

Oracle® Audit Vault

Auditor's Guide

10g Release 2 (10.2.2)

B28853-02

August 2007

Oracle Audit Vault Auditor's Guide, 10g Release 2 (10.2.2)

B28853-02

Copyright © 2007, Oracle. All rights reserved.

Primary Author: Ellen Desmond

Contributing Author: Rodney Ward

Contributors: Tammy Bednar, Jack Brinson, Raghavendran Hanumantharau, Vipul Shah, Prahlada Varadan Thirumalai, Janet Blowney

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Contents

Preface	ix
Audience	ix
Documentation Accessibility	ix
Related Documents	x
Conventions	x
 1 Introduction to Database Auditing	
1.1 Security Challenges	1-1
1.1.1 Insider Threats	1-2
1.1.2 Identity Theft	1-2
1.1.3 Corporate Governance and Compliance	1-2
1.2 Need for Database Auditing	1-3
1.3 Overview of Oracle Audit Vault	1-3
1.4 Using Oracle Audit Vault Dashboard	1-5
1.5 Viewing Collectors and Agents	1-8
1.5.1 Collectors Page	1-8
1.5.2 Agents Page	1-8
 2 Configuring Audit Policies	
2.1 Configuring Audit Settings	2-1
2.1.1 Viewing and Defining Audit Settings	2-1
2.1.1.1 Audit Settings Page	2-2
2.1.1.2 Search And Select: Audit Source Page	2-2
2.1.2 Overview Page	2-3
2.1.3 Defining a Statement Auditing Policy	2-5
2.1.3.1 Statement Page	2-5
2.1.3.2 Create Statement Audit Page	2-7
2.1.4 Creating an Object Auditing Policy	2-7
2.1.4.1 Object Page	2-8
2.1.4.2 Create Object Audit Page	2-9
2.1.5 Defining a Privilege Auditing Policy	2-10
2.1.5.1 Privilege Page	2-10
2.1.5.2 Create Privilege Audit Page	2-12
2.1.6 Creating a Fine-Grained Auditing (FGA) Policy	2-13
2.1.6.1 FGA Page	2-15

2.1.6.2	Create FGA Page.....	2-16
2.1.6.3	Fine-Grained Audit Detail Page.....	2-17
2.1.7	Creating a Capture Rule	2-17
2.1.7.1	Capture Rule Page.....	2-17
2.1.7.2	Create Capture Rule Page	2-19
2.2	Configuring Alerts	2-19
2.2.1	Creating an Alert.....	2-20
2.2.2	Audit Alerts Page.....	2-20
2.2.3	Alerts Page.....	2-22
2.2.4	Create Alert Rule Page.....	2-22
2.2.4.1	Basic Alert Condition	2-23
2.2.4.2	Advanced Alert Condition.....	2-23

3 Oracle Audit Vault Reports

3.1	Activity Reports	3-1
3.1.1	Activity Reports Page.....	3-2
3.1.2	Activity Overview Report	3-3
3.1.2.1	Report Fields and Filter Criteria on the Activity Overview Report Page	3-3
3.1.2.2	Activity Overview Actions	3-5
3.1.3	Common Features of Audit Event Activity Pages.....	3-6
3.1.3.1	Report Fields and Filter Criteria on Audit Event Activity Report Pages	3-6
3.1.3.2	Other Actions to Perform in Audit Event Activity Pages	3-8
3.1.3.3	Detail Report	3-8
3.1.4	Activity Reports	3-10
3.1.4.1	Account Management Activity.....	3-10
3.1.4.2	Application Management Activity	3-10
3.1.4.3	Audit Command Activity	3-11
3.1.4.4	Data Access Activity	3-11
3.1.4.5	Exception Activity	3-12
3.1.4.6	Invalid Audit Record Activity	3-12
3.1.4.7	Object Management Activity	3-12
3.1.4.8	Peer Association Activity	3-13
3.1.4.9	Role and Privilege Management Activity.....	3-13
3.1.4.10	Service and Application Access Activity	3-13
3.1.4.11	System Management Activity.....	3-14
3.1.4.12	Uncategorized Activity.....	3-14
3.1.4.13	User Session Activity	3-14
3.1.5	Creating Customized Reports.....	3-15
3.2	Alert Reports.....	3-20
3.2.1	Alert Report Page.....	3-20
3.2.1.1	Report Fields and Filter Criteria on the Alert Page	3-20
3.2.1.2	Actions to Perform on the Alert Report Page.....	3-22
3.3	Data Warehouse	3-22

A Data Warehouse Schema Reference

A.1	Oracle Audit Vault Audit Data Warehouse Architecture.....	A-1
A.2	Design of the Audit Data Warehouse	A-2

A.3	Fact Table and Dimension Tables.....	A-3
A.4	Fact Table Constraints and Indexes.....	A-5
A.5	Table Details	A-6
A.5.1	AUDIT_EVENT_FACT Table	A-7
A.5.2	CLIENT_HOST_DIM Table	A-9
A.5.3	CONTEXT_DIM Table	A-10
A.5.4	EVENT_DIM Table.....	A-10
A.5.5	PRIVILEGES_DIM Table	A-11
A.5.6	SOURCE_DIM Table	A-11
A.5.7	TARGET_DIM Table	A-11
A.5.8	TIME_DIM Table	A-12
A.5.9	USER_DIM Table	A-13

B Oracle Database Audit Events

B.1	Attributes by Event Category.....	B-1
B.1.1	Account Management Event Attributes.....	B-1
B.1.2	Application Management Event Attributes.....	B-2
B.1.3	Audit Command Event Attributes.....	B-4
B.1.4	Data Access Event Attributes.....	B-5
B.1.5	Exceptional Event Attributes	B-6
B.1.6	Invalid Record Event Attributes.....	B-7
B.1.7	Object Management Event Attributes	B-8
B.1.8	Peer Association Event Attributes.....	B-10
B.1.9	Role and Privilege Management Event Attributes	B-11
B.1.10	Service and Application Utilization Event Attributes.....	B-12
B.1.11	System Management Event Attributes	B-13
B.1.12	Unknown or Uncategorized Event Attributes	B-14
B.1.13	User Session Event Attributes.....	B-15
B.2	Source Event IDs	B-16
B.2.1	Account Management Events	B-16
B.2.2	Application Management Events	B-17
B.2.3	Audit Events	B-18
B.2.4	Data Access Events	B-18
B.2.5	Exceptional Events.....	B-19
B.2.6	Invalid Record Events	B-19
B.2.7	Object Management Events.....	B-19
B.2.8	Peer Association Events	B-20
B.2.9	Role and Privilege Management Events	B-21
B.2.10	Service and Application Utilization Events	B-21
B.2.11	System Management Events	B-21
B.2.12	Unknown or Uncategorized Events.....	B-22
B.2.13	User Session Events	B-22

Index

List of Figures

1-1	Oracle Audit Vault Architecture.....	1-4
1-2	Audit Vault Dashboard.....	1-6
2-1	Overview Page	2-3
2-2	Statement Page	2-6
2-3	Object Page.....	2-8
2-4	Privilege Page	2-11
2-5	Fine-Grained Auditing Page	2-15
2-6	Capture Rule Page	2-18
2-7	Audit Alerts Page.....	2-20
2-8	Create Alert Rule Page, Advanced Alert Condition.....	2-24
3-1	Activity Reports Page.....	3-2
3-2	Creating Customized Reports Showing the Pre-Query State.....	3-16
3-3	Creating Customized Reports Showing the Results of the Query	3-17
3-4	Creating Customized Reports Generating the Account Management Report	3-18
3-5	Activity Reports	3-19
3-6	My Customized Account Management Report: User Creation Failures.....	3-19
3-7	My Customized Report: SYS User Sessions.....	3-20
A-1	Architecture of the Oracle Audit Vault Audit Data Warehouse.....	A-2
A-2	Structure of the Audit Data Warehouse	A-3
A-3	Source Dimension Hierarchy	A-4
A-4	Tables in the Oracle Audit Vault Data Warehouse.....	A-7

List of Tables

2-1	Fields in the Audit Settings List.....	2-2
2-2	Overview Fields	2-4
2-3	Statement Fields	2-6
2-4	Create Statement Audit Fields	2-7
2-5	Object Fields.....	2-9
2-6	Create Object Fields	2-9
2-7	Privilege Fields	2-12
2-8	Create Privilege Fields.....	2-12
2-9	Fine-Grained Audit Fields	2-15
2-10	Create Fine-Grained Audit Fields	2-16
2-11	Fine-Grained Audit Detail Fields	2-17
2-12	Capture Rule Fields	2-18
2-13	Create Capture Rule Fields.....	2-19
2-14	Audit Alerts Fields.....	2-21
2-15	Alerts Page Fields.....	2-22
2-16	Create Alert Rule Fields	2-22
2-17	Basic Alert Condition Fields.....	2-23
3-1	Report Fields and Filter Criteria on the Activity Overview Report Page.....	3-3
3-2	Report Fields and Filter Criteria on Audit Event Activity Report Pages	3-6
3-3	Fields on the Detail Report Page.....	3-8
3-4	Report Fields and Filter Criteria on the Alert Report Page	3-21
A-1	Constraints Defined for the AUDIT_EVENT_FACT Table	A-5
A-2	Local Bitmap Indexes Defined on the AUDIT_EVENT_FACT Table	A-5
A-3	Bitmap Join Indexes Defined for the SOURCE_DIM and EVENT_DIM Columns	A-6
A-4	AUDIT_EVENT_FACT Table	A-7
A-5	CLIENT_HOST_DIM Table.....	A-9
A-6	CONTEXT_DIM Table	A-10
A-7	EVENT_DIM Table	A-10
A-8	PRIVILEGES_DIM Table	A-11
A-9	SOURCE_DIM Table	A-11
A-10	TARGET_DIM Table	A-11
A-11	TIME_DIM Table	A-12
A-12	USER_DIM Table	A-13
B-1	Account Management Event Attributes	B-2
B-2	Application Management Event Attributes	B-3
B-3	Audit Command Event Attributes	B-4
B-4	Data Access Event Attributes	B-5
B-5	Exceptional Event Attributes	B-6
B-6	Invalid Record Event Attributes	B-7
B-7	Object Management Event Attributes.....	B-9
B-8	Peer Association Event Attributes.....	B-10
B-9	Role and Privilege Management Event Attributes	B-11
B-10	Service and Application Utilization Event Attributes.....	B-12
B-11	System Management Event Attributes	B-13
B-12	Unknown or Uncategorized Event Attributes.....	B-14
B-13	User Session Event Attributes.....	B-15
B-14	Account Management Events and Event IDs	B-17
B-15	Application Management Events and Event IDs	B-17
B-16	Audit Events and Event IDs	B-18
B-17	Data Access Events and Event IDs	B-19
B-18	Exceptional Events and Event IDs.....	B-19
B-19	Invalid Record Events and Event IDs	B-19
B-20	Object Management Events and Event IDs.....	B-19

B-21	Peer Association Events and Event IDs	B-21
B-22	Role and Privilege Management Events and Event IDs.....	B-21
B-23	Service and Application Utilization Events and Event IDs	B-21
B-24	System Management Events and Event IDs	B-21
B-25	Unknown or Uncategorized Events and Event IDs.....	B-22
B-26	User Session Events and Event IDs	B-23

Preface

Oracle Audit Vault Auditor's Guide provides usage information for Audit Vault administrators who perform auditing tasks on an Audit Vault system.

Audience

This document is intended for administrators who have 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, seven days a week. For TTY support, call 800.446.2398.

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 Streams Concepts and Administration*
- *Oracle Database Reference*
- *Oracle Database Security Guide*
- *Oracle Database Advanced Security Administrator's Guide*
- *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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>monospace</code>	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Introduction to Database Auditing

The analysis of audit data has become an important tool for detecting fraud and data misuse. Audit trails can contain extensive, detailed, and sensitive information about production systems. Auditing enables the detection of unauthorized actions, as well as the actions performed by authorized users. It reveals who did what, and what was affected. Even audit information that might seem harmless by itself can be used to infer other confidential information after some correlation.

The job of the auditor is to view predefined reports based on audit event categories, detect security risks, create and evaluate alert scenarios, and create and manage detailed and summary reports of events across systems. The auditor can create custom audit reports and use the Data Warehouse service to analyze audit data for trends, intrusions, anomalies, and so on.

Oracle Database provides a depth of auditing that readily enables businesses to implement enhanced protections, early detection of suspicious activities, and finely tuned security responses to address compliance and privacy requirements.

See Also: *Oracle Database Security Guide* for detailed information about configuring database auditing.

This chapter contains the following sections:

- [Security Challenges](#)
- [Need for Database Auditing](#)
- [Overview of Oracle Audit Vault](#)
- [Using Oracle Audit Vault Dashboard](#)
- [Viewing Collectors and Agents](#)

1.1 Security Challenges

Database auditing is performed to protect and preserve privacy for the information stored in databases. Businesses leverage database auditing to address the following issues:

- [Insider Threats](#)
- [Identity Theft](#)
- [Corporate Governance and Compliance](#)

1.1.1 Insider Threats

Insiders pose a major threat to information security. The CSI/FBI 2005 Computer Crime and Security Survey have documented that more than 70% of information system data losses and attacks have been perpetrated by insiders, that is, by those authorized at least some level of access to the system and its data. Authorized users include employees, partners, hosting companies, guests, and clients. Insider security breaches can be much more costly than attacks from outside the enterprise.

1.1.2 Identity Theft

Every enterprise that collects personal information from its customers is responsible for protecting the privacy of that data. Securing sensitive customer information is a business necessity and, in many cases, it is mandated by law.

Identity theft has emerged as an organized criminal activity. Increased incidents of identity theft have caused growing concern among consumers regarding the privacy of their data. Recent headlines have trumpeted major thefts of customer data from banks, retailers, and information brokers. As a result, information protection and auditing have become top-level issues for many enterprises.

Businesses and governments have incurred substantial costs due to identity theft, including:

- Business disruption
- Time and money lost responding to the incidents
- Direct financial losses (government fines, stock market losses, or customer lawsuits)
- Imprisonment
- Negative publicity and damage to reputation
- Damage to national security
- Loss of life

1.1.3 Corporate Governance and Compliance

In response to severe corporate governance and structural failures over the last decade, governments and international bodies have dramatically increased their regulatory requirements. In addition, governments have enacted a wide range of legislation to safeguard investor, patient, consumer, and citizen data. Corporate governance and compliance regulations often require information systems auditing, log analysis and reporting, and log retention. Some of these regulations impose severe criminal penalties for noncompliance and malfeasance with protected data. International, U.S. federal and state laws, and regulations that require strong security and auditing include:

- Sarbanes-Oxley Act (corporate financial compliance)
- Basel Capital Accord (banking industry regulatory compliance)
- SEC 17a-3 and 17a-4, NASD 3010, and NYSE (financial industry compliance)
- FDA 21-CFR-11 (pharmaceutical industry regulatory compliance)
- Homeland Security Presidential Directive (HSPD-12)
- Gramm-Leach-Bliley Act (finance)
- HIPAA (health care regulatory compliance)

- Children's Online Privacy Protection Act (COPPA)
- California SB 1386 (consumer)
- Payment Card Industry (PCI) Data Security Standard
- Family Educational Rights and Privacy Act (FERPA)
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the European Union Privacy Protection Directive 2002/58/EC (privacy compliance)

1.2 Need for Database Auditing

Auditing can help compliance and security auditors to perform the following tasks:

- Determining the actions that occur within a system
- Detecting attempts of unauthorized individuals to access the system
- Detecting attempts by authorized users to misuse the system
- Verifying regulatory compliance

You typically use auditing to:

- Investigate suspicious activity

For example, if a user is deleting data from tables, then a security administrator might decide to audit all connections to the database and all successful and unsuccessful deletions of rows from all tables in the database.

- Notify an auditor of unauthorized actions by users

For example, the unauthorized user could be manipulating or deleting data. The user might have more privileges than expected, and it might be time to reassess user authorizations.

- Monitor and gather data about specific database activities

For example, the database administrator can gather statistics about which tables are being updated or how many concurrent users connect at peak times.

- Detect problems with an authorization or access control implementation

For example, you can create audit policies that you expect will never generate an audit record because the data is protected in other ways. However, if these policies do generate audit records, then controls are not properly implemented.

- Address auditing requirements for compliance

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

1.3 Overview of Oracle Audit Vault

Businesses use a wide variety of systems, databases, and applications that produce vast quantities of audit log data, and they must consolidate and monitor this data for a holistic view of enterprise data access. Auditors must analyze the audit log data in a timely fashion across disparate and heterogeneous systems. To facilitate the process, it

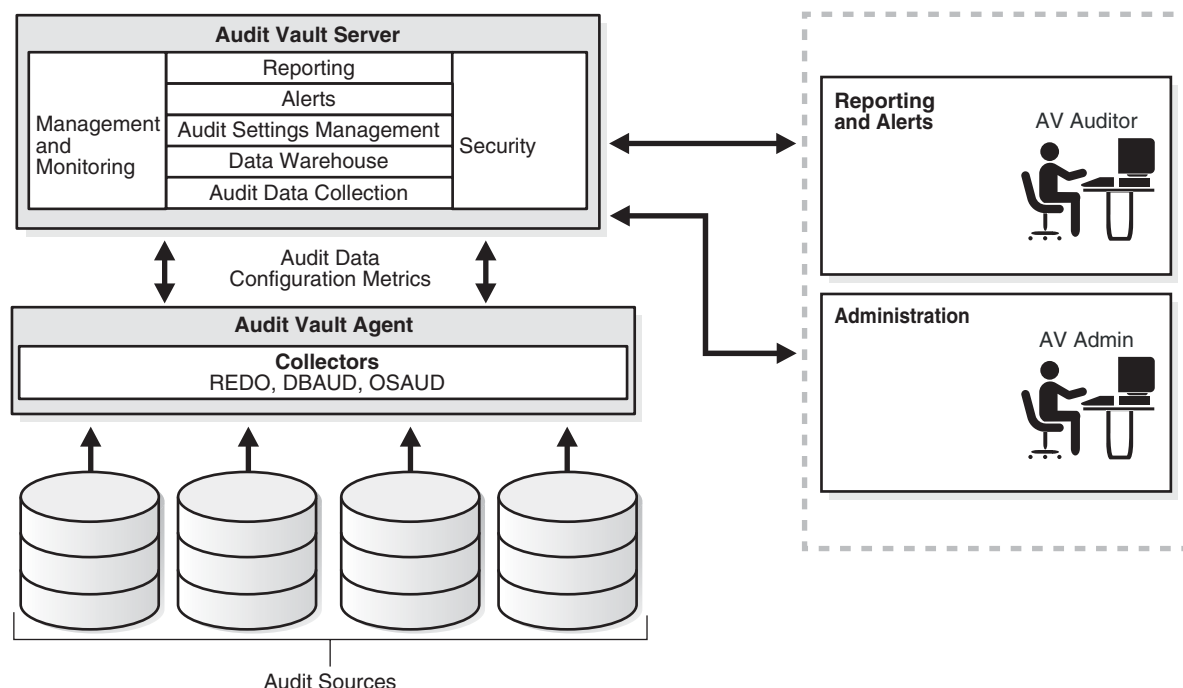
is essential that audit data from multiple systems reside in a single audit data warehouse that is secure, scalable, reliable, and highly available.

Oracle Audit Vault solves these security and audit problems by:

- Consolidating audit information from multiple systems across the enterprise
- Detecting data changes associated with regular and privileged users
- Protecting audit data from modification and tampering

Figure 1–1 shows an overview of the Oracle Audit Vault architecture. The architecture consists of a set of services and its collection system working within an enterprise. This set of services helps to facilitate storage management, policy enforcement, alerting, analysis, reporting, and activities. The collection infrastructure enables the utilization of audit collectors that function as adaptors between an audit source and Oracle Audit Vault Server.

Figure 1–1 Oracle Audit Vault Architecture



Oracle Audit Vault Components

Oracle Audit Vault consists of:

- Audit Vault Server
- Audit Vault Agents

Audit Vault Server

Audit Vault Server consists of:

- Audit Data Store
- Audit Vault Console
- The following services:
 - Collector management and monitoring

- Report management
- Alert management
- Audit settings management to establish your policy management
- Published data warehouse that can be used with reporting tools like Oracle Business Intelligence Publisher to create customized reports
- Audit data collection and storage management

Configuration services assist in defining information about what sources are known to Oracle Audit Vault. Oracle Audit Vault stores information (metadata) about the sources of audit data and policy information (database audit settings).

Audit Vault Agents

An Audit Vault Agent provides run-time support for audit data collection by Audit Vault collectors. It also contains the audit data collectors for Oracle Database sources. The following collectors are provided in Oracle Audit Vault 10g release 2 (10.2.2):

- DBAUD
- OSAUD

Note: XML files are not supported in the OSAUD collector.

- OSAUD for Windows (EVTLOG)
- REDO

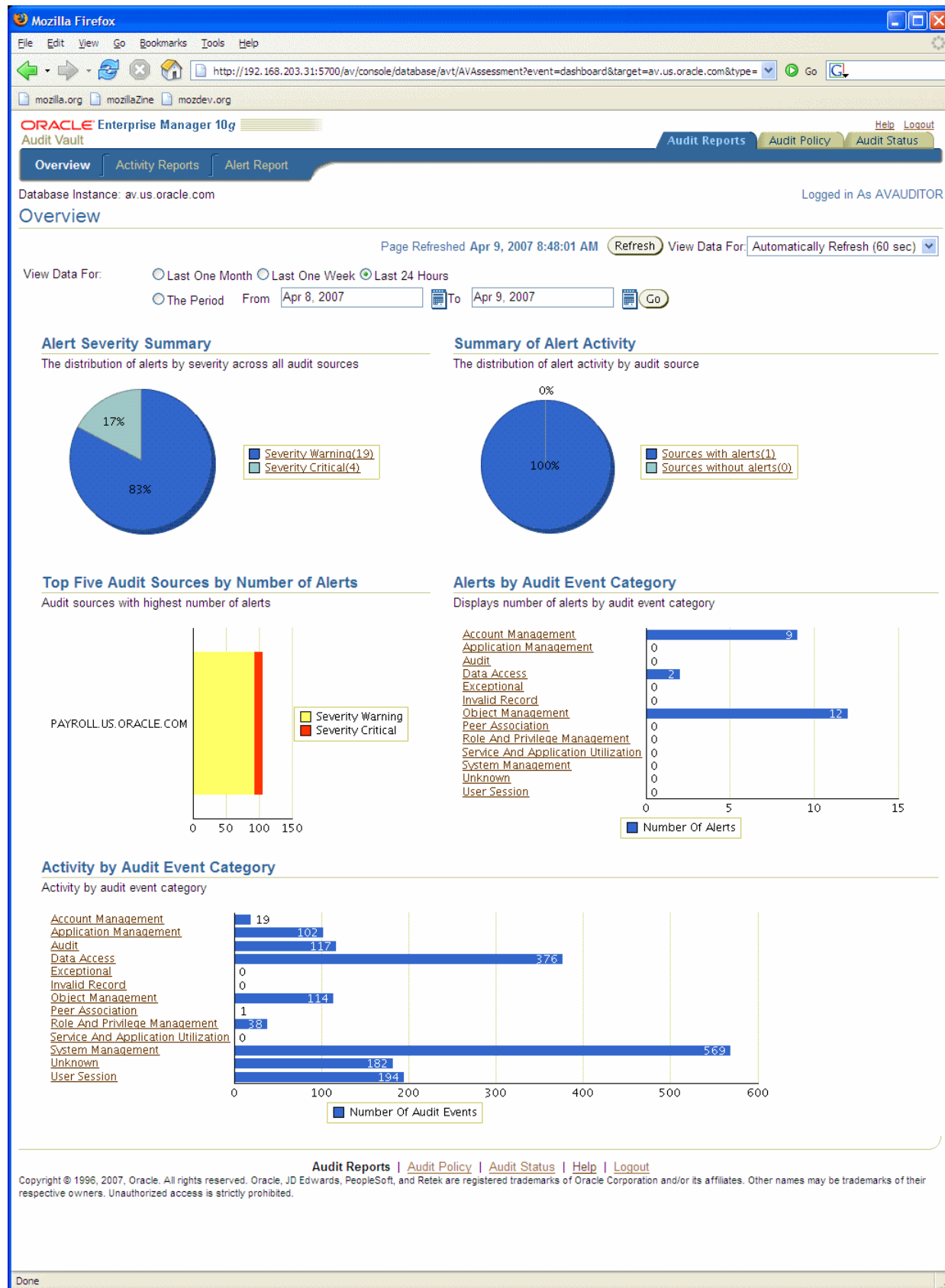
1.4 Using Oracle Audit Vault Dashboard

Oracle Audit Vault Dashboard, also called **Overview**, is the home page for auditors to view alert summaries, drill down to reports, and view agent and collector status. It is shown in [Figure 1-2](#).

When an audit record is generated, it is classified into a category. 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.

An alert is raised when data in a single audit record matches a predefined alert rule condition. For example, an alert rule condition might be defined for a logon event when three failed logon attempts by a user to gain access to a particular source of data are detected over a 5-minute period. When that rule condition is met, the audit event is evaluated and, because it matches the rule condition, an alert is raised. 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 1–2 Audit Vault Dashboard



From the Dashboard page, you can:

- Select an event start time and end time in which to view Audit Vault event data.
- View five types of graphical summaries (pie charts and bar graphs) of alert activity and event activity over the specified time period. Time periods are specified by either a month, week, or day time span or the period between a specified begin and end date. These graphical summaries include:
 - **Alert Severity Summary** (pie chart)
Click a section in this pie chart to drill down to a more detailed [Alert Report Page](#) to see what sources are showing a particular severity level.
 - **Summary of Alert Activity** (pie chart)
Click a section in this pie chart to drill down to an [Alert Report Page](#) 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 drill down to see a more detailed [Alert Report Page](#) showing the alerts for 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 a more detailed [Alert Report Page](#) showing 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 drill down to see events for that event category. You can generate activity reports for the following audit event categories:
 - * [Account Management Activity](#)
 - * [Application Management Activity](#)
 - * [Audit Command Activity](#)
 - * [Data Access Activity](#)
 - * [Exception Activity](#)
 - * [Invalid Audit Record Activity](#)
 - * [Object Management Activity](#)
 - * [Peer Association Activity](#)
 - * [Role and Privilege Management Activity](#)
 - * [Service and Application Access Activity](#)
 - * [System Management Activity](#)
 - * [Uncategorized Activity](#)
 - * [User Session Activity](#)
- Click a pie section or bar chart y-axis event category label to drill down to a more detailed report level.

1.5 Viewing Collectors and Agents

As an Audit Vault auditor, you can use the Audit Vault Console Dashboard to view Audit Vault agents and collectors. To view collectors, click the **Audit Status** tab on the dashboard, then click **Collectors** on the upper left to reach the [Collectors Page](#).

To view agents, click the **Audit Status** tab on the dashboard, then click the **Agents** tab on the upper left to reach the [Agents Page](#).

1.5.1 Collectors Page

From the Collectors page, you can view collectors listed by their name. Collector information includes the following column headings:

- **Collector** – Name of the collector
- **Agent** – The name of the agent to 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.

1.5.2 Agents Page

From the Agents page, you can view agents listed by name. Agent information includes the following column headings:

- **Agent** – The name of the agent
- **Host** – The name of host system where the agent resides
- **Port** – The port number for this agent
- **HTTPS** – Whether the agent is communicating with Audit Vault using a secure communication channel (HTTPS) or not
- **Status** – Whether or not the agent is running. When the agent is up, a green up arrow indicator is displayed. When the agent is down, a red down arrow indicator is displayed. When there is a problem, an error is displayed.

Configuring Audit Policies

To use Oracle Audit Vault effectively, you must configure the proper settings and alerts. The management of settings and alerts is an important part of the auditor's job.

This chapter includes the following sections:

- [Configuring Audit Settings](#)
- [Configuring Alerts](#)

2.1 Configuring Audit Settings

Auditing can be based on individual actions, such as the type of SQL statement run, or on combinations of factors that can include name, application, and time. Security policies can trigger auditing when specified elements in an Oracle Database are accessed or altered, including content.

Oracle Database auditing enables the use of several different mechanisms for auditing. The Oracle audit facility enables businesses to audit database activity by statement, by use of system privilege, by object, or by user.

For example, you can audit activity as general as all user connections to the database, and as specific as a particular user creating a table. You can also audit only successful or only unsuccessful operations. By auditing unsuccessful SELECT statements, you might catch users on "fishing expeditions" for data they are not privileged to see.

For a complete overview of database auditing, see *Oracle Database Advanced Security Administrator's Guide*. This section focuses on policies that can be set in Oracle Audit Vault.

2.1.1 Viewing and Defining Audit Settings

To view or define audit policies, you start from the [Audit Settings Page](#). To reach the [Audit Settings Page](#), click the **Audit Policy** tab on the dashboard. If necessary, click **Audit Settings** on the upper left.

The [Audit Settings Page](#) lists source names known to this Audit Vault instance. For each source, it shows the number of active (provisioned) and needed (desired) settings and the number of audit settings that require attention by the auditor. To view up-to-date policy information from the source, select the audit source from which you want to retrieve settings and click **Retrieve**. This operation fetches the latest policies from the source and loads them into Oracle Audit Vault.

From the [Audit Settings Page](#), you can view detailed information about the settings for an audit source by clicking the name of the audit source. This takes you to the [Overview Page](#), which lists the audit setting types and their number. Clicking one of

the tabs on the [Overview Page](#) takes you to a page that lists the policies of that type, if any exist. See the page descriptions for more information.

To define audit policies, go to the [Audit Settings Page](#). Then determine which Audit Source you want to define settings for and click the name of the Audit Source to go to the [Overview Page](#).

Starting from the [Overview Page](#), you select a policy type that you want to define for this source by clicking the corresponding tab. Clicking the tab takes you to a page where you define a policy type. Once you have defined policies, you click the **Overview** tab to return to the [Overview Page](#). On the [Overview Page](#), you can save, verify, and provision or export the policies you created.

2.1.1.1 Audit Settings Page

This page contains a complete list of source names known to this Audit Vault instance.

To retrieve policy information from the source, select the audit source from which you want to retrieve settings and click **Retrieve from Source**. This operation fetches the latest policies from the source and loads them into Oracle Audit Vault.

To filter the list of audit sources, enter text in the **Audit Source** text field or click the flashlight symbol to reach 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** field will be populated with your selections.

When you are satisfied with the selections in the **Audit Source** field, click **Go** to view information about the audit sources you have selected.

The audit settings list contains the fields shown in [Table 2–1](#).

Table 2–1 Fields in the Audit Settings List

Field	Description
Select	Click to select which audit source to retrieve
Audit Source	Displays the name of the audit source
In Use	Number of active settings on the source system
Needed	Number of audit settings set up by the auditor but not active on the source system (that is, not provisioned)
Problem	Number of audit settings that require attention by the auditor
Audit Trail	The location to which database audit records are directed. See <i>Oracle Database Reference</i> for a list of possible values for AUDIT_TRAIL.
Audit Sys	Whether 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

2.1.1.2 Search And Select: Audit Source Page

On the Search And Select: Audit Source page, enter text in the **Audit Source**, **Audit Source Host**, or **Audit Source Host IP** fields, or a combination of fields, then click **Go**. When you are satisfied with the result of your search, select the audit sources you want, then click **Select** to return to the [Audit Settings Page](#). The **Audit Source** field in the Audit Settings page will now be populated with the audit sources that you selected.

2.1.2 Overview Page

To define audit policies for an audit source, you start at the [Audit Settings Page](#), determine which audit source you want to define settings for, and click the name of the audit source to go to the Overview page shown in [Figure 2–1](#).

Figure 2–1 Overview Page

Oracle Enterprise Manager 10g
Audit Vault

Database Instance: [av.us.oracle.com](#) > [Audit Settings](#) > [PAYROLL.US.ORACLE.COM](#) Logged in As AVAUDITOR

[Overview](#) [Statement](#) [Object](#) [Privilege](#) [FGA](#) [Capture Rule](#)

Save Audit Settings

You can save your work by clicking on the Save All Audit Settings button below. Please note, saving your work does not automatically apply these settings to the source database

[Save All Audit Settings](#)

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 All | Select None

Select	Audit Settings Type	In Use	Needed	Problem
<input checked="" type="checkbox"/>	STATEMENTS	5	0	0
<input checked="" type="checkbox"/>	OBJECTS	4	0	0
<input checked="" type="checkbox"/>	PRIVILEGES	23	0	0
<input checked="" type="checkbox"/>	FGA	3	0	0
<input checked="" type="checkbox"/>	CAPTURE RULE	3	0	0

[Verify](#) [Export as SQL](#) * Audit Source User Name [Provision](#)
* Audit Source Password

Copy Audit Settings from Another Source

You can quickly replicate audit settings from one database to another to seed it with common audit settings. You can either use settings that are already in use on the database or settings that you have set up in Audit Vault but not yet applied to that database

Copy ☐ Actual(In Use) ☒ Needed(Not Yet In Use) Audit Settings

From [Load](#)

[Overview](#) [Statement](#) [Object](#) [Privilege](#) [FGA](#) [Capture Rule](#)

[Audit Reports](#) | [Audit Policy](#) | [Audit Status](#) | [Help](#) | [Logout](#)

Copyright © 1996, 2007, Oracle. All rights reserved. Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Unauthorized access is strictly prohibited.

Done

You use the Overview page to select a policy type that you want to define for this source. Links from this page take you to other pages where you define the policies.

Once you have defined the policies, you return to this page to save, verify, and provision or export the policies. To save your selections, click **Save All Audit Settings**.

As shown in [Figure 2–1](#), the Overview page lists five **Audit Settings Types**:

- Statement
- Object
- Privilege
- FGA
- Capture Rule

In addition to **Audit Statement Types**, the list has the fields shown in [Table 2–2](#).

Table 2–2 Overview Fields

Field	Description
In Use	Number of active settings on the source system
Needed	Number of audit settings set up by the auditor but not active on the source system (that is, not provisioned)
Problem	Number of audit settings that require attention by the auditor

There are tabs at the top and bottom of the page. Clicking **Overview** takes you back to this page. The next five tabs, **Statement**, **Object**, **Privilege**, **FGA**, and **Capture Rule**, correspond with the five audit categories **Audit Settings Type** column. Clicking one of those tabs takes you to a page that lists the policies of that type, if any exist. On each of those pages, you can click **Create** to create a policy of that type. The pages are:

- [Statement Page](#)
- [Object Page](#)
- [Privilege Page](#)
- [FGA Page](#)
- [Capture Rule Page](#)

Once you have used those pages to create policies, you can provision, save, or export those policies.

The user name and password are for a user with rights to provision audit settings. This can be the SYSTEM user or a user with privileges equivalent to the SYSTEM user. If you do not have the rights to provision audit settings, you cannot provision settings to the source database automatically. However, you can export settings to a file and send the file to someone with sufficient privileges.

Before saving, ensure that the appropriate check boxes are selected. Click **Select All** to select all audit setting types, or select one or more already defined audit setting types to be applied to a source by clicking the appropriate check box in the **Select** column in the **Apply Audit Settings** section. Click **Select None** to deselect all selections to clear the check boxes.

Click **Save All Audit Settings** to save the policies in Oracle Audit Vault. You must save the policies in Oracle Audit Vault before you verify, export, or provision them. Once policies are saved, they will be available for provisioning or exporting when you log in again.

Once you have saved a category, you can click **Verify** to perform a verification of semantic correctness.

To provision a policy, select the category you want to provision, enter the user name and password, then click **Provision**.

Note: To provision audit settings to a source, you must have database administrator (DBA) privileges over the source. That is, you must use the SYSTEM user or a user with privileges equivalent to the SYSTEM user to provision audit settings.

Click **Export as SQL** to save to an external file.

You can replicate settings from another database. In the Apply Audit Settings section of the Overview page, select **Actual** or **Needed** to use settings that are in use or not yet applied, respectively. Enter text into the **From** field, or click the flashlight icon to make a selection, then click **Go**.

2.1.3 Defining a Statement Auditing Policy

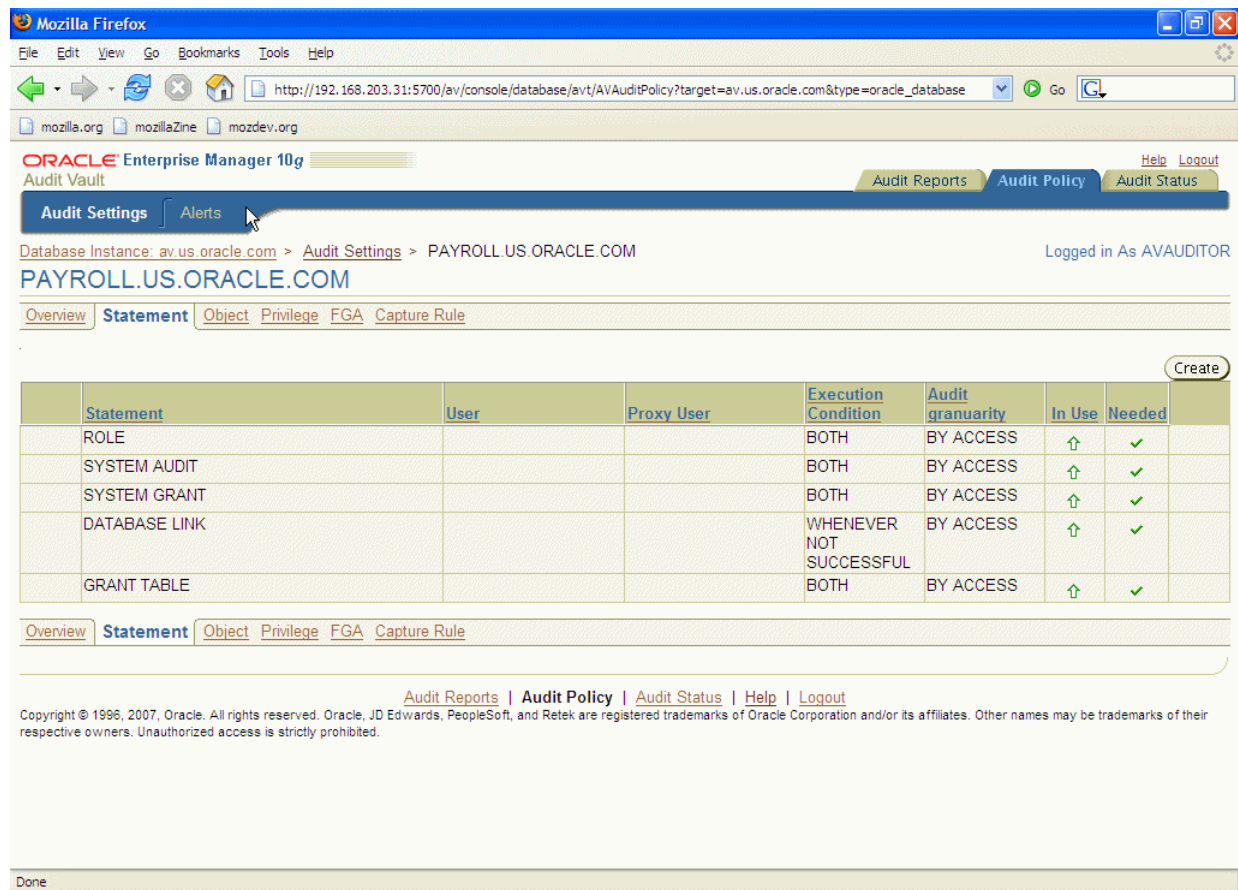
Statement Auditing is the selective auditing of related groups of statements regarding a particular type of database structure or schema object, but not a specifically named structure or schema object.

Statement auditing audits SQL statements by type of statement, not by the specific schema objects on which they operate. Statement auditing can be broad or focused, for example, by auditing the activities of all database users or of only a select list. Typically broad, statement auditing audits the use of several types of related actions for each option. These statements fall into 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.

2.1.3.1 Statement Page

You use the Statement page, shown in [Figure 2-2](#), to create a statement audit setting.

Figure 2–2 Statement Page

If statement audit settings have been created for this source, the page displays a list of existing audited statements. The list contains the fields shown in [Table 2–3](#).

Table 2–3 Statement Fields

Field	Description
(Left-most column)	An exclamation mark icon indicates one of the following conditions: <ul style="list-style-type: none"> The statement is needed but not in use. The statement is in use but not needed. The granularity needed is different from the granularity in use.
Statement	The statement to be audited
User	The user that this setting applies to
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 has been provisioned and downward if it has not been provisioned.

Table 2–3 (Cont.) Statement Fields

Field	Description
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 will point up after provisioning. If a policy that is in use is set to not needed, the row will vanish after provisioning.
(Right-most column)	Click the trash can icon to remove the policy.

Click **Create** to go to the [Create Statement Audit Page](#) and create an audited statement setting.

2.1.3.2 Create Statement Audit Page

To create an audited statement setting, provide data for the fields on the page. The fields are shown in [Table 2–4](#).

Table 2–4 Create Statement Audit Fields

Field	Description
Statement	The statements to be audited. Click the flashlight icon to use the Statements Audit Options page to select statements from a list. To filter the list, you can enter text in the Statements field and click Go . Select statements from the list, and click Select to return to the Create Statement Audit page.
Audited By	Select the appropriate option to indicate the users to be audited: All , User , or Proxy .
Users	The user that this setting applies to. You must set at least one user in this field or in the proxy user field. Click the flashlight icon to use the Search And Select: User page to select users from a list. To filter the list, you can enter text in the Audit Source or User field and click Go . Select users from the list, and click Select to return to the Create Statement Audit page.
Proxy User	The proxy user for the database. You must set at least one user in this field or in the User field. Click the flashlight icon to use the Search And Select: Proxy User and Client page to select proxy users from a list. The list will be populated if one or more proxy users is available. To filter the list, you can enter text in the Audit Source , Proxy , or Client Host field and click Go . Select proxy users from the list, and click Select to return to the Create Statement Audit page.
Statement Execution Condition	Choose WHENEVER SUCCESSFUL , WHENEVER NOT SUCCESSFUL , or BOTH as the execution condition to be audited.
DML Audit Granularity	Choose the level of granularity. You can audit BY ACCESS or BY SESSION .

Click **OK** to define this policy in Oracle Audit Vault or **Cancel** to return to the [Statement Page](#) without saving the policy.

2.1.4 Creating an Object Auditing Policy

Object Auditing is the auditing of specific statements on a particular schema object, such as **AUDIT SELECT ON** 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, schema object auditing can audit all SELECT and DML statements permitted by schema 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 provides the ability to audit the usage of powerful database commands that allow 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.

Schema object audit options are always set for all users of the database. These options cannot be set for a specific list of users.

2.1.4.1 Object Page

You use the Object page, shown in [Figure 2–3](#), to define an object auditing policy.

Figure 2–3 Object Page

Database Instance: [av.us.oracle.com](#) > [Audit Settings](#) > PAYROLL.US.ORACLE.COM

Logged in As AVAUDITOR

[Overview](#) [Statement](#) **[Object](#)** [Privilege](#) [FGA](#) [Capture Rule](#)

Statement	Schema	Object	Execution Condition	Audit granularity	In Use	Needed
GRANT	AUDUSR	EMP	BOTH	BY ACCESS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
AUDIT	HR	JOBS	BOTH	BY ACCESS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ALTER	SCOTT	EMP	BOTH	BY ACCESS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SELECT	AUDUSR	EMP	BOTH	BY ACCESS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Overview](#) [Statement](#) **[Object](#)** [Privilege](#) [FGA](#) [Capture Rule](#)

[Audit Reports](#) | **[Audit Policy](#)** | [Audit Status](#) | [Help](#) | [Logout](#)

Copyright © 1996, 2007, Oracle. All rights reserved. Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Unauthorized access is strictly prohibited.

If object audit settings have been created for a source, the page displays a list of existing settings. The list contains the fields shown in [Table 2–5](#).

Table 2–5 Object Fields

Field	Description
(Left-most column)	An exclamation mark icon indicates one of the following conditions: <ul style="list-style-type: none"> ■ The statement is needed but not in use. ■ The statement is in use but not needed. ■ The granularity needed is different from the granularity in use.
Statement	The statement to be 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 has been provisioned and downward if it has not been provisioned.
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 will point up after provisioning. If a policy that is in use is set to not needed, the row will vanish after provisioning.
(Right-most column)	Click the trash can icon to remove the policy.

Click **Create** to go to the [Create Object Audit Page](#) and create an object audit setting.

2.1.4.2 Create Object Audit Page

To create an audited object setting, provide data for the fields on the page. The fields are shown in [Table 2–6](#).

Table 2–6 Create Object Fields

Field	Description
Statements	The statements to be audited. Click the flashlight icon to use the Statements Audit Options page to select statements from a list. To filter the list, you can enter text in the Statements field and click Go . Select statements from the list, and click Select to return to the Create Object Audit page.
Object	The object that this setting applies to. Click the flashlight icon to use the Search And Select: Object page to select objects from a list. To filter the list, you can enter text in the Audit Source , Object Type , Object Owner , or Object field and click Go . Select objects from the list, and click Select to return to the Create Object Audit page.
Statement Execution Condition	Choose WHENEVER SUCCESSFUL, WHENEVER NOT SUCCESSFUL, or BOTH as the execution condition to be audited.
DML Audit Granularity	Choose the level of granularity. You can audit BY ACCESS or BY SESSION.

Select **Everyone**, **User**, or **Proxy** to indicate which users are to be audited.

Click **OK** to define this policy in Oracle Audit Vault or **Cancel** to return to the [Object Page](#) without saving the policy.

2.1.5 Defining a Privilege Auditing Policy

Privilege Auditing is the auditing of 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.

For example, when AUDIT SELECT ANY TABLE is in force, all statements issued by users with the SELECT ANY TABLE privilege are audited. This auditing capability is very important for the Sarbanes-Oxley (SOX) compliance requirements.

Sarbanes-Oxley and other compliance regulations that specifically 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 similar statement and privilege audit options are both set, 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 because each privilege auditing option audits only specific types of statements, not a related list of statements. It is more focused than statement auditing because it audits only the use of the target privilege. You can set privilege auditing to audit a selected user or every user in the database.

2.1.5.1 Privilege Page

You use the Privilege page to define a privilege auditing setting. The Privilege page is shown in [Figure 2-4](#).

Figure 2–4 Privilege Page

Oracle Enterprise Manager 10g
Audit Vault

Database Instance: av.us.oracle.com > Audit Settings > PAYROLL.US.ORACLE.COM

Logged in As AVAUDITOR

PAYROLL.US.ORACLE.COM

Overview Statement Object **Privilege** FGA Capture Rule

Create

Privilege	User	Proxy User	Execution Condition	Audit granularity	In Use	Needed
CREATE ANY TABLE			BOTH	BY ACCESS	↑	✓
DROP USER			BOTH	BY ACCESS	↑	✓
ALTER USER			BOTH	BY ACCESS	↑	✓
CREATE USER			BOTH	BY ACCESS	↑	✓
CREATE SESSION			BOTH	BY ACCESS	↑	✓
AUDIT SYSTEM			BOTH	BY ACCESS	↑	✓
ALTER SYSTEM			BOTH	BY ACCESS	↑	✓
CREATE EXTERNAL JOB			BOTH	BY ACCESS	↑	✓
CREATE ANY JOB			BOTH	BY ACCESS	↑	✓
GRANT ANY OBJECT PRIVILEGE			BOTH	BY ACCESS	↑	✓
EXEMPT ACCESS POLICY			BOTH	BY ACCESS	↑	✓
CREATE ANY LIBRARY			BOTH	BY ACCESS	↑	✓
GRANT ANY PRIVILEGE			BOTH	BY ACCESS	↑	✓
DROP PROFILE			BOTH	BY ACCESS	↑	✓
ALTER PROFILE			BOTH	BY ACCESS	↑	✓
DROP ANY PROCEDURE			BOTH	BY ACCESS	↑	✓
ALTER ANY PROCEDURE			BOTH	BY ACCESS	↑	✓
CREATE ANY PROCEDURE			BOTH	BY ACCESS	↑	✓
ALTER DATABASE			BOTH	BY ACCESS	↑	✓
GRANT ANY ROLE			BOTH	BY ACCESS	↑	✓
CREATE PUBLIC DATABASE LINK			BOTH	BY ACCESS	↑	✓
DROP ANY TABLE			BOTH	BY ACCESS	↑	✓
ALTER ANY TABLE			BOTH	BY ACCESS	↑	✓

Overview Statement Object **Privilege** FGA Capture Rule

[Audit Reports](#) | [Audit Policy](#) | [Audit Status](#) | [Help](#) | [Logout](#)

Copyright © 1996, 2007, Oracle. All rights reserved. Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Unauthorized access is strictly prohibited.

Done

If privilege audit settings have been created for this source, the page displays a list of existing settings. The list contains the fields shown in Table 2–7.

Table 2–7 Privilege Fields

Field	Description
(Left-most column)	An exclamation mark icon indicates one of the following conditions: <ul style="list-style-type: none"> ■ The statement is needed but not in use. ■ The statement is in use but not needed. ■ The granularity needed is different from the granularity in use.
Privilege	The privilege to be audited
User	The user that this setting applies to
Proxy User	The proxy user for the database, if any
Execution Condition	Choose WHENEVER SUCCESSFUL, WHENEVER NOT SUCCESSFUL, or BOTH as the execution condition to be audited.
Audit Granularity	Choose the level of granularity. You can audit BY ACCESS or BY SESSION.
In Use	The arrow points upward if the setting has been provisioned and downward if it has not been provisioned.
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 will point up after provisioning. If a policy that is in use is set to not needed, the row will vanish after provisioning.
(Right-most column)	Click the trash can icon to remove the policy.

Click **Create** to go to the [Create Privilege Audit Page](#) and create an audited privilege setting.

2.1.5.2 Create Privilege Audit Page

To create an audited privilege setting, provide data for the fields on the page. The fields are shown in [Table 2–8](#).

Table 2–8 Create Privilege Fields

Field	Description
Privilege	The privilege to be audited. Click the flashlight icon to use the Privileges Audit Options page to select statements from a list. To filter the list, you can enter text in the Privileges field and click Go . Select statements from the list, and click Select to return to the Create Privilege Audit page.
Audited By	Select the appropriate option to indicate the users to be audited: All , User , or Proxy .
Users	The user that this setting applies to. You must set at least one user in this field or in the proxy user field. Click the flashlight icon to use the Search And Select: User page to select users from a list. To filter the list, you can enter text in the Audit Source or User field and click Go . Select users from the list, and click Select to return to the Create Privilege Audit page.

Table 2–8 (Cont.) Create Privilege Fields

Field	Description
Proxy User	The proxy user for the database. You must set at least one user in this field or in the User field. Click the flashlight icon to use the Search And Select: Proxy User and Client page to select proxy users from a list. The list will be populated if one or more proxy users is available. To filter the list, you can enter text in the Audit Source, Proxy, or Client Host field and click Go . Select proxy users from the list, and click Select to return to the Create Privilege Audit page.
Statement Execution Condition	Choose WHENEVER SUCCESSFUL, WHENEVER NOT SUCCESSFUL, or BOTH as the execution condition to be audited.
DML Audit Granularity	Choose the level of granularity. You can audit BY ACCESS or BY SESSION.

Select **Everyone**, **User**, or **Proxy** to indicate which users are to be audited.

Click **OK** to define this policy in Oracle Audit Vault or **Cancel** to return to the [Privilege Page](#) without saving the policy.

2.1.6 Creating a Fine-Grained Auditing (FGA) Policy

Fine-grained auditing (FGA) enables you to create policies that define specific conditions that must take place for the audit to occur. Fine-grained auditing enables you to monitor data access based on content. It provides granular auditing of queries, as well as insert, update, and delete operations. For example, a central tax authority needs 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 SELECT privilege was used by a specific user on a particular table. Fine-grained auditing provides this deeper functionality.

In general, FGA policy is based on simple user-defined SQL predicates on table objects as conditions for selective auditing. During fetching, whenever policy conditions are met for a returning row, the query is audited. For example, you can use fine-grained auditing to audit the following types of actions:

- A table is accessed between 9 p.m. and 6 a.m. or on Saturday and Sunday
- An IP address from outside the corporate network is used
- A table column is selected or updated
- A value in a table column is used

FGA enables organizations to define audit policies, which specify the data access conditions that trigger the audit event, and to use an alert to notify administrators that the triggering event has occurred. Time and identity of the user accessing the data, information revealed, and modifications made are captured, creating meaningful audit trails supporting compliance requirements.

Oracle Database captures the exact SQL text of the statement that the user executed in audit tables. You can use FGA in conjunction with other database features such as Oracle Flashback Query to re-create the exact records returned to a user. This may be especially important to organizations that share sensitive information for which they require strict accountability. For example, many government law enforcement organizations at the international, federal, state and local levels share information among themselves. It is important that they audit access to sensitive information, such as informant and intelligence data, to know who accessed what exact data. For more

information about fine-grained auditing, please see *Oracle Database Advanced Security Administrator's Guide*.

FGA can serve as an early warning system of users misusing data access privileges, as well as an intrusion detection system for the database itself. FGA enables you to monitor data access based on content. A built-in audit mechanism in the database prevents users from bypassing the audit.

FGA allows audit policies to be associated with application tables. The policy determines when to generate an audit record. You can fine-tune the audit behavior by targeting a specific column, referred to as a *relevant column*, to be audited if a condition is met. The relevant-column capability enables you to focus on particularly important types of data to audit. For example, an audit record might be generated only when someone attempts to access sensitive account information after midnight, or attempts to access the investment account of a customer within a database at a financial investment firm or bank.

Other examples of relevant columns include privacy-related columns, such as those containing social security numbers, salaries, patient diagnoses, and so on. You could combine the fine-grained audit records to identify queries that address both name and social security number, a potential violation of privacy security laws. This combination of audit records could be useful in the retail industry.

A relevant-column audit helps reduce the instances of false or unnecessary audit records, because the audit must be triggered only when a particular column is referenced in the query. For example, an organization might want to audit executive salary access when only an employee name is accessed, because accessing salary information alone is not meaningful unless an HR clerk also selects the corresponding employee name.

If no relevant column is specified, then auditing applies to all columns, that is, auditing occurs whenever any specified statement type affects any column, independent of whether any rows are returned or not. For example, a large insurance company might allow HR clerks to access employee salary information, but audit access when salaries greater than \$500K are accessed. The audit policy ("where SALARY > 500000") is applied to the EMPLOYEES table through an audit policy interface (a PL/SQL package). Oracle Database 10g Release 2 extends 10g support for fine-grained auditing to INSERT, UPDATE and DELETE statements.

FGA can be used to reduce the amount of audit information generated and restrict auditing to especially sensitive information. It provides granular auditing of queries, as well as insert, update, and delete operations. For example, a health care organization or hospital must track access to patient records to guard against employee snooping or viewing high-profile patients, with enough detail to determine what data was accessed. It is not enough to know that SELECT privilege was used by a specific user on a particular table. Fine-grained auditing provides this deeper functionality. The Health Insurance Portability and Accountability Act (HIPAA) requires health care organizations to audit user activity relating to patient data.

The extensibility framework in FGA enables administrators optionally to define an appropriate audit event handler to process the event, for example, by sending e-mail to the administrator. The event handler provides organizations with flexibility in determining how to handle a triggering audit event. A triggering audit event could be written into a special audit table for further analysis, or could activate a pager for the security administrator. The event handler enables organizations to fine-tune their audit response to appropriate levels of escalation.

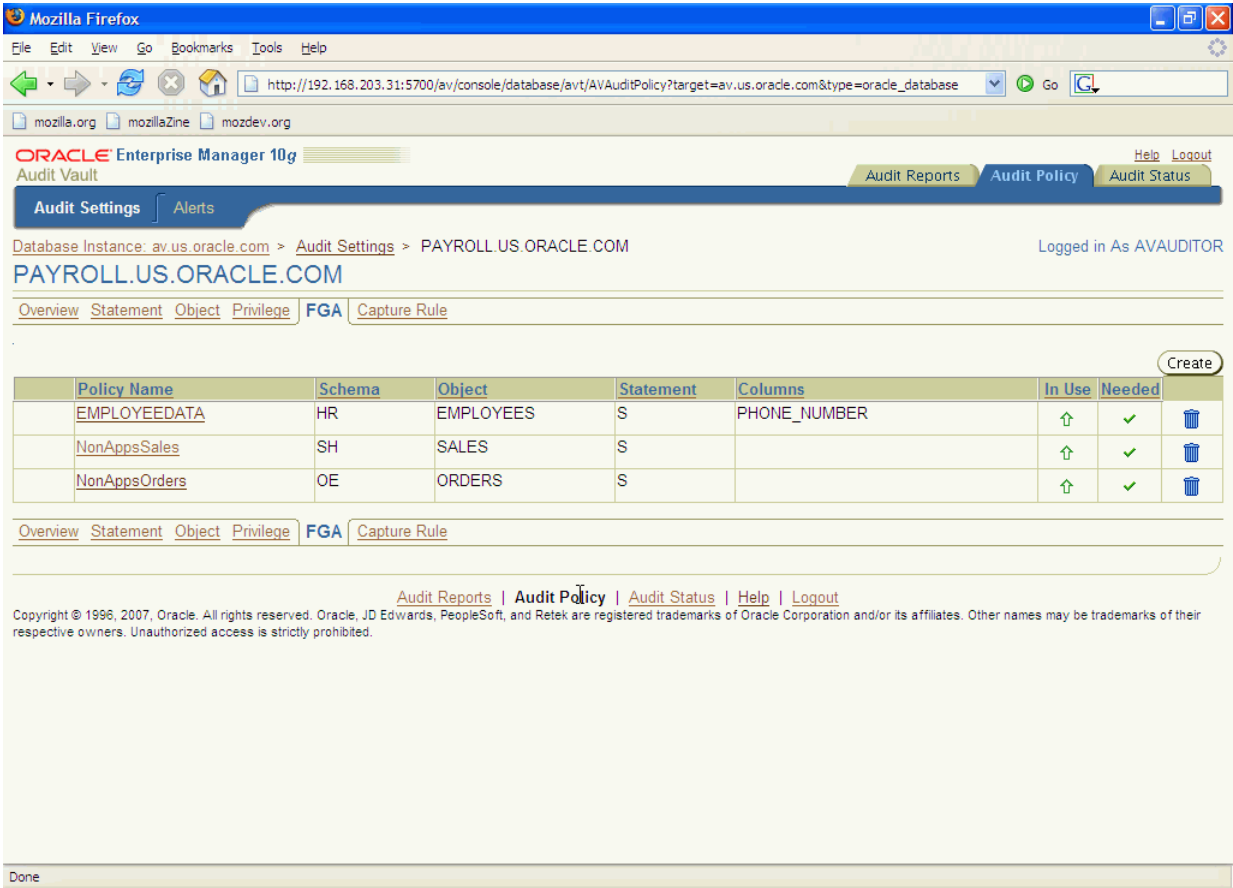
For additional flexibility in implementation, organizations can employ a user-defined function to determine the policy condition, and identify a relevant column for auditing

(audit column). For example, the function could allow unaudited access to any salary as long as the user is accessing data within the intranet, but audit access to executive-level salaries when they are accessed from the Internet.

2.1.6.1 FGA Page

You use the FGA page, shown in Figure 2–5, to define fine-grained audit settings.

Figure 2–5 Fine-Grained Auditing Page



If fine-grained audit settings have been created for a source, the page displays a list of existing settings. The list contains the fields shown in Table 2–9.

Table 2–9 Fine-Grained Audit Fields

Field	Description
(Left-most column)	An exclamation mark icon indicates one of the following conditions: <ul style="list-style-type: none">The statement is needed but not in use.The statement is in use but not needed.The granularity needed is different from the granularity in use.
Policy Name	The name of this fine-grained audit policy
Schema	The schema to which this policy applies
Object	The object to which this setting applies

Table 2–9 (Cont.) Fine-Grained Audit Fields

Field	Description
Statement	The statement to which this setting applies
Columns	The database columns being audited. If this field is empty, all columns are audited.
In Use	The arrow points upward if the setting has been provisioned and downward if it has not been provisioned.
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 will point up after provisioning. If a policy that is in use is set to not needed, the row will vanish after provisioning.
(Right-most column)	Click the trash can icon to remove the policy.

To view a fine-grained audit policy, click its name in the Policy Name column to go to the [Fine-Grained Audit Detail Page](#).

Click **Create** to go to the [Create FGA Page](#) and create an FGA setting.

Note: If you set up a fine-grained auditing policy, ensure that a database and collector are running against the source. Otherwise, you will not get audit records corresponding with this policy in Oracle Audit Vault.

2.1.6.2 Create FGA Page

To create a fine-grained audit setting, provide data for the fields on the page. The fields are listed in [Table 2–10](#).

Table 2–10 Create Fine-Grained Audit Fields

Field	Description
FGA Policy Name	Enter a name for this fine-grained audit policy.
Object	The object that this policy applies to. Click the flashlight icon to use the Search And Select: Object page to select objects from a list. To filter the list, you can enter text in the Audit Source , Object Type , Object Owner , or Object field and click Go . Select objects from the list, and click Select to return to the Create FGA page.
Statements	The type of statement that this policy applies to. Click the flashlight icon to use the Statement Type page to select statement types from the list. Click Select to return to the Create FGA page.
Columns	Enter the database columns to audit. If you enter more than one column, select All or Any as the condition that triggers this policy.
Condition	Enter the Boolean condition to be audited, for example: <code>< 1000</code> If this field is blank or Null, auditing occurs regardless of condition.

Table 2–10 (Cont.) Create Fine-Grained Audit Fields

Field	Description
Handler	The name of the event handler. For more information about fine-grained auditing handlers, see <i>Oracle Database Security Guide</i> .

Click **OK** to define this policy in Oracle Audit Vault or **Cancel** to return to the [FGA Page](#) without saving the policy. When you click **OK**, a View FGA Policy page is displayed. Click **Return** to return to the [FGA Page](#).

2.1.6.3 Fine-Grained Audit Detail Page

The Fine-Grained Audit Detail page lists the fields shown in [Table 2–11](#).

Table 2–11 Fine-Grained Audit Detail Fields

Field	Description
FGA Policy Name	The name for this fine-grained audit policy
Schema	The schema to which this policy applies
Object	The object to which this policy applies
Statements	The type of statements to which this policy applies
Columns	Whether all table columns are to be audited or the specified table columns are to be audited
Condition	The Boolean condition to be audited, for example, <1000. If Null, auditing occurs regardless of condition.
Handler Schema	The schema in which the handler event is stored
Handler package	The package containing the handler, for example: DBMS_FGA
Handler	The name of the event handler. For more information about fine-grained auditing handlers, see <i>Oracle Database Security Guide</i> .

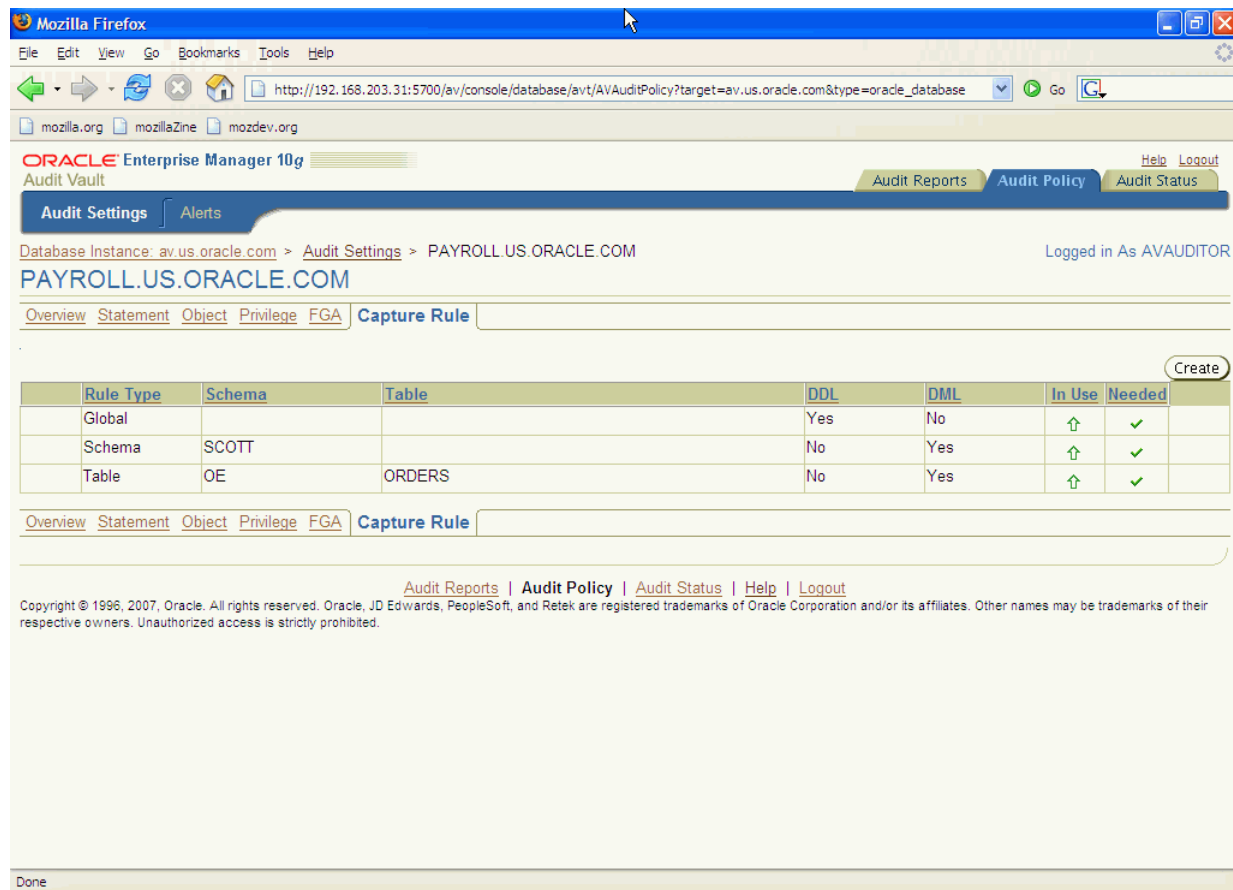
Click **Cancel** to return to the [FGA Page](#).

2.1.7 Creating a Capture Rule

Capture rules are used for Streams-based auditing. For information about Oracle Streams, see *Oracle Streams Concepts and Administration*.

2.1.7.1 Capture Rule Page

You use the Capture Rule page, shown in [Figure 2–6](#), to define capture rule settings.

Figure 2–6 Capture Rule Page

If capture rule audit settings have been created for a source, the page displays a list of existing settings. The list contains the fields shown in [Table 2–12](#).

Table 2–12 Capture Rule Fields

Field	Description
(Left-most column)	<p>An exclamation mark icon indicates one of the following conditions:</p> <ul style="list-style-type: none"> The statement is needed but not in use. The statement is in use but not needed. The granularity needed is different from the granularity in use.
Rule Type	The types are Global, Schema, or Table. Global capture rules are systemwide. Schema capture rules apply only to access of specific schema, and Table rules apply to access of specific tables in the schema.
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 DDL statements are audited.
DML	YES or NO indicates whether DML statements are audited.
In Use	The arrow points upward if the setting has been provisioned and downward if it has not been provisioned.

Table 2–12 (Cont.) Capture Rule Fields

Field	Description
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 will point up after provisioning. If a policy that is in use is set to not needed, the row will vanish after provisioning.
(Right-most column)	Click the trash can icon to remove the policy.

Click **Create** to go to the [Create Capture Rule Page](#) and create a capture rule audit setting.

Note: A REDO collector must be defined against this source. Otherwise, attempts to provision a capture rule will fail.

2.1.7.2 Create Capture Rule Page

To create a capture rule audit setting, provide data for the fields on the page. The fields are shown in [Table 2–13](#).

Table 2–13 Create Capture Rule Fields

Field	Description
Capture Rule Type	Select Global , Schema , or Table . Global capture rules are systemwide. Schema capture rules apply only to access of specific schema, and Table rules apply to access of specific tables in the schema.
Schema	For Schema rules, specify a schema name or click the flashlight icon to search for and select a schema name.
Table	For Table rules, specify a table name or click the flashlight icon to search for and select a table name.
Capture	Select DDL , DML , or Both .

Click **OK** to define this policy in Oracle Audit Vault or **Cancel** to return to the [Capture Rule Page](#) without saving the policy.

2.2 Configuring Alerts

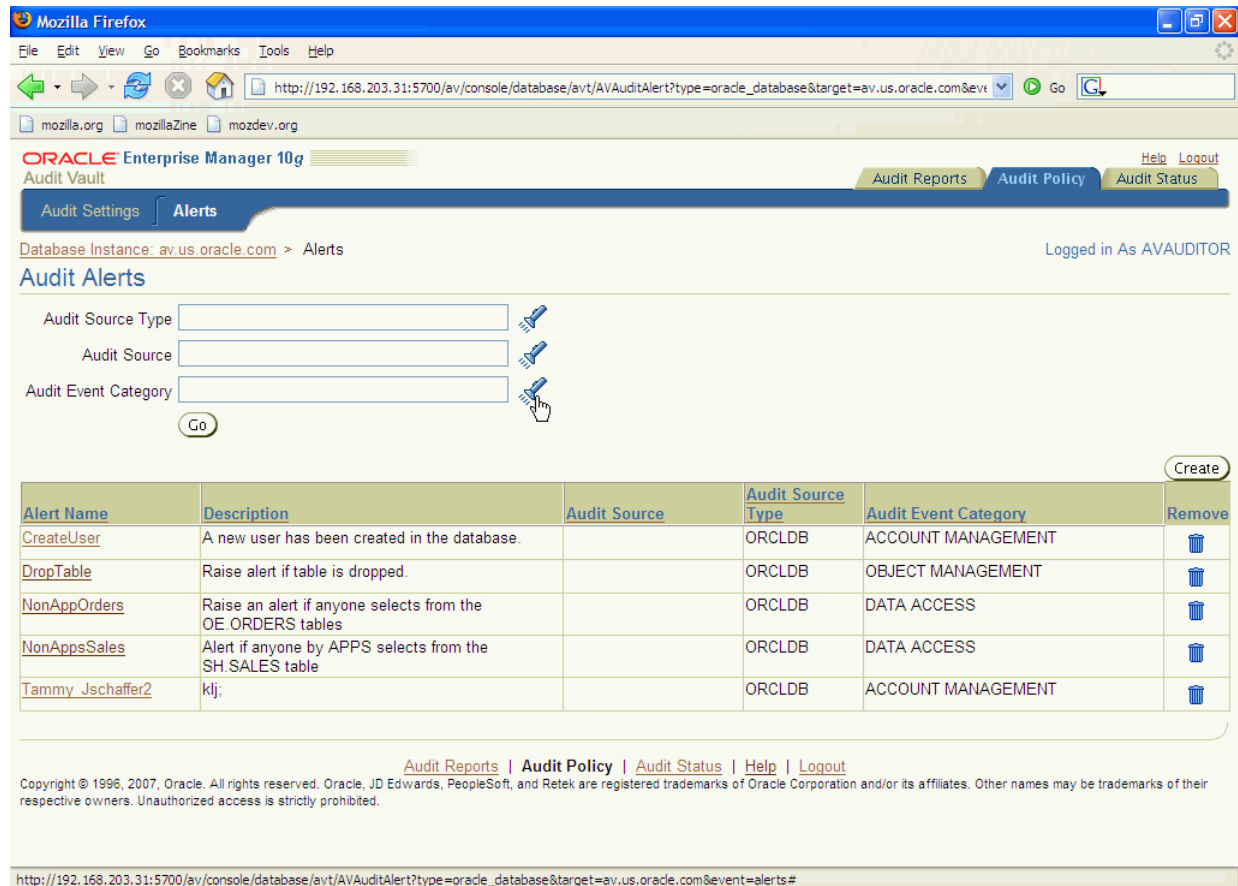
Oracle Audit Vault has the capability to raise alerts when the incoming audit data violates specific audit policies. The Oracle Audit Vault auditor can specify the conditions under which to raise these alerts on the Alerts page of the Audit Policy tab. When an incoming audit record meets the condition specified, an alert is raised and placed in the alert store, where the auditor can review it. The Oracle Audit Vault Dashboard is also updated to reflect the alert data. Also, the alert is placed in an output queue within the Audit Vault database. The Audit Vault administrator can install software that can read this queue and process the alert appropriately. Appropriate actions might include sending a page to a security officer or filing a trouble ticket within the appropriate tracking system.

It is important to understand that alerts are raised when the audit data reaches the 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. This frequency can be configured by the Audit Vault administrator.

To view or define alerts, you use the [Audit Alerts Page](#), shown in [Figure 2–7](#). To reach the Audit Alerts page from the dashboard, click the **Audit Policy** tab, then click **Alerts** on the upper left.

Figure 2–7 Audit Alerts Page



2.2.1 Creating an Alert

To add an alert, click **Create** on the [Audit Alerts Page](#). This takes you to the [Create Alert Rule Page](#). You define an audit rule by entering information on the [Create Alert Rule Page](#).

2.2.2 Audit Alerts Page

On the Audit Alerts page, you can:

- Specify or select filter criteria to show the audit alerts associated with a particular audit source type, audit source, or audit event category, or any combination of these three filter criteria.
- Click an alert name in the **Alert Name** column to view alert information for that alert.

You can specify the following filter criteria:

- **Audit Source Type** – Enter Audit Source Type criteria or click the flashlight icon for the Audit Source Type field. An audit source type defines the collection behavior of the audit sources classified for an audit source type.

At the **Search and Select: Audit Source Type** page, you can filter the list or search for a specific item by entering text in the text field for the **Audit Source** field, then click **Go** to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click **Select All** to select all items. You can also click **Select None** to deselect all selected items and begin again. After making your selections, click **Select** to populate the Audit Source Type field with your selected filter criteria, and return to the **Audit Alerts** page.

- **Audit Source** – Enter Audit Source criteria or click the flashlight icon for the **Audit Source** field. An audit source is where events are created.

At the **Search and Select: Audit Source** page, you can filter the list or search for a specific item by entering text in the text field for the **Audit Source** field, **Audit Source Host** field, and the **Audit Source Host IP** field, then click **Go** to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click **Select All** to select all items. You can also click **Select None** to deselect all selected items and begin again. After making your selections, click **Select** to populate the **Audit Source** field with your selected filter criteria, and return to the **Audit Alerts** page.

- **Audit Event Category** – Enter Audit Event Category criteria or click the flashlight icon for the **Audit Event Category** field.

At the **Search and Select: Audit Event Category** page, you can filter the list or search for a specific item by entering text in the text field for the **Audit Event Category** field, then click **Go** to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click **Select All** to select all items. You can also click **Select None** to deselect all selected items and begin again. After making your selections, click **Select** to populate the **Audit Event Category** field with your selected filter criteria, and return to the **Audit Alerts** page.

When you are satisfied with the selections in the **Audit Source Type**, **Audit Source**, or **Audit Event Category** field, click **Go**.

The **Alerts** report contains the column headings shown in [Table 2–14](#).

Table 2–14 Audit Alerts Fields

Field	Description
Alert Name	The name of the alert
Audit Source Type	The audit source type to which this alert applies
Audit Source	The audit source to which this alert is restricted
Audit Event Category	The audit category to which this alert is restricted
Status	When you create an alert, it is Active . If you remove it, it remains in the Audit Vault database, but is Inactive .
Remove	To make an Active alert Inactive, click the trash can icon in the row corresponding to that alert.

Click an alert name in the **Name** column to view the [Alerts Page](#), which contains alert information about that alert.

Click **Create** to go to the [Create Alert Rule Page](#) to create an alert rule.

Click **Next n** to view the next group of listed alerts returned or click **Previous** to view the previous group of listed alerts.

2.2.3 Alerts Page

The **Alerts** page contains the fields shown in [Table 2–15](#).

Table 2–15 Alerts Page Fields

Field	Description
Alert Name	The name of the alert
Description	A brief description of the alert
Audit Source	The audit source to which this alert is restricted
Audit Source Type	The audit source type to which this alert applies
Audit Event Category	The audit category to which this alert is restricted
Audit Severity	The severity level of the alert: CRITICAL or WARNING.
Condition	The condition when this alert rule should be evaluated. The alert condition must evaluate to a Boolean value and be based on either the event category format of the audit record or the source-type-specific event category format to which the audit record belongs.
Status	Whether the alert is ACTIVE or INACTIVE

Click **Return** to return to the [Audit Alerts Page](#).

2.2.4 Create Alert Rule Page

Use this page to add an alert that is to be raised when audit data violates specific audit policies.

Follow these steps to add an alert:

1. Enter the alert name and a brief description of the alert.
2. Specify the level of severity, source type, source, and event category for the alert.
3. Select **Basic** or **Advanced** to specify additional alert conditions in the [Basic Alert Condition](#) or [Advanced Alert Condition](#) sections and enter the additional alert conditions.
4. Click **OK** to save and add the alert to Oracle Audit Vault and return to the Audit Alerts page.

To begin to create an alert, enter or select information for the fields shown in [Table 2–16](#).

Table 2–16 Create Alert Rule Fields

Field	Description
Alert	Enter a name for the alert.
Description	Enter a brief description for the alert.
Alert Severity	Select a severity level for the alert: Critical or Warning .
Audit Source Type	Select an audit source type from the list.

Table 2–16 (Cont.) Create Alert Rule Fields

Field	Description
Audit Source	Select an audit source name from the list. If audit source information is specified, then audit source type information is not needed. However, when audit source information is specified, it is filtered by audit source type information if this information is specified.
Audit Event Category	Select the name of an audit event category from the list.

If both audit source and audit source type information are specified and they do not match, an error is raised and an error message is returned.

If audit source information is specified, the user and table fields are enabled and filtered by the audit source information.

The following combinations of audit source type and audit event category information are supported:

- If information for neither is specified
- If information for both is specified
- If only information for source type is specified

If audit event category information is specified, but audit source information is not specified, an error is raised and an error message is returned.

If information for the audit source type and audit event category are specified, then information for the audit event is enabled and filtered by both these fields.

2.2.4.1 Basic Alert Condition

Specify or select fields that describe when an alert should be raised. Alerts can be created on each field and certain combinations of fields. Specifying information for certain fields causes the information to be filtered as described in this section. Enter or select information for the fields shown in [Table 2–17](#).

Table 2–17 Basic Alert Condition Fields

Field	Description
User	Specify the name of a user or click the flashlight icon to search for and select a user name.
Table	Specify the name of a table or click the flashlight icon to search for and select a table name.
Audit Event	Select the name of an audit event from the list.
Audit Event Status	Select an option to represent whether the event has a status of Success , Failure , or Both .

2.2.4.2 Advanced Alert Condition

In the **Advanced Alert Condition** section, shown in [Figure 2–8](#), you can construct the Boolean condition for when this alert should be evaluated. When audit data violates the Boolean condition, it evaluates to a Boolean value that when true, triggers the alert to be raised and sent to an alert store and placed in an output queue.

Figure 2–8 Create Alert Rule Page, Advanced Alert Condition

Oracle Enterprise Manager 10g
Audit Vault

Audit Reports | Audit Policy | Audit Status

Audit Settings | Alerts

Database Instance: av.us.oracle.com

Logged in As AVAUDITOR

Create Alert Rule

Cancel OK

Please provide the data for all required fields

Alert: Alter_Jschafter

Description: Raise and alert if the database user JSCHAFFER is altered.

Alert Severity: Warning

Audit Source Type: ORCLDB

Audit Source:

Audit Event Category: ACCOUNT MANAGEMENT

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:

SOURCE_EVENTID=43 AND TARGET_OBJECT=JSCHAFFER

Select an event to insert it in the condition:

Select an attribute to insert it in the condition:

Cancel OK

[Audit Reports](#) | [Audit Policy](#) | [Audit Status](#) | [Help](#) | [Logout](#)

Copyright © 1996, 2007, Oracle. All rights reserved. Oracle, JD Edwards, PeopleSoft, and Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners. Unauthorized access is strictly prohibited.

Done

Enter a valid Boolean condition in the **Condition** field under which an alert should be raised. Construct the condition by choosing audit events and event attributes by double-clicking the specific audit event or event attribute desired. Complete the Boolean condition using valid expression syntax and valid values for the event attribute's data type.

Condition is the Boolean condition when this alert rule should be evaluated. The alert condition must evaluate to a Boolean value and be based on either the event category format of the audit record or the source-type-specific event category format to which the audit record belongs.

You can select audit events and event attributes from the menus at the bottom of the page to insert them into the condition field. When you select an audit event it is represented in the condition field by its Oracle Database source event ID. For example, for the account management event category, the audit event named CREATE USER is represented as `SOURCE_EVENTID= ' 51 '`. When you select an event attribute, the event attribute name appears in the Condition field.

You specify the alert condition as an expression containing audit events and event attributes from the incoming audit records. Which audit events and event attributes you can use in a condition depends on how you specify the record. All audit records contain a minimal set of event attributes that you can use. In addition, each type of auditable event adds event attributes specific to itself. The complete list of event attributes available to you is in [Appendix B, Section B.1](#). To use these additional event attributes, however, you must explicitly specify the type of auditable event in the Audit Event Category field.

For a failed logon event, for example, you would specify:

```
SOURCE_EVENTID = '100' AND EVENT_STATUS != 0
```

Oracle Databases use a numeric code to denote these events by their source event ID. You can restrict the alert to a specific type of event by using this field in your conditions. The complete list of Oracle Database events and source event IDs is in [Appendix B, Section B.2](#).

The other event attribute used in the preceding example is `EVENT_STATUS`. 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.

Click **OK** to create the alert rule and return to the [Alerts Page](#).

Oracle Audit Vault Reports

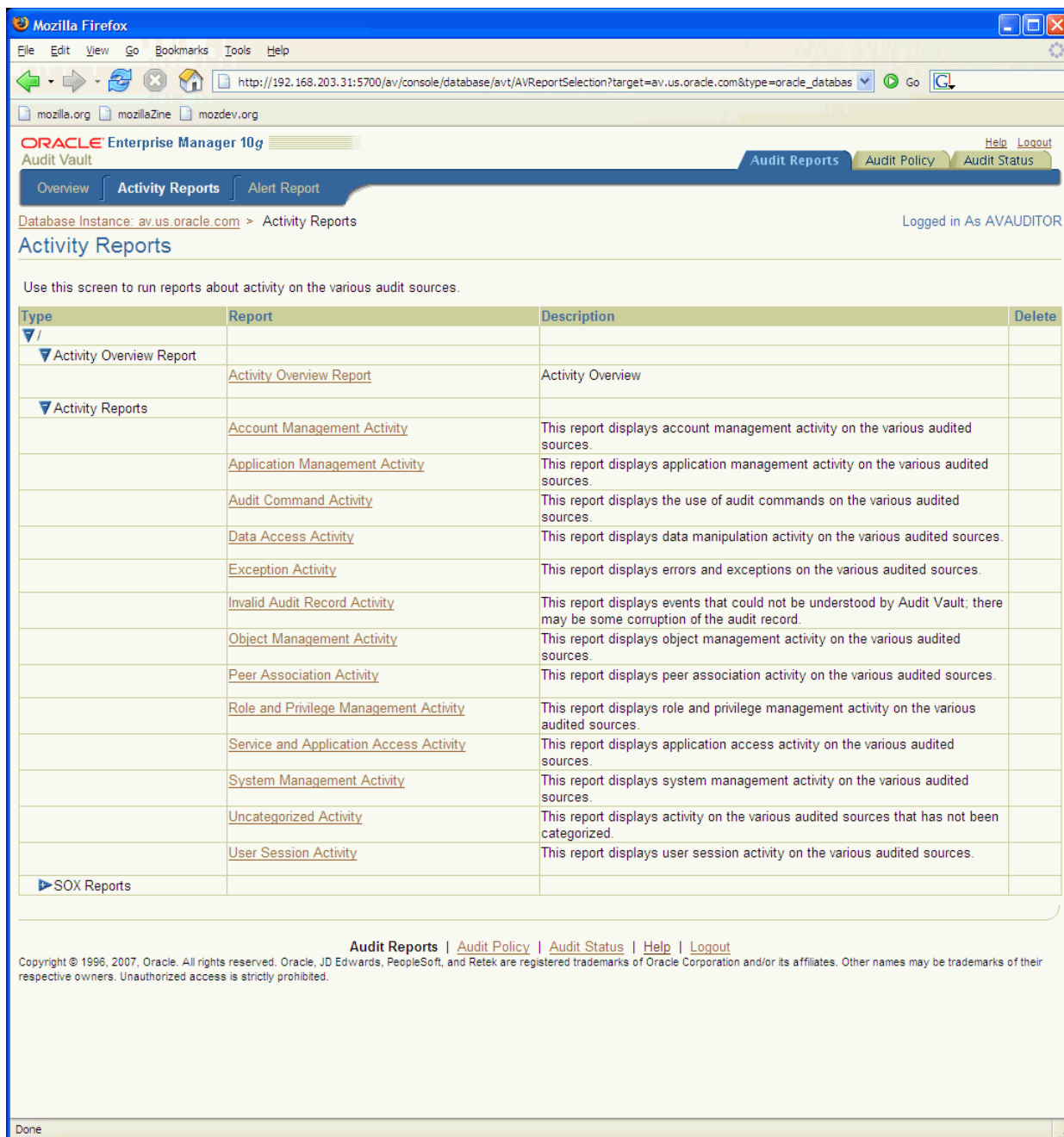
As auditor, you can generate reports of activity and alerts from systems monitored by Oracle Audit Vault. To do this, you start from the Audit Vault Dashboard, described in [Chapter 1](#).

This chapter includes the following sections:

- [Activity Reports](#)
- [Alert Reports](#)
- [Data Warehouse](#)

3.1 Activity Reports

From the Dashboard page, you click **Activity Reports** at the top of the page to go directly to the Activity Reports page, shown in [Figure 3-1](#).

Figure 3–1 Activity Reports Page

3.1.1 Activity Reports Page

In the Activity Reports page, you can:

- Click the plus sign (+) icon to expand or open the hierarchical view to show the **Activity Overview Report** link and the individual **Activity Reports** links.
- Click the **Activity Overview Report** link in the **Report** column to view the [Activity Overview Report](#) page.
- Click any audit event category **Activity Report** link in the **Report** column to view its report. A brief description of each type of audit event category activity report is provided in the **Description** column.

3.1.2 Activity Overview Report

The Activity Overview Report page displays all audit trail records created based on their audit event time. The data is sorted by time in descending order. Specify or select filter criteria to generate a report.

3.1.2.1 Report Fields and Filter Criteria on the Activity Overview Report Page

Table 3–1 describes how to use each of the report fields and the filter criteria.

Table 3–1 Report Fields and Filter Criteria on the Activity Overview Report Page

Field	Description
Audit Source	<p>Enter Audit Source criteria or click the search icon for the Audit Source field. An audit source is where events are created.</p> <p>At the Search and Select: Audit Source page, you can filter the list or search for a specific item by entering text in the text field for the Source field, Source Host field, and the Source Host IP field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Audit Source field with your selected filter criteria, and return to the Activity Overview Report page.</p>
User	<p>Enter User criteria or click the search icon for the User field. A user is someone associated with an event.</p> <p>At the Search and Select: User page, you can filter the list or search for a specific item by entering text in the text field for the User field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the User field with your selected filter criteria, and return to the Activity Overview Report page.</p>
Audit Event Category	<p>Enter Audit Event Category criteria or click the search icon for the Audit Event Category field.</p> <p>At the Search and Select: Audit Event Category page, you can filter the list or search for a specific item by entering text in the text field for the Audit Event Category field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Audit Event Category field with your selected filter criteria, and return to the Activity Overview Report page.</p>

Table 3–1 (Cont.) Report Fields and Filter Criteria on the Activity Overview Report Page

Field	Description
Audit Event	<p>Enter Audit Event criteria or click the search icon for the Event field. An audit event is the encapsulation into an audit record of some action in the audit data source.</p> <p>At the Search and Select: Audit Event page, you can filter the list or search for a specific item by entering text in the text field for the Audit Event field and the Audit Event Category field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Audit Event field with your selected filter criteria, and return to the Activity Overview Report page.</p>
Object	<p>Enter Object criteria or click the search icon for the Object field. An object is the entity on which an event is performed.</p> <p>At the Search and Select: Object page, you can filter the list or search for a specific item by entering text in the text field for the Owner field and the Object field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Object field with your selected filter criteria, and return to the Activity Overview Report page.</p>
Client Host	<p>Enter Client Host criteria or click the search icon for the Client Host field. A client host is the host system on which the event occurred.</p> <p>At the Search and Select: Client Host page, you can filter the list or search for a specific item by entering text in the text field for the Host field and the IP Address field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Client Host field with your selected filter criteria, and return to the Activity Overview Report page.</p>
Client Tool	<p>Enter Client Tool criteria or click the search icon for the Client Tool field. A client tool is the tool used on the client system to connect to the audit source associated with the event.</p> <p>At the Search and Select: Client Tool page, you can filter the list or search for a specific item by entering text in the text field for the Client Tool field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Client Tool field with your selected filter criteria, and return to the Activity Overview Report page.</p>

Table 3–1 (Cont.) Report Fields and Filter Criteria on the Activity Overview Report Page

Field	Description
Privilege	<p>Enter Privilege criteria or click the search icon for the Privilege field. A privilege represents the privileges used during the event.</p> <p>At the Search and Select: Privilege page, you can filter the list or search for a specific item by entering text in the text field for the Privilege field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Privilege field with your selected filter criteria, and return to the Activity Overview Report page.</p>
Audit Event Status	Select the Audit Event Status field to be Success , Failure , or Both by clicking the option preceding each field.
Audit Event Time	Select the Audit Event Time field as being either during the Last 24 hours , Last One Week , Last One Month , or by The Period by clicking the option preceding each field. If you select The Period , you must enter a From date and a To date.

3.1.2.2 Activity Overview Actions

When you have made your filter criteria selections, click **Go** to generate the report.

From the filtered report that appears, you can click the **Detail** icon in the **Detail** column for the desired row to see a detailed report for the audit record data representing that selected row.

Click **Next 25** to view the next 25 listed items returned or click **Previous** to view the previous 25 listed items.

Click **Save as CSV** to save the report as a comma-separated values (CSV) file format. The CSV file format is a delimited data format that has fields separated by the comma character and records separated by newlines.

Click **Save Definition** to go to the **Report Generation** page to create a report and save it as a report definition. At the **Report Generation** page, the **Audit Event Status** and **Audit Event Time** fields are populated with values specified from the event category report page from which the report save operation was initiated. Perform the following tasks:

1. Enter a name for the compliance category type to create a new compliance category type or click the flashlight icon to the right of the **Compliance Category** field to search for an existing name of a compliance category type. At the **Compliance Category Search** page, enter the name of the compliance category to search for, then click **Go**. Click the respective check box in the **Select** column, then click **Select** to select the compliance category of interest that is listed in the **Compliance Category** column.
2. Enter a description in the **Compliance Category Description** field.
3. Enter a report title in the **Report Title** field.
4. Enter a short report description in the **Short Report Description** field.
5. Enter a more detailed report description in the **Detail Report Description** field.
6. Check all entries, then click **Create Report** to create the report.

After creating the event category report, you are returned to the event category page from which you started. To view the complete list of event report types, including any newly created event report types, click the **Activity Reports** tab to go to the **Activity Reports** page. All created event report types are listed in the **Type** column on the **Activity Reports** page. Click the plus sign (+) icon for any event report type to expand its view of activity reports. See [Section 3.1.5](#) for more information about creating customized reports and for examples of how to do this.

3.1.3 Common Features of Audit Event Activity Pages

The audit trail records are categorized based on the type of record generated. Each of the reports can be filtered by various fields based on the type of category. This section describes features common to all audit event activity reports.

3.1.3.1 Report Fields and Filter Criteria on Audit Event Activity Report Pages

[Table 3–2](#) describes how to use each of the report fields and filter criteria for all categories of audit event.

Table 3–2 Report Fields and Filter Criteria on Audit Event Activity Report Pages

Field or Filter	Description and Actions
Audit Source	<p>Enter Audit Source criteria or click the search icon for the Audit Source field. A source is where events are created.</p> <p>At the Search and Select: Source page, you can filter the list or search for a specific item by entering text in the text field for the Audit Source field, Audit Source Host field, and the Audit Source Host IP field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Audit Source field with your selected filter criteria, and return to the individual activity report page.</p>
User	<p>Enter User criteria or click the search icon for the User field. A user is someone associated with an event.</p> <p>At the Search and Select: User page, you can filter the list or search for a specific item by entering text in the text field for the User field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the User field with your selected filter criteria, and return to the individual activity report page.</p>
Audit Event	<p>Enter Audit Event criteria or click the search icon for the Audit Event field.</p> <p>At the Search and Select: Event page, you can filter the list or search for a specific item by entering text in the text field for the Audit Event field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Audit Event field with your selected filter criteria, and return to the individual activity report page.</p>

Table 3–2 (Cont.) Report Fields and Filter Criteria on Audit Event Activity Report Pages

Field or Filter	Description and Actions
Object	<p>Enter Object criteria or click the search icon for the Object field. An object is the entity on which an event is performed.</p> <p>At the Search and Select: Object page, you can filter the list or search for a specific item by entering text in the text field for the Owner field and the Object field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Object field with your selected filter criteria, and return to the individual activity report page.</p>
Client Host	<p>Enter client host criteria or click the search icon for the Client Host field. A Client Host is the host system on which the event occurred.</p> <p>At the Search and Select: Client Host page, you can filter the list or search for a specific item by entering text in the text field for the Host field and the IP Address field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Client Host field with your selected filter criteria, and return to the individual activity report page.</p>
Client Tool	<p>Enter Client Tool criteria or click the search icon for the Client Tool field. A client tool is the tool used on the client system to connect to the audit source associated with the event.</p> <p>At the Search and Select: Client Tool page, you can filter the list or search for a specific item by entering text in the text field for the Client Tool field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Client Tool field with your selected filter criteria, and return to the individual activity report page.</p>
Privilege	<p>Enter Privilege criteria or click the search icon for the Privilege field. A privilege represents the privileges used during the event.</p> <p>At the Search and Select: Privilege page, you can filter the list or search for a specific item by entering text in the text field for the Privilege field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Privilege field with your selected filter criteria, and return to the Role and Privilege individual activity report page.</p>
Audit Event Status	Select the Audit Event Status field to be Success , Failure , or Both by clicking the option preceding each field.
Audit Event Time	Select the Audit Event Time field as being either during the Last 24 hours , Last One Week , Last One Month , or by The Period by clicking the option preceding each field. If you select The Period , you must enter a From date and a To date.

3.1.3.2 Other Actions to Perform in Audit Event Activity Pages

When you have made your filter criteria selections, click **Go** to generate the report.

Click **Next 25** to view the next 25 listed items returned or click **Previous** to view the previous 25 listed items.

Click **Save as CSV** to save the report as a comma-separated values (CSV) file format. The CSV file format is a delimited data format that has fields separated by the comma character and records separated by newlines.

You can click the **Detail** icon in the **Detail** column for the desired row to see a [Detail Report](#) for the audit record data representing that selected row.

3.1.3.3 Detail Report

From any of the audit record event reports, you can click the **Detail** icon in the **Detail** column for the desired row to see a Detail report for the audit record data representing that selected row.

3.1.3.3.1 Detail Report Fields [Table 3–3](#) provides a brief description of each of the Detail report fields.

Table 3–3 Fields on the Detail Report Page

Field	Description
Source Type	Name of the source type
Source	Name of the source
Source Host	Name of the host on which source resides
Source Version	Product version of the source
Source Host IP	Host IP address on which the source resides
Event	Event name
Event Category	Event category name to which the event belongs
Event Status	Status of the event
Event Time	Time the event occurred
Collection Time	Time the collection of events was made
Object	Name of the object
Owner	Owner of the object
Associated Object	Name of the associated object
Associated Object Owner	Name of the associated object owner
New Object	Name of the renamed object
New Object Owner	Name of the renamed object owner
User GUID	User's globally unique identifier of Oracle Internet Directory user (for EUS)
User	Name of the user
OS User	Operating system user name
End User	Name of the end user
Terminal	Name of the host terminal
Host	Name of the host system

Table 3–3 (Cont.) Fields on the Detail Report Page

Field	Description
Host IP	IP address of the host system
Subnet	Subnet address of the host system
Domain	Domain name of the host system
SCN	System change number
FGA Policy	Fine-grained audit trail policy name
Authentication Method	Name of the authentication method used
Client Tool	Name of the tool used on the client
Client Application Method	Method name of the client application
Privilege	Name of the privilege used
Object Privilege	Name of the privilege used on the object
System Privilege	Name of the system privilege used
Grantee User	Name of the user granted the privilege
Statement ID	Identifier of the SQL statement
Object ID	Identifier of the object
Thread ID	Server-side identifier of the thread
Process ID	Server-side identifier of the process
Instance Number	Number of the instance
Audit Option	Audit option used
Admin Option	Administrative option used
Proxy Session ID	Proxy user's session identifier
Session CPU	Number of the session CPU
Session Actions	The success or failure of operations in a session
Row ID	Identifier of the row
Context	Unique identifier for the context
Sub Context	Transaction ID for Oracle Database
Parent Context	Execution context ID for Oracle Database
Transaction	Transaction type
SQL Bind	Bind variables of the SQL statement
SQL Text	SQL text of the query
Undo SQL text	Text of the SQL statement to undo the transaction
Comment Text	Text comment on the audit trail entry.
Logoff Dlock	Deadlocks detected during the session
Logoff Lread	Logical reads for the session
Logoff Lwrite	Logical writes for the session
Logoff Pread	Physical reads for the session

3.1.3.3.2 Actions The system change number (SCN) is useful if the value has been changed more than once.

Use your browser's **Back** button to return to the [Detail Report](#).

When you finish viewing the Detail Report, click **Return** to return to the previous event category page.

3.1.4 Activity Reports

This section describes the report fields and filter criteria found in each type of audit event activity report.

This section includes the following topics:

- [Account Management Activity](#)
- [Application Management Activity](#)
- [Audit Command Activity](#)
- [Data Access Activity](#)
- [Exception Activity](#)
- [Invalid Audit Record Activity](#)
- [Object Management Activity](#)
- [Peer Association Activity](#)
- [Role and Privilege Management Activity](#)
- [Service and Application Access Activity](#)
- [System Management Activity](#)
- [Uncategorized Activity](#)
- [User Session Activity](#)

3.1.4.1 Account Management Activity

The Account Management Activity report displays audit records in which account management operations such as alter profile, alter user, or drop are performed. You can sort the report data by clicking on the desired header.

The Account Management Activity report contains the following report fields and filter criteria:

- [Audit Source](#)
- [User](#)
- Account Management [Audit Event](#)
- [Object](#)
- [Audit Event Status](#)
- [Audit Event Time](#)

3.1.4.2 Application Management Activity

The Application Management Activity report displays audit records in which application management operations such as alter function, alter Java, or alter package are performed. You can sort the report data by clicking on the desired header.

The Application Management Activity report contains the following report fields and filter criteria:

- [Audit Source](#)
- [User](#)
- Application Management [Audit Event](#)
- [Object](#)
- [Audit Event Status](#)
- [Audit Event Time](#)

3.1.4.3 Audit Command Activity

The Audit Command Activity report displays audit records in which operations such as audit default, audit object, or noaudit default are performed. You can sort the report data by clicking on the desired header.

The Audit Command Activity report contains the following report fields and filter criteria:

- [Audit Source](#)
- [User](#)
- [Audit Event](#)
- [Object](#)
- [Audit Event Status](#)
- [Audit Event Time](#)

3.1.4.4 Data Access Activity

The Data Access Activity report displays audit records in which data manipulation operations such as delete, insert, or select are performed. You can sort the report data by clicking on the desired header.

The Data Access Activity report contains the following report fields and filter criteria:

- [Audit Source](#)
- [User](#)
- Data Access [Audit Event](#)
- [Object](#)
- [Client Host](#)
- [Client Tool](#)
- [Audit Event Status](#)
- [Audit Event Time](#)

From the Detail report for Data Access Activity, you can click **Data Trace** to view a Data Trace report, which shows each value that has been changed by an UPDATE statement. The Data Trace report lists the column name, old value, and new value with the corresponding information:

- SCN information
- SQL Text information
- SQL Bind information
- Object information

3.1.4.5 Exception Activity

The Exception Activity report displays audit records in which errors and exceptions such as network errors have occurred. You can sort the report data by clicking on the desired header.

The Exception Activity report contains the following report fields and filter criteria:

- [Audit Source](#)
- [User](#)
- Exception [Audit Event](#)
- [Object](#)
- [Client Host](#)
- [Client Tool](#)
- [Audit Event Status](#)
- [Audit Event Time](#)

3.1.4.6 Invalid Audit Record Activity

The Invalid Audit Record Activity report displays audit records for events that could not be understood by Oracle Audit Vault. You can sort the report data by clicking on the desired header.

The Invalid Audit Record Activity report contains the following report fields and filter criteria:

- [Audit Source](#)
- [User](#)
- [Audit Event](#)
- [Object](#)
- [Audit Event Status](#)
- [Audit Event Time](#)

3.1.4.7 Object Management Activity

The Object Management Activity report displays audit records in which operations such as alter dimension, alter index, or alter materialized view are performed. You can sort the report data by clicking on the desired header.

The Object Management Activity report contains the following report fields and filter criteria:

- [Audit Source](#)
- [User](#)
- Object Management [Audit Event](#)
- [Object](#)
- [Audit Event Status](#)
- [Audit Event Time](#)

3.1.4.8 Peer Association Activity

The Peer Association Activity report displays audit records in which operations such as create database link or drop database link are performed. You can sort the report data by clicking on the desired header.

The Peer Association Activity report contains the following report fields and filter criteria:

- [Audit Source](#)
- [User](#)
- Peer Association [Audit Event](#)
- [Object](#)
- [Audit Event Status](#)
- [Audit Event Time](#)

3.1.4.9 Role and Privilege Management Activity

The Role and Privilege Management Activity report displays audit records in which operations such as create role, drop role, or grant object are performed. You can sort the report data by clicking on the desired header.

The Role and Privilege Management Activity report contains the following report fields and filter criteria:

- [Audit Source](#)
- [User](#)
- Role and Privilege [Audit Event](#)
- [Object](#)
- [Privilege](#)
- [Audit Event Status](#)
- [Audit Event Time](#)

3.1.4.10 Service and Application Access Activity

The Service and Application Access Activity report displays audit records in which operations such as call method, execute procedure, or PL/SQL execute are performed. You can sort the report data by clicking on the desired header.

The Service and Application Access Activity report contains the following report fields and filter criteria:

- [Audit Source](#)
- [User](#)
- Service and Application Access [Audit Event](#)
- [Object](#)
- [Audit Event Status](#)
- [Audit Event Time](#)

3.1.4.11 System Management Activity

The System Management Activity report displays audit records in which operations such as alter system, alter tablespace, or analyze cluster are performed. You can sort the report data by clicking on the desired header.

The System Management Activity report contains the following report fields and filter criteria:

- [Audit Source](#)
- [User](#)
- System Management [Audit Event](#)
- [Audit Event Status](#)
- [Audit Event Time](#)

3.1.4.12 Uncategorized Activity

The Uncategorized Activity report displays audit records in which uncategorized operations such as comment, create summary, or no-op are performed. You can sort the report data by clicking on the desired header.

The Uncategorized Activity report contains the following report fields and filter criteria:

- [Audit Source](#)
- [User](#)
- Uncategorized [Audit Event](#)
- [Object](#)
- [Client Host](#)
- [Client Tool](#)
- [Audit Event Status](#)
- [Audit Event Time](#)

3.1.4.13 User Session Activity

The User Session Activity report displays audit records in which operations such as alter session, commit, or create restore point are performed. You can sort the report data by clicking on the desired header.

The User Session Activity report contains the following report fields and filter criteria:

- [Audit Source](#)
- [User](#)
- User Session [Audit Event](#)
- [Object](#)
- [Client Host](#)
- [Client Tool](#)
- [Audit Event Status](#)
- [Audit Event Time](#)

3.1.5 Creating Customized Reports

A very useful feature of Audit Vault Reports is the ability to create customized reports from any of the audit event activity pages. By selectively filtering for information in the category activity page, reports can be generated that show very specific audit records. By selecting or defining compliance categories the generated customized reports can be organized under compliance categories that you define.

To create a customized report from any of the audit event activity pages, selectively filter for information in each category field, then click **Go** to run the query that is the basis of your report. If the query results are as you wish, then click **Save Definition** to go to the **Report Generation** page to create a report and save it as a report definition. At the **Report Generation** page, the **Audit Event Status** and **Audit Event Time** fields are populated with values specified from the event category report page from which the report save operation was initiated. Perform the following tasks:

1. Enter a name for the compliance category type to create a new compliance category type or click the flashlight icon to the right of the **Compliance Category** field to search for an existing name of a compliance category type. At the **Compliance Category Search** page, enter the name of the compliance category to search for, then click **Go**. Click the respective check box in the **Select** column, then click **Select** to select the compliance category of interest that is listed in the **Compliance Category** column.
2. Enter a description in the **Compliance Category Description** field.
3. Enter a report title in the **Report Title** field.
4. Enter a short report description in the **Short Report Description** field.
5. Enter a more detailed report description in the **Detail Report Description** field.
6. Check all entries, then click **Create Report** to create the report.

After creating the event category report, you are returned to the event category page from which you started. To view the complete list of event report types, including any newly created event report types, click the **Activity Report** tab to go to the **Activity Report** page. All created event report types are listed in the **Types** column on the **Activity Report** page. Click the plus sign (+) icon for any event report type to expand its view of reports.

As an example of creating a customized report, suppose as part of your auditing policy you created a policy to audit the failure creation of users. So each time a user who does not have privileges tries to create another user, an audit record is created. See [Section 2.1](#) for more information about how to create an audit policy. From such a policy, you can create two customized reports, one for account management and the other for user session activity that will contain only these audit records for a detailed analysis. Both reports will be specific to the same source database.

To create each report, follow these steps:

1. On the **Overview** page, for the **Activity by Audit Event Category** graph, click the link for the Account Management audit event category to display the Account Management Activity page as shown in [Figure 3-2](#).

Figure 3–2 Creating Customized Reports Showing the Pre-Query State

Oracle Enterprise Manager 10g
Audit Vault

Overview | **Activity Reports** | Alert Report

Database Instance: av.us.oracle.com > Account Management Activity Logged in As AVAUDITOR

Account Management Activity

This report displays account management activity on the various audited sources.

Audit Source

User

Account Management Audit Event

Object

Audit Event Status ☐ Success ☐ Failure ☒ Both

Audit Event Time ☐ Last 24 Hours ☐ Last One Week ☒ Last One Month

☐ The Period From : on Jun 24, 2007 To : on Jul 24, 2007

Audit Source	User	Audit Event	Object	End User	OS User	Audit Event Status	Time	Detail
RODSRC1.US.ORACLE.COM	USER20	CREATE USER	USER40		rhward	1031	Jul 13, 2007 5:51:06 PM UTC	
RODSRC1.US.ORACLE.COM	USER20	CREATE USER	USER30		rhward	1031	Jul 13, 2007 5:50:39 PM UTC	
RODSRC1.US.ORACLE.COM	USER5	CREATE USER	USER6		rhward	1031	Jul 13, 2007 4:20:53 PM UTC	
RODSRC1.US.ORACLE.COM	TEST4	DROP USER	TEST4		rhward	1031	Jul 11, 2007 6:49:03 PM UTC	

- On the **Account Management Activity** page, select the flashlight for each respective field: Audit Source, User, Account Management Audit Event, and Object to make selections and filter for specific information. Select the source, then the users, then the account management audit events. Select **Both** for Audit Event Status field. Then select the desired time interval for the report by making a selection in the Audit Event Time field.
- Click **Go** to run the query based on the values selected for the fields to filter the report information as shown in Figure 3–3.

Figure 3–3 Creating Customized Reports Showing the Results of the Query

The screenshot shows the Oracle Enterprise Manager 10g Audit Vault interface. The browser address bar displays the URL: `http://stacd05.us.oracle.com:5700/av/console/database/avt/AVAssessment?target=av.us.oracle.com&type=oracle_database&assessmentType=account`. The page title is "Account Management Activity". The user is logged in as "AVAUDITOR".

The configuration section includes the following fields and options:

- Audit Source:** RODSRC1.US.ORACLE.COM
- User:** (empty)
- Account Management Audit Event:** CREATE USER
- Object:** (empty)
- Audit Event Status:** ☐ Success ☐ Failure ☒ Both
- Audit Event Time:** ☐ Last 24 Hours ☐ Last One Week ☒ Last One Month
- The Period:** From 0 : 0 on Jun 24, 2007 To 0 : 0 on Jul 24, 2007

Buttons for "Save as CSV" and "Save Definition" are present. A "Go" button is also visible.

Audit Source	User	Audit Event	Object	End User	OS User	Audit Event Status	Time	Detail
RODSRC1.US.ORACLE.COM	USER20	CREATE USER	USER40		rhward	1031	Jul 13, 2007 5:51:06 PM UTC	
RODSRC1.US.ORACLE.COM	USER20	CREATE USER	USER30		rhward	1031	Jul 13, 2007 5:50:39 PM UTC	
RODSRC1.US.ORACLE.COM	USER5	CREATE USER	USER6		rhward	1031	Jul 13, 2007 4:20:53 PM UTC	

Buttons for "Save as CSV" and "Save Definition" are present at the bottom of the table.

- Click **Save Definition** to display the **Report Generation** page. Fill in information for each of the required fields. Select or define a compliance category to organize this report. Either select the compliance report name by clicking its flashlight for the **Compliance Category** field or enter the name of the compliance category name. Next enter information for the **Compliance Category Description**, **Report Title**, **Short Report Description**, and **Detail Report Description** fields as shown in Figure 3–4. Click **Create Report** to create your customized report and return to the **Account Management Activity** page. A success message should display indicating the report was generated.

Figure 3–4 Creating Customized Reports Generating the Account Management Report

Oracle Enterprise Manager 10g
Audit Vault

Database Instance: av.us.oracle.com

Report Generation

Audit Source: RODSRC1.US.ORACLE.COM

Audit Event Category: ACCOUNT MANAGEMENT

Audit Event: CREATE USER

Audit Event Status: Both

Audit Event Time: Last One Month

From: Jun 24, 2007 12:00 AM

To: Jul 24, 2007 12:00 AM

Compliance Category: Auditing User Creation Failures

Compliance Category Description: Auditing user creation failures

Report Title: My Customized Report: User Creation Failures

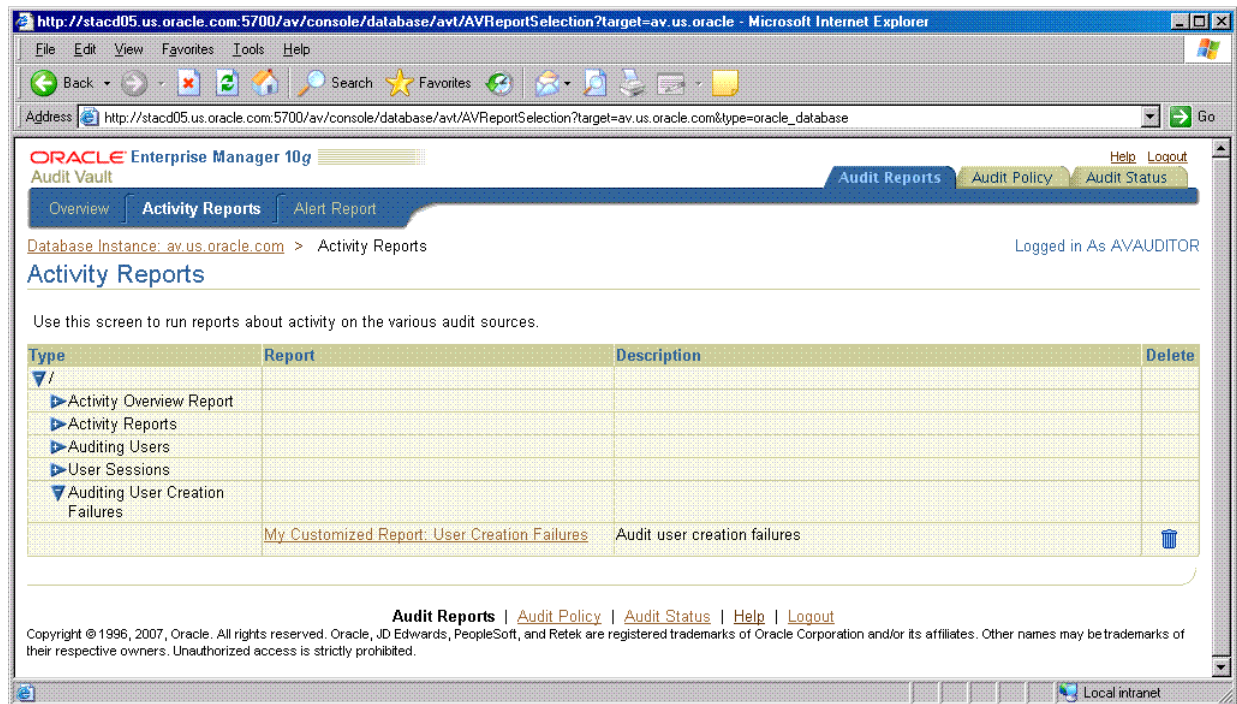
Short Report Description: Audit user creation failures

Detail Report Description: Auditing user creation failures

Create Report

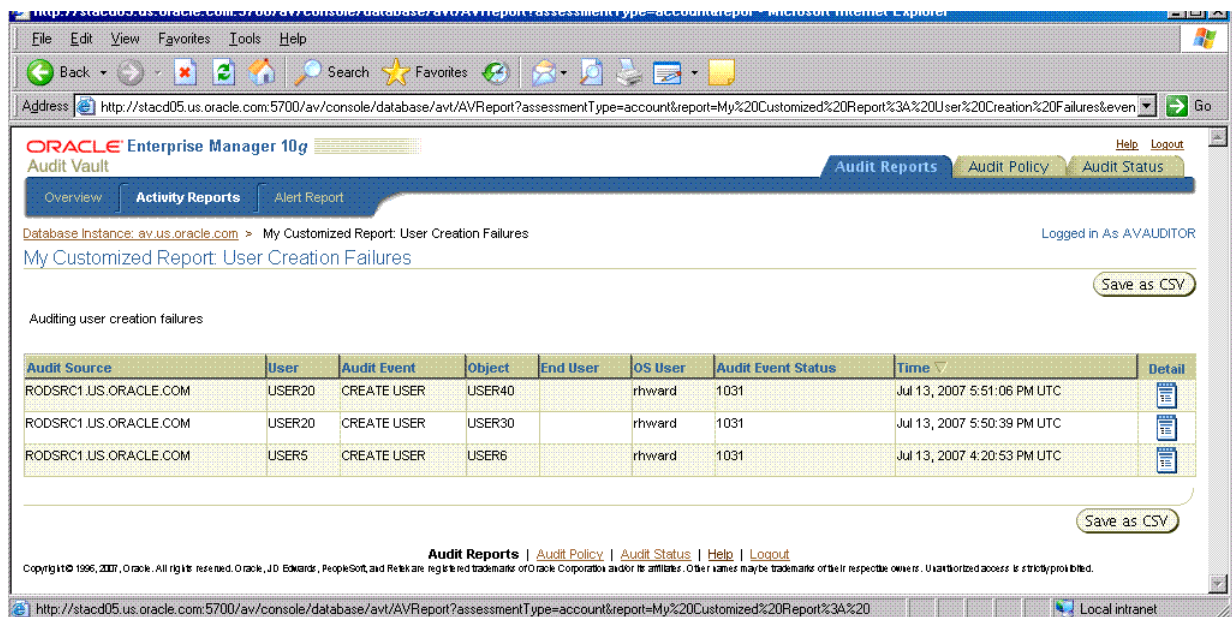
- To view the customized account management report, click the **Activity Reports** subtab to display the **Activity Reports** page. Click the plus sign (+) to open the name of the compliance category in which the report was created. In this example, the compliance category is named, "Auditing User Creation Failures". The report description is "Audit user creation failures" as shown in [Figure 3–5](#), which is the name given in Step 4 and shown in [Figure 3–4](#).

Figure 3–5 Activity Reports



- Click the report name "My Customized Report: User Creation Failures" to display your customized report as shown in Figure 3–6.

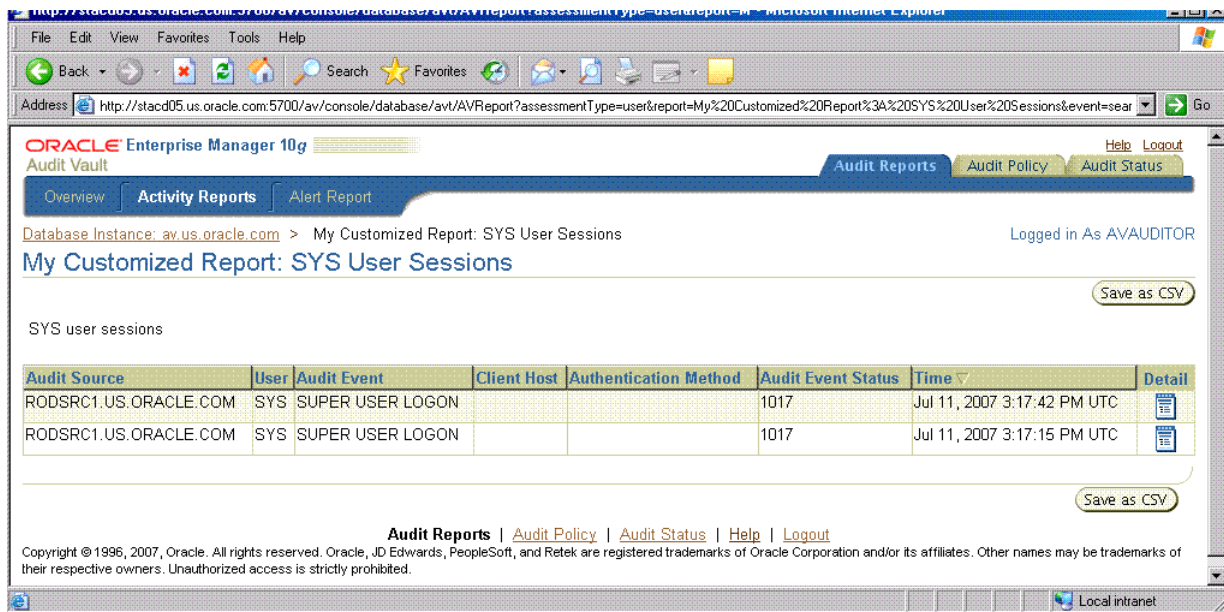
Figure 3–6 My Customized Account Management Report: User Creation Failures



Note that in Figure 3–4, this report was given a title of "My Customized Report: User Creation Failures" and a detail report description of "Auditing user creation failures". In Figure 3–6, the report title is the name of the report page, while the detail report description is the subheading for the report page.

- Repeat Steps 1 through 5 to create a customized user session report. A sample report is shown in [Figure 3–7](#) that shows a customized report of SYS user sessions.

Figure 3–7 My Customized Report: SYS User Sessions



Notice that you can create a variety of customized reports by filtering for specific event category information and then organize your customized reports by selecting or defining specific compliance categories under which to catalog your reports.

3.2 Alert Reports

An alert is raised when data in a single audit record matches a predefined alert rule condition. When that rule condition is met, the audit event is evaluated and, because it matches the rule condition, an alert is raised. 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, critical, all).

3.2.1 Alert Report Page

From the Dashboard page, you click **Alert Report** at the top of the page to go directly to the Alert Report page.

On the Alert Report page, specify or select filter criteria to generate a report.

3.2.1.1 Report Fields and Filter Criteria on the Alert Page

[Table 3–4](#) describes how to use each of the report fields and filter criteria.

Table 3–4 Report Fields and Filter Criteria on the Alert Report Page

Field	Description
Alert Name	<p>Enter Alert criteria or click the search icon for the Alert field. An alert is a situation in which data in an event matches an alert rule condition that causes the alert to be evaluated, raised, and stored in the alert queue for processing.</p> <p>At the Search and Select: Alert page, you can filter the list or search for a specific item by entering text in the text field for the Alert field, Event Category field, Source Type field, and the Alert Severity field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Alert field with your selected filter criteria, and return to the Alert Report page.</p>
Alert Severity	<p>Select the severity level from the Alert Severity field. The options are: ALL, CRITICAL, or WARNING.</p>
Audit Source	<p>Enter Source criteria or click the search icon for the Audit Source field. A source is where events are created.</p> <p>At the Search and Select: Audit Source page, you can filter the list or search for a specific item by entering text in the text field for the Audit Source field, Audit Source Host field, and the Source Host IP field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Source field with your selected filter criteria, and return to the Alert Report page.</p>
User	<p>Enter User criteria or click the search icon for the User field. A user is someone associated with an event.</p> <p>At the Search and Select: User page, you can filter the list or search for a specific item by entering text in the text field for the User field, then click Go to see the items that are returned. Next, you can select one or more of the returned items that display by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the User field with your selected filter criteria, and return to the Alert Report page.</p>
Audit Event Category	<p>Enter Audit Event Category criteria or click the search icon for the Audit Event Category field.</p> <p>At the Search and Select: Audit Event Category page, you can filter the list or search for a specific item by entering text in the text field for the Audit Event Category field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Audit Event Category field with your selected filter criteria, and return to the Alert Report page.</p>

Table 3–4 (Cont.) Report Fields and Filter Criteria on the Alert Report Page

Field	Description
Audit Event	<p>Enter Audit Event criteria or click the search icon for the Audit Event field. An event is the encapsulation into an audit record of some action in the audit data source.</p> <p>At the Search and Select: Audit Event page, you can filter the list or search for a specific item by entering text in the text field for the Audit Event field and the Audit Event Category field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Audit Event field with your selected filter criteria, and return to the Alert Report page.</p>
Object	<p>Enter Object criteria or click the search icon for the Object field. An object is the entity on which an event is performed.</p> <p>At the Search and Select: Object page, you can filter the list or search for a specific item by entering text in the text field for the Owner field and the Object field, then click Go to see the items that are returned. Next, you can select one or more of the returned items by clicking individual check boxes for each item listed, or click Select All to select all items. You can also click Select None to deselect all selected items and begin again. After making your selections, click Select to populate the Object field with your selected filter criteria, and return to the Alert Report page.</p>
Audit Event Time	<p>Select the Event Time field as being either during the Last 24 hours, Last One Week, Last One Month, or by The Period by clicking the option preceding each field. If you select The Period, you must enter a From date and a To date.</p>

3.2.1.2 Actions to Perform on the Alert Report Page

When you have made your filter criteria selections, click **Go** to generate the report. Once you have generated the report, you can perform the following actions:

- Click **Save as CSV** to save the report as a comma-separated values (CSV) file format. The CSV file format is a delimited data format that has fields separated by the comma character and records separated by newlines.
- From the filtered report that appears, you can click the **Detail** icon in the **Detail** column for the desired row to see a [Detail Report](#) report for the audit record data representing that selected row.
- Click **Next 25** to view the next 25 listed items returned or click **Previous** to view the previous 25 listed items.

3.3 Data Warehouse

The reports provided by Oracle Audit Vault are useful for assessing the type of audit data being collected. It is also possible to leverage the data for more sophisticated compliance reporting and analysis. Oracle Audit Vault stores the data in a data warehouse. The schema for this warehouse is available to customers, and can be used in conjunction with in-house reporting and analysis tools, such as Oracle Business Intelligence Publisher and the Oracle Business Intelligence Suite.

Details of the Audit Vault data warehouse are provided in [Appendix A](#).

Data Warehouse Schema Reference

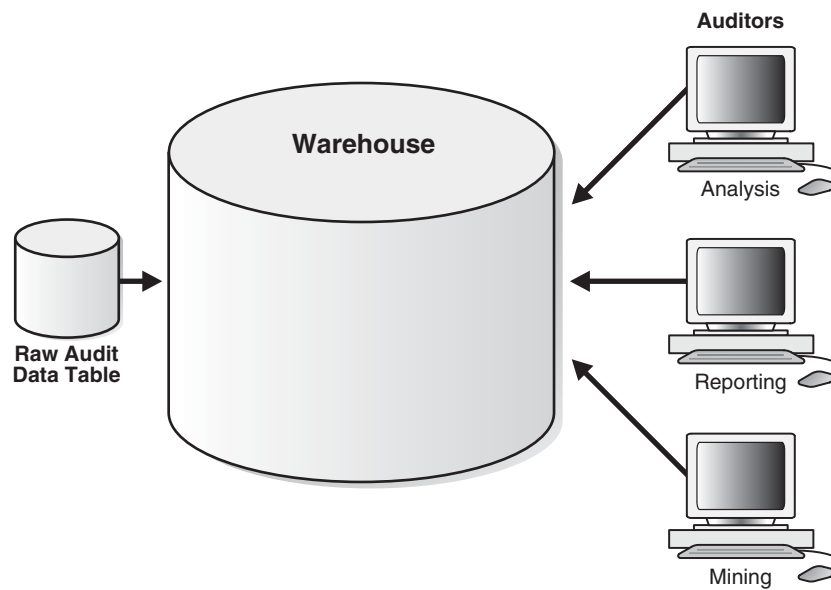
Oracle Audit Vault provides an audit data warehouse to facilitate data analysis of audit data combined with a report generation feature that lets you generate reports on the results of the data analysis. The audit data warehouse is a relational database optimized for query and analysis; it differs from the raw audit data table in that this table is optimized for transaction processing or insert performance. For more information about data warehouses, see *Oracle Database Data Warehousing Guide*.

This appendix includes the following sections:

- [Oracle Audit Vault Audit Data Warehouse Architecture](#)
- [Design of the Audit Data Warehouse](#)
- [Fact Table and Dimension Tables](#)
- [Table Details](#)

A.1 Oracle Audit Vault Audit Data Warehouse Architecture

[Figure A-1](#) shows the Oracle Audit Vault audit data warehouse architecture. Audit records are stored in the raw audit data table, which is typical of a traditional online transaction processing (OLTP) system that is optimized for insert performance as these records originate from a variety of audit sources.

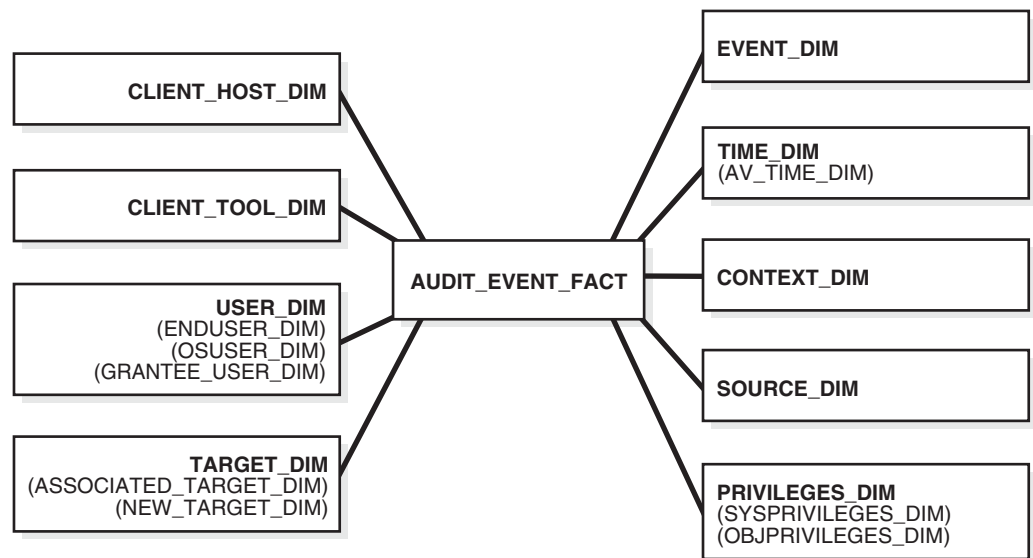
Figure A–1 Architecture of the Oracle Audit Vault Audit Data Warehouse

Audit Vault administrators with the AV_AUDITOR role can directly access audit data in the audit data warehouse for data analysis, generating reports, and performing data mining.

A.2 Design of the Audit Data Warehouse

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 other related information includes such items 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 *dimensions tables*.

Oracle Audit Vault uses a star schema to model the audit data warehouse, as shown in [Figure A–2](#), where 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.

Figure A-2 Structure of the Audit Data Warehouse

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.

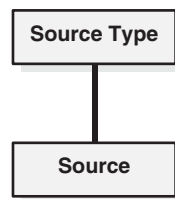
The audit data warehouse involves a fact (the entity), which is an action, and dimensions (the attributes), which are details about the action. For example, a logon attempt is a fact (an audit record). Who logged on, onto what system, at what time, using what authentication system, using what user name 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.

A.3 Fact Table and Dimension Tables

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, while 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 A-3](#).

Figure A–3 Source Dimension Hierarchy

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 dimension uses the CLIENT_HOST_DIM table as the dimension table. This table is populated 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. The CLIENT_TOOL_DIM table is used to store this information.
- **User** – This dimension is used to track the users information associated with the events occurring at the source. There is no hierarchy associated with the user information. The user dimension uses the USER_DIM table as the dimension table.
- **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 dimension uses the TARGET_DIM table as the dimension table. The TARGET_DIM table is updated 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 sources. A category of events is used by Oracle Audit Vault to group events, and this forms the hierarchy used by this dimension. At the lowest level, the event names as defined at the source are used.
- **Time** – This dimension is used to track actions over time and it is expected to be the most common use of this data warehouse. The hierarchy for time is based on calendar year.

The hierarchical information for time is stored in the TIME_DIM table. The time dimension is used for 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. This is used 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. These levels can be used to group events based on the context during analysis.

- Source – This dimension consists of the list of sources that send audit data to the data warehouse. The basic hierarchy for sources is based on source types. The source dimension is a Type-2 SCD. It keeps track of changes to the dimension attributes.
- Privileges – This dimension represents the information about the privileges used during the event. There is no hierarchy for this dimension.

A.4 Fact Table Constraints and Indexes

The AUDIT_EVENT_FACT table has the constraints listed in [Table A-1](#). 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 A-1 Constraints Defined for the AUDIT_EVENT_FACT Table

Constraint Name	Column Name	Reference Table
AV\$FACT_SOURCE_DIM_FK	SOURCE_DIM	SOURCE_DIM (DIMENSION_KEY)
AV\$FACT_EVENT_DIM_FK	EVENT_DIM	EVENT_DIM (DIMENSION_KEY)
AV\$FACT_TIME_DIM_FK	TIME_DIM	TIME_DIM (DIMENSION_KEY)
AV\$FACT_AV_TIME_DIM_FK	AV_TIME_DIM	TIME_DIM (DIMENSION_KEY)
AV\$FACT_TARGET_DIM_FK	TARGET_DIM	TARGET_DIM (DIMENSION_KEY)
AV\$FACT_USER_DIM_FK	USER_DIM	USER_DIM (DIMENSION_KEY)
AV\$FACT_OSUSER_DIM_FK	OSUSER_DIM	USER_DIM (DIMENSION_KEY)
AV\$FACT_ENDUSER_DIM_FK	ENDUSER_DIM	USER_DIM (DIMENSION_KEY)
AV\$FACT_CONTEXT_DIM_FK	CONTEXT_DIM	CONTEXT_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_PRIVILEGES_DIM_FK	PRIVILEGES_DIM	PRIVILEGES_DIM (DIMENSION_KEY)
AV\$FACT_ASSOC_TARGET_DIM_FK	ASSOC_TARGET_DIM	TARGET_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_SYSPRIVILEGES_DIM_FK	SYSPRIVILEGES_DIM	PRIVILEGES_DIM (DIMENSION_KEY)
AV\$FACT_GRANTEE_USER_DIM_FK	GRANTEE_USER_DIM	USER_DIM (DIMENSION_KEY)

The AUDIT_EVENT_FACT has local bitmap indexes defined as shown in [Table A-2](#).

Table A-2 Local Bitmap Indexes Defined on the AUDIT_EVENT_FACT Table

Index Name	Column Name
TIME_DIM_IDX	TIME_DIM
AV_TIME_DIM_IDX	AV_TIME_DIM
TARGET_DIM_IDX	TARGET_DIM
USER_DIM_IDX	USER_DIM
OSUSER_DIM_IDX	OSUSER_DIM
ENDUSER_DIM_IDX	ENDUSER_DIM
CONTEXT_DIM_IDX	CONTEXT_DIM

Table A–2 (Cont.) Local Bitmap Indexes Defined on the AUDIT_EVENT_FACT Table

Index Name	Column Name
CLIENT_HOST_DIM_IDX	CLIENT_HOST_DIM
CLIENT_TOOL_DIM_IDX	CLIENT_TOOL_DIM
PRIVILEGES_DIM_IDX	PRIVILEGES_DIM
ASSOC_TARGET_DIM_IDX	ASSOC_TARGET_DIM
NEW_TARGET_DIM_IDX	NEW_TARGET_DIM
OBJPRIVILEGES_DIM_IDX	OBJPRIVILEGES_DIM
SYSPRIVILEGES_DIM_IDX	SYSPRIVILEGES_DIM
GRANTEE_USER_DIM_IDX	GRANTEE_USER_DIM

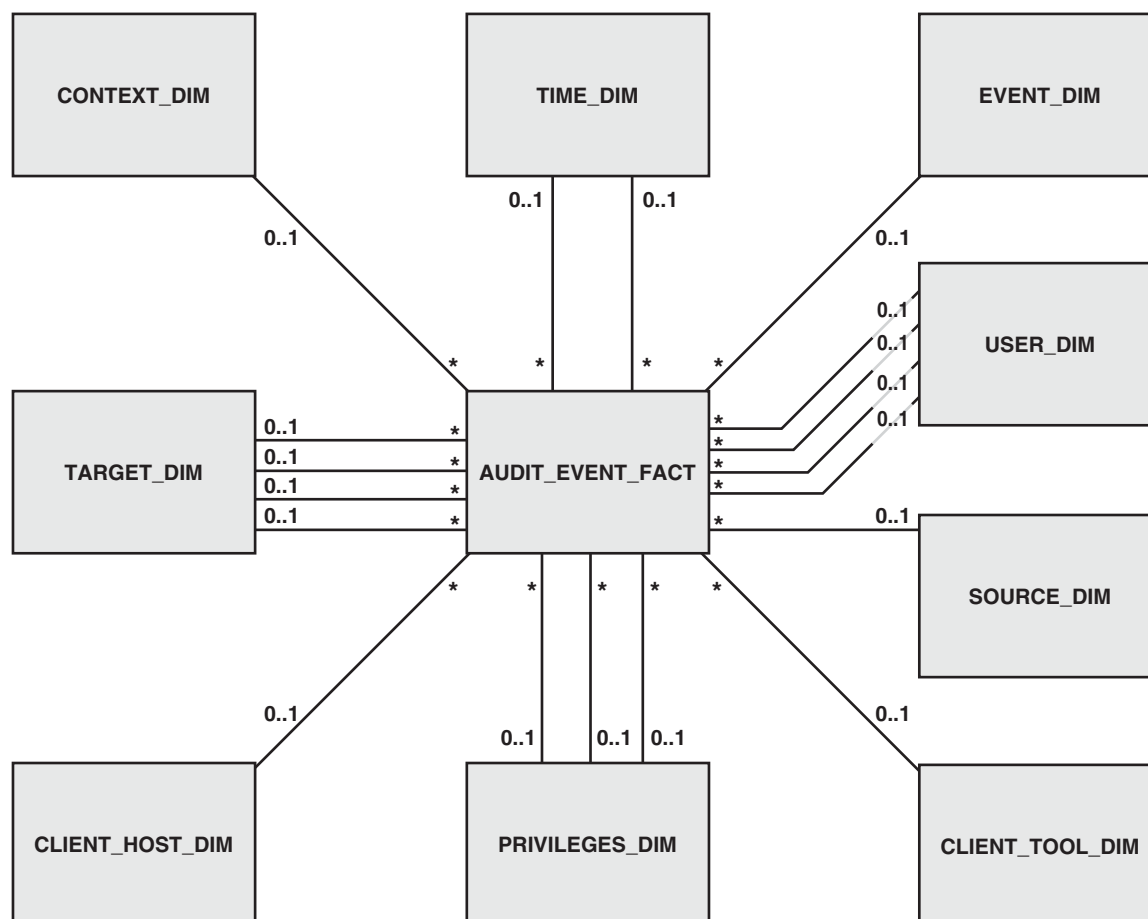
In addition to these indexes, two local bitmap join indexes are defined for SOURCE_DIM and EVENT_DIM columns as shown in [Table A–3](#).

Table A–3 Bitmap Join Indexes Defined for the SOURCE_DIM and EVENT_DIM Columns

Index Name	Dimension Name	Join Condition
SOURCE_DIM_IDX	SOURCE_DIM	SOURCE_DIM = DIMENSION_KEY
EVENT_DIM_IDX	EVENT_DIM	EVENT_DIM = DIMENSION_KEY

A.5 Table Details

[Figure A–4](#) shows the relationships between the tables of the Oracle Audit Vault data warehouse.

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

Tables A–4 through A–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.

A.5.1 AUDIT_EVENT_FACT Table

The AUDIT_EVENT_FACT table consists of the columns shown in [Table A–4](#).

Table A–4 AUDIT_EVENT_FACT Table

Column	Data Type	Can Be Null	References
ADMIN_OPTION_NUM	NUMBER	Y	None
ASSOC_TARGET_DIM	NUMBER	Y	TARGET_DIM
AUDIT_OPTION_ID	NUMBER	Y	None
AUTHENTICATION_METHOD_ID	NUMBER	Y	None
AV_TIME	TIMESTAMP WITH LOCAL TIME ZONE	Y	None
AV_TIME_DIM	NUMBER	Y	TIME_DIM
CLIENT_APPINFO_STR	VARCHAR2(4000)	Y	None

Table A-4 (Cont.) AUDIT_EVENT_FACT Table

Column	Data Type	Can Be Null	References
CLIENT_HOST_DIM	NUMBER	Y	CLIENT_HOST_DIM
CLIENT_ID	NUMBER	Y	None
CLIENT_TOOL_DIM	NUMBER	Y	CLIENT_TOOL_DIM
COMMENT_TEXT_ID	NUMBER	Y	None
CONTEXT_DIM	NUMBER	Y	CONTEXT_DIM
DATA_VALUES_CNT	NUMBER	Y	None
ENDUSER_DIM	NUMBER	Y	USER_DIM
ERROR_ID_NUM	NUMBER	Y	None
ERROR_MESSAGE_STR	VARCHAR2(4000)	Y	None
EVENT_DIM	NUMBER	Y	EVENT_DIM
EVENT_STATUS_ID	NUMBER	Y	None
EVENT_TIME	TIMESTAMP WITH LOCAL TIME ZONE	Y	None
FGA_POLICYNAME_ID	NUMBER	Y	None
GRANTEE_USER_DIM	NUMBER	Y	USER_DIM
INSTANCE_NUMBER_NUM	NUMBER	Y	None
LOGOFF_DLOCK_NUM	NUMBER	Y	None
LOGOFF_LREAD_NUM	NUMBER	Y	None
LOGOFF_LWRITE_NUM	NUMBER	Y	None
LOGOFF_PREAD_NUM	NUMBER	Y	None
MODULE_NAME_STR	VARCHAR2(4000)	Y	None
NEW_TARGET_DIM	NUMBER	Y	TARGET_DIM
OBJECT_ID_NUM	NUMBER	Y	None
OBJPRIVILEGES_DIM	NUMBER	Y	PRIVILEGES_DIM
ORIGINAL_CONTENT1_STR	VARCHAR2(4000)	Y	None
ORIGINAL_CONTENT2_STR	VARCHAR2(4000)	Y	None
ORIGINAL_CONTENT3_STR	VARCHAR2(4000)	Y	None
OSUSER_DIM	NUMBER	Y	USER_DIM
PRIVILEGES_DIM	NUMBER	Y	PRIVILEGES_DIM
PROCESS#	NUMBER	Y	None
PROXY_SESSIONID_NUM	NUMBER	Y	None
RECORD_ID	NUMBER	Y	None
ROW_ID_STR	VARCHAR2(4000)	Y	None
SCN_NUM	NUMBER	Y	None
SESSION_ACTIONS_ID	NUMBER	Y	None
SESSION_CPU_NUM	NUMBER	Y	None

Table A-4 (Cont.) AUDIT_EVENT_FACT Table

Column	Data Type	Can Be Null	References
SEVERITY_NUM	NUMBER	Y	None
SOURCE_DIM	NUMBER	Y	None
SQL_BIND_STR	VARCHAR2(4000)	Y	None
SQL_TEXT_STR	VARCHAR2(4000)	Y	None
STATEMENTID_NUM	NUMBER	Y	None
SYSPRIVILEGES_DIM	NUMBER	Y	PRIVILEGES_DIM
TARGET_DIM	NUMBER	Y	TARGET_DIM
THREAD#	NUMBER	Y	None
TIME_DIM	NUMBER	Y	TIME_DIM
TRANSACTION_NAME_ID	NUMBER	Y	None
UNDO_SQL_TEXT_STR	VARCHAR2(4000)	Y	None
USER_DIM	NUMBER	Y	USER_DIM
USER_GUID_ID	NUMBER	Y	None

A.5.2 CLIENT_HOST_DIM Table

The CLIENT_HOST_DIM table consists of the columns shown in [Table A-5](#).

Table A-5 CLIENT_HOST_DIM Table

Column	Data Type	Can Be Null
DIMENSION_KEY	NUMBER	N
DOMAIN_DESCRIPTION	VARCHAR2(255)	Y
DOMAIN_ID	NUMBER	Y
DOMAIN_NAME	VARCHAR2(255)	Y
HOST_DESCRIPTION	VARCHAR2(255)	Y
HOST_ID	NUMBER	Y
HOST_IP	VARCHAR2(255)	Y
HOST_NAME	VARCHAR2(255)	Y
SUBNET_DESCRIPTION	VARCHAR2(255)	Y
SUBNET_DOMAIN	VARCHAR2(255)	Y
SUBNET_ID	NUMBER	Y
SUBNET_NAME	VARCHAR2(255)	Y
TERMINAL_DESCRIPTION	VARCHAR2(255)	Y
TERMINAL_HOST	VARCHAR2(255)	Y
TERMINAL_ID	NUMBER	Y
TERMINAL_IP	VARCHAR2(255)	Y
TERMINAL_NAME	VARCHAR2(255)	Y
DIMENSION_KEY	NUMBER	N

Table A-5 (Cont.) CLIENT_HOST_DIM Table

Column	Data Type	Can Be Null
TOOL_DESCRIPTION	VARCHAR2(255)	Y
TOOL_ID	NUMBER	Y
TOOL_NAME	VARCHAR2(4000)	Y

A.5.3 CONTEXT_DIM Table

The CONTEXT_DIM table consists of the columns shown in [Table A-6](#).

Table A-6 CONTEXT_DIM Table

Column	Data Type	Can Be Null
CONTEXT	VARCHAR2(4000)	Y
CONTEXT_DESCRIPTION	VARCHAR2(4000)	Y
CONTEXT_ID	NUMBER	Y
DIMENSION_KEY	NUMBER	N
PARENT_CONTEXT	VARCHAR2(4000)	Y
PARENT_CONTEXT_DESCRIPTION	VARCHAR2(4000)	Y
PARENT_CONTEXT_ID	NUMBER	Y
SUB_CONTEXT	VARCHAR2(4000)	Y
SUB_CONTEXT_DESCRIPTION	VARCHAR2(4000)	Y
SUB_CONTEXT_ID	NUMBER	Y

A.5.4 EVENT_DIM Table

The EVENT_DIM table consists of the columns shown in [Table A-7](#).

Table A-7 EVENT_DIM Table

Column	Data Type	Can Be Null
CATEGORY_DESCRIPTION	VARCHAR2(255)	Y
CATEGORY_ID	NUMBER	Y
CATEGORY_NAME	VARCHAR2(255)	Y
DIMENSION_KEY	NUMBER	Y
EVENT_DESCRIPTION	VARCHAR2(255)	Y
EVENT_ID	NUMBER	Y
EVENT_NAME	VARCHAR2(255)	Y
SOURCETYPE_EVENT_DESC	VARCHAR2(255)	Y
SOURCETYPE_EVENT_ID	NUMBER	Y
SOURCETYPE_EVENT_NAME	VARCHAR2(255)	Y
SOURCETYPE_ID	NUMBER	Y

A.5.5 PRIVILEGES_DIM Table

The PRIVILEGES_DIM table consists of the columns shown in [Table A-8](#).

Table A-8 PRIVILEGES_DIM Table

Column	Data Type	Can Be Null
DIMENSION_KEY	NUMBER	N
PRIV_DESCRIPTION	VARCHAR2(4000)	Y
PRIV_ID	NUMBER	Y
PRIV_NAME	VARCHAR2(4000)	Y

A.5.6 SOURCE_DIM Table

The SOURCE_DIM table consists of the columns shown in [Table A-9](#).

Table A-9 SOURCE_DIM Table

Column	Data Type	Can Be Null
DIMENSION_KEY	NUMBER	N
EFFECTIVE_DATE	TIMESTAMP WITH LOCAL TIME ZONE	Y
EXPIRATION_DATE	TIMESTAMP WITH LOCAL TIME ZONE	Y
SOURCE_DESCRIPTION	VARCHAR2(255)	Y
SOURCE_HOST	VARCHAR2(255)	Y
SOURCE_HOSTIP	VARCHAR2(255)	Y
SOURCE_ID	NUMBER	Y
SOURCE_NAME	VARCHAR2(255)	Y
SOURCE_POLICY	NUMBER	Y
SOURCE_STATUS	NUMBER	Y
SOURCE_VERSION	VARCHAR2(30)	Y
SOURCETYPE_DESCRIPTION	VARCHAR2(30)	Y
SOURCETYPE_ID	NUMBER	Y
SOURCETYPE_NAME	SOURCETYPE_NAME	Y

A.5.7 TARGET_DIM Table

The TARGET_DIM table consists of the columns shown in [Table A-10](#).

Table A-10 TARGET_DIM Table

Column	Data Type	Can Be Null
DIMENSION_KEY	NUMBER	N
OWNER_DESCRIPTION	VARCHAR2(4000)	Y
OWNER_ID	NUMBER	Y

Table A–10 (Cont.) TARGET_DIM Table

Column	Data Type	Can Be Null
OWNER_NAME	VARCHAR2(4000)	Y
TARGET_DESCRIPTION	VARCHAR2(4000)	Y
TARGET_ID	NUMBER	Y
TARGET_NAME	VARCHAR2(4000)	Y

A.5.8 TIME_DIM Table

The TIME_DIM table consists of the columns shown in [Table A–11](#).

Table A–11 TIME_DIM Table

Column	Data Type	Can Be Null
CALENDAR_MONTH_CODE	NUMBER	Y
CALENDAR_MONTH_DESCRIPTION	VARCHAR2(255)	Y
CALENDAR_MONTH_END_DATE	DATE	Y
CALENDAR_MONTH_ID	NUMBER	Y
CALENDAR_MONTH_NAME	VARCHAR2(255)	Y
CALENDAR_MONTH_OF_QUARTER	NUMBER	Y
CALENDAR_MONTH_OF_YEAR	NUMBER	Y
CALENDAR_MONTH_START_DATE	DATE	Y
CALENDAR_MONTH_TIME_SPAN	NUMBER	Y
CALENDAR_QUART_CODE	NUMBER	Y
CALENDAR_QUART_DESCRIPTION	VARCHAR2(255)	Y
CALENDAR_QUART_END_DATE	DATE	Y
CALENDAR_QUART_ID	NUMBER	Y
CALENDAR_QUART_NAME	VARCHAR2(255)	Y
CALENDAR_QUART_OF_YEAR	NUMBER	Y
CALENDAR_QUART_START_DATE	DATE	Y
CALENDAR_QUART_TIME_SPAN	NUMBER	Y
CALENDAR_YEAR_CODE	NUMBER	Y
CALENDAR_YEAR_DESCRIPTION	VARCHAR2(255)	Y
CALENDAR_YEAR_END_DATE	DATE	Y
CALENDAR_YEAR_ID	NUMBER	Y

Table A-11 (Cont.) TIME_DIM Table

Column	Data Type	Can Be Null
CALENDAR_YEAR_NAME	VARCHAR2(255)	Y
CALENDAR_YEAR_START_DATE	DATE	Y
CALENDAR_YEAR_TIME_SPAN	NUMBER	Y
DAY	DATE	Y
DAY_CODE	NUMBER	Y
DAY_DESCRIPTION	VARCHAR2(255)	Y
DAY_END_DATE	DATE	Y
DAY_ID	NUMBER	Y
DAY_NAME	VARCHAR2(255)	Y
DAY_OF_CAL_MONTH	NUMBER	Y
DAY_OF_CAL_QUARTER	NUMBER	Y
DAY_OF_CAL_WEEK	NUMBER	Y
DAY_OF_CAL_YEAR	NUMBER	Y
DAY_START_DATE	DATE	Y
DAY_TIME_SPAN	NUMBER	Y
DIMENSION_KEY	NUMBER	N

A.5.9 USER_DIM Table

The USER_DIM table consists of the columns shown in [Table A-12](#).

Table A-12 USER_DIM Table

Column	Data Type	Can Be Null
DIMENSION_KEY	NUMBER	N
USER_DESCRIPTION	VARCHAR2(255)	Y
USER_ID	NUMBER	Y
USER_NAME	VARCHAR2(255)	Y

Oracle Database Audit Events

When creating alerts, you can specify the type of alerts that are triggered based on event category. If an audit event category is selected, you can choose the attribute of the alert to be fine-grained. You use audit event categories in the [Advanced Alert Condition](#) section of the [Create Alert Rule Page](#).

This appendix contains reference information about audit events. It includes the following sections:

- [Attributes by Event Category](#)
- [Source Event IDs](#)

B.1 Attributes by Event Category

This section lists event attributes, by event category, and their attribute types. The event categories are:

- [Account Management Event Attributes](#)
- [Application Management Event Attributes](#)
- [Audit Command Event Attributes](#)
- [Data Access Event Attributes](#)
- [Exceptional Event Attributes](#)
- [Invalid Record Event Attributes](#)
- [Object Management Event Attributes](#)
- [Peer Association Event Attributes](#)
- [Role and Privilege Management Event Attributes](#)
- [Service and Application Utilization Event Attributes](#)
- [System Management Event Attributes](#)
- [Unknown or Uncategorized Event Attributes](#)
- [User Session Event Attributes](#)

B.1.1 Account Management Event Attributes

Account management event attributes are shown in [Table B-1](#).

Table B–1 Account Management Event Attributes

Attribute Name	Attribute 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)
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.1.2 Application Management Event Attributes

Application management event attributes are shown in [Table B–2](#).

Table B–2 Application Management Event Attributes

Attribute Name	Attribute 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)
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.

B.1.3 Audit Command Event Attributes

Audit command event attributes are shown in [Table B-3](#).

Table B-3 Audit Command Event Attributes

Attribute Name	Attribute 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)
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.1.4 Data Access Event Attributes

Data access event attributes are shown in [Table B–4](#).

Table B–4 Data Access Event Attributes

Attribute Name	Attribute Type
client_appinfo	VARCHAR2(4000)
client_id	VARCHAR2(4000)
col_namelist	VARCHAR2(4000)
col_newval1	VARCHAR2(4000)
col_newval10	VARCHAR2(4000)
col_newval11	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)
col_oldval1	VARCHAR2(4000)
col_oldval10	VARCHAR2(4000)
col_oldval11	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)
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)

Table B–4 (Cont.) Data Access Event Attributes

Attribute Name	Attribute Type
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)
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.

B.1.5 Exceptional Event Attributes

Exceptional event attributes are shown in [Table B–5](#).

Table B–5 Exceptional Event Attributes

Attribute Name	Attribute Type
client_appinfo	VARCHAR2(4000)
client_id	VARCHAR2(4000)
comment_text	VARCHAR2(4000)
contextid	VARCHAR2(4000)
enduser	VARCHAR2(4000)
event_status	VARCHAR2(30)

Table B–5 (Cont.) Exceptional Event Attributes

Attribute Name	Attribute Type
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.

B.1.6 Invalid Record Event Attributes

Invalid record event attributes are shown in [Table B–6](#).

Table B–6 Invalid Record Event Attributes

Attribute Name	Attribute Type
client_appinfo	VARCHAR2(4000)
client_id	VARCHAR2(4000)
comment_text	VARCHAR2(4000)
contextid	VARCHAR2(4000)
enduser	VARCHAR2(4000)

Table B–6 (Cont.) Invalid Record Event Attributes

Attribute Name	Attribute 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.

B.1.7 Object Management Event Attributes

Object management event attributes are shown in [Table B–7](#).

Table B–7 Object Management Event Attributes

Attribute Name	Attribute 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)
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.1.8 Peer Association Event Attributes

Peer association event attributes are shown in [Table B–8](#).

Table B–8 Peer Association Event Attributes

Attribute Name	Attribute Type
client_appinfo	VARCHAR2(4000)
client_id	VARCHAR2(4000)
comment_text	VARCHAR2(4000)
contextid	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)
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.1.9 Role and Privilege Management Event Attributes

Role and privilege management event attributes are shown in [Table B–9](#).

Table B–9 Role and Privilege Management Event Attributes

Attribute Name	Attribute 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)

Table B–9 (Cont.) Role and Privilege Management Event Attributes

Attribute Name	Attribute Type
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.1.10 Service and Application Utilization Event Attributes

Service and application utilization event attributes are shown in [Table B–10](#).

Table B–10 Service and Application Utilization Event Attributes

Attribute Name	Attribute 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)
statementid	NUMBER
sub_contextid	VARCHAR2(4000)
target_object	VARCHAR2(4000)
target_owner	VARCHAR2(4000)
thread#	NUMBER
tools_used	VARCHAR2(4000)

Table B–10 (Cont.) Service and Application Utilization Event Attributes

Attribute Name	Attribute Type
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.1.11 System Management Event Attributes

System management event attributes are shown in [Table B–11](#).

Table B–11 System Management Event Attributes

Attribute Name	Attribute 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)
statementid	NUMBER
sub_contextid	VARCHAR2(4000)
target_object	VARCHAR2(4000)
target_owner	VARCHAR2(4000)
thread#	NUMBER

Table B–11 (Cont.) System Management Event Attributes

Attribute Name	Attribute Type
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.1.12 Unknown or Uncategorized Event Attributes

Unknown or uncategorized event attributes are shown in [Table B–12](#).

Table B–12 Unknown or Uncategorized Event Attributes

Attribute Name	Attribute 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)
statementid	NUMBER
sub_contextid	VARCHAR2(4000)
target_object	VARCHAR2(4000)
target_owner	VARCHAR2(4000)

Table B–12 (Cont.) Unknown or Uncategorized Event Attributes

Attribute Name	Attribute Type
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.1.13 User Session Event Attributes

User session event attributes are shown in [Table B–13](#).

Table B–13 User Session Event Attributes

Attribute Name	Attribute 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)
parent_contextid	VARCHAR2(4000)
privileges_used	VARCHAR2(4000)
process#	NUMBER
proxy_sessionid	NUMBER
scn	NUMBER
session_actions	VARCHAR2(255)
source_eventid	VARCHAR2(255)

Table B–13 (Cont.) User Session Event Attributes

Attribute Name	Attribute 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.

B.2 Source Event IDs

Source event IDs are numbers that represent the events in each category. A logon event, for example, is specified as:

```
SOURCE_EVENTID = '100'
```

This section lists events, by category, and their corresponding Oracle Database (ORCLDB) events. The event categories are:

- [Account Management Events](#)
- [Application Management Events](#)
- [Audit Events](#)
- [Data Access Events](#)
- [Exceptional 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.2.1 Account Management Events

Account management events and event IDs are shown in [Table B–1](#).

Table B–14 Account Management Events and Event IDs

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

B.2.2 Application Management Events

Application management events and event IDs are shown in [Table B–15](#).

Table B–15 Application Management Events and Event IDs

Event	ORCLDB 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
CREATE OPERATOR	163
CREATE PACKAGE	94
CREATE PACKAGE BODY	97
CREATE PROCEDURE	24
CREATE TRIGGER	59
CREATE TYPE	77
CREATE TYPE BODY	81

Table B–15 (Cont.) Application Management Events and Event IDs

Event	ORCLDB Event ID
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

B.2.3 Audit Events

Audit events and event IDs are shown in [Table B–16](#).

Table B–16 Audit Events and Event IDs

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

B.2.4 Data Access Events

Data access events and event IDs are shown in [Table B–17](#).

Table B–17 Data Access Events and Event IDs

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

B.2.5 Exceptional Events

Exceptional events and event IDs are shown in [Table B–18](#).

Table B–18 Exceptional Events and Event IDs

Event	ORCLDB Event ID
NETWORK ERROR	122

B.2.6 Invalid Record Events

Invalid record events and event IDs are shown in [Table B–19](#).

Table B–19 Invalid Record Events and Event IDs

Event	ORCLDB Event ID
INVALID RECORD	30000

B.2.7 Object Management Events

Object management events and event IDs are shown in [Table B–20](#).

Table B–20 Object Management Events and Event IDs

Event	ORCLDB 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

Table B–20 (Cont.) Object Management Events and Event IDs

Event	ORCLDB Event ID
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
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

B.2.8 Peer Association Events

Peer association events and event IDs are shown in [Table B–21](#).

Table B–21 Peer Association Events and Event IDs

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

B.2.9 Role and Privilege Management Events

Role and privilege management events and event IDs are shown in [Table B–22](#).

Table B–22 Role and Privilege Management Events and Event IDs

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

B.2.10 Service and Application Utilization Events

Service and application utilization events and event IDs are shown in [Table B–23](#).

Table B–23 Service and Application Utilization Events and Event IDs

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

B.2.11 System Management Events

System management events and event IDs are shown in [Table B–24](#).

Table B–24 System Management Events and Event IDs

Event	ORCLDB 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

Table B–24 (Cont.) System Management Events and Event IDs

Event	ORCLDB Event ID
CREATE ROLLBACK SEG	36
CREATE TABLESPACE	39
DISABLE ALL TRIGGERS	121
DROP CLUSTER	8
DROP ROLLBACK SEG	38
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

B.2.12 Unknown or Uncategorized Events

Unknown or uncategorized events and event IDs are shown in [Table B–25](#).

Table B–25 Unknown or Uncategorized Events and Event IDs

Event	ORCLDB 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

B.2.13 User Session Events

User session events and event IDs are shown in [Table B–26](#).

Table B–26 User Session Events and Event IDs

Event	ORCLDB Event ID
ALTER SESSION	42
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

Index

A

- account management audit events
 - activity reports, 3-10
 - event attributes, B-1
 - event IDs, B-16
- activity reports, 3-1
 - account management, 3-10
 - application management, 3-10
 - audit command, 3-11
 - data access, 3-11
 - exceptional, 3-12
 - invalid record, 3-12
 - object management, 3-12
 - peer association, 3-13
 - role and privilege management, 3-13
 - service and application utilization, 3-13
 - system management, 3-14
 - uncategorized, 3-14
 - user session, 3-14
- agents, 1-8
- alert activity summary, 1-7
- alert reports, 3-20
- alert rules, 2-22
- alerts, 2-19
 - creating, 2-20
 - listing, 2-20, 2-22
- application management audit events
 - activity reports, 3-10
 - event attributes, B-2
 - event IDs, B-17
- architecture, 1-4
- audit command audit events
 - activity reports, 3-11
 - event attributes, B-4
 - event IDs, B-18
- audit event categories, B-1
- audit events, B-1
- audit reports, 3-1
- audit settings
 - review, 2-1
- Audit Vault architecture, 1-4
- Audit Vault Dashboard, 1-5
- auditing
 - fine-grained, 2-13
 - privilege, 2-10

- reasons for, 1-3
- schema object, 2-7

C

- collectors, 1-8
- compliance with regulations, 1-2
- corporate governance, 1-2
- creating customized reports, 3-15

D

- dashboard, 1-5
- data access audit events
 - activity reports, 3-11
 - event attributes, B-5
 - event IDs, B-18
- data warehouse, 3-22
 - architecture, A-1
 - design, A-2
 - schema, A-1
 - tables, A-6
- detail reports, 3-8
- dimension tables, A-3

E

- event activity summary, 1-7
- event attributes, B-1
- exceptional event audit events
 - activity reports, 3-12
 - event attributes, B-6
 - event IDs, B-19

F

- fact table, A-3
- fine-grained auditing, 2-13

I

- identity theft, 1-2
- insider threats, 1-2
- invalid record audit events
 - activity reports, 3-12
 - event attributes, B-7

event IDs, B-19

O

object auditing, 2-7
object management audit events
 activity reports, 3-12
 event attributes, B-8
 event IDs, B-19
overview page, 1-5

P

peer association audit events
 activity reports, 3-13
 event attributes, B-10
 event IDs, B-20
privilege auditing, 2-10

R

reasons for auditing, 1-3
reports
 activity, 3-2
 creating customized, 3-15
 detail, 3-3
 generating, 3-2
 user interface, 3-1
role and privilege management audit events
 activity reports, 3-13
 event attributes, B-11
 event IDs, B-21

S

schema
 data warehouse, A-1
service and application utilization audit events
 activity reports, 3-13
 event attributes, B-12
 event IDs, B-21
sources, 1-8
system management audit events
 activity reports, 3-14
 event attributes, B-13
 event IDs, B-21

U

uncategorized audit events
 activity reports, 3-14
 event attributes, B-14
 event IDs, B-22
user session audit events
 activity reports, 3-14
 event attributes, B-15
 event IDs, B-22