALTER_NODEGROUP
ALTER_OBJECT	ALTER_OBJECT
ALTER_TABLESPACE	ALTER_TABLESPACE
BACKUP_DB	BACKUP_DB
BIND	BIND
CLOSE_HISTORY_FILE	CLOSE_HISTORY_FILE
CONFIGURE	CONFIGURE
CREATE_BUFFERPOOL	CREATE_BUFFERPOOL
CREATE_DATABASE	CREATE_DATABASE
CREATE_DB_AT_NODE	CREATE_DB_AT_NODE
CREATE_EVENT_MONITOR	CREATE_EVENT_MONITOR
CREATE_INSTANCE	CREATE_INSTANCE
CREATE_NODEGROUP	CREATE_NODEGROUP
CREATE_OBJECT	CREATE_OBJECT
CREATE_TABLESPACE	CREATE_TABLESPACE
DB2AUDIT	DB2AUDIT
DB2REMOT	DB2REMOT
DB2SET	DB2SET
DEACTIVATE_DB	DEACTIVATE_DB

Table D–18 (Cont.) IBM System Management Events and Event IDs

Event Name	Event ID
DELETE_INSTANCE	DELETE_INSTANCE
DROP_BUFFERPOOL	DROP_BUFFERPOOL
DROP_DATABASE	DROP_DATABASE
DROP_EVENT_MONITOR	DROP_EVENT_MONITOR
DROP_NODEGROUP	DROP_NODEGROUP
DROP_OBJECT	DROP_OBJECT
DROP_TABLESPACE	DROP_TABLESPACE
FETCH_HISTORY_FILE	FETCH_HISTORY_FILE
FORCE_APPLICATION	FORCE_APPLICATION
KILLDBM	KILLDBM
MIGRATE_DB	MIGRATE_DB
MIGRATE_DB_DIR	MIGRATE_DB_DIR
MIGRATE_SYSTEM_DIRECTORY	MIGRATE_SYSTEM_DIRECTORY
OPEN_HISTORY_FILE	OPEN_HISTORY_FILE
QUIESCE_TABLESPACE	QUIESCE_TABLESPACE
REBIND	REBIND
RENAME_TABLESPACE	RENAME_TABLESPACE
RESET_ADMIN_CFG	RESET_ADMIN_CFG
RESET_DB_CFG	RESET_DB_CFG
RESET_DBM_CFG	RESET_DBM_CFG
RESTORE_DB	RESTORE_DB
ROLLFORWARD_DB	ROLLFORWARD_DB
SET_APPL_PRIORITY	SET_APPL_PRIORITY
SET_TABLESPACE_CONTAINERS	SET_TABLESPACE_CONTAINERS
START_DB2	START_DB2
STOP_DB2	STOP_DB2
UNQUIESCE_TABLESPACE	UNQUIESCE_TABLESPACE
UPDATE_ADMIN_CFG	UPDATE_ADMIN_CFG
UPDATE_AUDIT	UPDATE_AUDIT
UPDATE_DB_CFG	UPDATE_DB_CFG
UPDATE_DBM_CFG	UPDATE_DBM_CFG

Table D–19 lists the IBM DB2 system management event attributes.

Table D–19 IBM DB2 System Management Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2(4000)
COORDINATOR_NODE_NUM	NUMBER

Table D–19 (Cont.) IBM DB2 System Management Event Attributes

Attribute Name	Data Type
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2(4000)

D.13 Unknown or Uncategorized Events

Unknown or uncategorized events track audited activity that cannot be categorized. The Uncategorized Activity Report, described in Section 3.5.3, uses these events.

Table D–20 lists the IBM DB2 unknown or uncategorized event and event ID.

Table D–20 IBM DB2 Unknown or Uncategorized Events and Event IDs

Event Name	Event ID
ALTER_OBJECT	ALTER_OBJECT
CREATE_OBJECT	CREATE_OBJECT
DROP_OBJECT	DROP_OBJECT

Table D–21 lists the IBM DB2 unknown or uncategorized event attributes.

Table D–21 IBM DB2 Unknown or Uncategorized Event Attributes

Attribute Name	Data Type
CONTEXTID	VARCHAR2(4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2(4000)

Table D–21 (Cont.) IBM DB2 Unknown or Uncategorized Event Attributes

Attribute Name	Data Type
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2(4000)

D.14 User Session Events

User session events track audited authentication events for users who log in to the database. The User Sessions Report, described in Section 3.3.6, uses these events.

Table D–22 lists the IBM DB2 user session events and event IDs.

Table D–22 IBM DB2 User Session Events and Event IDs

Event Name	Event ID
ATTACH	ATTACH
AUTHENTICATE	AUTHENTICATE
COMMIT	COMMIT
CONNECT	CONNECT
CONNECT RESET	CONNECT RESET
DETACH	DETACH
ROLLBACK	ROLLBACK
VALIDATE_USER	VALIDATE_USER

Table D–23 lists the IBM DB2 user session event attributes.

Table D–23 IBM DB2 User Session Event Attributes

Attribute Name	Data Type
AUTHENTICATION_METHOD	VARCHAR2(255) **CHAR LENGTH OKAY?**
CONTEXTID	VARCHAR2(4000)
COORDINATOR_NODE_NUM	NUMBER
ENDUSER	VARCHAR2(4000)
EVENT_STATUS	VARCHAR2(30)
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE
HOST_IP	VARCHAR2(255)
HOST_NAME	VARCHAR2(255)
HOST_TERMINAL	VARCHAR2(255)
ORIGIN_NODE_NUM	NUMBER
OSUSER_NAME	VARCHAR2(4000)
PACKAGE_INFO_STR	VARCHAR2
PARENT_CONTEXTID	VARCHAR2(4000)
PRIVILEGES_USED	VARCHAR2(4000)
PROCESS#	NUMBER
SOURCE_EVENTID	VARCHAR2(255)
SUB_CONTEXTID	VARCHAR2(4000)
TARGET_OBJECT	VARCHAR2(4000)
TARGET_OWNER	VARCHAR2(4000)
THREAD#	NUMBER
TOOLS_USED	VARCHAR2(4000)
TRUSTED_CONTEXT_STR	VARCHAR2
USERNAME	VARCHAR2(4000)

Index